Научно-технический журнал

H&ES RESEARCH

Scientific and Technical Journal

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 комиссиейРоссии (ВАК РФ), в систему российского индекса научного цитирования (РИНЦ), а также включен в Международный классификатор периодических изданий.

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

- 05.07.00 Авиационная и ракетно-космическая техника
- 05.12.00 Радиотехника и связь
- 05.13.00 Информатика, вычислительная техника и управление.

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 Nomenclature of specialties:

- 05.07.00 Aviation, space-rocket hardware
- 05.12.00 RF technology and communication
- 05.13.00 Informatics, computer engineering and control.

ИНДЕКСИРОВАНИЕ ЖУРНАЛА H&ES RESEARCH

JOURNAL H&ES RESEARCH INDEXING

• 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.**

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.**

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.

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 Rur.
Postgraduate students for publication
of the manuscript will not be charged

ISSN 2409-5419 (Print) ISSN 2412-1363 (Online) WWW.H-ES.RU Дата выхода: 20 августа 2022

Т.14 4 2022

Учредитель:
ООО "ИД Медиа Паблишер"

Издатель:
ДЫМКОВА С.С.

Главный редактор:
ЛЕГКОВ К.Е.

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.

СОДЕРЖАНИЕ

CONTENTS

Founder:
"Media Publisher", LLC

Publisher:
DYMKOVA S.S.

Editor in chief:
LEGKOV K.E.

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

doi: 10.36724/2409-5419-2022-14-4-4-18

ОЦЕНКИ МОЩНОСТИ КЛАССОВ ОТОБРАЖЕНИЙ, ПРИМЕНЯЕМЫХ В ПРОТОКОЛАХ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

ПАНКОВ
Константин Николаевич[1]

АННОТАЦИЯ

Введение: Квантовая криптография в ближайшее время будет играть важную роль в поддержании достаточного уровня информационной безопасности современных телекоммуникационных сетей в условиях квантового вызова, под которым понимается появление квантовых компьютеров, которые будут способны эффективно решать задачи, на которых основаны, к примеру, современные системы открытого распределения ключей. Сейчас квантовая криптография активно используется коммерческими и государственными структурами во всем мире и, в частности, в Российской Федерации. При этом проводится большое количество исследования в области разработки и реализации систем квантового распределения ключей, как основной части квантовой криптографии. В связи с этим является актуальной задача разработки новых и уточнения уже существующих протоколов квантового распределения ключа, а также изучения различных математических и физических объектов, которые связаны с этими протоколами. В частности, с одним из этапов классического протокола BB84, реализуемого в квантовом канале с шумом, связана задача изучения корреляционно-иммунных и устойчивых отображений, частью которой является задача оценки их числа, которая до настоящего времени полностью не решена. **Цель исследования:** найти математические выражения для точных и асимптотических оценок мощностей классов (n,m,k)-устойчивых и корреляционной-иммунных порядка k отображений. **Результаты:** получены наилучшие на текущий момент асимптотические верхние и нижние оценки числа таких отображений с числом выходов больше либо равных пяти. Также были доказаны рекуррентные соотношения, которые позволяют найти точное распределения мощностей классов подобных отображений для случая небольших чисел n и m. **Практическая значимость:** полученные результаты позволяют оценить вероятность того, что при случайном выборе отображения для усиления секретности на этапе вторичной обработки протокола BB84 будет нейтрализована ситуация, когда противник имеет доступ к k фотонам из посылаемым по каналу связи по своему выбору.

Сведения об авторе:

[1] к.ф.-м.н., доцент Московского технического университета связи и информатики, г. Москва, Россия, pankov_kn@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: *информационная безопасность, квантовая криптография, квантовое распределение ключей, протокол BB84, корреляционно-иммунные отображения, устойчивые отображения.*

Для цитирования: Панков К.Н. Оценки мощности классов отображений, применяемых в протоколах квантового распределения ключей // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 4-18. doi: 10.36724/2409-5419-2022-14-4-4-18

Введение

В 2017 году Минкомсвязи (сейчас – Минцифры) России, выполняя поручение Президента, подготовило программу «Цифровая экономика Российской Федерации» (далее – ЦЭРФ), которая была утверждена решением Правительства России. В этой программе был приведен список основных сквозных цифровых технологий (СЦТ), одной из которых являлись квантовые технологии. Частью этой СЦТ является квантовая криптография, которая является инструментом обеспечения информационной безопасности в условиях квантового вызова, угрожающего широко используемым в настоящее время асимметричным системам шифрования и распределения секретного ключа.

В начале 2019 года для исключения дублирования программных документов в области развития цифровой экономики данная программа была признана утратившей силу, однако в действующей редакции паспорта национальной программы (НП) «Цифровая экономика Российской Федерации», утвержденного 4 июня 2019 года, употребляется только само понятие «СЦТ» без уточнения о каких именно технологиях идет речь. Если судить по подписанным 10 октября 2019 года и опубликованным на сайте Минцифры России дорожным картам развития СЦТ, которые упоминаются в федеральном проекте «Цифровые технологии», являющемся структурной единицей национального проекта «НП «ЦЭРФ»», то можно сделать вывод, что квантовые технологии по прежнему являются СЦТ с точки зрения руководства России.

СЦТ квантовые технологии, согласно утвержденной Дорожной карте[1], делится в основном на три субтехнологии, одной из которых являются квантовые коммуникации (КК), определяемые в тексте карты как технология криптографической защиты информации, использующая для передачи ключей индивидуальные квантовые частицы. Авторы карты, рассматривают защищенность информации, гарантированную законами квантовой механики, в качестве главного преимущества КК. КК и квантовая криптография признаны синонимами исходя из текста Дорожной карты.

Классическая криптография для обеспечения конфиденциальности передаваемой информации использует математические методы, квантовая же криптография опирается на постулаты квантовой механики, из которых следует, что невозможно измерить один параметр фотона, который является механизмом передачи информации в линиях волоконно-оптической связи, не исказив другие параметры. Следовательно, можно построить канал передачи информации, который может обнаруживать попытку измерения (подслушивание) со стороны противника (Евы в традиционных протоколах), которое приведет к увеличению уровня шума в канале. Это увеличение может быть обнаружено законными пользователями (Алисой и Бобом).

Идея применения квантовой механики в задачах информационной безопасности была выдвинута в семидесятых годах XX века [1], но научный мир не принял ее, поэтому первая публикация этой идеи относится к 1983 году [2]. В 1984 году Чарльзом Беннетом и Жилем Брассаром был предложен протокол BB84 для создания защищённого канала для квантового распределения ключа (КРК), являющегося основой КК [3]. Этот протокол, в ходе выполнения которого Алиса и Боб обмениваются сообщениями, представленными в виде поляризованных фотонов, признается ныне классическим. Ева, которая пытается исследовать передаваемые по квантовому каналу фотоны, вызывает шум, обнаруживаемый Алисой и Бобом.

Технологии КРК в настоящее время активно используются Центрами обработки данных, крупными финансовыми структурами и государственными организациями. Общемировой рынок для КК эксперты оценивали в 2021 году суммой в 490 миллионов долларов. Согласно оценкам компании Hyperion Research, представленным на рисунке 1, в 2024 году этот рынок вырастет до 888 миллионов [4].

Таким образом, является актуальной задача исследования состояния технологии КРК в Российской Федерации и в Мире, а также исследования различных задач с ней связанных.

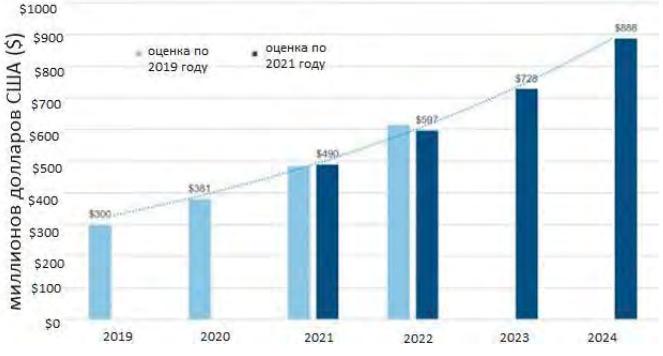

Рис. 1. Рынок квантовой криптографии за 2019-2021 годы с оценками для 2022-2024 [4]

Квантовые коммуникации в России с учетом современных тенденций

В России, согласно [5], первые попытки лабораторной реализации КРК состоялись в начале 2000-х годов в Институте физики полупроводников Сибирского отделения РАН. Университет ИТМО в 2014 году представил прототип работающей системы КК для передачи данных на дистанции в 1 км [5]. Информация передавалась на территории университета.

В 2016 году Российский Квантовый Центр (РКЦ) запустил первую в России полноценную линию КК, использовавшую волоконно-оптическую линию связи и соединившую между собой два офиса “Газпромбанка”, расстояние между которыми составляло около 30 км. Научно-производственная компания QRate, являющаяся дочерней компанией РКЦ, несколько лет назад разработала серийную установку для КРК, которая использует созданные в РКЦ детекторы и источники одиночных фотонов. Главными осо-

[1] Дорожная карта развития «сквозной» цифровой технологии «Квантовые технологии». Подписана 10.10.2019 // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/uploaded/files/07102019kvantyi.pdf (Дата обращения 02.06.2022)

бенностями этой установки являются возможность интеграции в уже существующие телекоммуникационные сети и адаптации для обеспечения информационной безопасности к работе с криптографическими протоколами [5].

В настоящее время ряд крупнейших городов Российской Федерации имеет созданные или спроектированные квантовые сети, как опытно-экспериментальные, так и коммерческие. Примером является квантовая сеть с открытым доступом между НИТУ «МИСиС» и МТУСИ, запущенная 13 октября 2021 года [6].

Кроме РКЦ и QRate, реализацией проектов в области КК в Российской Федерации занимаются ученые из МГУ совместно с ОАО «ИнфоТеКС», а также ученые и разработчики из университета ИТМО (компания "Квanттелеком"). К примеру, в 2019 году "Инфотекс" представил опытные образцы квантового телефона, под которым мы понимаем систему голосовой связи, в которой защита аудио информации обеспечивается с помощью КРК[2].

Нужно отметить, что в РКЦ в 2017 году впервые в мире представили квантово защищенный блокчейн — практически невзламываемую систему распределенного хранения данных, защищенную при помощи КРК от угроз, которые будут вызваны появлением эффективно работающего квантового компьютера[3]. Таким образом, был предложен еще один подход к обеспечению информационной безопасности другой СЦТ-технологии систем распределенного реестра, проблемы обеспечения которой рассматривалась, к примеру, в работах [7], [8], [9].

17 февраля 2021 года было объявлено, что группой ученых и инженеров, которые представляли РКЦ, компанию QRate и Центр квантовых коммуникаций МИСиС, был установлен новый мировой рекорд для некоторых алгоритмов в системах КРК. В частности, им удалось сократить долю ключа, используемую для аутентификацию данных и предложить алгоритм коррекции ошибок, использующий полярные коды[4].

В 2017 году регулятором сферы, связанной со средствами криптографической защиты информации (СКЗИ) в Российской Федерации были утверждены временные требования для систем КРК[5], которыми смогут воспользоваться специалисты, разрабатывающие системы квантовой криптографии для коммерческих компаний, а также для структур муниципальной и государственной власти, не обрабатывающих информацию, содержащую государственную тайну. Согласно мнению экспертов, это означает, что перспективность использования КРК стало очевидным для государственных структур, и широкое внедрения этого метода защиты информационной безопасности является делом ближайшего будущего [10]. К сожалению, на конец мая 2021 года ни одна из существующих систем КРК не прошла сертификации как СКЗИ. Заметим, что подобная проблема для систем, основанных на СЦТ систем распределенного реестра подробно рассматривалась в работе [11].

В прошлом 2021 году техническим комитетом по стандартизации ТК-26 приняты методические рекомендации [12], в которых был описан протокол, который рекомендуется использовать в сетях с квантово-криптографическим оборудованием, позволяющим осуществлять выработку и распределение ключей, для защищенного обмена данными между квантово-криптографической аппаратурой выработки и распределения ключей и СКЗИ.

Большинство существующих систем КРК обладают существенным недостатком – они привязаны к проводным (оптико-проводным) сетям связи. Однако, в настоящее время проводятся эксперименты по разработке беспроводных систем, в которых КРК проводится в других средах.

В 2020 году канадские ученые смогли построить линию КК под водой с турбулентным течением на расстоянии 30 м [13]. Отметим важное прикладное значение данного эксперимента: квантовое распределение ключей может предоставить подводным лодкам возможность осуществлять безопасную связь, как на глубине, так и на скорости. В России в 2021 году учеными МТУСИ был проведен эксперимент, в котором под водой с помощью лазера был передан полезный сигнал [14], что показало принципиальную возможность организации оптической подводной связи для передачи данных с большой скоростью с помощью компактных и дешевых оптических систем на расстояния до 100 м. В дальнейшем этот коллектив ученых планирует разработать систему КРК для этого канала.

Также в 2020 году в КНР смогли провести испытание системы КРК в воздушной среде с помощью беспилотных летательных аппаратов между точками на расстоянии 1 км [15]. Согласно информации с сайта РАН[6] подобные эксперименты с использованием квадрокоптеров были проведены и в Российской Федерации.

12 мая 2021 года стало известно о том, что был успешно реализован метод защиты с помощью КРК информационной безопасности для систем беспилотного автомобиля, управляемого в автономном режиме. Специалисты Университета Иннополис и уже упоминаемой нами ранее компании QRate смогла создать канал передачи данных через открытое пространство. Канал был установлен между центром обработки данных и автомобилем и основан на технологии 4G, конфиденциальность информации для которой обеспечивалась OpenVPN с применением КРК[7].

---

[2] Завершен первый этап создания Университетской квантовой сети. 25.08.2021 // Infotecs. URL: https://infotecs.ru/about/press-centr/news/zavershen-pervyy-etap-sozdaniya-universitetskoy-kvantovoy-seti.html (Дата обращения 02.06.2022)

[3] Физики из России создали первый в мире квантовый блокчейн. 26.05.2017 // РИА новости. URL: https://ria.ru/20170526/1495086879.html (Дата обращения 02.06.2022)

[4] Ученые из России обновили мировой рекорд в области квантовой криптографии. 17.02.2021 // РИА Новости. URL: https://ria.ru/20210217/rekord-1597773434.html (Дата обращения 03.06.2022)

[5] Об утверждении временных требований к квантовым криптографическим системам выработки и распределения ключей для средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну. 03.08.2017 // Федеральная Служба Безопасности Российской Федерации. URL: http://www.fsb.ru/fsb/science/single.htm%21id%3D10438445%40fsbResearchart.html (Дата обращения 02.06.2022)

[6] 18 мая 2021 года состоялось очередное заседание Президиума Российской академии наук. 19.05.2021 // Российская академия наук. URL: http://www.ras.ru/news/shownews.aspx?id=e3198483-41a6-4297-a48f-70af61f582d6&print=1 (Дата обращения 03.06.2022)

[7] Университет Иннополис внедрил в беспилотники систему квантового распределения ключей для защиты их от взлома. 12.05.2021 // Университет Иннополис. URL: https://media.innopolis.university/news/self-driving-car-quants/ (Дата обращения 03.06.2022)

Рис. 2. Расположение точек приемника и передатчика квантового канала связи при эксперименте В МТУСИ

В феврале 2022 года совместными усилиями ученых из МТУСИ и специалистов компаний QRate и «Мостком» был проведен эксперимент по КРК по квантовому каналу в открытом пространстве на 180 (см рис. 2) и 3100 м[8].

Согласно [16] современные атмосферные, подробно рассмотренные в [17], и подводные системы для реализации КРК принципиально ограничены по расстоянию из-за потерь в канале, и реализация глобальной квантовой сети возможна только с помощью спутниковых систем КРК, что объясняется незначительными потерями фотонов и ничтожно малой декогеренцией в вакууме.

Рис. 3. Реализация КРК с помощью спутника в Китае [19]

Практическая реализация систем КРК в космическом пространстве в настоящее время осуществлена Китаем. 9 сентября 2017 года с помощью спутника «Мо Цзы» (Micius) была организована линия связи между президентами академий наук Китайской народной республики и Австрии, для обеспечения информационной безопасности которой было использовано КРК. Расстояние между столицами государств – Пекином и Веной – составляет больше 7400 километров, что стало рекорд дальности для КК [18]. В 2020 году с помощью того же спутника было организовано КРК на расстоянии 1120 километров с более строгими требованиями к параметрам выработанного ключа [19] (см. рис. 3).

В Российской Федерации работы по проведению экспериментов в космическом пространстве только планируются. К примеру, QRate планирует участвовать в запуске малого космического спутника стандарта CubeSat с передатчиком квантового сигнала на борту и организовать КРК для двух наземных станций [5]. На первом этапе этого проекта планируется разработать свой наземный приемный модуль[9]. Кроме этого, компания QSpace Technologies LLC, которая разрабатывает атмосферные и спутниковые системы КРК через открытое пространство, в начале 2022 года объявил о закрытии этапа привлечения средств для проекта создания в Российской Федерации системы квантовой спутниковой коммуникации. Первым этапом этого проекта будет запуск малого спутника, на борту которого будет размещен квантовый передатчик [20]. В ближайшее время, согласно [21], госкорпорация "Роскосмос" и РЖД планируют провести совместный эксперимент по отработке квантовой связи на Международной космической станции (МКС).

Таким образом, в силу распространенности и востребованности КРК в современном мире, вообще, и в России, в частности, требуется проводить дальнейшие исследования по уточнению существующих и разработке новых протоколов, реализуемых в ходе реализации КРК. При этом необходимо проводить подробные исследования используемых в этих протоколах физических и математических механизмов

Корреляционно-иммунные и k-устойчивые отображения в задачах защиты информации и оценки их числа реестров

В соответствии с [1] в классическом протоколе КРК BB84 выделяют несколько этапов. На первом, описанном в исходной работе [3] для идеальных условий и именуемом в [1] передачей сигнальных состояний, после пересылки набора одиночных фотонов, кодирующих случайные биты в случайно выбранном базисе, от Алисы к Бобу, согласования базисов и оценки уровня ошибок в канале, который характеризует вмешательство Евы, у Алисы и Боба оказывается битовая строка или просеянный ключ, который полностью совпадает в случае, если в канале связи отсутствует шум.

В реальной ситуации в квантовом канале шум или искажение всегда присутствует, и его действие может как замаскировать факт наблюдения за каналом Евы, так и исказить сам ключ. Поэтому требуются еще этапы коррекции ошибок и усиления секретности, которые иногда объединяют в общий этап вторичной обработки просеянного ключа. На этапе коррекции ключа обычно используются классические процедуры [1], а после него у Алисы и Боба на руках имеются по одинаковой битовой строке. Также они могут оценить доступную противнику информацию.

[8] Российские учёные испытали беспроводную квантовую криптографию. 22.02.2022 // Мостком. Bridge your data. URL: http://www.moctkom.ru/ru/российские-учёные-испытали-беспрово/ (Дата обращения 03.06.2022)

[9] Квантовая связь освоит космос. 02.06.2021 // COMNEWS. Спутниковая связь. Конкурсы/тендеры. URL: https://www.comnews.ru/content/214773/2021-06-02/2021-w22/kvantovaya-svyaz-osvoit-kosmos (Дата обращения 03.06.2022)

На следующем этапе, который носит название этап усиления секретности, происходит выработка секретного ключа, информации о котором у противника не имеется. На этом этапе происходит, обычно, значительное сокращение длины ключа по сравнению с исходной битовой строкой. Согласно [22] усиление секретности проводится с помощью хеш-функций.

Согласно [22] подобный способ построения этапа вторичной обработки не подходит для случая, когда Ева имеет доступ к k фотонам из посылаемым по каналу связи по своему выбору. В этом случае [22] предлагает использовать для усиления секретности (n,m,k)-функции, определение которых повторяет определение (n,m,k)-устойчивых отображений, предложенных в [23], или k-эластичных отображений в терминологии, предложенной в [24]. В свою очередь k-эластичные отображения являются частным случаем корреляционно-иммунных порядка k отображений.

Введем ряд обозначений, которые помогут нам строго определить данные понятия.

Обозначим через V_n множество всех двоичных векторов n (n-я декартова степень множества $F_2 = \{0,1\}$). Пусть n и m – два натуральных числа. Обозначим через B_n^m множество всех отображений из V_n в V_m:

$$B_n^m = \left\{ f(x) = \left(f_1(x), f_2(x), ..., f_m(x) \right) : V_n \to V_m, \right\},$$

где $f(x)$ – двоичное отображений (булева вектор-функция), $f_i(x) : V_n \to F_2$ для всех $i \in \{1,...,m\} = \overline{1,m}$ – координатных функций $f(x)$.

Двоичное отображение $f(x) = f(x_1,...,x_n) \in B_n^m$ называется устойчивым по отношению к множеству $I = \{i_1,...,i_t\} \subset \overline{1,n}$ (или I- устойчивым), если случайные векторы $f(X_1,...,X_n)$ и $\left(X_{i_1},...,X_{i_t}\right)$ независимы, где $\left\{X_i, i \in \overline{1,n}\right\}$ – множество независимых равномерно распределенных на F2 случайных величин. $f(x)$ называется корреляционно-иммунным порядка k, если для каждого множества $I \subset \overline{1,n}$ мощности не превосходящей k, отображение $f(x)$ является I-устойчивым.

Двоичное отображение $f(x)$ называется сбалансированным по выходу, если для любого вектора $\beta \in V_m$ выполняется равенство

$$\mathrm{P}\left(f(X_1,...,X_n) = \beta \right) = \frac{1}{2^m}.$$

Булева вектор-функция $f(x) \in B_n^m$ называется (n,m,k)-устойчивым или *k*-эластичным, если оно корреляционно-иммунно порядка *k* и сбалансировано по выходу [25] .

Определенные нами классы отображений используются не только в задачах, связанных с КРК. Например, устойчивые отображения могут быть использованы при синтезе поточных систем шифрования в качестве комбинирующих функций, поскольку их применение позволяет не бояться корреляционной атаки. Корреляционно-иммунные же функции связаны с простыми ортогональными массивами (таблицами) [26], изучающимися в комбинаторике и статистике при планировании экспериментов, а в классической криптографии - при построении кодов аутентификации [27] каналов. Также существует связь этих функций с синтезом генераторов ключевых последовательностей для поточных шифров и некоторыми объектами, изучающимися в теории кодирования [28].

Из сказанного выше, следует необходимость изучения свойств данных отображений, чем в последние полвека, начиная с работ Л.В. Ларионова [24], и занимаются многие ученые. С обзором работ, посвященных корреляционно-иммунным и устойчивым отображениям, в основном для m=1, можно познакомиться в [29]. Одна из известнейших задач, которая стоит перед современными исследователями – это подсчет числа подобных отображений. Точного числа корреляционно-иммунных и устойчивых вектор-функций для больших значений m, n и k в настоящее время не найдено. К настоящему моменту известны только асимптотические оценки, к примеру [30], [31], [32], [33].

Обозначим через $K[n,m,k]$ множество корреляционно-иммунныхпорядка k двоичных отображений из B_n^m, а через $R[n,m,k]$ – множество (n,m,k)-устойчивых двоичных отображений. Обозначим с помошью $|A|$ мощность множества A.

Автором статьи в работе [34] были предложены лучшие на сегодняшний момент точные асимптотические оценки для значений $|K[n,m,k]|$ и $|R[n,m,k]|$, при $m \le 4$. К сожалению, при $m \ge 5$ полученные в [34] оценки зависят от мощности не до конца изученного множества S(m), которое может быть определено следующим образом:

$$S(m) = \left\{ r = \left(r_J, J \subset \overline{1,m}, J \neq \varnothing \right) \in \left\{0,1,...,2^{m-1}-1\right\}^{2^m-1}, \right.$$

$$\left. \forall s \in \overline{1,m}, \forall \delta \in V_m : \sum_{J \subset \overline{1,m}, s \in J} (-1)^{\langle \delta, ch_m(J) \rangle} r_J \in 2^{m-1}\mathbb{Z} \right\},$$

где $ch_m(J)$ – индикаторный вектор подмножества J множества $\overline{1,m}$ [35], $\langle x, y \rangle$ – скалярное произведение векторов x и y, $\mathbb{Z}$ – множество целых чисел.

Оценим мощность этого множества, улучшив оценки, предложенные ранее в [24] .

Теорема 1. *Пусть* $m \ge 5$, *тогда*

$$\frac{m^2 - m - 12}{2} + 17 \le \log_2 |S(m)| \le (16m - 47)2^{m-4} - m + 3.$$

Доказательство.

Легко видеть, что множество S(m) изоморфно множеству $S'(m)$:

$$S'(m)=\left\{r=\left(r_J, J\subset\overline{1,m}, J\neq\varnothing\right)\in\left(\mathbb{Z}_{2^{m-1}}\right)^{2^m-1},\right.$$

$$\left.\forall s\in\overline{1,m}, \forall\delta\in V_m: \sum_{J\subset\overline{1,m}, s\in J}(-1)^{\langle\delta, ch_m(J)\rangle} r_J=0\right\}.$$

Легко видеть, что множество S'(m) является кольцом относительно стандартных операций.

Из результатов работы [24] (утверждения 1 и элементов доказательства утверждения 3) следует, что множество S'(m) может быть представлено как объединение двух непересекающихся множеств одинаковой мощности:

$$S'(m)=S_{even}(m)\bigcup S_{odd}(m),$$

где

$$S_{even}(m)=\left\{r=\left(r_J, J\subset\overline{1,m}, J\neq\varnothing\right)\in S'(m):\right.$$
$$\left.r_J=2k, k\in\left\{0,...,2^{m-2}-1\right\}\right\},$$
$$S_{odd}(m)=\vec{1}+S_{even}(m),$$

где $\vec{1}$ – вектор $(1,1,...,1)$, состоящий из единиц размерности 2^m-1.

Обозначим через $P(m)$ множество всех подмножеств $\overline{1,m}$. Очевидно, что

$$P(m)=P(m-1)\cup P_{\{m\}}(m-1),$$

где $P_{\{m\}}(m-1)=\left\{J\cup\{m\}: J\in P(m-1)\right\}$.

Пусть $s\in\overline{1,m-1}$, $\delta=(\delta',\alpha)$, где $\delta'\in V_{m-1}$, $\alpha\in\{0,1\}$. Следовательно, для любых $r\in S_{even}(m)$ выполняется

$$\sum_{J\subset\overline{1,m}, s\in J}(-1)^{\langle\delta, ch_m(J)\rangle} r_J=\sum_{\substack{K\in P(m-1),\\ s\in K}}(-1)^{\langle\delta', ch_{m-1}(K)\rangle} r_K+$$
$$+(-1)^{\alpha}\sum_{T\subset P(m-1), s\in T}(-1)^{\langle\delta', ch_{m-1}(T)\rangle} r_{T\cup\{m\}}. \quad (1)$$

Обозначим через $A(\delta')$ первую сумму в правой части равенства (1), а через $B(\delta')$ – вторую сумму. Разобьем все вектора $\delta\in V_m$ на пары $(\delta',0)$ и $(\delta',1)$. Поскольку $A(\delta')\pm B(\delta')\in 2^{m-1}\mathbb{Z}$, то, $A(\delta'), B(\delta')\in 2^{m-2}\mathbb{Z}$.

Следовательно, для всех $s\in\overline{1,m-1}$ и $\delta'\in V_{m-1}$ получаем

$$\sum_{K\subset P(\overline{1,m-1}), s\in K}(-1)^{\langle\delta', \psi_{m-1}(K)\rangle} r_K\in 2^{m-2}\mathbb{Z}, \quad (2)$$

$$\sum_{T\subset P(\overline{1,m-1}), s\in T}(-1)^{\langle\delta', \psi_{m-1}(T)\rangle} r_{T\cup\{m\}}\in 2^{m-2}\mathbb{Z}. \quad (3)$$

Если обозначить через r_J^* остаток от деления r_J на 2^{m-2}, то при замене r_J на r_J^* равенства (2) и (3) останутся верными. Очевидно, что

$$\left(r_K^*, \varnothing\neq K\subset\overline{1,m-1}\right), \left(r_{T\cup\{m\}}^*, \varnothing\neq T\subset\overline{1,m-1}\right)\in$$
$$\in S_{even}(m-1).$$

Также $r_{\{m\}}$ может принимать не более 2^{m-2} значений. Таким образом

$$\left|S_{even}(m)\right|\leq 2^{m-2}\left(\left|S_{even}(m-1)\right|2^{2^{m-1}-1}\right)^2,$$
$$\log_2\left|S_{even}(m)\right|\leq m-2+2\left(2^{m-1}-1+\log_2\left|S_{even}(m-1)\right|\right)$$

Используя метод математической индукции, можно доказать, что

$$\log_2\left|S_{even}(m)\right|\leq\sum_{t=0}^{s-1}2^t(m-t-2)+\sum_{t=0}^{s-1}2^{t+1}\left(2^{m-t-1}-1\right)+$$
$$+2^s\log_2\left|S_{even}(m-s)\right|=(m-4)\left(2^s-1\right)-(s-1)2^s-2+$$
$$+2^m s+2^s\log_2\left|S_{even}(m-s)\right|$$

для всех $s<m$.

Если $s=m-4$, то

$$\log_2\left|S_{even}(m)\right|\leq\left(16m-63+\log_2\left|S_{even}(4)\right|\right)2^{m-4}-m+2.$$

Мощность множества S'(4) может быть найдена перебором, к примеру с помощью системы Wolfram Mathematica:

$$\log_2\left|S'(4)\right|=17,$$

$$\log_2\left|S_{even}(4)\right|=16.$$

Следовательно, для всех $m\geq 5$

$$\log_2\left|S(m)\right|\leq(16m-47)2^{m-4}-m+3$$

Теперь найдем нижнюю оценку для S(m)/
Рассмотрим вектор

$$r=\left(r_J, J\subset\overline{1,m-1}, J\neq\varnothing\right)\in S'(m-1)$$

и вектор $t=\left(t_J, J\subset\overline{1,m}, J\neq\varnothing\right)$, в котором $t_K=2r_K\left(\mathrm{mod}\,2^{m-1}\right)$ для $\varnothing\neq K\subset\overline{1,m-1}$ и $t_S=0$ for $m\in S$.

Для всех $s\in\overline{1,m}$ и $\delta=(\delta',\alpha)$, в которых $\delta'\in V_m$ и $\alpha\in\{0,1\}$ получаем

$$\sum_{J\subset\overline{1,m}, s\in J}(-1)^{\langle\delta, \psi_m(J)\rangle} t_J=$$
$$=\sum_{K\subset P(\overline{1,m-1}), s\in K}(-1)^{\langle\delta', \psi_{m-1}(K)\rangle} 2r_K\in 2\cdot 2^{m-2}\mathbb{Z}=2^{m-1}\mathbb{Z}.$$

Если $s = m$, то

$$\sum_{J\subset\overline{1,m},s\in J}(-1)^{\langle\delta,\psi_m(J)\rangle}t_J = 0 \in 2^{m-1}\mathbb{Z}.$$

Следовательно, $t \in S'(m)$.

В доказательстве утверждения 3 [24], было показано, что $s=\left(s_J = k, J\subset\overline{1,m-1}, J\neq\varnothing\right)\in S'(m)$ для всех $k\in\mathbb{Z}_{2^{m-1}}$. Следовательно, $t+s\in S'(m)$ и

$$\left|S'(m-1)\right|2^{m-1}\le\left|S'(m)\right|.$$

Используя метод математической индукции, легко доказать, что

$$\log_2\left|S'(m)\right|\ge\sum_{t=0}^{s-1}(m-t-1)+\log_2\left|S'(m-t-1)\right| =$$
$$=\frac{s(2m-s-1)}{2}+\log_2\left|S'(m-s)\right|.$$

Если $s = m-4$, то

$$\log_2\left|S'(m)\right|\ge\frac{(m-4)(m+3)}{2}+\log_2\left|S'(4)\right|.$$

Окончание доказательства.

Можно отметить, что нижняя граница из теоремы 1 существенно лучше, чем граница m-1 из [24], а верхняя граница может быть записана как

$$\log_2\left|S(m)\right|\le\left(m-2\frac{15}{16}\right)2^m-m+3,$$

что также лучше, чем $(m-2)2^m-m+3$ из [24] для $m\ge5$.

Используя утверждение 1 и теорему 5 из [34], с помощью теоремы 1 можно доказать следующие следствия, анонсированные в [36]:

Следствие 1. *Пусть* $m\ge5$, *и при всех достаточно больших n для любого* $0<a<\frac{5}{18}$ *выполняется неравенство* $k(5+2\log_2 n)+6m\le n\left(\frac{5}{18}-a\right)$. *Тогда Если* $m\ge5$, *то существует натуральное* n_0 *такое, что для любых* $\varepsilon_1,\varepsilon_2>0$ *и* $n>n_0$

$$m2^n-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$
$$\left(\frac{m^2-m-12}{2}+17\right)\sum_{i=0}^{k}\binom{n}{i}-\varepsilon_1\le\log_2\left|R[n,m,k]\right|\le$$
$$\le m2^n-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$
$$+\left((16m-47)2^{m-4}-m+3\right)\sum_{i=0}^{k}\binom{n}{i}+\varepsilon_2$$

Следствие 2. *Пусть* $m\ge5$, *и при всех достаточно больших n для любого* $0<a<\frac{1}{3}$ *выполняется неравенство* $k(5+2\log_2 n)+6m\le n\left(\frac{1}{3}-a\right)$. *Тогда существует натуральное* n_0 *такое, что для любых* $\varepsilon_1,\varepsilon_2>0$ *и* $n>n_0$

$$m2^n+\left(\frac{n+1+\log_2\pi}{2}-k\right)\left(2^m-1\right)-m2^{m-1}-$$
$$-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$
$$+\left(\frac{m^2-m-12}{2}+17\right)\sum_{i=0}^{k}\binom{n}{i}-\varepsilon_1\le\log_2\left|K[n,m,k]\right|\le$$
$$\le m2^n-m2^{m-1}+\varepsilon_2+\left((16m-47)2^{m-4}-m+3\right)\sum_{i=0}^{k}\binom{n}{i}-$$
$$-\left(2^m-1\right)\left(\frac{n-k}{2}\binom{n}{k}+\sum_{i=0}^{k}\binom{n}{i}\log_2\sqrt{\frac{\pi}{2}}\right)+$$
$$+\left(\frac{n+1+\log_2\pi}{2}-k\right)\left(2^m-1\right).$$

Оценки из следствий 1 и 2 являются на сегодняшний момент самыми сильными и улучшают результаты работ [37], [24] и [34]. Экспериментальное подтверждение полученных результатов для малых значений m, n и k является актуальной и нерешенной задачей.

Рекуррентные формулы для классов двоичных отображений

Заметим, что полученные в предыдущем разделе оценки обладают существенным недостатком, - они выполняются, начиная с некоторого, возможно, очень большого натурального n_0. Получим результаты, которые можно применить при небольших значениях m, n и k. Для этого введем ряд дополнительных определений и обозначений.

Пусть $\varnothing\neq J\subset\overline{1,m}$. Компонентной функцией или компонентой [38] f^J будем называть линейную комбинацию координатных функций двоичного отображения $f(x)\in B_n^m$ следующего вида:

$$f^J=f_{j_1}\oplus\ldots\oplus f_{j_s}, J=\{j_1,\ldots,j_s\}\subset\overline{1,m}$$

Известно, что многие свойства двоичного отображения могут быть выражены через свойства всех его компонент [29]. Эти свойства, в частности включают и корреляционную иммунность, которая в терминологии [29] называется сводимым и вторичным свойством.

Обозначим через $\|g\|$ вес булевой функции $g\in B_n^1$, т.е число векторов $x\in V_n$ для которых $g(x)=1$.

Для любых подмножеств $I=\{i_1,...,i_t\}\subset\overline{1,n}$ и $\varnothing\neq J\subset\overline{1,m}$, обозначим через $w_I^J(f)$ вес $\left\|\left(f^J\right)_{i_1,...,i_{|I|}}^{1,...,1}\right\|$ подфункции $\left(f^J\right)_{i_1,...,i_{|I|}}^{1,...,1}$ компоненты f^J двоичного отображения $f(x)\in B_n^m$, получаемой, если значения переменных $x_{i_1},...,x_{i_t}$ положить равными 1.

Также для любых $I=\{i_1,...,i_t\}\subset\overline{1,n}$ и $\varnothing\neq J\subset\overline{1,m}$ обозначим через $F_I^J(f)$ спектральный коэффициент Фурье-Уолша-Адамара [31] , называемый еще коэффициентом статистической структуры [37]:

$$F_I^J(f)=2^{n-1}-\left\|f^J(x)\oplus\langle ch_n(I),x\rangle\right\|.$$

$$F_I^J(f)=\frac{1}{2}W_f\left(ch_n(I)\right),$$

где $W_f\left(ch_n(I)\right)$ – преобразование Уолша f^J [39].

Порядок корреляционной иммунности отображения может быть определен с помощью вектора

$$F_k(f)=\left(F_I^J(f):J\subset\overline{1,m},J\neq\varnothing,I\subset\overline{1,n},|I|\le k\right)$$

который состоит из первых (т.е. соответствующих подмножествам мощности 0, ... , k) коэффициентов статистической структуры для каждой компоненты отображения $f(x)\in B_n^m$.

К примеру,

$$f(x)\in R[n,m,k]\Leftrightarrow F_k(f)=\vec{0},$$

где $\vec{0}$ – вектор из всех нулей размерности $\left(2^m-1\right)\sum_{i=0}^{k}\binom{n}{i}$ [37].

Рассмотрим следующие формулы, связывающие веса подфункций и спектральные коэффициенты [31]:

$$F_I^J=\sum_{L\subset I}(-1)^{|L|}\left(2^{n-1}-2^{|L|}w_L^J\right),\qquad(4)$$

$$w_I^J-2^{n-|I|-1}=2^{-|I|}\cdot\sum_{L\subset I}(-1)^{|L|+1}F_L^J,\qquad(5)$$

Формула (5) при замене $F_I^J(f)$ на $W_f\left(ch_n(I)\right)$ часто называется равенством Саркара [28]. Поскольку работы [31] и [40] были опубликованы практически одновременно и независимо друг от друга, было бы правильно назвать формулы (4) and (5) равенством Денисова-Саркара.

Из формул (4) и (5) следует взаимооднозначное соответствие между вектора $F_k(f)$ и $W_k(f)$:

$$W_k(f)=\left(w_I^J(f):J\subset\overline{1,m},J\neq\varnothing,I\subset\overline{1,n},|I|\le k\right).$$

В [24] и [37] были доказаны локальные предельные теоремы для распределения векторов of $F_k(f)$ случайного двоичного отображения f.

Обозначим

$$z_I^J(f)=2^{n-|I|-1}-w_I^J(f).$$

Докажем вспомогательную лемму.

Лемма 1. *Для произвольных натуральных n, m и k, где $k<n$, верно*

$$\left|f\in B_n^m:w_I^J(f)=2^{n-|I|-1}-z_I^J(f)\;\forall I\subset\overline{1,n},|I|\le k,\right.$$

$$\forall J\subset\overline{1,m},J\neq\varnothing\Big|=\sum_{\substack{J\subset\overline{1,m},J\neq\varnothing,K\subset\overline{1,n-1};|K|=k\\ z(K,J)\in\left\{-2^{n-|I|-2},...,2^{n-|I|-2}\right\}}}\left|\left\{h(x)\in B_{n-1}^m:\right.\right.$$

$$w_I^J(h)=2^{(n-1)-|I|-1}-z_{I\cup\{n\}}^J(f)\;\forall I\subset\overline{1,n-1},|I|<k,$$

$$w_K^J(h)=2^{(n-1)-|K|-1}-z(K,J)\;\forall K\subset\overline{1,n-1},$$

$$|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\Big\}\Big|\times$$

$$\times\left|\left\{g(x)\in B_{n-1}^m:=2^{(n-1)-|I|-1}-\left(z_I^J(f)-z_{I\cup\{n\}}^J(f)\right)\right.\right.$$

$$\forall I\subset\overline{1,n-1},|I|<k,w_I^J(g)=2^{(n-1)-|I|-1}-\left(z_I^J(f)-\right.$$

$$\left.\left.-z(I,J)\right)\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}\Big|.$$

Доказательство.

Существует взаимнооднозначное соответствие между $f^J\in B_n^1$ и парой подфункций $\left\{\left(f^J\right)_n^1,\left(f^J\right)_n^0\right\}$:

$$h(x_1,...,x_{n-1})=\left(f^J\right)_n^1=x_nf^J$$

$$g(x_1,...,x_{n-1})=\left(f^J\right)_n^0=(x_n\oplus1)f^J=f^J-x_nf^J$$

Следовательно, для любого $K=\{i_1,...,i_t\}\subset\overline{1,n-1}$

$$w_K^J(h)=\left\|\left(f^J\right)_{i_1,...,i_{|I|}n}^{1,...,1,1}\right\|=w_{K\cup\{n\}}^J(f),\qquad(6)$$

$$w_K^J(g)=\left\|\left(f^J\right)_{i_1,...,i_{|I|}n}^{1,...,1,0}\right\|=w_K^J(f)-w_{K\cup\{n\}}^J(f).\qquad(7)$$

Также для любого $I\subset\overline{1,n-1}$

$$z_I^J(h)=2^{(n-1)-|I|-1}-w_I^J(h)=2^{n-(|I|+1)-1}-w_{I\cup\{n\}}^J(f)=$$

$$=z_{I\cup\{n\}}^J(f),$$

$$z_I^J(g)=2^{(n-1)-|I|-1}-w_I^J(g)=\left(2^{n-|I|-1}-w_I^J(f)\right)-$$

$$-\left(2^{n-(|I|+1)-1}-w^J_{I\cup\{n\}}(f)\right)=z^J_I(f)-z^J_{I\cup\{n\}}(f).$$

Таким образом, для каждого фиксированного вектора из целых чисел

$$\left(z(I,J)\in\mathbb{Z}:\forall J\subset\overline{1,m},J\neq\varnothing,\forall I\subset\overline{1,n-1},|I|=k\right)$$

размерности $\left(2^m-1\right)\binom{n-1}{k}$ существует взаимнооднозначное соответствие между отображениями $f(x)\in B^m_n$, удовлетворяющих условиям

$$\forall I\subset\overline{1,n}:|I|\le k;\forall J\subset\overline{1,m},J\neq\varnothing:$$
$$w^J_I(f)=2^{n-|I|-1}-z^J_I(f)$$
$$\forall I\subset\overline{1,n-1}:|I|=k;\forall J\subset\overline{1,m},J\neq\varnothing:$$
$$w^J_{I\cup\{n\}}(f)=2^{n-(|I|+1)-1}-z(I,J)$$

и декартовым произведением множеств

$$\left\{h(x)\in B^m_{n-1}:w^J_I(h)=2^{(n-1)-|I|-1}-z^J_{I\cup\{n\}}(f)\right.$$
$$\forall I\subset\overline{1,n-1},|I|<k,w^J_K(h)=2^{(n-1)-|I|-1}-z(K,J)$$
$$\left.\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}$$

и

$$\left\{g(x)\in B^m_{n-1}:w^J_I(g)=2^{(n-1)-|I|-1}-\left(z^J_I(f)-\right.\right.$$
$$-z^J_{I\cup\{n\}}(f)\Big)\forall I\subset\overline{1,n-1},|I|<k,w^J_I(g)=2^{(n-1)-|I|-1}-$$
$$\left.-\left(z^J_I(f)-z(I,J)\right)\forall K\subset\overline{1,n-1},|K|=k;\forall\varnothing\neq J\subset\overline{1,m}\right\}$$

Легко доказать, что

$$-2^{n-|I|-2}\le z(I,J)\le 2^{n-|I|-2}$$

Конец доказательства.

Теорема 2. *Для произвольных натуральных n, m и k, где* $k<n$ *, верно*

$$\left|f\in B^m_n:F^J_I(f)=F^J_I\ \forall I\subset\overline{1,n},|I|\le k,\forall\varnothing\neq J\subset\overline{1,m}\right|=$$
$$=\sum_{\substack{J\subset\overline{1,m},J\neq\varnothing,K\subset\overline{1,n-1};|K|=k\\F(K,J)\in\{-2^{n-1},\dots,2^{n-1}\}}}\left|\left\{h(x)\in B^m_{n-1}:F^J_I(h)=\right.\right.$$
$$=\frac{F^J_I-F^J_{I\cup\{n\}}}{2}\forall I\subset\overline{1,n-1},|I|<k,F^J_K(h)=\frac{F^J_K}{2}-$$
$$\left.\left.-\frac{F(K,J)}{2}\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}\right|\times$$
$$\times\left|\left\{g(x)\in B^m_{n-1}:F^J_I(g)=\frac{F^J_I+F^J_{I\cup\{n\}}}{2}\forall I\subset\overline{1,n-1},\right.\right.$$
$$\left.\left.|I|<k,F^J_K(g)=\frac{F^J_K+F(K,J)}{2}\right.\right.$$
$$\left.\left.\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}\right|.$$

Доказательство.
Легко видеть, что

$$F^J_I(f)=\sum_{L\subset I}(-2)^{|L|}z^J_L(f),\qquad(8)$$

$$z^J_I(f)=2^{-|I|}\cdot\sum_{L\subset I}(-1)^{|L|}F^J_L.\qquad(9)$$

Из (8) следует, что условия (6) и (7) эквивалентны

$$F^J_I(f)=\sum_{L\subset I}(-2)^{|L|}z^J_L(f)$$
$$\forall I\subset\overline{1,n}:|I|\le k;\forall J\subset\overline{1,m},J\neq\varnothing,\qquad(10)$$

$$F^J_{I\cup\{n\}}(f)=\sum_{L_1\subset I\cup\{n\}}(-2)^{|L|}z^J_{L_1}(f)$$
$$\forall I\subset\overline{1,n-1}:|I|=k;\forall J\subset\overline{1,m},J\neq\varnothing,\qquad(11)$$

где $z^J_{I\cup\{n\}}(f)=z(I,J)$.

Из (8) и (9) следует, что

$$\forall I\subset\overline{1,n-1}:|I|\le k;\forall J\subset\overline{1,m},J\neq\varnothing:$$
$$F^J_I(h)=\sum_{I_1\subset I}(-2)^{|I_1|}z^J_{I_1\cup\{n\}}(f)=$$
$$=\sum_{I_1\subset I}(-2)^{|I_1|}\left(2^{-|I_1|-1}\cdot\sum_{L\subset I_1\cup\{n\}}(-1)^{|L|+1}F^J_L\right)=$$
$$=\frac{1}{2}\sum_{I_1\subset I}(-1)^{|I_1|}\left(\sum_{I_2\subset I_1}(-1)^{|I_2|}F^J_L+\sum_{I_2\subset I_1}(-1)^{|I_2|+1}F^J_{I_2\cup\{n\}}\right)=$$
$$=\frac{1}{2}\sum_{I_1\subset I}(-1)^{|I_1|}\sum_{I_2\subset I_1}\left((-1)^{|I_2|}F^J_{I_2}(f)+(-1)^{|I_2|+1}F^J_{I_2\cup\{1\}}\right)=$$
$$=\frac{1}{2}\sum_{I_2\subset I}(-1)^{|I_2|}\left(F^J_{I_2}(f)-F^J_{I_2\cup\{n\}}\right)\sum_{I_1:I_2\subset I_1\subset I}(-1)^{|I_1|}.$$

Очевидно, что:

$$\sum_{I_1:I_2\subset I_1\subset I}(-1)^{|I_1|}=\mathrm{Ind}\{I_2=I\},$$

где $\mathrm{Ind}\{A\}$ - индикатор события A.

Таким образом,

$$F^J_I(h)=\frac{F^J_I(f)-F^J_{I\cup\{n\}}(f)}{2}.$$

Обозначим через $F(I,J)$ величину $F^J_{I\cup\{n\}}(f)$ для $\forall I\subset\overline{1,n-1}:|I|=k;\forall J\subset\overline{1,m},J\neq\varnothing$, $-2^{n-1}\le F(I,J)\le 2^{n-1}$.

Также $\forall I \subset \overline{1,n-1}: |I| \le k; \forall J \subset \overline{1,m}, J \ne \varnothing$ выполняется:

$$F_I^J(g) = \sum_{I_1 \subset I} (-2)^{|I_2|} \left(z_I^J(f) - z_{I\cup\{n\}}^J(f) \right) =$$

$$= \sum_{I_1 \subset I} (-2)^{|I_2|} z_I^J(f) - \sum_{I_1 \subset I} (-2)^{|I_2|} z_{I\cup\{n\}}^J(f) =$$

$$= F_I^J(f) - F_I^J(h) = F_I^J(f) - \frac{F_I^J(f) - F_{I\cup\{n\}}^J(f)}{2} =$$

$$= \frac{F_I^J(f) + F_{I\cup\{n\}}^J(f)}{2}.$$

Из леммы 1 следует, что для любого целочисленного вектора

$$\left(F(I,J) \in \mathbb{Z} : \forall J \subset \overline{1,m}, J \ne \varnothing, \forall I \subset \overline{1,n-1}, |I| = k \right)$$

размерности $\left(2^m - 1\right)\binom{n-1}{k}$ существует взаимнооднозначное соответствие между отображениями $f(x) \in B_n^m$, удовлетворяющих условиям (10) и (11) и декартовым произведением множеств

$$\left\{ h(x) \in B_{n-1}^m : F_I^J(h) = \frac{F_I^J(f) - F_{I\cup\{n\}}^J(f)}{2} \forall I \subset \overline{1,n-1}, \right.$$

$$|I| < k, F_K^J(h) = \frac{F_K^J(f) - F(K,J)}{2}$$

$$\left. \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing \right\}$$

и

$$\left\{ g(x) \in B_{n-1}^m : F_I^J(g) = \frac{F_I^J(f) + F_{I\cup\{n\}}^J(f)}{2} \right.$$

$$\forall I \subset \overline{1,n-1}, |I| < k, F_K^J(g) = \frac{F_K^J(f) + F(K,J)}{2}$$

$$\left. \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing \right\}.$$

Окончание доказательства.

Доказанная теорема, которая была экспериментально проверена при малых значениях n, m и k, позволяет, в частности, доказать аналогичные формулы для корреляционно-иммунных и (n,m,k)-устойчивых булевых отображений. Рассмотрим следующие формулы, связывающие спектральные коэффициенты функции:

$$\forall I \subset \overline{1,n}; \forall J \subset \overline{1,m}, J \ne \varnothing$$

$$\sum_{L \subset I} (-1)^{|L|} F_L^J(f) \equiv 0 \left(\bmod 2^{|I|} \right), \qquad (12)$$

$$\sum_{\varnothing \ne S \subset J, L \subset I} (-1)^{|L|+|S|} F_L^S(f) \equiv 0 \left(\bmod 2^{|I|+|J|-1} \right). \qquad (13)$$

Эти формулы были доказаны как следствие 2 в [41]

Следствие 3. *Для произвольных натуральных n, m и k, где $k < n$, верно*

$$\left| R[n,m,k] \right| = \sum_{\substack{s(K,J) \in \left\{-2^{n-k-2}, \ldots, 2^{n-k-2}\right\}: \\ J \subset \overline{1,m}, J \ne \varnothing; K \subset \overline{1,n-1}; |K| = k}} \left| \left\{ h \in B_{n-1}^m : F_I^J(h) = 0 \right.\right.$$

$$\forall I \subset \overline{1,n-1}, |I| < k, F_K^J(h) = 2^k s(K,J)$$

$$\left. \left. \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing \right\} \right| \times$$

$$\times \left| \left\{ g \in B_{n-1}^m : F_I^J(g) = 0 \, \forall I \subset \overline{1,n-1}, |I| < k, F_K^J(g) = \right.\right.$$

$$\left. \left. = -2^k z(K,J) \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing, \right\} \right|.$$

Доказательство.

Легко видеть, что:

$$\left| R[n,m,k] \right| = \left| \left\{ f(x) \in B_n^m : F_k(f) = \vec{0} \right\} \right|.$$

Из теоремы 2 следует, что,

$$\left| R[n,m,k] \right| = \sum_{\substack{J \subset \overline{1,m}, J \ne \varnothing, I \subset \overline{1,n-1}; |I| = k \\ F(I,J) \in \left\{-2^{n-1}, \ldots, 2^{n-1}\right\}}} \left| \left\{ h(x) \in B_{n-1}^m : \right.\right.$$

$$F_I^J(h) = 0 \forall I \subset \overline{1,n-1}, |I| \le k, F_K^J(h) =$$

$$\left. \left. = -\frac{1}{2} F(K,J) \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing \right\} \right| \times$$

$$\times \left| \left\{ g(x) \in B_{n-1}^m : F_I^J(g) = 0 \forall I \subset \overline{1,n-1}, |I| \le k, F_K^J(g) = \right.\right.$$

$$\left. \left. = \frac{1}{2} F(K,J) \forall K \subset \overline{1,n-1}, |K| = k; \forall J \subset \overline{1,m}, J \ne \varnothing \right\} \right|.$$

Из (12) следует, что

$$\sum_{L \subset K, L \ne K} (-1)^{|L|+1} F_L^J(f) \equiv F_K^J(f) \left(\bmod 2^{|I|} \right).$$

Следовательно,

$$F(K,J) = F_{K\cup\{n\}}^J(f) \equiv 0 \left(\bmod 2^{k+1} \right),$$

$$\exists s(K,J) : F(K,J) = 2^{k+1} s(K,J),$$

$$s(K,J) \in \left\{ -2^{n-k-2}, \ldots, 2^{n-k-2} \right\}.$$

Окончание доказательства.

Следствия 3 было доказано как теорема 5 в [44].

Из результатов [37] следует, что

$$f(x) \in K[n,m,k] \Leftrightarrow$$

$$\Leftrightarrow F_I^J(f) = 0 \; \forall I \subset \overline{1,n}, 1 \le |I| \le k, \forall J \subset \overline{1,m}, J \ne \varnothing,$$

Из (12) следует, что

$$F_\varnothing^J(f) \equiv 0 \left(\bmod 2^k \right) \quad \forall f(x) \in K[n,m,k].$$

Следовательно,

$$F_{\varnothing}^{J}(f)=2^{n-1}-\left\|f^{J}\right\|,$$
$$\forall f(x)\in K[n,m,k]\;\exists t_J\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\}:$$
$$F_{\varnothing}^{J}(f)=2^{k}t_J,\left\|f^{J}\right\|=2^{n-1}-F_{\varnothing}^{J}(f).$$

Обозначим через $K_{\left(t_J,\varnothing\neq J\subset\overline{1,m}\right)}[n,m,k]$ множество корреляционно-иммунных порядка k отображений $f\in B_n^m$ таких, что $\left\|f^{J}\right\|=2^{n-1}-2^{k}t_J$, $t_J\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\}$, $J\subset\overline{1,m}$, $J\neq\varnothing$.

Из (12) следует, что это множество будет пусто, если не будет выполнено условие:

$$\sum_{\varnothing\neq S\subset J}(-1)^{|S|}2^{k}t_J\equiv 0\left(\mathrm{mod}\,2^{|J|-1}\right).$$

Следствие 4. *Для произвольных натуральных n, m и k, где $k<n$, верно*

$$\left|K_{\left(t_J,\varnothing\neq J\subset\overline{1,m}\right)}[n,m,k]\right|=\sum_{\substack{s(K,J)\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\}:\\ J\subset\overline{1,m},J\neq\varnothing;K\subset\overline{1,n-1};|K|=k}}\left|\left\{h\in B_{n-1}^{m}:\right.\right.$$
$$F_I^J(h)=0\forall I\subset\overline{1,n-1},1\le|I|<k,F_{\varnothing}^{J}(h)=2^{k-1}t_J,$$
$$=2^{k-1}s(K,J)\forall K\subset\overline{1,n-1},|K|=k;\forall\varnothing\neq J\subset\overline{1,m}\Big\}\Big|\times$$
$$\times\left|\left\{g(x)\in B_{n-1}^{m}:F_I^J(g)=2^{k-1}t_J,F_I^J(g)=0\forall I\subset\overline{1,n-1},\right.\right.$$
$$1\le|I|<k,F_K^J(h)=-2^{k-1}s(K,J)$$
$$\left.\left.\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}\right|.$$

Доказательство.
Легко видеть, что:

$$\left|K_{\left(t_J,J\subset\overline{1,m},J\neq\varnothing\right)}[n,m,k]\right|=$$
$$=\sum_{\substack{J\subset\overline{1,m},J\neq\varnothing,K\subset\overline{1,n-1};|K|=k\\ F(K,J)\in\left\{-2^{n-1},...,2^{n-1}\right\}}}\left|\left\{h(x)\in B_{n-1}^{m}:F_{\varnothing}^{J}(h)=2^{k-1}t_J,\right.\right.$$
$$F_I^J(h)=0\forall I\subset\overline{1,n-1},1\le|I|<k,F_K^J(h)=$$
$$=-\frac{1}{2}F(K,J)\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\Big\}\Big|\times$$
$$\times\left|\left\{g(x)\in B_{n-1}^{m}:F_I^J(g)=2^{k-1}t_J,F_I^J(g)=0\forall I\subset\overline{1,n-1},\right.\right.$$
$$1\le|I|<k,F_K^J(g)=$$
$$\left.\left.=\frac{1}{2}F(K,J)\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\right\}\right|.$$

Из (12) следует, что

$$2^{k}t_J+(-1)^{k+1}F(K,J)\equiv 0\left(\mathrm{mod}\,2^{k+1}\right).$$

Следовательно,

$$\exists s(K,J):F(K,J)=2^{k}s(K,J),$$
$$s(K,J)\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\}.$$

Окончание доказательства.
Отсюда получаем:

Следствие 5. *Для произвольных натуральных n, m и k, где $k<n$, верно*

$$\left|K[n,m,k]\right|=$$
$$\sum_{\substack{t_J\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\},\\ J\subset\overline{1,m},J\neq\varnothing:\\ \varnothing\neq S\subset J}(-1)^{|S|}2^{k}t_J\equiv 0\left(\mathrm{mod}\,2^{|J|-1}\right)}\;\sum_{\substack{s(K,J)\in\left\{-2^{n-k-1},...,2^{n-k-1}\right\}:\\ J\subset\overline{1,m},J\neq\varnothing;K\subset\overline{1,n-1};|K|=k}}\left|\left\{h\in B_{n-1}^{m}:\right.\right.$$
$$F_I^J(h)=0\forall I\subset\overline{1,n-1},1\le|I|<k,F_K^J(h)=2^{k-1}s(K,J)$$
$$\forall K\subset\overline{1,n-1},|K|=k;F_{\varnothing}^{J}(h)=2^{k-1}t_J\forall\varnothing\neq J\subset\overline{1,m}\Big\}\Big|\times$$
$$\times\left|\left\{g(x)\in B_{n-1}^{m}:F_{\varnothing}^{J}(g)=2^{k-1}t_J,F_I^J(g)=0\forall I\subset\overline{1,n-1},\right.\right.$$
$$1\le|I|<k,F_K^J(h)=-2^{k-1}s(K,J)$$
$$\left.\left.\forall K\subset\overline{1,n-1},|K|=k;\forall\varnothing\neq J\subset\overline{1,m}\right\}\right|.$$

Возможность доказательства следствия 5 была анонсирована в [7].

Видно, что множество отображений в правой части равенств в следствиях 3, 4 и 5 являются подмножествами $R[n-1,m,k-1]$ и $K[n-1,m,k-1]$ соответственно.

Следствия 3-5 позволяют вычислить мощность множеств корреляционно-иммунных и (n,m,k)-устойчивых булевых отображений для параметров (n,m,k), если известно распределение мощности множеств с фиксированным вектором коэффициентов Фурье-Уолша-Адамара для параметров (n-1,m,k).

Также очевидно

Следствие 6. *Пусть для произвольных натуральных n, m и k, где $k<n$, отображение f случайно и равновероятно выбирается из B_n^m, а отображение h - из B_{n-1}^m. Тогда*

$$\mathrm{P}\left(f\in R[n,m,k]\right)=\sum_{\substack{s(K,J)\in\left\{-2^{n-k-2},...,2^{n-k-2}\right\}:\\ J\subset\overline{1,m},J\neq\varnothing;K\subset\overline{1,n-1};|K|=k}}\mathrm{P}\Big(F_I^J(h)=0$$
$$\forall I\subset\overline{1,n-1},|I|<k,F_K^J(h)=2^{k}s(K,J)$$
$$\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing\Big)\times\frac{1}{2^{2^m}}\times$$
$$\times\left|\left\{g\in B_{n-1}^{m}:F_I^J(g)=0\,\forall I\subset\overline{1,n-1},|I|<k,F_K^J(g)=\right.\right.$$
$$\left.\left.=-2^{k}z(K,J)\forall K\subset\overline{1,n-1},|K|=k;\forall J\subset\overline{1,m},J\neq\varnothing,\right\}\right|.$$

Заключение

Подводя итог данной работы, можно сказать, что квантовые коммуникации как синоним квантовой криптографии играют важную роль в формировании в Российской Федерации цифровой экономики. Главной задачей этих технологий является поддержание достаточного уровня информационной безопасности в условиях грядущего квантового вызова, который связан с появлением в скором времени квантовых вычислителей, способных эффективно решать задачи, на которых основаны, в частности, современные системы открытого распределения ключей для существующих криптографических систем.

В настоящее время КК активно используются коммерческими и государственными структурами во всем мире и, в частности, в Российской Федерации. При этом широко проводятся исследования в области разработки и реализации систем квантового распределения ключей, как основной части квантовой криптографии. Эти системы предназначены для функционирования в различных средах, в том числе и в космическом пространстве с помощью искусственных спутников Земли.

В связи с этим является актуальной задача разработки новых и уточнения уже существующих протоколов квантового распределения ключа, а также изучения различных математических и физических объектов, которые связаны с этими протоколами.

В частности, с одним из этапов классического протокола BB84, реализуемого в квантовом канале с шумом, связана задача изучения корреляционно-иммунных и устойчивых отображений, частью которой является задача оценки их числа, которая до настоящего времени полностью не решена.

В рамках данной работы получены наилучшие на текущий момент асимптотические верхние и нижние оценки числа (n,m,k)-устойчивых и корреляционной-иммунных порядка k отображений с числом выходов $m \geq 5$. Также были доказаны рекуррентные соотношения, которые позволяют найти точное распределения мощностей классов этих отображений для случая небольшого числа входов n и выходов

Полученные результаты позволяют, к примеру, оценить вероятность того, что при случайном выборе отображения для усиления секретности на этапе вторичной обработки протокола BB84 будет нейтрализована ситуация, когда Ева имеет доступ к k фотонам из посылаемым по каналу связи по своему выбору.

Литература

1. *Кронберг Д.А. Ожигов Ю.И., Чернявский А.Ю.* Квантовая криптография. М.: МАКС Пресс, 2011. 111 с.

2. *Wiesner, S.* Conjugate coding // SIGACT News. 1983. 15, pp. 78-88.

3. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Svs, and Sign. Proees,, Bangalore, India, 1984, pp. 175-179.

4. *Карасев С.* Объём мирового рынка квантовых вычислений достиг почти $500 млн. 06.02.2022 // Servernews. Все самое свежее из мира больших мощностей. URL: https://servernews.ru/1059594 (Дата обращения 02.06.2022).

5. *Marks* Справочная: квантовая криптография на пальцах. 15.07.2019 // Хабр. URL: https://habr.com/ru/post/460165/ (Дата обращения 02.06.2022).

6. *Лебедева Д.* В России запустили квантовую сеть, открытую для присоединения. 14.10.2021 // CNews. URL: https://www.cnews.ru/news/top/2021-10-14_v_moskve_ofitsialno_zapustili (Дата обращения 02.06.2022)

7. *Pankov K.* Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage // Conference of Open Innovations Association, FRUCT. 2019. No. 24, pp. 300-306. DOI 10.23919/FRUCT.2019.8711894

8. *Григоренко Л.А.* Технология блокчейн с точки зрения информационной безопасности // Актуальные проблемы современной науки, техники и образования : Тезисы докладов 79-й международной научно-технической конференции, Магнитогорск, 19-23 апреля 2021 года. Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова. 2021. С. 391.

9. *Pankov K.N., Saksonov E.A.* Using Probabilistic Methods in the Analysis of Information Security of Distributed Ledger Systems // 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings, Moscow, 16–18 march 2021. Moscow, 2021, pp. 9416006. DOI 10.1109/IEEECONF51389.2021.9416006.

10. *Белокопытова В.* Квантовая криптография получила официальный статус. 09.08.2017 // Известия. URL: https://iz.ru/630033/vasilisa-belokopytova/kvantovaia-kriptografiia-poluchila-ofitcialnyi-status (Дата обращения 02.06.2022).

11. *Панков К.Н., Эйнман А.Д.* Сертификация систем распределенного реестра как инструмент обеспечения информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 2. С. 37-49.

12. МР 26.4.004-2021 «Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации». М.: Росстандарт, 2021.

13. *Hufnagel F., Sit A., Bouchard F., Zhang Y., England D., Heshami K., Sussman B.J., Karimi E.* Investigation of underwater quantum channels in a 30 meter flume tank using structured photons // New Journal of Physics. 2020. No. 22, pp. 093074.

14. *Titovets P.A., Kazantsev S.Yu., Miroshnikova N.E., Podgorny A.A.* Wireless underwater optical communication with quantum key distribution // Proc. SPIE 12086, XV International Conference on Pulsed Lasers and Laser Applications, (2 December 2021); 120860X; https://doi.org/10.1117/12.2601666

15. *Liu H.-Y., Tian X.-H., Gu C., Fan P., Ni X. R., Yang J.-N. Zhang M. Hu J. Guo X. Cao Hu, Zhao X.G. Lu Y.-Q. Gong Y.-X., Xie Z., Zhu S.-N.* Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes // Phys. Rev. Lett. 2021. No. 126, pp. 020503

16. *Румянцев К.Е. Цыцорин Д.А.* Особенности квантового распределения ключа между спутниковой и наземной станциями // Digital Era : Материалы II Всероссийской научно-практической конференции, Грозный, 25 марта 2022 года. Грозный: Чеченский государственный университет имени Ахмата Абдулхамидовича Кадырова, 2022. С. 90-93. DOI 10.36684/59-2022-2-90-93

17. *Кулик С.* Квантовое распределение ключей через атмосферные каналы связи. Слайды выступления на конференции 25.03.2021 // РусКрипто. URL: https://www.ruscrypto.ru/resource/archive/rc2021/files/07_kulik.pdf (Дата обращения 03.06.2022)

18. *Liao S.-K.; Cai W.-Q.; Handsteiner J.; Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M. , Deng L., Xi T., Ma L., Hu T., Li L., Liu N.-L. , Koidl F., Wang P., Chen Y.-A., Wang X.-B. , Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang*

J.-Y., Zeilinger A., Pan J.-W. Satellite-Relayed Intercontinental Quantum Network // Physical Review Letters. 2018. No. 120(3), pp. 030501. doi:10.1103/PhysRevLett.120.030501

19. *Yin J., Li Y.-H., Liao S.-K., Yang M., Cao Y., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li S.-L., Shu R., Huang Y.-M., Deng L., Li L., Zhang Q., Liu N.-L., Chen Y.-A., Lu C.-Y., Wang X.-B., Xu F., Wang J.-Y., Peng C.-Z., Ekert A.K., Pan J.-W.* Entanglement-based secure quantum cryptography over 1,120 kilometres // Nature. 2020. No. 582, pp. 501-505. doi:10.1038/s41586-020-2401-y

20. *Никифорова А.* В России создают квантовую спутниковую связь. На проект потратят $1 млн. 28.01.2022 // Хайтек. URL: https://hightech.fm/2022/01/28/qspace (Дата обращения 03.06.2022).

21. *Вьюгин И.* Ключ в надёжном месте. ОАО «РЖД» и «Роскосмос» развивают квантовую сеть передачи данных. 27.04.2022 // Гудок URL: https://gudok.ru/content/science_education/1601824/ (Дата обращения 03.06.2022)

22. *Bennett C.H., Brassard G., Robert J.M.:* Privacy amplification by public discussion. SIAM J. Comput. 1988. No. 17(2), pp. 210-229.

23. *Chor B., Goldreich O., Hastad J., Friedman J., Rudich S. Smolensky R.* The bit extraction problem or t -resilient functions // Proc. 26th IEEE Symp. Foundations of Computer Science, 1985, pp. 396-407.

24. *Панков К.Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Матем. вопр. криптогр. 2014. № 5:4. С. 73-97.

25. *Gopalakrishnan K., Stinson, D. R.* Three characterizations of non-binary correlation-immune and resilient functions // Designs, Codes and Cryptography. 1995. No. 5(3), pp. 241-251.

26. *Pankov K.N.* Asymptotic Enumeration of Binary Orthogonal Arrays // Proceedings of the International Conference Technology & Entrepreneurship in Digital Society (TEDS) : Proceedings of the International Conference, Moscow, 07 ноября 2018 года. М.: Издательский дом "Реальная экономика", 2019. С. 86-89.

27. *Зубов А.Ю.* Математика кодов аутентификации. М.: Гелиос АРВ, 2007. 480 с.

28. *Таранников Ю.В.* Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011. 152 с.

29. *Logachev O.A., Salnikov A.A., Yashchenko V.V.* Boolean Functions in Coding Theory and Cryptography. Rhode Island, USA: American Mathematical Society Providence, 2011. 334 p.

30. *Denisov O.V.* An asymptotic formula for the number of correlation-immune of order q boolean functions // Discrete Mathematics and Applications. 1992. No. 2(4), pp. 279-288.

31. *Denisov O.V.* A local limit theorem for the distribution of a part of the spectrum of a random binary function. // Discrete Mathematics and Applications. 2000. No. 10(1), pp. 87-101.

32. *Bach E.* Improved asymptotic formulas for counting correlation immune Boolean functions // SIAM Journal on Discrete Mathematics. 2009. No. 23(3). Pp. 1525—1538

33. *Canfield E.R., Gao Z., Greenhill C.S., McKay B.D., Robinson R.W.* Asymptotic enumeration of correlation-immune boolean functions. // Cryptography and Communications. 2010. No. 2(1), pp. 111-126.

34. *Pankov K.N.* Improved asymptotic estimates for numbers of correlation-immune and (n,m,k)-resilient vectorial boolean functions // Discrete Mathematics and Applications. 2019. No. 29(3), pp. 195-213.

35. *Сачков В.Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013. 336 с.

36. *Панков К.Н.* Улучшенные оценки для числа k-эластичных и корреляционно-иммунных двоичных отображений // Прикладная дискретная математика. Приложение. 2021. № 14. С. 48-51. DOI 10.17223/2226308X/14/8.

37. *Панков К.Н.* Локальная предельная теорема для распределения части вектора весов подфункций компонент случайного двоичного отображения // Математические вопросы криптографии. 2014. Т. 5. № 3. С. 49-80.

38. *Carlet C.* Vectorial Boolean Functions. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, UK: Cambridge University Press, 2010, pp. 398-472.

39. *Carlet C., Sarkar P.* Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. Finite Fields and Their Applications. 2002. No. 8(1), pp. 120-130.

40. *Sarkar P.* Spectral domain analysis of correlation immune and resilient boolean functions. 2000 // Cryptology ePrint Archive. URL: https://eprint.iacr.org/2000/049 (Дата обращения 04.06.2022).

41. *Панков К.Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4(18). С. 14-30.

ESTIMATES FOR NUMBERS OF BOOLEAN MAPPINGS USED IN QUANTUM KEY DISTRIBUTION PROTOCOLS

KONSTANTIN N. PANKOV
Moscow, Russian Federation, pankov_kn@mtuci.ru

KEYWORDS: *Information Security, quantum cryptography, quantum key distribution, protocol BB84, correlation-immune Boolean mapping, resilient Boolean mappings.*

ABSTRACT

Introduction: In the near future, quantum cryptography will play an important role in maintaining a sufficient level of information security of modern telecommunication networks in the conditions of a quantum challenge, which refers to the emergence of quantum computers that will be able to effectively solve the mathematical problems on which, for example, modern key distribution systems are based. Now quantum cryptography is actively used by commercial and government agencies around the world and, in particular, in the Russian Federation. At the same time, a large amount of research is being carried out in the field of development and implementation of quantum key distribution systems, as the main part of quantum cryptography. In this regard, the task of developing new and refining existing protocols for quantum key distribution, as well as studying various mathematical and physical objects that are associated with these protocols, is an urgent task. In particular, one of the stages of the classical BB84 protocol implemented in a noisy quantum channel is associated with the problem of studying correlation-immune and stable mappings, part of which is the problem of estimating their number, which has not been completely solved. **Purpose:** to find mathematical expressions for exact and asymptotic estimates of the cardinalities of classes of (n,m,k)-stable and correlation-immune of order k boolean mappings. **Results:** The best currently asymptotic upper and lower bounds for the number of such classes of mappings with the number of outputs greater than or equal to five are obtained. Recurrent relations were also proved, which allow one to find the exact distribution of the cardinalities of classes of similar mappings for the case of small numbers n and m. **Practical relevance:** the results obtained allow us to estimate the probability that with a random choice of mapping to enhance secrecy at the stage of secondary processing of the BB84 protocol, the situation will be neutralized when the adversary has access to k photons sent over a communication channel of his choice.

REFERENCES

1. Kronberg D.A. Ozhigov Yu.I., CHernyavskij A.YU. Quantum cryptography. Moscow: MAKS Press, 2011. 111 p. (In Rus)

2. Wiesner, S. Conjugate coding. *SIGACT News*. 1983. no. 15, pp. 78-88.

3. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proc.of IEEE Int. Conf. on Comput. Svs, and Sign. Proees*, Bangalore, India, 1984, pp. 175-179.

4. Karasev S. The global quantum computing market has reached almost $500 million. 06.02.2022. *Servernews*. All the latest from the world of high power. URL: https://servernews.ru/1059594 (date of access 02.06.2022). (In Rus)

5. Background: quantum cryptography real simple. 15.07.2019 // Habr. URL: https://habr.com/ru/post/460165/ (date of access 02.06.2022) (In Rus)

6. Lebedeva D. Russia has launched a quantum network open for joining.14.10.2021 // CNews. URL: https://www.cnews.ru/news/top/2021-10-14_v_moskve_ofitsialno_zapustili (date of access 02.06.2022). (In Rus)

7. Pankov K. Enumeration of Boolean Mapping with Given Cryptographic Properties for Personal Data Protection in Blockchain Data Storage. *Conference of Open Innovations Association, FRUCT*. 2019. No 24, pp. 300-306. DOI 10.23919/FRUCT.2019.8711894

8. Grigorenko L.A. Blockchain technology from the point of view of information security. *Aktual'nye problemy sovremennoj nauki, tekhniki i obrazovaniya : Tezisy dokladov 79-j mezhdunarodnoj nauchno-tekhnicheskoj konferencii*. Magnitogorsk: Magnitogorskij gosudarstvennyj tekhnicheskij universitet im. G.I. Nosova, 2021, pp. 391.

9. Pankov K.N., Saksonov E.A. Using Probabilistic Methods in the Analysis of Information Security of Distributed Ledger Systems. *2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Conference Proceedings*, Moscow, 16-18 March 2021. Moscow, 2021, pp. 9416006. DOI 10.1109/IEEECONF51389.2021.9416006

10. Belokopytova V. Quantum cryptography received official status. 09.08.2017. *Izvestiya* [News] URL: https://iz.ru/630033/vasilisa-belokopytova/kvantovaia-kriptografiia-poluchila-ofitcialnyi-status (date of access 02.06.2022). (In Rus)

11. Pankov K.N., Ejnman A.D. Certification of distributed ledger systems as a tool for ensuring information security. *REDS: Telecommunication devices and systems*. 2021. Vol. 11. № 2, pp. 37-49. (In Rus)

12. MR 26.4.004-2021 A secure protocol for the interaction of quantum-cryptographic equipment for generating and distributing keys and means of cryptographic information protection. Moscow: Rosstandart, 2021. (In Rus)

13. Hufnagel F., Sit A., Bouchard F., Zhang Y., England D., Heshami K., Sussman B.J., Karimi E. Investigation of underwater quantum channels in a 30 meter flume tank using structured photons. *New Journal of Physics.* 2020. No. 22. P. 093074

14. Titovets P.A., Kazantsev S.Yu., Miroshnikova N.E., Podgorny A.A. Wireless underwater optical communication with quantum key distribution. *Proc. SPIE 12086, XV International Conference on Pulsed Lasers and Laser Applications*, (2 December 2021); 120860X; https://doi.org/10.1117/12.2601666

15. Liu H.-Y., Tian X.-H., Gu C., Fan P., Ni X. R., Yang J.-N. Zhang M. Hu J. Guo X. Cao Hu, Zhao X.G. Lu Y.-Q. Gong Y.-X., Xie Z., Zhu S.-N. Optical-Relayed Entanglement Distribution Using Drones as Mobile Nodes // Phys. Rev. Lett. 2021. No. 126. Pp. 020503

16. Rumyancev, K.E. Cycorin D.A. Features of quantum key distribution between satellite and ground stations. *Digital Era: Proceedings of the II All-Russian Scientific and Practical Conference*, Grozny, March 25, 2022. Groznyj: Chechenskij gosudarstvennyj universitet imeni Ahmata Abdulhamidovicha Kadyrova, 2022, pp. 90-93. DOI 10.36684/59-2022-2-90-93.

17. Kulik S. Quantum distribution of keys through atmospheric communication channels. lides of the speech at the conference 25.03.2021. *RusCrypto*. URL: https://www.ruscrypto.ru/resource/archive/rc2021/files/07_kulik.pdf (date of access 03.06.2022). (In Rus)

18. Liao S.-K.; Cai W.-Q.; Handsteiner J.; Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M. , Deng L., Xi T., Ma L., Hu T., Li L., Liu N.-L. , Koidl F., Wang P., Chen Y.-A., Wang X.-B. , Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang J.-Y., Zeilinger A., Pan J.-W. Satellite-Relayed Intercontinental Quantum Network. *Physical Review Letters*. 2018. No. 120(3), pp. 030501. doi:10.1103/PhysRevLett.120.030501

19. Yin J., Li Y.-H., Liao S.-K., Yang M., Cao Y., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li S.-L., Shu R., Huang Y.-M., Deng L., Li L., Zhang Q., Liu N.-L., Chen Y.-A., Lu C.-Y., Wang X.-B., Xu F., Wang J.-Y., Peng C.-Z., Ekert A.K., Pan J.-W. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*. 2020. No. 582, pp. 501-505. doi:10.1038/s41586-020-2401-y

20. Nikiforova A. V. In Russia, quantum satellite communications are being created. The project will cost $1 million. 28.01.2022. *Hightech.* URL: https://hightech.fm/2022/01/28/qspace (date of access 03.06.2022). (In Rus)

21. V'yugin I. The key is in a safe place. Russian Railways and Roscosmos are developing a quantum data transmission network. 27.04.2022. *Gudok* [Horn]. URL: https://gudok.ru/content/science_education/1601824/ (date of access 03.06.2022). (In Rus)

22. Bennett C.H., Brassard G., Robert J.M. Privacy amplification by public discussion. *SIAM J. Comput*. 1988. No. 17(2), pp. 210-229.

23. Chor B., Goldreich O., Hastad J., Friedman J., Rudich S. Smolensky R. The bit extraction problem or t-resilient functions. *Proc. 26th IEEE Symp. Foundations of Computer Science*, 1985, pp. 396-407.

24. Pankov K.N. Asymptotic estimates for numbers of Boolean mappings with given cryptographic properties. *Matematicheskie voprosy kriptografii* [Mathematical Aspects of Cryptography]. 2014. No. 5:4, pp. 73-97. (In Rus)

25. Gopalakrishnan K., Stinson, D. R. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography*. 1995. No. 5(3), pp. 241-251.

26. Pankov K.N. Asymptotic Enumeration of Binary Orthogonal Arrays. *Proceedings of the International Conference Technology & Entrepreneurship in Digital Society (TEDS)* : Proceedings of the International Conference, Moscow, 07 November 2018. Moscow: Izdatel'skij dom "Real'naya ekonomika, 2019, pp. 86-89.

27. Zubov A.Yu. Mathematics of authentication codes. Moscow: Gelios ARV, 2007. 480 p. (In Rus)

28. Tarannikov Yu.V. Combinatorial properties of discrete structures and applications to cryptology. Moscow: MCNMO, 2011. 152 p. (In Rus)

29. Logachev O.A., Salnikov A.A., Yashchenko V.V. Boolean Functions in Coding Theory and Cryptography. Rhode Island, USA: American Mathematical Society Providence, 2011. 334 p.

30. Denisov O. V. An asymptotic formula for the number of correlation-immune of order q boolean functions. *Discrete Mathematics and Applications*. 1992. No. 2(4), pp. 279-288.

31. Denisov O. V. A local limit theorem for the distribution of a part of the spectrum of a random binary function. *Discrete Mathematics and Applications*. 2000. No. 10(1), pp. 87-101.

32. Bach E. Improved asymptotic formulas for counting correlation immune Boolean functions. *SIAM Journal on Discrete Mathematics*. 2009. No. 23(3), pp. 1525-1538

33. Canfield E. R., Gao Z., Greenhill C. S., McKay B. D., Robinson R. W. Asymptotic enumeration of correlation-immune boolean functions. *Cryptography and Communications*. 2010. No. 2(1), pp. 111-126.

34. Pankov K.N. Improved asymptotic estimates for numbers of correlation-immune and (n,m,k)-resilient vectorial boolean functions. *Discrete Mathematics and Applications*. 2019. No. 29(3), pp. 195-213.

35. Sachkov V.N. Course of combinatorial analysis. Izhevsk: NIC "Regulyarnaya i haoticheskaya dinamika", 2013, 336 p. (In Rus)

36. Pankov K.N. Improved estimates for the number of (n,m,k)-resilient and correlation-immune Boolean mappings. *Prikladnaya diskretnaya matematika. Prilozhenie* [Applied Discrete Mathematics. Supplement.]. 2021. No. 14, pp. 48-51. DOI 10.17223/2226308X/14/8. (In Rus)

37. Pankov K.N. Local limit theorem for the distribution of incomplete vector formed by the weights of subfunctions of random binary mapping components. *Matematicheskie voprosy kriptografii* [Mathematical Aspects of Cryptography]. 2014. Vol. 5. No 3, pp. 49-80. (In Rus)

38. Carlet C. Vectorial Boolean Functions. In: Boolean Models and Methods in Mathematics, *Computer Science, and Engineering*. Cambridge, UK: Cambridge University Press, 2010, pp. 398-472.

39. Carlet C., Sarkar, P. Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. *Finite Fields and Their Applications*. 2002. No. 8(1), pp. 120-130.

40. Sarkar P. Spectral domain analysis of correlation immune and resilient boolean functions. 2000. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2000/049 (date of access 04.06.2022)

41. Pankov K.N. Speeds of convergence in limit theorems for joint distributions of some random binary mappings characteristics. *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics]. 2012. No. 4(18), pp. 14-30.

INFORMATION ABOUT AUTHOR:

Konstantin N. Pankov, PhD, Assistant professor, Moscow Technical University of Communications and Informatics, Moscow, Russia

For citation: Pankov K.N. Estimates for numbers of boolean mappings used in quantum key distribution protocols. *H&ES Reserch*. 2022. Vol. 14. No 4. P. 4-18. doi: 10.36724/2409-5419-2022-14-4-4-18 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-19-25

ТЕХНОЛОГИИ РАЗВИТИЯ МОРСКИХ ИНТЕГРИРОВАННЫХ СИСТЕМ СВЯЗИ

ПАВЛИКОВ
Сергей Николаевич[1],

КОПАЕВА
Екатерина Юрьевна[2]

КОЛЕСОВ
Юрий Юрьевич[3],

КРЮЧКОВ
Андрей Николаевич[4]

АННОТАЦИЯ

Цель повышение качества информационного взаимодействия объектов путем увеличения надежности доставки сообщений адресатам и пропускной способности за счет интеграции сетей, использующих различные сигналы и физические каналы. Проведен поиск новых технических решений по созданию интегрированных (гибридных) технологий связи, ориентированных на расширение возможностей по созданию адаптивных, самоорганизующихся, устойчивых к дестабилизирующим факторам систем связи с повышенным качеством предоставляемых услуг на обширных территориях. Метод решения поставленных задач основан на анализе тенденций развития и прогнозировании требований к интегрированным мобильным системам связи. **Новизна** заключается в разработке и оценке вариантов построения структур интегрированных систем связи, представленных разнообразными, дополняющими друг друга подсистемами, использующих различные методы разделения каналов, в том числе и в физических средах, а также алгоритмов их работы. **Основные выводы**. Разработан комплекс технологий для развития приморских интегрированных систем связи: структура системы на основе гибридной ячеистой топологии; базовая форма несущего сигнала с управляемыми параметрами в зависимости от физического канала; принцип управления ортогональными сигналами в смежных каналах узлов коммутации и ретрансляции, а также между узлами сети; метод гидроакустической связи. Гидроакустическая связь для приморских районов является потенциалом роста количества одновременно используемых информационных каналов в единице объема взаимодействия морских объектов жизнедеятельности и позволяет связать спутниковые, воздушные, надводные, подводные и донные подсистемы телекоммуникаций. Проведенные исследования показали устойчивость работы предложенных методов в условиях превышения помех над сигналом.

Сведения об авторах:

[1]кандидат технических наук, профессор, профессор Морского государственного университета им. адм. Г.И. Невельского, г. Владивосток, Россия, psn1953@mail.ru

[2]аспирант Морского государственного университета им. адм. Г.И. Невельского, г. Владивосток, Россия, katya.kopaeva.97@mail.ru

[3]аспирант Морского государственного университета им. адм. Г.И. Невельского, г. Владивосток, Россия, kolesov_jr@mail.ru

[4]кандидат технических наук, доцент,доцент кафедры радиоэлектроники и радиосвязи Морского государственного университета им. адм. Г.И. Невельского, г. Владивосток, Россия, kryuch_101053@mail.com

КЛЮЧЕВЫЕ СЛОВА: *подвижная связь, методы обработки, технологии, интеграция подсистем, сети.*

Для цитирования: Павликов С.Н., Копаева Е.Ю., Колесов Ю.Ю., Крючков А.Н. Технологии развития морских интегрированных систем связи // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 19-25. doi: 10.36724/2409-5419-2022-14-4-19-25

Введение

Развитие морских систем связи определяется конвенционными соглашениями под руководством Международной морской организации (IMO), что обеспечило разработку и внедрение ГМССБ, повысившую безопасность жизнедеятельности на море. Аналогичные задачи для информационного обеспечения воздушного транспорта решаются под руководством ИКАО. Задачи у них общие и назрела необходимость кооперации в разработке интегрированных систем связи. Кроме транспортных систем связи и другие системы строятся по интегрированному сценарию. Сотовая связь использует технологии WI-Hi, LTE, Bluetooth, NFC. Подвижнее системы связи интегрированы с GPS, ГЛОНАСС и др.

Спутниковые системы связи комплексируются из группировок LEO, MEO, GEO др. Система V2X также интегрирована и содержит технологии V2V, V2N, V2P, V2I и др. Инфокоммуникационные компоненты перечисленных систем продолжают совершенствоваться, одни опережают другие, появляются новые технические решения, не включенные международными соглашениями в состав бортового оборудования, но обладающие повышенными качественными параметрами с возможностями модернизации в течение длительного периода.

Рассмотрено одно из возможных направлений развития инфокоммуникационных технологий и систем связи (ИКТСС) с интеграцией последних достижений в области мобильных (подвижных) систем связи в интересах более широкого круга потребителей, что позволит одинаковые проблемы решать сообща.

Перспективным направлением является интеграция в дополнении к существующим методам разделения каналов способов множественного доступа по физическим каналам различных физических сред. Это позволяет путем распараллеливания потоков повысить надежность доставки сообщений, увеличить пропускную способность системы. Наряду с понятием интегрированная система связи (ИСС) используются термины гибридная, комплексная. Такие системы представляют собой совокупность подсистем и средств связи. Цифровая ИСС представляет сеть связи с несколькими уровнями, характеризующих наличие в сети связи технического, методологического и организационного единства.

Опыт развития ИКТСС показал, что применение однородных методов не гарантирует её способность удовлетворять растущие требования потребителей ИКТСС.

1. Анализ физических каналов потенциально использование, которых позволит расширить спектр функциональных задач ИСС

Известны следующие потенциальные направления по увеличению эффективности ИКТСС, это увеличение ортогональных сочетаний сигналов и физических каналов, а также их комплексное использование.

Перспективы развития ИКТСС освещены в работах [1-4].

Наибольшее развитие получили технологии мобильной связи [5,6]. Модели сигналов, каналов, систем рассмотрены в [2, 7].

Перспективы развития до 2030 [3,8] включают следующие направления:

– уменьшение времени реакции сети [9];

– увеличение связанности электронных узлов и абонентов [10];

– многоуровневая архитектура сети [11];

– интеграция существующих сетей в единое информационное пространство, охватывающее несколько регионов, например в Арктике [12];

– алгоритмы построения одномерных и многомерных маршрутов [5, 13, 14].

– мониторинг среды и параметров каналов, адаптация сигналов, маршрутов, стандартов [15];

– интеллектуализация в распределенных динамически меняющейся архитектуре сети и трасс доставки сообщений [16-19];

– методы моделирования и применение свойства само подобия [20, 21];

– самоу равление сети, гармонизация потоков [13, 22-24].

Приведенные технологии позволяют решить поставленную проблему по построению ИСС.

2. Требования и состав ИКТСС

В статье [1] отражены основные тенденции, совпадающие с данными других авторов [13, 25], в которых предприняты попытки прогнозирования развития качественных параметров ИКТСС, основные из которых:

– сокращение реакции и времени доставки сообщения – до 0,1 мс;

– снижение требуемого отношение сигнал/помеха до 0,6;

– увеличение мобильности абонентов относительно друг друга до предельных скоростей в физических каналах;

– увеличение количества одновременно работающих в заданном объеме пространства абонентов на несколько порядков;

– увеличение количества методов разделения каналов в два раза.

Ориентируясь на возросшие требования, необходимо поновому строить структуру, состав и связи в ИСС.

Связь объектов через различные физические каналы приведена в таблице 1.

Примеры таких технических решений известны с использованием опускаемых, поднимаемых, буксируемых, синтезированных и др. антенн [12].

В случае совмещения физических каналов в узлах ретрансляции информационная связанность объектов возрастает, а вместе с ней повышается надежность, устойчивость, скрытность, пропускная способность, достоверность доставки пакетов и сообщений при заданных условиях.

В районах, где имеются проблемы в обеспечении связи, например, в Арктической зоне создаются ведомственные различные, слабо согласованные с другими сети связи.

Построение ИСС уровня IP на базе ВОЛС, спутниковых, радиорелейных и тропосферных линий связи, сложная задача. Технологии различаются свойствами, параметрами и ресурсами.

Таблица 1

Связь объектов через различные физические каналы

№ п/п	Каналы	Связь между объектами
1	2	3
1	Электромагнитные	Спутник – спутник
2		Спутник – суда морские, речные, платформы
3		Спутник – воздушные суда
4		Наземные абоненты (далее земля) - земля
5		Земля – суда морские, речные, платформы
6		Земля – воздушные суда
7		Суда морские, речные, платформы – суда морские, речные, платформы
8		Суда морские, речные, платформы – воздушные суда
9	Гидроакустические	Подводные – подводные
10		Подводные – суда морские, речные, подводные и платформы
11		Суда морские, речные, подводные и платформы – суда морские, речные, подводные и платформы
12	Оптоволоконные	Земля – земля
13		Подводные - подводные
14	Электрические	Земля – земля
15		Внутри объектов
16	Лазерные	Спутник – спутник
		Суда – суда

Для осуществления связи суда оснащены гидроакустическими станциями (ГАС), опускаемыми с борта в воду на кабель-тросе с помощью лебедки до нужной глубины.

Анализ показал, что ни одна из рассмотренных систем не позволяет удовлетворить прогнозируемый рост потребностей ИСС в районах с недостаточно развитой инфраструктурой. Предлагается для достижения поставленной цели обеспечить в системе полную информационную связанность элементов. Учитывая тот факт, что большую часть планеты занимают моря и океаны, предлагается включить в состав ИСС гидроакустические каналы.

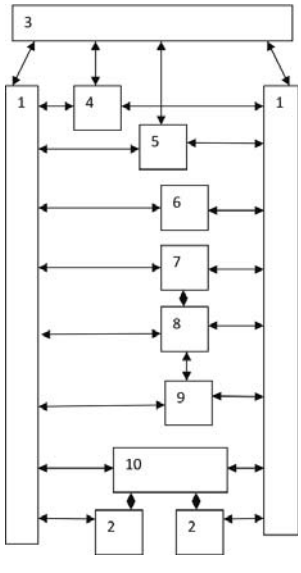

Рис. 1.

Расширенный состав функций и каналов, работающих в различных средах, через различные ретрансляторы, позволяет, контролируя работоспособность последних и осуществить автоматическую коммутацию сигналов, пакетов и каналов. Решение по трассам доставки осуществляется в соответствии с заданными критериями.

Предлагается в состав интегрированной морской интеллектуальной системы связи (ИМИСС) включить следующие подсистемы (см. рис. 1).

На рисунке 1 обозначены:

1. Объекты (судна, нефтегазовой платформы).

2. Источники и потребители информации.

3. Подсистема спутниковой связи (СС), в состав которой входят орбитальный комплекс 3.1 и комплекс СС объектов 3.2. Первый из которых содержит: несколько групп спутников на разных орбитах различных стандартов связи, соединенных радиоканалами с комплексами 3.2 спутниковой связи объектов, а также навигационное оборудование [25, 26].

В состав каждого спутника входят: многоканальный блок радиоприема/передачи, соединенный с блоком наблюдения, диспетчирования и организации каналов связи, подключенного к блоку потребителей, а также связанного через блок сопряжения со спутниками одного стандарта (орбиты) с первым разъемом блока лазерных приема/передатчиков, второй разъем последнего соединен через блок сопряжения со спутниками различных стандартов, а также с блоком наблюдения, диспетчирования и организации каналов связи.

Второй комплекс подсистемы СС на объектах содержит последовательно включенные многоканальный блок радиоприема/передачи, устройство организации каналов связи объектов, узел межсетевого сопряжения, коммутируемую телефонную сеть общего пользования объекта, а также терминалы абонентов связи, выполненные с возможностью работы с различными стандартами, соединенные каналами с блоком радиоприема/передачи и проводными каналами с центром наблюдения, диспетчирования и организации маршрутизации пакетов каналов связи.

4. Подсистема радиосвязи различных стандартов и методов (КВ, СВ, УКВ и др.), включающая пользовательские терминалы связи, соединенные радиоканалами с аналогичными пользовательскими терминалами других объектов, а также связанные радиоканалами с блоками наблюдения, диспетчирования и организации каналов связи, подключенных через центр коммутации обслуживания и узел межсетевого сопряжения с сетью общего пользования.

5. Подсистема мобильной сотовой связи, состоящая из нескольких блоков наблюдения, диспетчирования и организации маршрутизации пакетов каналов сотовой связи на каждом объекте, соединенных радиоканалами с несколькими пользовательскими терминалами связи и связанные друг с другом через центр коммутации мобильного обслуживания по оптическим каналам, при этом центр коммутации мобильного обслуживания соединен через узел сопряжения мобильной сотовой связи с телефонной сетью общего пользования.

6. Подсистему лазерной связи различных стандартов, состоящую аналогично подсистеме 5.

7. Подсистема гидроакустической связи различных стандартов, включающую гидроакустические станции (ГАС) нескольких абонентов связи с соответствующими стандартами подключенных внутри объектов носителей ГАС к последовательно соединенным блоку наблюдения, диспетчирования и организации маршрутизации пакетов каналов связи, центр коммутации гидроакустического обслуживания и узел сопряжения с сетью общего пользования объекта их носителя (судна, нефтегазовой платформы).

При этом ГАС связи нескольких абонентов связи с соответствующими стандартами соединены гидроакустическими каналами с другими аналогичными ГАС, установленными на других объектах;

8. ГАС, установленными в тоще воды или у дна (ДГАС) в точках с известными координатами и связанных гидроакустическими каналами друг с другом и с ГАС других объектов и образующими сеть донных ГАС, при этом каждая ДГАС соединена через последовательно включенные блок наблюдения, диспетчирования и организации маршрутизации пакетов каналов связи, центр коммутации гидроакустического обслуживания, узел сопряжения с оптоволоконной сетью и оптоволоконные кабели с соседними ДГАС, образующих сеть ДГАС, часть из которых (крайних ДГАС); соединены оптоволоконным кабелем 9 с установленной на береговом объекте ГАС связи различных стандартов, которая состоит из ДГАС, которая в отличие от других ДГАС содержит гидроакустическую станцию, соединенную через последовательно включенные блок наблюдения, диспетчирования и организации маршрутизации пакетов каналов связи как с узлом сопряжения с оптоволоконной сетью, так и с узлом межсетевого сопряжения, подключенным через телефонную сеть общего пользования;

9. Оптоволоконный кабель.

10. Телефонная сети общего пользования берегового объекта подключена к подсистемам: гидроакустической, спутниковой, мобильной сотовой, радиосвязи и лазерной связи.

Управление потоками осуществляется в соответствии с заданными требованиями по качеству предоставляемой услуги и условиям: по уровню шума, динамике передаточной характеристики канала, мобильности абонентов, координатам, которые известны друг другу и дисперсии среды.

В таблице 2 приведены варианты связи одного судна с другим через элементы системы.

Повышение связанности подсистем позволяет повысить надежность и качество предоставляемых услуг за счет распараллеливания и дублирования, а также резервирования.

3. Технологии развития морских интегрированных систем связи

Выбор формы сигналов носителей информации и методов обработки. Определение параметров для получения ортогональных сигналов стандартными методами для различных элементов ИСС. Имитационное моделирование способа разделения каналов при уровне отношения сигнал/помеха 0,6 коэффициент автокорреляционной функции получен не хуже 10^4 в зависимости от физического канала и скоростей относительного перемещения абонентов [27].

Таблица 2

Варианты связи одного судна с другим через элементы системы

№ варианта	Каналы	Трассы
1	Радиоканал	Судно – судно
		Судно – береговой узел –судном
2	Спутниковые радиоканалы	Судно – спутник – судно
		Судно – спутник – береговой узел – судном
3	Гидроакустические	Судно – судно
4		Судно – донный узел – судно
5	Комбинированные	Судно – донный узел – оптоволоконный кабель – береговой узел – по радиоканалу с судном
6		Судно – донный узел – оптоволоконный кабель – береговой узел – по радиоканалу через спутник с судном
7		Судно – береговой узел – по радиоканалу с судном
8		Судно – донный узел – оптоволоконный кабель – донный узел – судно

1. Выбор протоколов обмена в многомерной пространстве признаков с адаптацией маршрутов для обхода вышедших из строй элементов или не удовлетворяющих требованиям, за базовую технологи. предлагается взять семейство протоколов STP, RSTP, LACP.
2. Выбор за базовый элемент ячеистую архитектуру структуры системы, при этом каждый уровень состоит из слоев, например LEO, MEO, GEO, построенных по принципу перекрытия малых, средних и больших ячеек, а связь между орбитальными группировками по принципу радиальной, сотовой или гибридной архитектуры;
3. Методы адаптации системы к меняющимся условиям, например измерение и учет передаточной характеристики канала, реализуемый в реальном масштабе времени;
4. Метод гидроакустической связи с адаптацией к условиям среды [26, 28];
5. Расширение сопряженных физических каналов позволяет повысить пропускную способность системы при реализации принципа UTMH [25] путем минимальной задержки начала ретрансляции от момента приема символа за счет ортогональности сигналов на входе и выходе в том числе используемых в различных физических каналах и средах.

Заключение

Разработан комплекс технологий для развития морских интегрированных систем связи. Предложена избыточная структура системы на основе гибридной, слоистой ячеистой топологии.

Выбрана базовая форма несущего сигнала с управляемыми параметрами в зависимости от физического канала, функционально устойчивая к уровню помех, не стационарности канала и мобильности абонентов.

Анализ состояния каналов системы позволяет управлять ортогональными сигналами каналов из расширенного алфа-

вита для смежных линий связи, узлов коммутации и ретрансляции.

Увеличено количество методов разделения сигналов за счет интеграции радио и гидроакустических каналов.

Литература

1. *Ал-Али Хайдер Тахсин Али, Аль-Фархан Гхассан Хассан Али, Бурнашев И.Я., Звездина М.Ю., Назарова О.Ю., Прыгунов А.Г., Русанов Р.И., Шокова Ю.А*. Современное развитие телекоммуникационных систем и компьютерных сетей : монография. Эл. изд. Нижний Новгород: НОО "Профессиональная наука", 2018. Режим доступа: http://scipro.ru/conf/monographtelecommunicationsystems.pdf.

2. *Aloi G., Caliciuri G., Fortino G., Gravina R., Pace P., Russo W., Savaglio C.* Enabling IoT interoperability through opportunistic smartphone-based mobile gateways // Journal of Network and Computer Applications. 2017. Vol. 81, pp. 74-84.

3. *Ateya A., Muthanna A., Koucheryavy A.* 5G framework based on multi-level edge computing with D2D enabled communication // In Advanced 128 Communication Technology (ICACT), 2018 20th International Conference on, IEEE, pp. 507-512, Feb. 2018.

4. *Волков А. Н., Мутханна А. С. А., Кучерявый А. Е.* Сети связи пятого поколения: на пути к сетям 2030 // Информационные технологии и телекоммуникации. 2020. Том 8. № 2. С. 32-43.

5. *Атея А.А., Мутханна А.С., Кучерявый А.Е.* Интеллектуальное ядро для сетей связи 5G и тактильного интернета на базе программно-конфигурируемых сетей // Электросвязь. 2019. № 3. С. 34-40.

6. Ateya A., Al-Bahri M.; Muthanna A., Koucheryavy A. End-to-end system structure for latency sensitive applications of 5G // Электросвязь, (6), pp. 56-61, 2018.

7. *Макаренко С. И., Олейников А. Я, Черницкая Т. Е.* Модели интероперабельности информационных систем // Системы управления, связи и безопасности. 2019. № 4. С. 215-245. DOI: 10.24411/2410-9916- 2019-10408.

8. *Мутханна А.С.* Интеллектуальная распределенная архитектура сети связи для поддержки беспилотных автомобилей // Электросвязь. 2020. № 7. С. 29-34.

9. *Волков А. Н., Кучерявый А. Е.* Идентификация трафика сервисов в сетях связи IMT-2020 и последующего поколения на основе метаданных потоков и алгоритмов машинного обучения // Электросвязь. 2020. № 11. С. 21-28.

10. *Кучерявый А. Е.* Сети связи с ультрамалыми задержками // Труды НИИР. 2019. № 1. С. 69-74.

11. *Нуриллоев И. Н., Парамонов А. И., Кучерявый А. Е.* Метод оценки и обеспечения связности беспроводной сенсорной сети // Электросвязь. 2017. № 7. С. 39-44.

12. Селезнёв С. П., Яковлев В. В. Интегрированная сеть связи в Арктической зоне России // International Journal of Open Information Technologies, vol. 7, no.4, 2019. С. 30-35. ISSN: 2307-8162

13. Степутин А. Н., Николаев А. Д. Мобильная связь на пути к 6G. Вологда: Инфра-инженерия, 2018. Т. 2. 420 с.

14. *Chen Y., Wang J., Feng J.* Understanding the Fractal Dimensions of Urban Forms through Spatial Entropy. Entropy 2017 // MDPI and ACS Style, 19, 600. https://doi.org/10.3390/e19110600.

15. Zhou H., Yu Q., Shen (Sherman) X. et al. Dynamic sharing of wireless Spectrum. Springer International Publishing AG, 2017. 113 p.

16. *Volkov A., Ateya A. A., Muthanna A., Koucheryavy A.* A novel AI-based scheme for traffic detection and recognition in 5G based networks // In Internet of Things, Smart Spaces, and Next Generation Networks and Systems. 2019, pp. 243-255.

17. *Volkov A., Proshutinskiy K., Adam A.B. et al.* SDN Load Prediction Algorithm Based on Artificial Intelligence // In Communications in Computer and Information Science. Springer. 2019. Vol. 1141, pp. 27-28. https://doi.org/10.1007/978-3-030-36 625-4.

18. *Kovalenko V., Alzaghir, A. Volkov et al.* Clustering algorithms for UAV placement in 5G and Beyond Networks // 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2020, pp. 301-307.

19. *Ateya A. A., Muthanna A., Koucheryavy A.* 5G framework based on multi-level edge computing with D2D enabled communication // In 20th international conference on advanced communication technology (ICACT). 2018, pp. 507-512.

20. *Andreev S., Gerasimenko M., Galinina O. et al.* Intelligent Access Network Selection in Converged MultiRadio Heterogeneous Networks // IEEE Wireless Communications, 2017. Vol. 21, no. 6, pp. 86-96.

21. *Бородин А.С., Кучерявый А.Е., Парамонов А.И.* Особенности использования D2D-технологий в зависимости от плотности пользователей и устройств // Электросвязь. 2018. № 10. С. 40-45.

22. *Borodin A., Yastrebova A., Kirichek R., Koucheryavy Y., Koucheryavy A.* Future Networks 2030: Architecture & Requirements // 10th International Congress ICUMT, 2018.

23. Kekal K.G., Kebkal V.K., Kebkal A.G. and PetrocciaR. Experimental Estimation of Delivery Success of Navigation Data Packages transmitted via Digital Hydroacoustic Communication Channel // GYROSCOPY AND NAVIGATION. 2016. Vol. 7. No 4, pp. 343-352.

24. *Lmai S., Chitre M., Laot C., Houcke S.* Throughput-efficient super-TDMA MAC transmission schedules in ad hoc linear underwater acoustic networks, IEEE Journal of Oceanic Engineering, 2017, vol. 42, pp. 156-174.

25. Пат. РФ 2600104, Система и способ осуществления связи с высокой пропускной способностью в сети с гибридной ячеистой топологией/ Хемли Ромел, Аппельбаум Офир (IL). Заявл. 11.01.2012 Опубл. 20.02.2015. Бюл. №29.

26. *Morozs N., Mitchell P.D., Zakharov Y.* TDA-MAC: TDMA Without Clock Synchronization in Underwater Acoustic Networks, IEEE Access., 2018, vol. 6, pp. 1091-1108.

27. *Павликов С.Н., Убанкин Е.И.* Прямое аналоговое мультиплексирование по форме сигналов // Ракетно-космическое приборостроение, информационные системы. 2020. Т.7. Вып. 3. С. 4-12.

28. *Павликов С.Н., Копаева Е.Ю., Колесов Ю.Ю., Крючков А.Н.* Метод гидроакустической связи, Морские интеллектуальные технологии. 2022. Т. 1. № 1. С. 208-214.

TECHNOLOGIES FOR THE DEVELOPMENT OF MARINE INTEGRATED COMMUNICATION SYSTEMS

SERGEY N. PAVLIKOV
Vladivostok, Russia, psn1953@mail.ru

EKATERINA YU. KOPAEVA
Vladivostok, Russia, lerospongebob@mail.ru

YURIY YU. KOLESOV
Vladivostok, Russia, kolesov_jr@mail.ru

ANDREY N. KRYUCHKOV
Vladivostok, Russia, kryuch_101053@mail.ru

KEYWORDS: *mobile communication, processing methods, technologies, integration of subsystems, networks.*

ABSTRACT

The goal is to improve the quality of information interaction of objects by increasing the reliability of message delivery to recipients and bandwidth through the integration of networks using various signals and physical channels. A search for new technical solutions for the creation of integrated (hybrid) communication technologies aimed at expanding the possibilities for creating adaptive, self-organizing, resistant to destabilizing factors communication systems with an increased quality of services provided in vast areas was carried out. The method of solving the tasks is based on the analysis of development trends and forecasting the requirements for integrated mobile communication systems. The novelty lies in the development and evaluation of options for building the structures of integrated communication systems, represented by diverse, complementary subsystems using various methods of channel separation, including in physical environments, as well as algorithms for their operation. Key findings. A set of technologies for the development of coastal integrated communication systems has been developed: the structure of the system based on a hybrid mesh topology; the basic form of the carrier signal with controlled parameters depending on the physical channel; the principle of control of orthogonal signals in adjacent channels of switching and relay nodes, as well as between network nodes; hydroacoustic communication method. Hydroacoustic communication for coastal areas is a potential for increasing the number of simultaneously used information channels per unit of the volume of interaction of vital objects and makes it possible to connect satellite, air, surface, underwater and bottom subsystems of telecommunications. The conducted studies have shown the stability of the proposed methods in conditions of excess of interference over the signal.

REFERENCES

1. Al-Ali Haider Tahsin Ali, Al-Farhan Ghassan Hassan Ali, Burnashev I.Ya., Zvezdina M.Yu., Nazarova O.Yu., Prygunov A.G., Rusanov R.I., Shokova Yu.A. Modern development of telecommunication systems and computer networks. Nizhny Novgorod: NOO "Professional Science", 2018. Access mode: http://scipro.ru/conf/monographtelecommunicationsystems.pdf. (In Rus.)

2. Aloi G., Caliciuri G., Fortino G., Gravina R., Pace P., Russo W., Savaglio C. Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. *Journal of Network and Computer Applications*. 2017. Vol. 81, pp. 74-84.

3. Ateya A., Muthanna A., Koucheryavy A. 5G framework based on multi-level edge computing with D2D enabled communication. *Advanced 128 Communication Technology (ICACT), 2018 20th International Conference on, IEEE*, pp. 507-512, Feb. 2018.

4. Volkov A. N., Mutkhanna A. S. A., Kucheryavy A. E. Networks of communication of the fifth generation: on the way to networks 2030. *Information technologies and telecommunications*. 2020. Vol. 8. No. 2, pp. 32-43. (In Rus.)

5. Ateya A.A., Mutkhanna A.S., Kucheryavy A.E. Intellectual core for 5G communication networks and tactile Internet on the basis of software-configurable networks. *Electrosvyaz*. 2019. № 3, pp. 34-40. (In Rus.)

6. Ateya A., Al-Bahri M., Muthanna A., Koucheryavy A. End-to-end system structure for latency sensitive applications of 5G. *Telecommunications*. No. 6, pp. 56-61, 2018.

7. Makarenko S. I., Oleynikov A. Ya, Chernitskaya T. E. Models of interoperability of information systems. *Systems of management, communications and security*. 2019. No. 4, pp. 215-245. DOI: 10.24411/2410-9916- 2019-10408. (in Rus.)

8. Muthanna A.S. Intelligent distributed architecture of the communication network to support unmanned vehicles. *Electrosvyaz*. 2020. No. 7, pp. 29-34. (in Rus.)

9. Volkov A.N., Kucheryavy A.E. Identification of service traffic in communication networks IMT-2020 and the next generation based on metadata of streams and algorithms of machine learning. *Electrosvyaz*. 2020. No. 11, pp. 21-28. (In Rus.)

10. Kucheryavy A.E. Networks of communication with ultramal delays. *Trudy NIIR*. 2019. No. 1, pp. 69-74. (In Rus.)

11 Nurilloev I.N., Paramonov A.I., Kucheryavy A.E. Method of assessment and provision of connectivity of wireless sensor network. *Telecommunication*. 2017. No. 7, pp. 39-44.

12. Seleznyov S.P., Yakovlev V.V. *International Journal of Open Information Technologies.* ISSN: 2307-8162, vol. 7, no.4, 2019, pp. 30-35. (In Rus.)

13. Steputin A.N., Nikolaev A.D. Mobile communication on the way to 6G. Vologda: Infra-engineering, 2018. Vol 2. 420 p. (In Rus)

14. Chen Y., Wang J., Feng J. Understanding the Fractal Dimensions of Urban Forms through Spatial Entropy. Entropy 2017. *MDPI and ACS Style*, 19, 600. https://doi.org/10.3390/e19110600.

15. Zhou H., Yu Q., Shen (Sherman) X. et al. Dynamic sharing of wireless Spectrum. Springer International Publishing AG, 2017. 113 p.

16. Volkov A., Ateya A.A., Muthanna A., Koucheryavy A. A novel AI-based scheme for traffic detection and recognition in 5G based networks. *In Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. 2019, pp. 243-255.

17. Volkov A., Proshutinskiy K., Adam A.B. et al. SDN Load Prediction Algorithm Based on Artificial Intelligence. *In Communications in Computer and Information Science*. Springer. 2019. Vol. 1141, pp. 27-28. https://doi.org/10.1007/978-3-030-36-625-4.

18. Kovalenko V., Alzaghir A. Volkov et al. Clustering algorithms for UAV placement in 5G and Beyond Networks. *12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*. 2020, pp. 301-307.

19. Ateya A.A., MuthannaA., Koucheryavy A. 5G framework based on multi-level edge computing with D2D enabled communication. *20th international conference on advanced communication technology (ICACT)*. 2018, pp. 507-512.

20. Andreev S., Gerasimenko M., Galinina O. et al. Intelligent Access Network Selection in Converged MultiRadio Heterogeneous Networks. *IEEE Wireless Communications*, 2017. Vol. 21, no. 6, pp. 86-96.

21. Borodin A.S., Kucheryavy A.E., Paramonov A.I. Features of the use of D2D-technologies depending on the density of users and devices. *Electrosvyaz*. 2018. No. 10, pp. 40-45. (In Rus.)

22. Borodin A., Yastrebova A., Kirichek R., Koucheryavy Y., Koucheryavy A. Future Networks 2030: Architecture & Requirements. *10th International Congress ICUMT*, 2018.

23. Kekal K.G.,Kebkal V.K., Kebkal A.G., Petroccia R. Experimental Estimation of Delivery Success of Navigation Data Packages transmitted via Digital Hydroacoustic Communication Channel. *Gyroscopy and navigation*. 2016. Vol. 7. No. 4, pp. 343-352.

24. Lmai, S., Chitre, M., Laot, C., Houcke, S., Throughput-efficient super-TDMA MAC transmission schedules in ad hoc linear underwater acoustic networks. *IEEE Journal of Oceanic Engineering*, 2017, vol. 42, pp. 156-174.

25. Patent RF 2600104, System and method of high-bandwidth communication in a network with a hybrid mesh topology / Hemley Romel, Appelbaum Ofir (IL), Said. 11.01.2012 Publ. 20.02.2015. No.29. (in Rus.).

26. Morozs N., Mitchell P.D., Zakharov Y. TDA-MAC: TDMA Without Clock Synchronization in Underwater Acoustic Networks, *IEEE Access*. 2018, vol. 6, pp. 1091-1108.

27. Pavlikov S.N., Ubankin E.I. Direct analog multiplexing by the form of signals. *Rocket and space instrumentation, information systems.* 2020. Vol.7. Vol.3, pp. 4-12. (in Rus.)

28. Pavlikov S.N., Kopaeva E.Yu., Kolesov Yu.Yu., Kryuchkov A.N. Method of hydroacoustic communication, Marine intelligent technologies. 2022. Vol. 1. No. 1, pp. 208-214. (in Rus.)

INFORMATION ABOUT AUTHORS:

Sergey N. Pavlikov, PhD, Full Professor, Professor Maritime State University, named after adm. G.I. Nevelskogy, Vladivostok, Russia
Ekaterina Yu. Kopaeva, postgraduate student, Maritime State University, named after adm. G.I. Nevelskogy, Vladivostok, Russia
Yuriy Yu. Kolesov, postgraduate student Maritime State University, named after adm. G.I. Nevelskogy, Vladivostok, Russia
Andrey N. Kryuchkov, PhD, Docent, Assistant professor, Maritime State University, named after adm. G.I. Nevelskogy, Vladivostok, Russia

For citation: Pavlikov S.N., Kopaeva E.Yu., Kolesov Yu.Yu., Kryuchkov A.N. Technologies for the development of marine integrated communication systems. H&ES Reserch. 2022. Vol. 14. No 4. P. 19-25. doi: 10.36724/2409-5419-2022-14-4-19-25 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-26-32

СТАБИЛИЗАЦИЯ ЧАСТОТЫ НА ОСНОВЕ ПЕРВИЧНО-ФУНДАМЕНТАЛЬНЫХ СВОЙСТВ БОЛЬШИХ СИСТЕМ

САФАРЬЯН
Ольга Александровна[1]

АЛФЕРОВА
Ирина Александровна[2]

ЕНГИБАРЯН
Ирина Алешаевна[3]

ЮХНОВ
Василий Иванович[4]

Сведения об авторах:

[1] к.т.н, доцент, доцент кафедры "Кибербезопасность информационных систем", Донской Государственный Технический университет, Ростов-на-Дону, Россия, safari_2006@mail.ru

[2]старший преподаватель кафедры "Кибербезопасность информационных систем", Донской Государственный Техниче-ский университет, Ростов-на-Дону, Россия, ia.alferova.donstu@yandex.ru

[3]к.т.н, доцент кафедры "Инфокоммуникационных технологий и систем связи", Северо-Кавказский филиал ордена Трудо-вого Красного Знамени ФГБОУ ВО "Московский технический университет связи и информатики", г. Ростов-на-Дону, Россия, eirina@live.ru

[4]к.т.н, доцент, заведующий кафедрой "Инфокоммуникационные технологии и системы связи", Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО "Московский технический университет связи и информатики", г. Ростов-на-Дону, Россия, juchnov@mail.ru

АННОТАЦИЯ

Введение. Тенденции современного этапа развития технических систем в различных отраслях характеризуются требованиями постоянного повышения точности получаемых данных, увеличения объема передаваемой информации. Повышение разрешения получаемых изображений при мониторинге и соответствующее увеличение объема получаемой информации требует высоких скоростей передачи данных с борта аппарата на наземные станции. В настоящее время требуемая стабильность частоты в радиотехнических системах достигается при использовании методов фазовой автоподстройки частоты (ФАПЧ) с высокостабильными генераторами радиосигналов. **Цель.** В статье рассматриваются вопросы, связанные с проявлением первично-фундаментальных свойств больших систем, таких как синергичность и эмерджентность, потенциально присущих большим системам с одинаковыми или близкими по свойствам составными частями. Данные свойства могут быть реализованы на некотором временном интервале при измерении значений фаз сигнала единовременно. Показано, что проявление свойства синергичности в системе одновременно и независимо работающих генераторов позволяет уменьшить погрешность оценки случайных флуктуаций частоты генераторов, а проявление свойства эмерджентности – исключить постоянное смещение частоты от номинального значения. **Результаты исследования.** На основе проведенного анализа свойств получаемых оценок сформулированы условия получения несмещенных эффективных оценок частоты каждого из генераторов. Показано проявление свойств синергичности и эмерджентсности в системе одновременно и независимо функционирующих генераторов. Отмечено, что с физической точки зрения повышение точности оценивания частоты сигналов соответствует многократным неравноточным косвенным измерениям. Показаны смоделированные отклонения частоты каждого из генераторов и разность между значениями отклонения частоты и соответствующими значениями полученных оценок. Приведены результаты математического моделирования, подтверждающие правильность полученных теоретических результатов и основные отмеченные закономерности.

КЛЮЧЕВЫЕ СЛОВА: *система одновременно и независимо работающих генераторов, синергичность, эмерджентность, гармонический сигнал, фаза сигнала, стабильность частоты, оценка частоты, несмещенность и эффективность оценок.*

Для цитирования: Сафарьян О.А., Алферова И.А., Енгибарян И.А., Юхнов В.И. Стабилизация частоты на основе первично-фундаментальных свойств больших систем // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 26-32. doi: 10.36724/2409-5419-2022-14-4-26-32

Тенденции современного этапа развития технических систем в различных отраслях характеризуются требованиями постоянного повышения точности получаемых данных, увеличения объема передаваемой информации. В качестве примера можно привести радиотехнические системы сотовой связи, дистанционного зондирования поверхности Земли, осуществляемого с помощью космических и летательных аппаратов в радиодиапазоне длин волн, получение геоинформационных данных о состоянии крупных объектов (мосты, плотины и т.д.) и ряд других направлений научной и практической деятельности [1-3].

Повышение разрешения получаемых изображений при мониторинге и соответствующее увеличение объема получаемой информации требует высоких скоростей передачи данных с борта аппарата на наземные станции. Для реализации указанных возможностей широкое применение находят сложные сигналы, эффективное применение которых связано с требованием высокой стабильности частоты, как правило, с относительной нестабильностью 10^{-8} – 10^{-9} и выше [3, 4].

В настоящее время требуемая стабильность частоты в радиотехнических системах достигается при использовании методов фазовой автоподстройки частоты (ФАПЧ) с высокостабильными генераторами радиосигналов. Система ФАПЧ позволяет обеспечить высокую стабильность частоты сигналов. Однако эксплуатация таких генераторов представляет собой сложную техническую задачу по обеспечению заданных требований стабильности температурно-влажностного режима, напряжения питания, малых уровней вибрации и т.д. Кроме того, система ФАПЧ имеет ограниченное быстродействие и полосу захвата для последующей стабилизации частоты сигнала. Несмотря на большое число работ, посвященных вопросам стабилизации частоты генераторов с использованием системы ФАПЧ, большое число вопросов не нашло своего разрешения [4-21].

Однако для ряда радиотехнических систем с большим числом одновременно и независимо работающих генераторов, которые могут быть отнесены к большим системам, повышение стабильности частоты возможно при использовании свойств синергичности и эмерджентности, являющихся первично-фундаментальными свойствами большой системы и потенциально присущих любой системе близких по назначению элементов [22-25].

Целью доклада является анализ предпосылок, обусловленных свойствами синергичности и эмерджентности системы одновременно и независимо работающих генераторов, и теоретические основы их реализации для повышения частоты формируемых этими генераторами сигналов.

Рассмотрим систему N одновременно и независимо формирующих гармонические сигналы генераторов. Формируемые генераторами сигналы поступают или могут быть поданы на общее устройство, в котором происходит измерение их фаз и совместная оценка параметров частоты каждого генератора. Известными являются предполагаемые значения частоты и относительной нестабильности сигнала, формируемого каждым генератором. На основе полученных оценок параметров частоты сигналов может проводиться коррекция параметров генераторов, используемых при формировании, модуляции и демодуляции сигналов в системе.

Обобщенное представление структурной схемы системы, позволяющее рассмотреть предпосылки и теоретические основы анализируемого метода стабилизации частоты, приведено на рисунке 1.

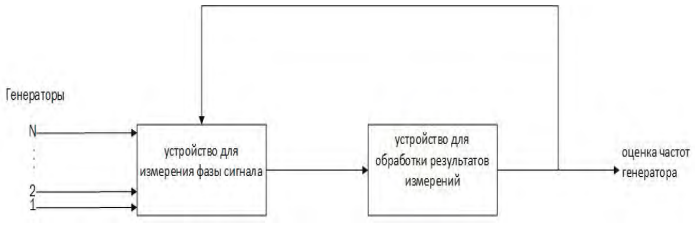

Рис. 1. Структурная схема системы стабилизации частоты N одновременно и независимо формирующих гармонические сигналы генераторов

Физической реализацией служит, как отмечалось выше, совокупность генераторов, формирующих сигналы абонентов в сети связи и устройства базовой станции, используемые для приема, передачи и преобразования сигналов. Указанные сигналы одновременно и независимо поступают на вход устройства, где в течение некоторых интервалов времени t_m (m = 1,…,M) происходит измерение фаз сигналов. Для каждого сигнала предполагаются номинальные значения частоты $\omega_n^{(0)}$ и относительной нестабильности $\sigma_n^{(0)}$ ($n = 1,...,N$)

Кроме того, предполагается номинальная длительность $t_m^{(0)}$ и дисперсия номинальной длительности $\sigma_t^{(0)}$ m-го измерительного интервала. Требуется оценить текущую частоту каждого генератора на каждом измерительном интервале.

Представим текущее значение частоты n-го генератора на m-м измерительном интервале следующим соотношением

$$\omega_{n,m} = \omega_n^{(0)} + \Delta\omega_n + \delta\omega_{n,m} \qquad (1)$$

где $\Delta\omega_n$ - постоянная для всех M измерительных интервалов составляющая отклонения частоты n-го генератора от предполагаемого номинального значения; $\delta\omega_{n,m}$ – случайная, принимающая на каждом из M измерительных интервалов свое значение составляющая отклонения частоты n-го генератора от предполагаемого номинального значения. При этом дополнительно будем считать, что математическое ожидание $\delta\omega_{n,m} = 0$, ($n = 1,...,N$, $m = 1,...,M$).

С учетом соотношения (1) запишем линеаризованное значение фазы сигнала n-го генератора на m-м измерительном интервале в виде

$$\Phi_{n,m} = \Phi_{n,m}^{(0)} + \omega_n^{(0)}\Delta t_m + \Delta\omega_n t_m^{(0)} + \delta\omega_{n,m} t_m^{(0)} \qquad (2)$$

где $\Phi_{n,m}^{(0)} = \omega_n^{(0)} t_m^{(0)}$; Δt_m – отклонение длительности m-го интервала измерений от предполагаемого номинального значения $t_m^{(0)}$, имеющее постоянную и случайную, принимающую на каждом измерительном составляющие.

Составляющие $\Delta\omega_n \cdot \Delta t_m$ и $\delta\omega_{n,m} \cdot \Delta t_m$, имеющие более высокий порядок малости, в соотношение (2) опущены.

Выразим из соотношения (2) значение случайной составляющей отклонения частоты каждого из N генераторов на m-м измерительном интервале следующим образом

$$\delta\omega_{n,m} = \frac{\Phi_{n,m} - \Phi_{n,m}^{(0)} - \omega_n^{(0)}\Delta t_m - \Delta\omega_n t_m^{(0)}}{t_m^{(0)}} \quad (3)$$

Как следует из соотношения (3) в пренебрежении ошибками измерений точность оценивания частоты сигналов генераторов полностью определяется точностью оценок Δt_m смещением оценки и среднеквадратической ошибкой (СКО).

Рассмотрение начнем с частного случая $\Delta\omega_n = 0$, (n = 1,…,N_n). Данное предположение соответствует случаю совпадения на каждом m-м измерительном интервале (m = 1,…,M) средней частоты каждого генератора с соответствующим предполагаемым для него значением частоты.

Для реализации потенциально присущего системе N одновременно и независимо функционирующих генераторов проведем одновременную обработку результатов измеренных значений фаз сигналов генераторов. Выражение (3) показывает, что значения $\delta\omega_{n,m}$ при сделанном предположении $\Delta\omega_n = 0$, (n = 1,…,N) могут быть легко найдены по результатам измерений фаз при известном значении Δt_m.

Для определения Δt_m составим функцию правдоподобия M переменных в следующей форме

$$L(\mathbf{\Delta t}) = \prod_{m=1}^{M}\prod_{n=1}^{N} p(\delta\omega_{n,m}) \quad (4)$$

где $\mathbf{\Delta t} = \{\Delta t_1,\ldots, \Delta t_M\}$. В случае, если значения Δt_M на различных измерительных интервалах являются статистически независимыми, функция правдоподобия (4) распадается на произведение M функций правдоподобия, аргументом каждой из которых является Δt_m

$$L(\mathbf{\Delta t}) = \prod_{m=1}^{M} L^{(m)}(\Delta t_m) \quad (5)$$

$$L^{(m)}(\Delta t_m) = \prod_{n=1}^{N} p(\delta\omega_{n,m}), \quad m = 1,...,M \quad (6)$$

Оценка Δt_m в этом случае определяется из условия

$$L^{(m)}(\Delta t_m) \underset{\Delta t_m}{\rightarrow} \max \quad (7)$$

Оценивание Δt_m в соответствии с (7) сводится к решению уравнения

$$\frac{\partial L^{(m)}(\Delta t_m)}{\partial \Delta t_m} = 0 \quad (8)$$

С физической точки зрения соотношения (5) и (6) означают:

- для оценивания отклонения длительности Δt_m m-го измерительного интервала (m = 1,…,M) достаточно результатов измерений фаз сигналов генераторов, выполненных только на этом измерительном интервале;
- оценивание каждого Δt_m по результатам измерений фаз сигналов N генераторов соответствует N-кратным непрямым измерениям Δt_m на основе результатов прямых измерений $\Phi_{n,m}$ (n = 1,…,N) на m-м измерительном интервале.

В частном, для наиболее широко распространенного на практике случая распределения $\delta\omega_{n,m}$ по нормальному закону выражение (6) принимает вид

$$L^{(m)}(\Delta t_m) = (2\pi)^{-1/2}\prod_{n=1}^{N}\left(\sigma_n^{(0)}\right)^{-1}\frac{\left(\Phi_{n,m} - \Phi_{n,m}^{(0)} - \omega_n^{(0)}\Delta t_m\right)^2}{2\left(t_m^{(0)}\sigma_n^{(0)}\right)^2}. \quad (9)$$

С учетом (8) оценка Δt_m, получаемая из (9), определяется зависимостью

$$\Delta\hat{t}_m = \sum_{n=1}^{N}\frac{\left(\Phi_{n,m} - \Phi_{n,m}^{(0)}\right)\cdot\omega_n^{(0)}}{\left(\sigma_n^{(0)}\right)^2}\left(\sum_{n=1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\sigma_n^{(0)}\right)^2}\right)^{-1} \quad (10)$$

Проанализируем основные свойства получаемых оценок Δt_m. Для математического ожидания оценки $\Delta\hat{t}_m$ может быть записано следующее представление

$$M\left\{\Delta\hat{t}_m\right\} = \sum_{n=1}^{N}\frac{\left(M\left\{\Phi_{n,m}\right\} - \Phi_{n,m}^{(0)}\right)\cdot\omega_n^{(0)}}{\left(\ {}^{(0)}_{n}\right)^2}\cdot\left(\sum_{1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\ {}^{(0)}_{n}\right)^2}\right)^{-1} \quad (11)$$

При условии $\Delta\omega_n = 0$ можно с учетом (2) записать

$$M\left\{\Delta\hat{t}_m\right\} = \Delta t_m\cdot\left(\sum_{n=1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\sigma_n^{(0)}\right)^2}\right)\cdot\left(\sum_{n=1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\sigma_n^{(0)}\right)^2}\right)^{-1} = \Delta t_m \quad (12)$$

В соотношении (12) усреднение рассматривается по ансамблю генераторов. Таким образом, независимо от значений рабочей частоты $\omega_n^{(0)}$ и относительной нестабильности $\sigma_n^{(0)}$ всех генераторов (n = 1,…, N) получаемая оценка является несмещенной.

Для доказательства эффективности получаемых оценок рассмотрим соотношение

$$M\left\{\left(\Delta\hat{t}_m\right)^2 - \left(\Delta t_m\right)^2\right\} = M\left\{\left(\Delta\hat{t}_m\right)^2\right\} - \left(\Delta t_m\right)^2 \quad (13)$$

С учетом соотношения (2) и результата (12) можно записать

$$M\left\{\left(\Delta\hat{t}_m\right)^2\right\} = \frac{M\left\{\sum_{n=1}^{N}\sum_{p=1}^{N}\left(\omega_n^{(0)}\omega_p^{(0)}\left(\Delta t_m\right)^2 + \delta\omega_{p,m}t_m^{(0)}\omega_n^{(0)}\Delta t_m + \delta\omega_{n,m}t_m^{(0)}\omega_p^{(0)}\Delta t_m + \delta\omega_{n,m}\delta\omega_{p,m}\left(t_m^{(0)}\right)^2\right)\right\}}{\left(\sum_{n=1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\sigma_n^{(0)}\right)^2}\right)^2} \quad (14)$$

Первое слагаемое из правой части (14) после преобразований вычисляется и равно $(\Delta t_m)^2$. Второе и третье слагаемые равны нулю. После преобразований четвертого слагаемого в (14) с учетом (13) и независимости статистического распределения случайных значений $\delta\omega_{n,m}$ и $\delta\omega_{p,m}$ окончательное выражение для дисперсии оценки $\Delta\hat{t}_m$ приводится к виду

$$M\left\{\left(\Delta\hat{t}_m\right)^2\right\} = M\left\{\sum_{n=1}^{N}\left(\delta\omega_{n,m}\omega_n^{(0)}t_m^{(0)}\right)^2\right\}\left(\sum_{n=1}^{N}\frac{\left(\omega_n^{(0)}\right)^2}{\left(\sigma_n^{(0)}\right)^2}\right)^2 \quad (15)$$

Для совокупности одновременно и независимо работающих генераторов с одинаковыми параметрами ($\omega_n^{(0)} = \omega^{(0)}$, $\sigma_n^{(0)} = \sigma^{(0)}$) из соотношения (12) непосредственно следует

$$M\left\{\Delta\hat{t}_m - \Delta t_m\right\} = 0 \quad (16)$$

$$D\left\{\Delta\hat{t}_m\right\} = \frac{\sigma_t^{(0)}}{\sqrt{N}} \quad (17)$$

где $M\left\{\Delta\hat{t}_m\right\}$ и $D\left\{\Delta\hat{t}_m\right\}$ соответственно математическое ожидание и дисперсия получаемой оценки $\Delta\hat{t}_m$.

С учетом соотношения (3) можно непосредственно показать, что

$$D\left\{\delta\omega_n\right\} = \frac{\omega^{(0)}\cdot\sigma_t^{(0)}}{\sqrt{N}} \quad (18)$$

В более общем случае системы генераторов с различными параметрами (рабочей частотой и относительной нестабильностью) формула (13) приобретает более сложный вид, но, как следует из (10), указанная закономерность сохраняется.

Полученные результаты позволяют сделать следующие выводы:

- совместная обработка измеряемых значений фазы сигналов для системы генераторов позволяет уменьшить дисперсию оценки частоты формируемого сигнала и соответственно путем управления параметрами генератора уменьшить нестабильность частоты формируемого сигнала;
- все генераторы системы независимо от собственных параметров (рабочей частоты и относительной нестабильности) будут характеризоваться одинаковой нестабильностью частоты формируемого сигнала.

Указанные выводы определяют проявление свойства синергичности в системе одновременно и независимо функционирующих генераторов.

Перейдем к рассмотрению более общего случая $\Delta\omega_n \neq 0$. Более общим подходом для определения несмещенного текущего значения $\Delta\hat{t}_m$ будет являться проведение измерений фаз сигналов на нескольких измерительных интервалах ($M > 1$). Последующая оценка значений $\Delta\omega_n$ ($n = 1,\ldots,N$) проводится из обеспечения выполнения следующего условия

$$\sum_{n=1}^{N}\left(\sum_{m=1}^{M}\Delta\hat{t}_m\right)^2 \underset{\Delta\omega}{\rightarrow}\min \quad (19)$$

С физической точки зрения данное условие определяет исключение из оценки $\Delta\hat{t}_m$ составляющей, обусловленной $\Delta\omega_n \neq 0$, и связано с реализацией свойства эмерджентности системы одновременно и независимо работающих генераторов.

С использованием предложенных соотношений проанализированы численные результаты проявления синергичности и эмерджентности в системе одновременно и независимо работающих генераторов. На рисунке 2 для системы из 100 генераторов ($N = 100$) показаны смоделированные отклонения частоты каждого из генераторов (линия точек) и разность между значениями отклонения частоты и соответствующими значениями полученных оценок (штриховая линия). При моделировании частота всех генераторов полагалась равной $\omega_n = 2\pi\cdot10^9\ рад/с$, относительная нестабильность всех генераторов – $\sigma_n^{(0)} = 10^{-7}$.

Как следует из приведенного графика, реализация свойства синергичности в системе генераторов при указанных параметрах позволяет повысить точность получаемых оценок случайной составляющей отклонения частоты в 10 раз.

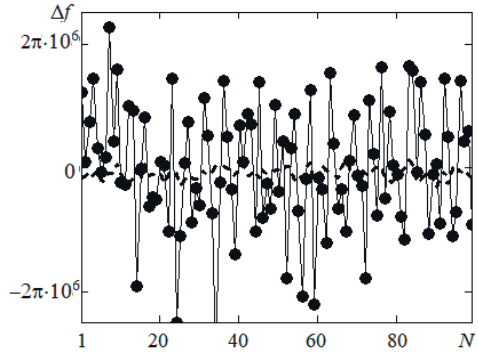

Рис. 2. Колебания частоты сигналов генератора и отклонения полученных оценок в $\Delta\omega_n = 0$

На рисунках 3, 4 представлены результаты исследований, позволяющие проиллюстрировать проявление свойства эмерджентности для рассматриваемой системы генераторов. Линией точек показаны отклонения длительности временного интервала Δt_m от номинального значения $t_m^{(0)} = 10^{-3}\ c$, штриховой линией - оценки отклонения длительности

измерительного интервала $\Delta\hat{t}_m$. Исследования проводились при $\sum_{n=1}^{N}\Delta\omega_n = 2\pi\cdot 10^3\ рад/с$, $t_m^{(0)} = 10^{-3}\ с$.

В частности, на рисунке 3 приведены результаты, полученные при проведении измерений фаз сигналов на десяти измерительных интервалах (M = 10), а на рисунке 4 – при проведении измерений на ста измерительных интервалах (M = 100).

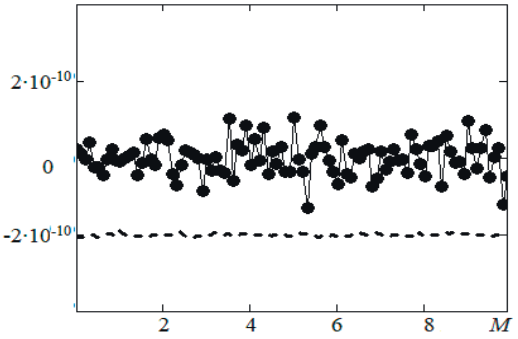

Рис. 3. Колебания частоты сигналов генератора и отклонения полученных оценок в M = 10

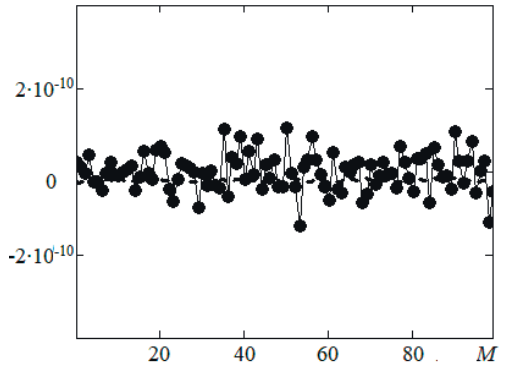

Рис. 4. Колебания частоты сигналов генератора и отклонения полученных оценок в M = 100

Представленные результаты показывают, что проявление свойства эмерджентности, реализуемое путем наложения условия (19), в рассматриваемой системе генераторов связано с увеличением числа измерительных интервалов, позволяющим исключить постоянную составляющую отклонения оценки длительности временного интервала измерений.

Проведенные исследования, что использование свойств синергичности и эмерджентности, потенциально присущих системам с однотипными элементами в системе одновременно и независимо работающих генераторов позволяет повысить точность получаемых оценок частоты формируемых сигналов (уменьшить СКО и возможное смещение оценки частоты). Уменьшение среднеквадратического отклонения частоты сигналов генераторов связано с реализацией свойства синергичности. В случае распределения отклонений частоты сигналов от номинальных значений по нормальному закону повышение точности получаемых оценок частоты сигналов изменяется к закону $N^{-1/2}$.

Свойство эмерджентности проявляется в возможности исключения медленно меняющихся отклонений частоты сигналов при проведении многократных измерений фаз формируемых сигналов на большом числе интервалов измерений. Такие системы генераторов и возможность реализации потенциально присущих таким системам указанных свойств возникает в современных информационно-телекоммуникационных системах. При этом построение систем стабилизации частоты на основе предлагаемого подхода связано с меньшими сложностями, эксплуатации в отличие от системы ФАПЧ.

Литература

1. *Глотов А.Ф.* Интеллектуализация информационных систем: подходы и направления // *Геоматика,* 2015. С. 18-24.
2. *David B.* Lesson. Oscillator Phase Noise: A 50-Year Review // IEEE Transactions on Ultrasonics, Ferroelectrics and Frequencies control. 2016. № 8, pp. 1208-1225.
3. *Demir, A. Mehrotra, J.* Roychowdhure. Phase noise in oscillators: A unifying theory and numerical methods for characterization // IEEE Trans. Circuitts Syst. I. Fundam. Theory Appl., May 2000, vol. 47, no. 5, pp. 655-674.
4. *Zheng T., Chen L., Chen T., Wei S.M.*, Virtual synchronous generator technology and prospects // Autom. Electric Power Syst., 2015, № 39 (21), pp. 165-175.
5. *Shao H., Li P., Fu W.B., Yang G.H.*, Wind-solar grid-connected technology based on virtual synchronous generator control strategy // Electr. Autom., 2018, № 40 (5), pp. 16-18.
6. *Ling Y.L.*, Adaptive control of distributed power inverter based on VSG // Energy Conserv., 2020. № 39 (4), pp. 5-9.
7. *Ren D.J., Wei Y.B., Xi Z.F., Zhang J.*, Control strategy of inverter power sharing based on VSG // Power Electron. Technol., 2020, №54 (2) p. 28–31.
8. *Huo X.X., Wu P., Huang X., Yan J.J., Wang K.Y., Xu K., Yao C., Chen P.Y.*, Microgrid Stability Control Based on Adaptive Parameter Virtual Synchronous Machine// Electric Power Construct., 2019, № 40 (2), pp. 79-86.
9. *Cheng G., Shao X., Wang G.*, Adaptive control strategy for virtual synchronous generator parameters // Renewable Energy, 2021. № 39 (12), pp. 1655-1661.
10. *Lu Z., Sheng W., Zhong Q., Liu H., Zeng Z.*, Virtual synchronous generator and its applications in micro-grid // Proc. CSEE, 2014. № 34 (16), pp. 2591-2603.
11. *Zhao D.M., Zhang N., Liu Y.H., Zhang X.*, Integrated control strategy for smooth switching of microgrid and island operation mode based on energy storage // Power Syst. Technol., 2013. № 37 (2), pp. 301-306.
12. *Li P., Zhang X.S., Zhao B., Wang Z.L., Sun J.R.*, Microgrid design and mode switching control strategy of multi-microgrid and multigrid point structure // Autom. Electric Power Syst. 2015. № 39 (9), pp. 172-178.
13. *Wang J.S., Tang C.H., Chen N., Tan K., Mao J.X.*, A microgrid on-off and off-grid smooth switching control strategy based on self-recognition of operating mode // Autom. Electric Power Syst., 2015. № 39 (9), pp. 185-191.
14. *Yang Y.C., Zhou Z.G.*, Distributed power grid-connected inverter seamless switching control strategy // J. Electric Power Syst. Autom. 2016. № 28 (8), pp. 91-97.
15. *Shi R.L., Zhang X., Xu H.Z., Liu F., Hu C., Yu Y.*, Seamless switching control strategy of microgrid operation mode based on virtual synchronous generator // Autom. Electric Power Syst. 2016. №40 (10), pp. 16-23.

16. *Wang C.S., Xiao Z.X., Wang S.X.*, Integrated control and analysis of microgrid // Autom. Electric Power Syst, 2008. № 7, pp. 98-103.
17. *Bai W., Liu L.Q., Zhang C.M., Ma L.Q.*, Seamless switching control technology of virtual synchronous generator // Autom. Instrument, 2017. №38 (12), pp. 13-17.
18. *Gu B.S., Wang J.H., Luo F.F., Ji Z.D., Lv Z.P., Gu W., Wang T.*, Three phase four leg virtual synchronous generator pre synchronization, multi loop control and load imbalance control method // Acta Electrotech. Sinica - 2017, №32 (S1), pp. 138-150.
19. *Wan X.F., Zhan Z.L., Liao Z.P., Xi R.X.*, Research on seamless switching strategy of virtual synchronous generator on and off grid // J. Electron. Measure. Instrument, 2018. №32 (5), pp. 33-40.
20. *Ji Y., Su J., Ding B.*, Microgrid inverter VSG off-grid switching and fault handling // Control Eng., 2021, № 28 (7), pp. 1496-1504.
21. *Li B., Zhou L., Yu X.R., Zheng C., Liu J.H.*, A microgrid inverter secondary frequency modulation scheme based on improved virtual synchronous generator algorithm // Power Syst. Technol., 2017, №41 (8), pp. 2680-2687.
22. *Safaryan O.A., Pilipenko I.A., Boldyrikhin N.V., Yukhnov V.I.*, Multidimensional likelihood function in the problem of estimating time-frequency parameters of signals // Conference Proceedings, 2021 Radiation and Scattering of Electromagnetic Waves, RSEMW 2021, pp. 393-396
23. *Safaryan O.A., Pilipenko I.A., Saharov I.A.,* Features of Frequency Generators Stabilization in Distributed Information-Measuring Systems// Conference Proceedings, 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019, pp. 208-211.
24. *Сафарьян О.А., Пилипенко И.А.* Метод оценивания параметров стабильности генераторов // Радиолокация, навигация, связь / сборник трудов XXVI Международной научно-технической конференции: в 6 т. Воронеж, 2020. С. 204-211.
25. *Safaryan O.A., Pilipenko I.A.,* Prerequisites and Theoretical Foundations of the Statistical Method of Frequency Stabilization in Information and Telecommunication Systems // Electronics, 2022, №11(18), pp. 1-9.

FREQUENCY STABILIZATION BASED ON PRIMARY FUNDAMENTAL PROPERTIES OF LARGE SYSTEMS

OLGA A. SAFARYAN
Rostov-on-Don, Russia, roma.perov@list.ru

IRINA A. ALFEROVA
Rostov-on-Don, Russia, roma.perov@list.ru

IRINA A. ENGIBARYAN
Rostov-on-Don, Russia, roma.perov@list.ru

VASILIY I. YUKHNOV
Rostov-on-Don, Russia, roma.perov@list.ru

KEYWORDS: *a system of simultaneously and independently operating generators, synergy, emergence, harmonic signal, signal phase, frequency stability, frequency estimation, non-bias and efficiency of estimates.*

ABSTRACT

Introduction. The article deals with issues related to the manifestation of the primary fundamental properties of large systems, such as synergy and emergence, potentially inherent in large systems with the same or similar properties of components. These properties can be implemented at a certain time interval when measuring the values of the signal phases at a time. It is shown that the manifestation of the synergistic property in the system of simultaneously and independently operating generators makes it possible to reduce the error in estimating random fluctuations in the frequency of generators, and the manifestation of the emergent property eliminates a constant frequency shift from the nominal value. Based on the analysis of the properties of the obtained estimates, the conditions for obtaining unbiased effective estimates of the frequency of each of the generators are formulated. **Result.** The manifestation of the properties of synergy and emergence in a system of simultaneously and independently functioning generators is shown. It is noted that from a physical point of view, an increase in the accuracy of estimating the frequency of signals corresponds to multiple unequal indirect measurements. The simulated frequency deviations of each of the generators and the difference between the values of the frequency deviation and the corresponding values of the estimates obtained are shown. The results of mathematical modeling are presented, confirming the validity of the theoretical results obtained and the main patterns noted.

REFERENCES

1. Glotov A.F. Intellectualization of information systems: approaches and directions. *Geomatics-2015*, pp.18-24.

2. David B. Lesson. Oscillator Phase Noise: A 50-Year Review. *IEEE Transactions on Ultrasonics, Ferroelectrics and Frequencies control*. 2016, no. 8, pp. 1208-1225.

3. Demir A. Mehrotra J. Roychowdhure. Phase noise in oscillators: A unifying theory and numerical methods for characterization. *IEEE Trans. Circuitts Syst. I. Fundam. Theory Appl.,* May 2000, vol. 47, no. 5, pp. 655-674.

4. Zheng T., Chen L., Chen T., Wei S.M., Virtual synchronous generator technology and prospects. *Autom. Electric Power Syst*. 2015, no. 39 (21), pp.165-175.

5. Shao H., Li P., Fu W.B., Yang G.H., Wind-solar grid-connected technology based on virtual synchronous generator control strategy. *Electr. Autom*. 2018, no. 40 (5), pp.16-18.

6. Ling Y.L., Adaptive control of distributed power inverter based on VSG. *Energy Conserv*. 2020, no. 39 (4), pp. 5-9.

7. Ren D.J., Wei Y.B., Xi Z.F., Zhang J., Control strategy of inverter power sharing based on VSG. *Power Electron. Technol* 2020, no.54 (2), pp. 28-31.

8. Huo X.X., Wu P., Huang X., Yan J.J., Wang K.Y., Xu K., Yao C., Chen P.Y., Microgrid Stability Control Based on Adaptive Parameter Virtual Synchronous Machine. *Electric Power Construct*. 2019, no. 40 (2), pp. 79-86.

9. Cheng G., Shao X., Wang G., Adaptive control strategy for virtual synchronous generator parameters. *Renewable Energy*. 2021, no. 39 (12), pp.1655-1661.

10. Lu Z., Sheng W., Zhong Q., Liu H., Zeng Z., Virtual synchronous generator and its applications in micro-grid. *Proc. CSEE*. 2014, no. 34 (16), pp. 2591-2603.

11. Zhao D.M., Zhang N., Liu Y.H., Zhang X., Integrated control strategy for smooth switching of microgrid and island operation mode based on energy storage. *Power Syst. Technol.,* 2013, no. 37 (2), pp.301-306.

12. Li P., Zhang X.S., Zhao B., Wang Z.L., Sun J.R., Microgrid design and mode switching control strategy of multi-microgrid and multi-grid point structure. *Autom. Electric Power Syst*. 2015, no. 39 (9), pp.172-178.

13. Wang J.S., Tang C.H., Chen N., Tan K., Mao J.X., A microgrid on-off and off-grid smooth switching control strategy based on self-recognition of operating mode. *Autom. Electric Power Syst*. 2015, no. 39 (9), pp.185-191.

14. Yang Y.C., Zhou Z.G., Distributed power grid-connected inverter seamless switching control strategy. *J. Electric Power Syst. Autom*. 2016, no. 28 (8), pp. 91-97.

15. Shi R.L., Zhang X., Xu H.Z., Liu F., Hu C., Yu Y., Seamless switching control strategy of microgrid operation mode based on virtual synchronous generator. *Autom. Electric Power Syst*. 2016, no. 40 (10), pp. 16-23.

16. Wang C.S., Xiao Z.X., Wang S.X., Integrated control and analysis of microgrid. *Autom. Electric Power Syst*. 2008, no. 7, pp. 98-103.

17. Bai W., Liu L.Q., Zhang C.M., Ma L.Q., Seamless switching control technology of virtual synchronous generator. *Autom. Instrument.* 2017, noo.38 (12), pp. 13-17.

18. Gu B.S., Wang J.H., Luo F.F., Ji Z.D., Lv Z.P., Gu W., Wang T., Three phase four leg virtual synchronous generator pre synchronization, multi loop control and load imbalance control method. *Acta Electrotech. Sinica*. 2017, no.32 (S1), pp. 138-150.

19. Wan X.F., Zhan Z.L., Liao Z.P., Xi R.X., Research on seamless switching strategy of virtual synchronous generator on and off grid. *J. Electron. Measure. Instrument*. 2018, no.32 (5), pp. 33-40.

20. Ji Y., Su J., Ding B., Microgrid inverter VSG off-grid switching and fault handling. *Control Eng*. 2021, no. 28 (7), pp. 1496-1504.

21. Li B., Zhou L., Yu X.R., Zheng C., Liu J.H., A microgrid inverter secondary frequency modulation scheme based on improved virtual synchronous generator algorithm. *Power Syst. Technol.* 2017, no.41 (8), pp. 2680-2687.

22. Safaryan O.A., Pilipenko I.A., Boldyrikhin N.V., Yukhnov V.I., Multidimensional likelihood function in the problem of estimating time-frequency parameters of signals. *Conference Proceedings. 2021 Radiation and Scattering of Electromagnetic Waves, RSEMW 2021*, pp. 393-396.

23. Safaryan O.A., Pilipenko I.A., Saharov I.A., Features of Frequency Generators Stabilization in Distributed Information-Measuring Systems. *Conference Proceedings. 2019 Radiation and Scattering of Electromagnetic Waves, RSEMW 2019*. 2019, pp. 208-211.

24. Safaryan O.A., Pilipenko I.A. Method of estimating the stability parameters of generators. *Radar, navigation, communication. Proceedings of the XXVI International Scientific and Technical Conference*: in 6 vol. Voronezh. 2020, pp. 204-211.

25. Safaryan O.A., Pilipenko I.A., Prerequisites and Theoretical Foundations of the Statistical Method of Frequency Stabilization in Information and Telecommunication Systems. *Electronics*. 2022, no.11(18), pp. 1-9.

INFORMATION ABOUT AUTHORS:

Olga A. Safaryan, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department "Cybersecurity of Information Systems", Don State Technical University, Rostov-on-Don, Russia, safari_2006@mail.ru

Irina A. Alferova, Senior Lecturer, Department of Cybersecurity of Information Systems, Don State Technical University, Rostov-on-Don, Russia, ia.alferova.donstu@yandex.ru

Irina A. Engibaryan, Candidate of Technical Sciences, Associate Professor of the Department of Infocommunication Technologies and Communication Systems, North Caucasian branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia, eirina@live.ru

Vasily I. Yukhnov, Candidate of Technical Sciences, Associate Professor, Head of the Department of Infocommunication Technologies and Communication Systems, North Caucasian Branch of Moscow Technical University of Communications and Informatics, Rostov-on-Don, Russia, juchnov@mail.ru

For citation: Safaryan O.A., Alferova I.A., Engibaryan I.A., Yukhnov V.I. Frequency stabilization based on primary fundamental properties of large systems. H&ES Reserch. 2022. Vol. 14. No 4. P. 26-32. doi: 10.36724/2409-5419-2022-14-4-26-32 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-33-38

МЕТОД ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИОННЫХ СИСТЕМ

ГРАЧЕВ
Михаил Иванович[1]

ПРИМАКИН
Алексей Иванович[2]

ВОРОНОВ
Сергей Алексеевич[3]

ЕФИМОВА
Анна Борисовна[4]

Сведения об авторах:

[1] старший инженер информационного центра, Санкт-Петербургский университет МВД России, г. Санкт-Петербург, Россия, mig2500@mail.ru,

[2] доктор технических наук, профессор, профессор кафедры информатики и математики, Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии, г. Санкт-Петербург, Россия, a.primakin@mail.ru

[3] кандидат педагогических наук, заместитель начальника кафедры математики и информатики, Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии, г. Санкт-Петербург, Россия, voronov-sci@mail.ru

[4] преподаватель кафедры информатики и математики, Санкт-Петербургский военный институт войск национальной гвардии Российской Федерации, г. Санкт-Петербург, Россия, abefimova020770@mail.ru

АННОТАЦИЯ

Введение. В современных условиях имеет место повсеместное внедрение цифровых информационных технологий во все сферы жизни общества и как следствие в органи-зационные системы. Для проведения анализа поступающей информации и своевременного реагирования на недостоверную, требуется задействование большого количества мощностей как информационных, так и технических, применение информационных технологий. Для противодействия информационным угрозам необходимо располагать различными ресурсами: защищенными сетями, современными аппаратно-программными комплексами, обученным кадровым составом, а также владения вопросами своевременного прохождения переподготовки. **Цель** проводимого исследования заключается в предложении применять сетевую модель ЛПР для более наглядного способа распределения времени и ресурсов по реше-нию задачи управления. **Методы.** В статье предлагается метод взаимодействия технического обеспечения и кадрового состава организационной системы. Предлагаемый метод помогает преодолеть негативные воздействия информации. **Теоретическая значимость** заключается в проведении анализа и нахождении харак-теристик, способствующих развитию организации на основе своевременного внедрения в контур управления комплексных мер направленных на модернизацию программного комплекса, технического комплекса, так и подготовки кадрового штата сотрудников организации. **Результаты исследования.** В статье сформулированы рекомендации по противодействию возникающим угрозам в системе. В процессе функционирования сложных систем внедряются web-технологии и другие программные модули, которые задействуются в процессе управления ими с целью достижения цели управления, через информационные потоки и процессы задействования технических средств, непосредственно влияющих на процесс управления рассматриваемой системы. В таких системах важное значение отводится быстрое взаимодействие человека и технических средств для своевременного нахождения слабых сторон и своевременного принятия решения для превентивных мер. Рассматривается вопрос взаимодействия располагаемыми резервами у лица, принимающего решение. Метод исследования предложен в виде сетевой модели и являющийся частью комплексного подхода, который должен быть использован для проведения противодействия возникающим вопросам в системе управления. Для решения вопроса управления предполагается использовать методы моделирования как части комплекса мер направленных на реализацию штатной работы системы.

КЛЮЧЕВЫЕ СЛОВА: *информационные поводы, решение задачи управления, информационная угроза, организационные системы, управление, моделирование*

Для цитирования: Грачев М.И., Примакин А.И., Воронов С.А., Ефимова А.Б. Метод повышения информационной безопасности организационных систем // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 33-38. doi: 10.36724/2409-5419-2022-14-4-33-38

Введение

Современное развитие информационных систем и технологий, а также скорость их внедрения в жизнедеятельность людей во всем мире привело к необходимости обращать внимание на вопросы информации и управления ею, что стало началом противодействия информационным угрозам [1].

Информационные угрозы становятся все более коварными и действенными, соответственно для противодействия им необходимо использовать информационные технологии [2]. Методы ведения превентивных мер должны включать в себя комплекс проводимых мероприятий: сбор информации, её анализ и принятие соответствующих мер.

Для руководителя важно располагать математической моделью, которая будет гарантировать достижение цели деятельности и позволять решить сложившуюся ситуацию за счет ресурсов, которыми располагает лицо, принимающее решение (ЛПР) [3].

Для противодействия информационным угрозам необходимо располагать различными ресурсами: защищенными сетями, современными аппаратно-программными комплексами, обученным кадровым составом, а также владения вопросами своевременного прохождения переподготовки [4].

Среди технологий информационного воздействия широко применяется различные средства массовой информации (кино, радио, интернет, мессенджеры, web-ресурсы) [5, 6].

Вопросы информационного воздействия рассматривались российскими и зарубежными авторами: Л.Н. Кунаковой [7], Г.Б. Прончевым [8], П.И. Фроловой [9], Н.В. Лопатиной [10], И.Н. Панариным [11], В.В. Кихтан [12-15], С. М. Воробьев [16], Т. Р. Красикова [17], Д. Н. Кравцов [18], Лебедь, Б. И. Терещенко, К. А. Восканян [19], Bartles Charles K. [20], Kasapoglu C. [21], Monaghan A. [22] и др.

Приведенные выше авторы рассматривают важность вопросов своевременного реагирования на информационные сообщения негативного характера и описывают всю важность работы с ними с целью уменьшения отрицательного эффекта, но методики или модели по противодействию возникающей угрозе они не выделяют. Рассмотрение данного вопроса является актуальной задачей для быстрого и своевременного решения вопросов принятия управленческого решения по вопросам противодействия недостоверной информации.

Только комплексный подход и своевременное управленческое решение по задействованию располагаемыми ресурсами позволит решать вопросы противодействия информационным угрозам [23].

Решение вопроса противодействия информационным негативным последствиям следует рассматривать не в одностороннем порядке, а комплексном. Комплексом может выступать последовательность проводимых работ и мероприятий, имеющих направленность в скорейшем решении задачи управления и достижении цели деятельности. Важнейшим направлением работы ЛПР является организация слаженной работы управляемым подразделением, так как в случае возникающих угроз меры противодействия должны быть задействованы своевременно.

Цель проводимого исследования заключается в предложении применять сетевую модель ЛПР для более наглядного способа распределения времени и ресурсов по решению задачи управления.

Результаты исследования

В основе действий для дискредитации лежит информационный повод. Информационный повод (инфоповод) – это факт, обладающий относительными характеристиками, который может использоваться для освещения в СМИ. Как правило, такими характеристиками выступают масштабность, значимость, актуальность, а в зависимости от формата массмедиа дополнительно играет роль неоднозначность интерпретации события [16].

Инфоповод может быть как случайным, так и спланированным событием, заранее подготовленным результатом проведенных действий. Так как событие определяется общественно значимым, если оно попало в информационную повестку web-ресурсов, то важно указать такую дефиницию, как медиасобытие (инфоповод, который нашел свое отражение в СМИ).

Негативная информации является центральным объектом в инфоповоде. Анализ работ в области действий, направленных на дискредитацию и имеющие разрушительный эффект [18, 19], позволяет выделить характеристики, которыми должна обладать такая информация:

– масштабность распространения информации (СМИ, ограниченная группа абонентов, адресное информирование и т.д.);

– уровень недостоверности (искажение сведений, ложная, провокационная и т.д.);

– размер причиненного вреда (ущерба).

Управление располагаемыми ресурсами подразумевает, что для своевременного анализа поступающей информации должно быть в наличии соответствующее оборудование и современное программное обеспечение способное по своим характеристикам производить мониторинг web-страниц. Необходимо обратить внимание на подачу информационного повода, и как в СМИ конструируют представление медиасобытий. Не зависимо от формата представления, медиатекст является основным инструментом вербальной коммуникации с пользователями. СМИ конструируют социально значимые события в медиатексте, определяя значимость события, пространство, масштаб, категорию события. Одно и тоже событие может иметь общий конструктив, отличаясь по содержанию.

В текстах информационных ресурсов в сети Интернет наиболее распространенным лексическим приемом считается прием навязывания мнения и прием интерпретации фактов [24].

Это обусловлено более легким и выгодным способом навязывания адресату заданного мнения. Использование различных приемов намек или метафора применяются как эффективное средство дискредитации. На этом этапе человек может пропустить негативную информацию и тут нужна помощь искусственного интеллекта для противодействия таким фактам.

На данном этапе развития организации должны отслеживаться своевременные веяния по развитию науки и техники,

что, несомненно, влечёт за собой наличие соответствующего финансирования, так как нанесённый урон может быть гораздо более тяжелые последствия для организации, чем обновление, например, программного обеспечения в организации за год.

Соответственно, для ЛПР, располагающего как техническими ресурсами, так и кадровыми. Необходимо проводить мониторинг их возможностей к преодолению возникающих трудностей, тем самым проводить как обновление техники и программного обеспечения, так и переподготовку или повышение квалификации кадрового персонала [25].

Одним из методов решения задачи управления как способу решения возникающих затруднений, может быть применение сетевого моделирования, позволяющего рассматривать руководителю перечень событий и запланированных мероприятий соизмеримо имеющимся ресурсам и самое важное рассчитывать время, которое необходимо затратить для преодоления затруднений [26].

В данном случае можно рассматривать события и наглядно отображать их на сетевом графике с запланированными событиями и запланированными работами (рис. 1).

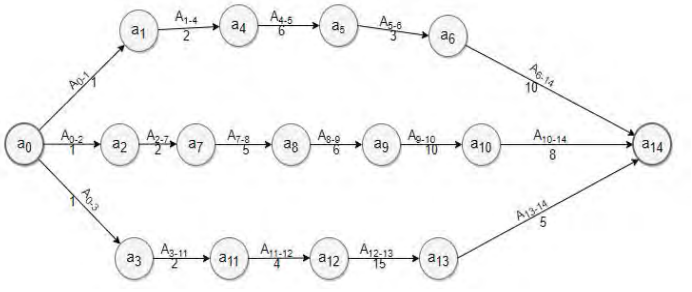

Рис. 1. Сетевой график проводимых мероприятий по мониторингу состояния управляемой системы

На данном рисунке показателями от a_0 до a_{14} прописываются события, которые отслеживаются в управляемой ОС, а остальными показателями от $A_{0\text{-}2}$ до $A_{13\text{-}14}$ прописываются запланированные работы. Как правило, эти данные отображаются в табличной форме и могут быть представлены с указанием затрачиваемого времени на проведение того или иного мероприятия, а также служить планом реализации проведения переподготовки кадрового состава управляемой ОС или планом обновления программно-аппаратного комплекса.

Путем проведения анализа всех проводимых мероприятий находится свободное время и формируется соответствующий временной резерв Δtp.

Общее затрачиваемое время Δto можно будет уменьшить за счет использования и перераспределения свободного времени и резервов времени.

Необходимый запас временного ресурса мы можем получить при сетевом моделировании процесса задействования имеющихся ресурсов, который позволит нам разложить имеющиеся ресурсы, далее выявить свободное время Δt_c, которое можно будет использовать, и перераспределять по мере его необходимости между проблемными ситуациями, Δt – время выполнения задачи управления с учетом перераспределения резервов времени и свободного времени [26].

Создаются таблицы с указанием запланированных событий системы (табл. 1) и запланированных работ системы (табл. 2) для более наглядного отображения. Отраженные временные диапазоны и события во времени, обозначенном на сетевой модели, должны соответствовать событиям реализации программы обновления аппаратно-программного комплекса и переподготовку кадрового состава, которым располагает ЛПР.

Сетевое моделирование служит графиком выполнения решаемых задач и может визуально служить подсказкой следующих решаемых задач при управлении требуемым участком. В данных таблицах мы представили схему анализа и декомпозиции ресурсов при решении задачи управления. Ресурсы рассматриваются как кадровый состав, техническое и программное обеспечение [26].

Таблица 1

Перечень состояний системы мониторинга

Обозначение	Наименование событий
a_0	Система в состоянии покоя (нет воздействия)
a_1	Состояние системы рассмотрения аппаратной части
a_2	Состояние системы рассмотрения программной части
a_3	Состояние системы рассмотрения кадрового состава
…	…
a_{14}	Состояние системы, в которой проводится анализ выполненных работ

Таблица 2

Перечень событий процесса системы мониторинга

Обозначение работ	Наименование работ	Время выполнения работы, мин
$A_{0\text{-}1}$	Получение информации от датчиков технической системы	8
$A_{0\text{-}2}$	Проведение анализа через web-интерфейс программных компонентов	23
$A_{0\text{-}3}$	Проведение совещания по вопросам проведения переподготовки кадрового состава	60
…	…	
$A_{6\text{-}14}$	Анализ информации, полученной от датчиков всего оборудования	45
$A_{10\text{-}14}$	Анализ используемого программного фонда	60
$A_{13\text{-}14}$	Получение выписки кадрового состава, которые требуется направить на переподготовку	30

Основными вычисляемыми параметрами сетевого графика являются:

1. Наиболее раннее возможное время наступления *j*-го события $T_p(j)$, вычисляемое по формуле:

$$T_P(j) = \frac{\max}{i \subset j}(T_P(i) - t_{ij}), \quad (1)$$

где *i* и j обозначаются номера предшествующего и последующего событий соответственно; t_{ij} – продолжительность (*i*, *j*)-й работы.

Из обозначения $i \subset j$ следует, что событие *i* предшествует событию *j* [4, 26].

2. амое позднее допустимое время наступления i-го события Тп (i), вычисляемое по формуле:

$$T_{\Pi}(j) = \frac{\min}{i \supset j}(T_{\Pi}(i) - t_{ij}) \quad (2)$$

где из обозначения $i \subset j$ следует, что событие *j* предшествует событию *i* [4, 26].

3. Полный резерв времени работы $r_п$ (*i*,*j*), вычисляемый по формуле (3).

Полный резерв любой работы складывается из собственного свободного резерва и минимального из полных резервов непосредственно следующих работ.

Полный резерв работы показывает максимальное время, на которое можно увеличить длительность работы или отсрочить ее начало, чтобы не нарушился срок завершения проекта в целом.

$$r_{\Pi}(\mathrm{i},\mathrm{j}) = (T_{\Pi}(j) - T_P(i) - t_{ij}) \quad (3)$$

Смысл полного резерва времени работы заключается в том, что задержка в выполнении работы (*i*,*j*) на величину $\Delta t_{ij} \geq r_п$ (*i*,*j*), приводит к задержке в наступлении завершающего события на величину ($\Delta t_{ij} - r_п$ (*i*,*j*)) [4, 26].

По полученным данным формул (1), (2), (3) мы получаем показатели времени необходимые для достижения цели деятельности. Основным показателем будет критический (полный) путь выполнения работ и времени, затраченного при этом. Далее, руководитель задействует имеющиеся у него резервы для уменьшения времени проведения полного цикла работ, как на отдельных участках, так и на всём критическом (полном) пути выполнения работ [4].

Выводы

В работе предложен один из методов решения задачи, направленной на противодействие возникающим угрозам в системе управления, что подразумевает комплекс действий, таких как численные методы, математическое моделирование и имитационное моделирование по полученным данным.

В данной работе мы рассмотрели только пример сетевого моделирования. Практическая значимость заключается в том, что предложен метод решения задачи управления по нахождению критического пути, то есть наибольшего времени решения задачи и выявлении резервов времени способных на отдельных участках проведения работы использовать выявленные резервы, тем самым уменьшая общее время выполнения работ. Данная постановка вопроса направлена на повышение эффективности управленческого решения, за счет уменьшения времени, требуемого для достижения цели управления/

Теоретическая значимость заключается в проведении анализа и нахождении характеристик, способствующих развитию организации на основе своевременного внедрения в контур управления комплексных мер, направленных на модернизацию программного комплекса, технического комплекса, так и подготовки кадрового штата сотрудников организации.

Литература

1. *Burlov V., Grachev M.* Management model in digital ecosystems // IOP Conference Series: Earth and Environmental Science, Kaliningrad, 05–10 октября 2020 года. Kaliningrad, 2021. P. 012010. DOI 10.1088/1755-1315/689/1/012010. EDN ALPCBO.

2. *Andreev A. V., Burlov V. G., Grachev M. I.* Information technologies and synthesis of the management process model in the enterprise // 2019 International Science and Technology Conference "EastConf", EastConf 2019, Vladivostok, 01-02 марта 2019 года. Vladivostok, 2019. P. 8725428. DOI 10.1109/Eastonf.2019.8725428. EDN CDNIJD.

3. *Бурлов В. Г., Грачев М. И.* Аналитическо-динамическая модель управленческого решения в социально-экономических системах на примере руководителя учебного заведения высшего образования // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. № 10. С. 27-34. DOI 10.2 1/2072-8735-2018-10314. EDN SNJZQR.

4. *Бурлов В. Г., Грачев М. И.* Оценивание эффективности принятия управленческих решений в социально-экономических системах на примере учебного заведения высшего образования // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 2. С. 32-38. DOI 10.36724/2072-8735-2020-14-2-32-38. EDN YKNJZI.

5. *Воронов С. А.* Значение социальных медиа в экстремистской деятельности: информационное противоборство // Информационные войны. 2021. № 4(60). С. 9-13. EDN TWEQUT.

6. *Красикова Т. Р.* Дискурсивное конструирование события в массмедиа: анализ российского телевидения : автореф. дис. … канд. филол. наук : 10.01.10 / Т. Р. Красикова Татьяна Романовна. Воронеж, 2018. 22 с.

7. *Кунакова Л. Н.* Информационная война как объект научного анализа (понятие и основные характеристики информационной войны) // Альманах современной науки и образования. 2012. № 6. С. 93-96. EDN OZGEKF.

8. *Pronchev G. B., Mikhailov A. P., Lyubimov A. P., Solovyev A. A.* Particularities of the Internet-based virtual social environments within the context of information warfare // EurAsian Journal of BioSciences. 2020. Vol. 14. No 2, pp. 3731-3739. EDN PPNIFU.

9. *Фролова П. И.* Информационное манипулирование массовым сознанием в условиях современных информационных войн // Актуальные проблемы информационного противоборства в современном мире: вызовы и угрозы для России и Русского мира : Материалы Международной научно-практической конференции, Донецк, 30 октября 2019 года / Под общей редакцией С.В. Беспаловой. Донецк: Донецкий национальный университет, 2019. С. 207-210. EDN XJTACD.

10. *Лопатина Н. В.* Современная информационная культура и информационные войны // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2014. № 7. С. 1-4. EDN SLQWYX.

11. *Панарин И. Н.* Информационная война и геополитика. М.: Поколение, 2006. 553 с. (Великий путь). ISBN 5-9763-0001-4. EDN QOFHXJ.

12. *Кихтан В. В.* Исследование процессов манипулирования массовым сознанием в современных средствах массовой информации // Вестник Волжского университета им. В.Н. Татищева. 2018. Т. 2. № 2. С. 221-227. EDN XREBMD.

13. *Кихтан В. В., Качмазова З. Н.* Информационная война: понятие, содержание и основные формы проявления // Вестник Волжского университета им. В.Н. Татищева. 2018. Т. 2. № 2. С. 228-235. EDN USGUUQ.

14. *Кихтан В. В., Мамиева Б. Ю.* К вопросу о манипулировании в современных СМИ // Вестник Волжского университета им. В.Н. Татищева. 2018. Т. 2. № 2. С. 236-242. EDN XREBMT.

15. *Кихтан В. В., Качмазова З. Н.* Информационная война: понятие, содержание и основные формы проявления // Вестник Волжского университета им. В.Н. Татищева. 2018. Т. 2. № 2. С. 228-235. EDN USGUUQ.

16. *Воробьев С. М.* Дискредитация институтов государственной власти в России западными акторами: теоретический анализ // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». 2017. № 9. С. 18-32. EDN XGXYLI

17. *Красикова Т. Р.* Вербальный аспект конструирования социально значимых событий в медиатекстах // Современный дискурс-анализ. 2014. № 2(11). С. 50-63.

18. *Кравцов Д. Н.* Роль и значение современных информационно-психологических войн в системе обеспечения национальной безопасности // Антропос: Логос и Теос. 2018. № 4. С. 212-219. EDN WRSNQQ.

19. *Лебедь В. Н., Терещенко Б. И., Восканян К. А.* Управление процессами обеспечения кибербезопасности как фактор международной стабильности // Коммуникология: электронный научный журнал. 2017. Т. 2. № 4. С. 30-37. EDN STJUHW.

20. *Bartles Charles K.* Getting Gerasimov Right. Military Review, 2016. № 1 (96), pp. 30-37.

21. *Kasapoglu C.* Rissia's Renewed Military Thinking: Non-Linear Warfare and Reflexife Control. Rome: Research Division – NATO Defence Colledge, 2015. № 121, pp. 1-12.

22. *Monaghan A.* The «War» in Rusian's «Hybrid Warfare». Parameters, 2016. №4, pp. 65-74.

23. *Бурлов В. Г., Грачев М. И., Капицын С. Ю., Абрамов В. М.* Создание математической модели принятия управленческого решения для противодействие возникающих угроз в системе // Региональная информатика и информационная безопасность : Сборник трудов XII Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 27-29 ноября 2021 года. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2021. С. 81-84. EDN UHDSRB.

24. *Воронов С.А., Сидоров И.А.* Механизмы поисковой системы Google, используемые в информационном противоборстве // Вестник НГУ. Серия: Информационные технологии. 2021. Том 19. №1. С. 26-38.

25. *Грачев М. И.* Технический и человеческий фактор в проведении характеризационного анализа // Нейрокомпьютеры и их применение : XVIII Всероссийская научная конференция. Тезисы докладов. Москва, 17 марта 2020 года. М.: Московский государственный психолого-педагогический университет, 2020. С. 245-247. EDN UXABJG.

26. *Бурлов В. Г., Грачев М. И.* Применение сетевых моделей в социальных и экономических системах // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15. № 2. С. 33-38. DOI 10.36724/2072-8735-2021-15-2-33-38. EDN UIBNRM.

INFORMATION SECURITY IMPROVEMENT METHOD ORGANIZATIONAL SYSTEMS

MIKHAIL I. GRACHEV
St. Petersburg, Russia, mig2500@mail.ru

ALEKSEY I. PRIMAKIN
St. Petersburg, Russia, a.primakin@mail.ru

SERGEI A. VORONOV
St. Petersburg, Russia, voronov-sci@mail.ru

ANNA B. EFIMOVA
St. Petersburg, Russia, abefimova020770@mail.ru

KEYWORDS: *informational occasions, solving the problem of management, information warfare, organizational systems, management, modeling.*

ABSTRACT

Introduction. In modern conditions, there is a widespread introduction of digital information technologies into all spheres of society and, as a result, into organizational systems. In order to analyze incoming information and respond to unreliable information in a timely manner, it requires the use of a large number of capacities, both informational and technical, and the use of information technologies. **The article proposes a method** of interaction of technical support and personnel of the organizational system. The proposed method helps to overcome the negative effects of information. The article formulates recommendations for countering emerging threats in the system. In the process of functioning of complex systems, web technologies and other software modules are introduced, which are involved in the process of managing them in order to achieve the management goal, through information flows and processes involving technical means that directly affect the management process of the system in question. In such systems, the importance is given to the rapid interaction of human and technical means for timely finding weaknesses and timely decision-making for preventive measures. The issue of interaction with the available reserves of the decision-maker is being considered. **Results.** The research method is proposed in the form of a network model and is part of an integrated approach that should be used to counter emerging issues in the management system. To solve the management issue, it is proposed to use modeling methods as part of a set of measures aimed at implementing the regular operation of the system.

REFERENCES

1. Burlov V, Grachev M. Management model in digital ecosystems. *IOP Conference Series: Earth and Environmental Science*, Kaliningrad, October 05-10, 2020. Kaliningrad, 2021. P. 012010. DOI 10.1088/1755-1315/689/1/012010.

2. Andreev A. V., Burlov V. G., Grachev M. I. Information technologies and synthesis of the management process model in the enterprise. *2019 International Sci-ence and Technology Conference "EastConf", EastConf 2019*, Vladivostok, March 01-02, 2019 of the year. Vladivostok, 2019. P. 8725428. DOI 10.1109/Eastonf.2019.8725428.

3. Burlov V. G., Grachev M. I. Analytical-dynamic model of management decision in socio-economic systems on the example of the head of an educational institution of higher education. T-Comm. 2019. Vol. 13. No. 10, pp. 27-34. DOI 10.24411/2072-8735-2018-10314.

4. Burlov V. G., Grachev M. I. Evaluation of the effectiveness of managerial decision-making in socio-economic systems on the example of an educational institution of higher education. T-Comm. 2020. Vol. 14. No. 2, pp. 32-38. DOI 10.36724/2072-8735-2020-14-2-32-38.

5. Voronov S. A. The value of social media in extremist activity: information confronta-tion. Information wars. 2021. No. 4 (60), pp. 9-13.

6. Krasikova T. R. Discursive construction of an event in the mass media: analysis of Russian television: author. dis. ... cand. philol. Sciences: 10.01.10 / T. R. Krasikova Tatyana Romanovna. Voronezh, 2018. 22 p.

7. Kunakova L.N. Information warfare as an object of scientific analysis (the concept and main characteristics of information warfare). *Almanac of modern science and education*. 2012. No. 6, pp. 93-96.

8. Pronchev G. B., Mikhailov A. P., Lyubimov A. P., Solovyev A. A. Particularities of the Internet-based virtual social environments within the context of information warfare. *Eur-Asian Journal of BioSciences*. 2020. Vol. 14. No 2, pp. 3731-3739.

9. Frolova P. I. Information manipulation of mass consciousness in the conditions of modern information wars. *Actual problems of information confrontation in the modern world: challenges and threats for Russia and the Russian world: Proceedings of the In-ternational scientific and practical conference*, Donetsk, October 30, 2019 / Under the general editorship of S.V. Bespalova. Donetsk: Donetsk National University, 2019, pp. 207-210.

10. Lopatina N. V. Modern information culture and information wars. *Scientific and technical information. Series 1: Organization and methodology of information work*. 2014. No. 7, pp. 1-4.

11. Panarin I. N. Information war and geopolitics. Moscow: Generation, 2006. 553 p. (Great way). ISBN 5-9763-0001-4.

12. Kikhtan V. V. Study of the processes of manipulation of mass consciousness in modern media. *Bulletin of the Volga University. V.N. Tatishchev*. 2018. Vol. 2. No. 2, pp. 221-227.

13. Kikhtan V. V., Kachmazova Z. N. Information war: concept, content and main forms of manifestation. *Bulletin of the Volga University. V.N. Tatishchev*. 2018. Vol. 2. No. 2, pp. 228-235.

14. Kikhtan V. V., Mamieva B. Yu. On the issue of manipulation in modern media. *Bulletin of the Volga University. V.N. Tatishchev*. 2018. Vol. 2. No. 2, pp. 236-242.

15. Kikhtan V. V., Kachmazova Z. N. Information war: concept, content and main forms of manifestation. *Bulletin of the Volga University. V.N. Tatishchev*. 2018. Vol. 2. No. 2, pp. 228-235.

16 Vorobyov S. M. Discrediting the institutions of state power in Russia by Western actors: theoretical analysis. *Bulletin of the public research laboratory "Interaction of the penitentiary system with civil society institutions: historical, legal and theoretical -methodological aspects*. 2017. No. 9, pp. 18-32.

17. Krasikova T. R. The verbal aspect of constructing socially significant events in media texts. *Modern discourse analysis*. 2014. No. 2(11), pp. 50-63.

18. Kravtsov D. N. The role and significance of modern information-psychological warfare in the national security system. *Anthropos: Logos and Theos*. 2018. No. 4, pp. 212-219.

19. Lebed V. N., Tereshchenko B. I., Voskanyan K. A. Management of cybersecurity processes as a factor of international stability. *Communicology: electronic scientific journal*. 2017. Vol. 2. No. 4, pp. 30-37.

20. Bartles Charles K. Getting Gerasimov Right. *Military Review*, 2016. No. 1 (96), pp. 30-37.

21. Kasapoglu C. Rissia's Renewed Military Thinking: Non-Linear Warfare and Reflexife Control. Rome: Research Division - NATO Defense College, 2015. No. 121, pp. 1-12.

22. Monaghan A. The "War" in Rusian's "Hybrid Warfare". *Parameters*, 2016. No. 4, pp. 65-74.

23. Burlov V. G., Grachev M. I., Kapitsyn S. Yu., Abramov V. M. Creation of a mathematical model for making a managerial decision to counteract emerging threats in the system. *Regional informatics and information security: Collection of works XII St. Petersburg Interregional Conference*, St. Petersburg, November 27-29, 2021. St. Petersburg: Regional public organization "St. Petersburg Society of Informatics, Computer Engineering, Communication and Control Systems", 2021, pp. 81-84.

24. Voronov S.A., Sidorov I.A. Mechanisms of the Google search engine used in information warfare. *Bulletin of the Novosibirsk State University. Series: Information technologies*. 2021. Vol. 19. No. 1, pp. 26-38.

25. Grachev M. I. Technical and human factor in characterization analysis. *Neurocomputers and their application: XVIII All-Russian Scientific Conference*. Moscow, March 17, 2020. Moscow: Moscow State Psychological and Pedagogical University, 2020, pp. 245-247.

26. Burlov V. G., Grachev M. I. Application of network models in social and economic systems. T-Comm. 2021. Vol. 15. No. 2, pp. 33-38. DOI 10.36724/2072-8735-2021-15-2-33-38

INFORMATION ABOUT AUTHORS:

Mikhail I. Grachev, St. Petersburg University of the Ministry of Internal Affairs of Russia, Senior Engineer of the Information Center, St. Petersburg, Russia, mig2500@mail.ru

Aleksey I. Primakin, St. Petersburg Military Institute of the National Guard Troops Order of Zhukov, Doctor of Technical Sciences, Professor, Professor of the Department of Informatics and Mathematics, St. Petersburg, Russia, a.primakin@mail.ru

Sergei A. Voronov, St. Petersburg Military Institute of the National Guard Troops Order of Zhukov, Candidate of Pedagogical Sciences, Deputy Head of the Department of Mathematics and Informatics, St. Petersburg, Russia, voronov-sci@mail.ru

Anna B. Efimova, St. Petersburg Military Institute of the National Guard Troops of the Russian Federation, lecturer at the Department of Informatics and Mathematics, St. Petersburg, Russia, abefimova020770@mail.ru

For citation: Grachev M.I., Primakin A.I., Voronov S.A., Efimova A.B. Information security improvement method organizational systems. H&ES Reserch. 2022. Vol. 14. No 4. P. 33-38. doi: 10.36724/2409-5419-2022-14-4-33-38 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-39-46

ПРОГНОЗИРОВАНИЕ ПОЛНОГО ЭЛЕКТРОННОГО СОДЕРЖАНИЯ ИОНОСФЕРЫ НА ОСНОВЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

ЗАМОГИЛЬНЫЙ Дмитрий

АННОТАЦИЯ

Введение. В работе представлена и описана технология применения алгоритма машинного обучения в прогнозировании вертикального полного электронного содержания ионосферы. Ионосферная погрешность является одним из наиболее значимых источников погрешностей измерения псевдодальностей по сигналам ГНСС. **Методы.** Повышающееся с каждым годом требования к точности позиционирования и навигации по сигналам ГНСС приводит к необходимости разработки новых методов уменьшения влияния различных погрешностей измерений, в том числе ионосферной погрешности. На данный момент для ионосферной коррекции измерений используются модели ионосферы различных типов. Существующие на данный момент широко используемые ионосферные модели не позволяют в значительной степени повысить точность позиционирования по сигналам ГНСС. На данный момент создание новой эффективной методики моделирования и прогнозирования ионосферы отвечающим современным требования к точности позиционирования является важной и актуальной задачей. Целью настоящей работы является создание методики моделирования и прогнозирования полного электронного содержания ионосферы с применением алгоритмов машинного обучения. Машинное обучение на данный момент является довольно распространённым и популярным методом решения задач классификации, распознавания и прогнозирования. Метод уже многие года применяется в медицине, робототехнике, промышленности, финансах и множестве других отраслях современной науки и экономики. **Цели и задачи исследования.** Для достижения поставленной цели необходимо решить ряд задач. В первую очередь необходимо подобрать и собрать данные для обучения модели, далее необходимо выбрать метод машинного обучения и гиперпараметры для выбранного метода. Далее необходимо выполнить прогнозирование ПЭС на основе обученной модели и выполнить оценку точности полученных результатов. сравнение полученных результатов с точностью других существующих моделей. **Результаты.** Показано, что машинного обучение хорошо справляется с задачей прогнозирования полного электронного содержания. Полученная обученная модель позволяет получать прогноз с точностью сопоставимой с точностью моделей Klobuchar, NeQuick, а в некоторых случаях и значительно точнее.

Сведения об авторе:

Преподаватель кафедры прикладной геодезии Московского Государственного университета геодезии и картографии, Москва, Россия, dmt.zam@gmail.com

КЛЮЧЕВЫЕ СЛОВА: *полное электронное содержание, ГНСС, ионосфера, машинное обучение, случайный лес.*

Для цитирования: Замогильный Д. Прогнозирование полного электронного содержания ионосферы на основе алгоритмов машинного обучения // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 39-46. doi: 10.36724/2409-5419-2022-14-4-39-46

Введение

Ионосфера Земли – это заряженная часть атмосферы, на высоте 60-1000 км. Эта среда оказывает значительное влияние, а распространение сигналов ГНСС и других радиоизмерительных систем.

Прогнозирование и моделирование параметров ионосферы в настоящее время является весьма актуальной задачей ГНСС, систем радионавигации, радиосвязи и радиолокации. Особенно это актуально при позиционировании по сигналам ГНСС, поскольку требования к точности позиционирования увеличиваются каждый год, а качественный учёт ионосферной задержки радиосигналов является одной из основных возможностей повысить точность позиционирования [1,2].

Полное электронное содержание (ПЭС) ионосферы является важным параметром ионосферы, который может быть использован для коррекции ионосферных погрешностей измерений [3]. ПЭС – это количество электронов вдоль столба сечением в один метр. Единица измерения ПЭС – TECU, 1 TECU = 10^{16} м$^{-2}$.

Машинное обучение (Machine Learning) – обширный подраздел искусственного интеллекта, изучающий методы построения алгоритмов, способных обучаться. Искусственный интеллект (ИИ), в частности, машинное обучение (ML), быстро развивались, в последние годы особенно в сфере анализа данных и вычислений [4]. ML обычно предоставляет системам возможность автоматически учиться и совершенствоваться на основе опыта, без специального программирования, и обычно упоминается как самая популярная и новейшая технологии четвертой промышленной революции (Индустрия 4.0) [5, 6].

“Индустрия 4.0” [7], как правило, представляет собой непрерывную автоматизацию традиционных производственных и промышленных процессов, включая исследовательскую обработку данных, с использованием новых интеллектуальных технологий, таких как автоматизация машинного обучения. Таким образом, для интеллектуального анализа этих данных и разработки соответствующих реальных приложений алгоритмы машинного обучения являются ключевыми.

Различают два типа обучения. Обучение по прецедентам, или индуктивное обучение, основано на выявлении общих закономерностей по частным эмпирическим данным. Дедуктивное обучение предполагает формализацию знаний экспертов и их перенос в компьютер в виде базы знаний. Дедуктивное обучение принято относить к области экспертных систем, поэтому термины машинное обучение и обучение по прецедентам можно считать синонимами [8].

Целью машинного обучения является частичная или полная автоматизация решения сложных профессиональных задач в самых разных областях человеческой деятельности. Машинное обучение позволяет решать задачи классификации, регрессии, прогнозирования, фильтрации, кластеризации.

Машинное обучение может применяться для решения широкого спектра задач, включая медицинскую диагностику, биоинформатику и химическую информатику, обнаружение мошенничества с кредитными картами, анализ фондового рынка, классификацию последовательностей ДНК, распознавание речи и рукописного ввода, распознавание объектов в компьютерном зрении, игры, передвижение роботов и в том числе для решения геодезических задач [9,10].

Применение машинного обучения в прогнозировании ионосферы может открыть новое направление в данной сфере и новый метод оценки ионосферных задержек без привязки к ионосферным моделям.

Материалы и методы

Основной алгоритм работы с машинным обучения заключается в решении ряда задач. В первую очередь необходимо подобрать алгоритм машинного обучения. Далее выполняется подбор параметров для обучения. Выбираемые параметры должны каким-либо образом характеризовать прогнозируемую величину, в нашем случае ПЭС. Также в обучающие данные включаются и величины прогнозируемого параметра. Далее собранные данные собираются в отдельный массив, который используется в дальнейшем для обучения модели. После формирования массива данных выполняется обучение модели на основе собранных данных с использованием выбранного алгоритма обучения. Обученная модель сохраняется в отдельный файл в формате .sav. Используя файл обученной модели, можно выполнить прогнозирование ПЭС, для этого необходим массив данных, включающий такие же параметры, как и при обучении, за исключением прогнозируемого параметра, но на даты, на которые выполняется прогноз.

Для описанного выше подхода. Разработка проводилась в интегрированной среде Pycharm [11] на языке программирования Python [12]. В основу разработки легла бесплатная библиотека scikit-learn [13].

В качестве параметров обучения выбраны индекс солнечной активности и поток радиоизлучения с длиной волны 10.7 см (Kp, f107) высота слоя F2 ионосферы и критическая частота слоя F2 (hmF2, foF2), вычисляемые зенит и азимут на солнце, данные о моменте наблюдений (Год, время, день в году). Эти параметры необходимы как для обучения, так и для прогноза, однако для обучения также необходимы и значения ПЭС, которые полученные путем интерполяции финальной ионосферной сетки IGS в формате IONEX. Все параметры получены на промежуток в 5 лет начиная с 01.01 2016 по 31.12.2020 года. Все параметры, а также источники от куда они получены приведены в таблице 1.

Таблица 1

Данные обучения и их источники

№	Параметр	Источник
1	Kp	Omni [14]
2	foF2	Измиран[15]
3	hmF2	Измиран
4	F10.7	Omni
5	ПЭС	IGS[16]
6	Зенит на солнце	Вычислены
7	Азимут на солнце	Вычислены
8	Год	-
9	Время	-
10	День в году	-

Правильность выбора параметров подтверждается выполненным тестом важности параметров (рис. 1). По результатам теста видно, что в целом все параметры оказывают значительное влияние на точность прогноза. Исключением являются только Kp индекс, время и год. Такой вывод можно сделать и из анализа кумулятивной выборочной дисперсии (рис. 2), из которого видно, что 6 из 9 параметров полностью объясняют дисперсию данных. Однако было решено не исключать эти параметры из модели обучения, поскольку даже эти параметры могут, хоть и незначительно, но повысить точность модели, не оказав влияния на производительность.

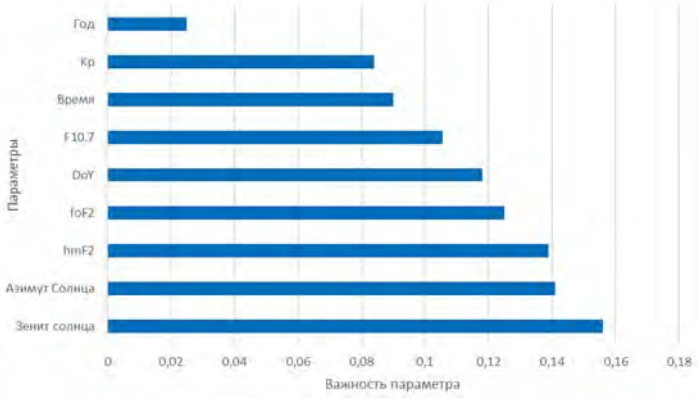

Рис. 1. Оценка важности параметров

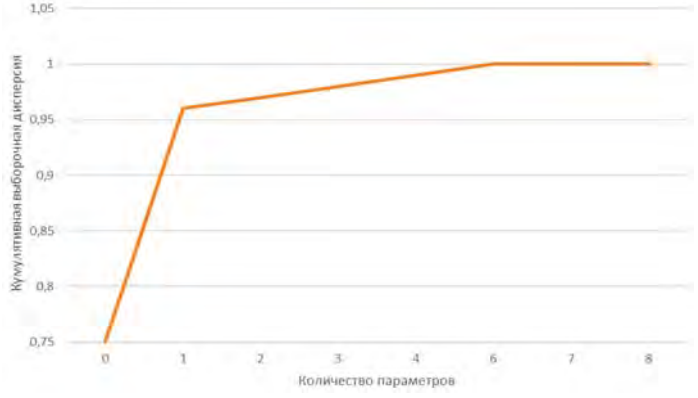

Рис. 2. Анализ кумулятивной выборочной дисперсии

В качестве метода машинного обучения выбран алгоритм Random Forest. Random forest или случайный лес это классификатор ансамбля, который создает несколько деревьев решений, используя случайно выбранное подмножество обучающих выборок и переменных [17,18].

Деревья решений или древовидные модели включает в себя рекурсивное разбиение набора данных на две группы на основе определенного критерия до тех пор, пока не будет выполнено заранее определенное условие остановки. В нижней части деревьев решений находятся так называемые листовые узлы или листья.

Рисунок 3 иллюстрирует рекурсивное разбиение двумерного входного пространства с выровненными по оси границами, то есть каждый раз, когда входное пространство разбивается в направлении, параллельном одной из осей.

Здесь первое разделение произошло при x2 ≥ a2. Затем два подпространства были снова разделены: Левая ветвь была разделена на x1 ≥ a4. Правая ветвь была сначала разделена на x1 ≥ a1, а одна из ее ответвлений была разделена на x2 > a3. Рисунок 4 представляет собой графическое представление подпространств, разделенных на рисунке 3.

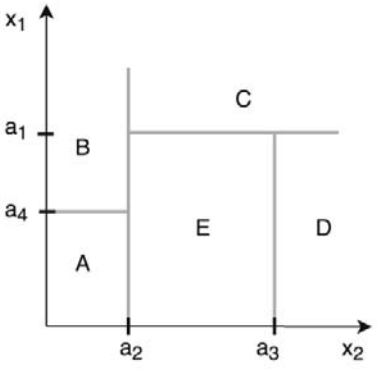

Рис. 3. Рекурсивное двоичное разбиение двумерных подпространств

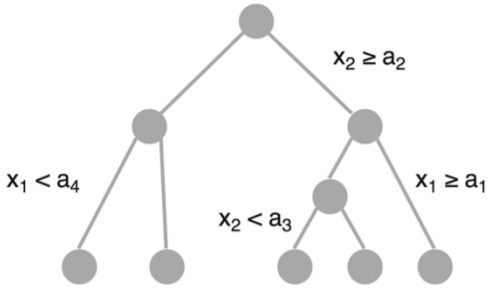

Рис. 4. Графическое представление дерева решений на рисунке 3

В зависимости от того, как заданы критерии разделения и остановки, деревья решений могут быть спроектированы как для задач классификации (категориальный результат, например, логистическая регрессия), так и для задач регрессии (непрерывный результат). Как для задач классификации, так и для задач регрессии подмножество переменных-предикторов, выбранных для разделения внутреннего узла, зависит от заранее определенных критериев разделения, которые сформулированы как задача оптимизации. Общим критерием разделения в задачах классификации является энтропия, которая является практическим применением теоремы Шеннона [19] о исходном кодировании, которая определяет нижнюю границу длины битового представления случайной величины. В каждом внутреннем узле дерева решение энтропии задается формулой:

$$E = -\sum_{i=1}^{c} p_i \log(p_i) \quad (1)$$

где c - количество уникальных классов, а p_i - априорная вероятность каждого данного класса. Это значение максимизируется, чтобы получить максимальную информацию при каждом разделении дерева решений. Для задач регрессии обычно используемым критерием разделения является среднеквадратичная ошибка в каждом внутреннем узле.

Недостатком деревьев решений является то, что они подвержены переобучению, это означает, что модель слишком точно следует особенностям тестового набора данных и плохо работает с новым набором данных. Переобучение деревьев решений приводит к низкой общей точности прогнозирования. Одним из способов повысить точность прогнозирования является рассмотрение только подмножества наблюдений и построение множества отдельных деревьев. Впервые представленная [20], эта идея метода случайного подпространства была позже расширена и официально представлена Брейманом [21] как случайный лес. Модель случайного леса представляет собой алгоритм обучения на основе ансамбля деревьев; то есть алгоритм усредняет прогнозы по множеству отдельных деревьев. Отдельные деревья строятся на основе так называемых bootstrap выборок, а не на исходном образце.

Метод bootstrap заключается в следующем. Пусть имеется выборка X размера N. Равномерно возьмем из выборки N объектов с возвращением. Это означает, что мы будем N раз выбирать произвольный объект выборки (считаем, что каждый объект «достается» с одинаковой вероятностью $\frac{1}{N}$) причем каждый раз мы выбираем из всех исходных N объектов. Можно представить себе мешок, из которого достают шарики: выбранный на каком-то шаге шарик возвращается обратно в мешок, и следующий выбор опять делается равновероятно из того же числа шариков. Отметим, что из-за возвращения среди них окажутся повторы. Обозначим новую выборку через X. Повторяя процедуру M, сгенерируем M подвыборок $X_1, \dots, X_M$. Теперь мы имеем достаточно большое число выборок и можем оценивать различные статистики исходного распределения.

Отдельные деревья решений легко поддаются интерпретации, но эта интерпретируемость теряется в случайных лесах, поскольку многие деревья решений агрегируются. Однако, в обмен на это, случайные леса часто намного лучше справляются с задачами прогнозирования. Кроме того, лес решений имеет ряд преимуществ, основными из которых является быстрая скорость обучения и прогнозирования, возможность работы с большими объёмами данных, а также возможность работы с любыми видами и форматами данных без необходимости их масштабирования. Все эти преимущества делают данный метод идеальным для решения задачи по прогнозирования полного электронного содержания ионосферы.

После выбора данных и метода обучения необходимо подобрать конфигурацию гиперпараметров или выполнить настройку модели для наилучшего результата моделирования и прогноза. Подбор выполняется методом перебора различных конфигураций с различными гиперпараметрами и выбора наиболее оптимальных. Анализу подвергались следующие гиперпараметры:

1. n_estimators – число «деревьев» в «случайном лесу».
2. max_features – число признаков для выбора расщепления.
3. max_depth – максимальная глубина деревьев.
4. min_samples_split – минимальное число объектов, необходимое для того, чтобы узел дерева мог бы расщепиться.
5. min_samples_leaf – минимальное число объектов в листьях.
6. bootstrap – использование для построения деревьев подвыборки с возвращением.

На рисунке 5 представлены результаты перебора различных конфигураций. По полученным данным видно, что значения гиперпараметров не значительно влияют на качество модели, что позволяет сделать акцент на производительность модели.

Далее выполнено обучение модели. Для этого собранные данные за пять лет собираются в единый файл формата .csv. Полученный файл был разделен на данные, предназначенные для обучения и проверочные данные, на основе которых выполнялось исследование результатов прогнозирования в соотношении 0.8 к 0.2 соответственно.

Модель была обучена на данных за четыре года, в результате чего модель сформировала лес деревьев решений. Полученный лес деревьев представляет собой довольно большое количество связанных между собой деревьев решений. Отдельное дерево полученного леса представлено на рисунке 6.

По полученной обученной модели сделан прогноз значений ПЭС на период с 20 января по 31 декабря 2020 года. Для прогнозирования в алгоритм были загружены файл обученной модели в формате .sav и файл с массивом данных тестовой выборки, включающий в себя все вышеперечисленные параметры, за исключение ПЭС, за период с 20.01.2020 по 31.12. 2020. Далее запускается прогнозирование, в результате которого модель на основе выявленных в результате обучения закономерностей и заданных параметров определяет значения ПЭС и выводит их в отдельный массив данных. Вывод результатов прогнозирования проводился в файлы формата .csv.

Результаты

По результатам прогнозирования получены ПЭС на период с 20.01.2020 по 31.12. 2020. На рисунках 7-8 представлено сравнение истинных значений ПЭС с прогнозируемыми. За истинные значения приняты значения ПЭС из тестовой выборки, полученные путём интерполяции финальной ионосферной сетки IGS в формате IONEX. Видно, что прогнозируемые значения ПЭС совпадают с истинными значениями с небольшими отклонениями.

Рассмотрим СКП прогнозируемых значений ПЭС на каждый месяц прогнозирования. СКП рассчитывалась на основе разницы прогнозируемых значений и истинных значений, за которые были приняты значения ПЭС из тестовой выборки. При расчёте СКП, погрешности исходных данных, а именно данных IGS IONEX, не учитывались.

Рассматривая полученные СКП (рис. 9), можно заметить явную зависимость точности прогноза от дальности прогнозирования. В январе СКП прогноза составила 0.47 TECU, когда в ноябре и декабре СКП составляет уже 1.38 и 1.14 TECU. Это объясняется в первую очередь 11-летней цикличностью солнечной активности [22]. Данные, используемые для обучения, попадают в 24 цикл солнечной активности, когда прогноз выполняется на период начала 25 цикла. По данным SWPC видно [23], что в январе 2020 года месячный индекс F10.7 составляет $72.3 \cdot 10^{-22}\, W \cdot m^{-2} \cdot Hz^{-1}$, а в декабре уже $87.3 \cdot 10^{-22}\, W \cdot m^{-2} \cdot Hz^{-1}$.

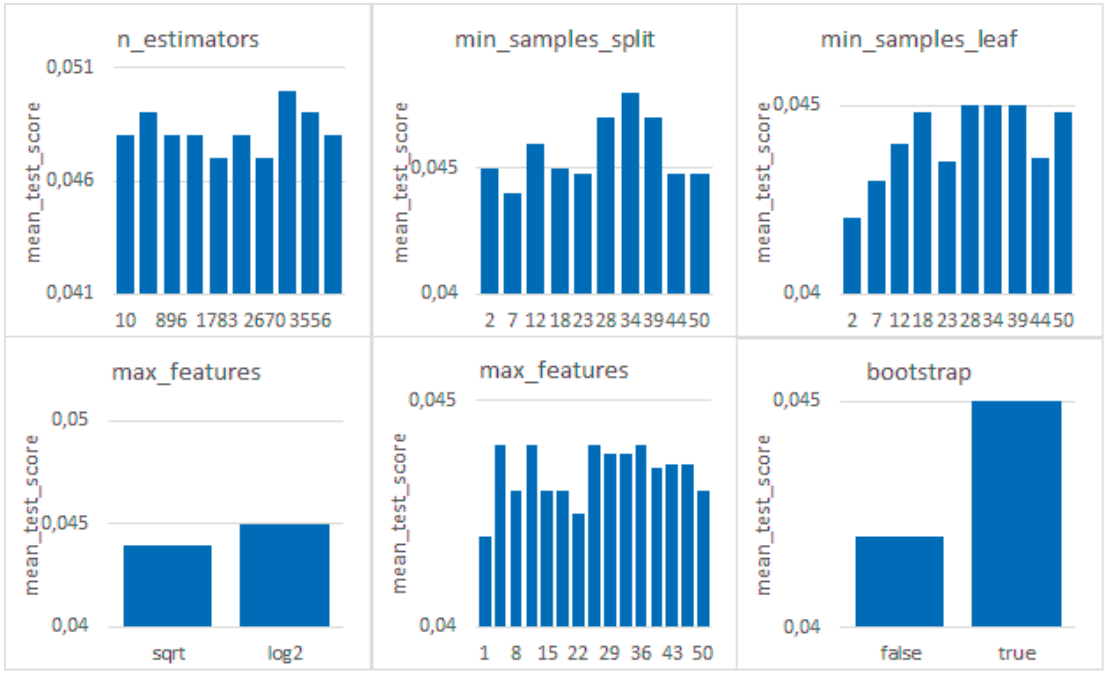

Рис. 5. Результаты перебора конфигураций геперпараметров

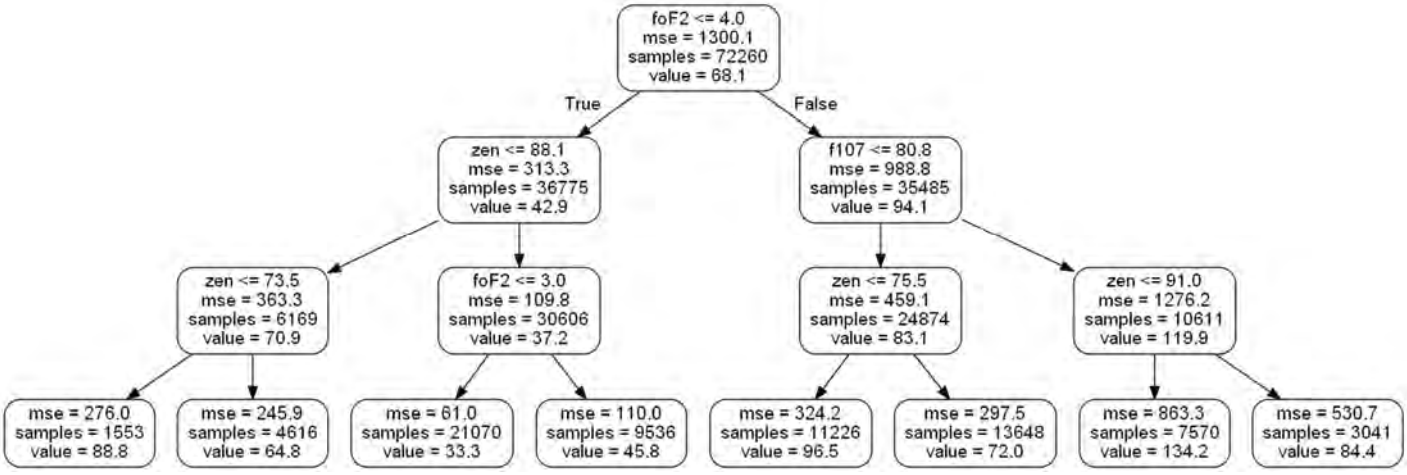

Рис. 6. Отдельное дерево решений

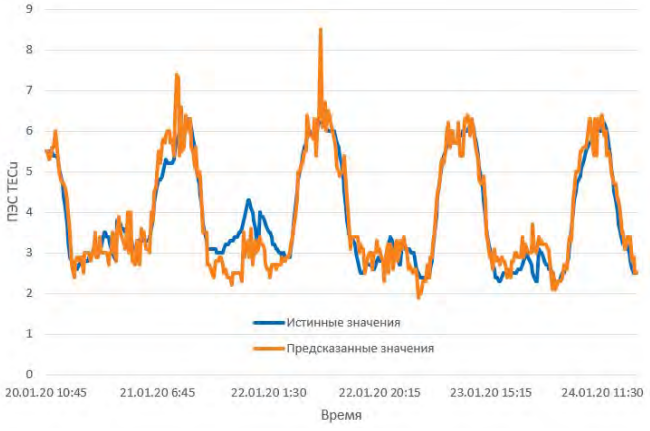

Рис. 7. Сравнение измеренных и прогнозируемых ПЭС

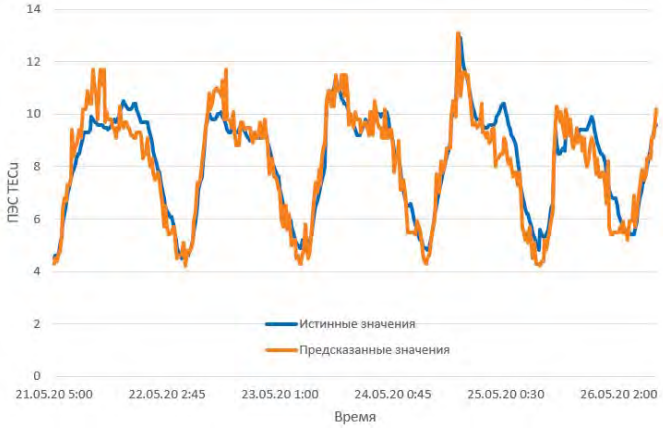

Рис. 8. Сравнение измеренных и прогнозируемых ПЭС

Соответственно обученная модель не может учесть изменения ПЭС, вызванные 11-летней цикличностью солнечной активности.

Также, поскольку модель обучалась на данных до января 2020 года, чем дальше от этой даты выполняется прогноз, тем более устаревшими становятся данными обучения. По этой причине точность прогноза на более удалённые даты значительно уменьшается.

Рис. 9. СКП прогноза ПЭС

Рассмотрим также относительную ошибку полученного прогноза. На рисунке 10 представлены средние относительный ошибки прогноза за каждый месяц в процентах. Из графика видно, что в целом относительная ошибка составляет не более 10% от абсолютного значения ПЭС. Исключением является ноябрь и декабрь, по тем же причинам связанными с устареванием данных обучения и 11-летней цикличностью. Вторым исключением является май и июнь в которые наблюдается наименьшая относительная ошибка. Это связано с большими абсолютными значениями ПЭС в эти месяцы из-за повышенной солнечной активности.

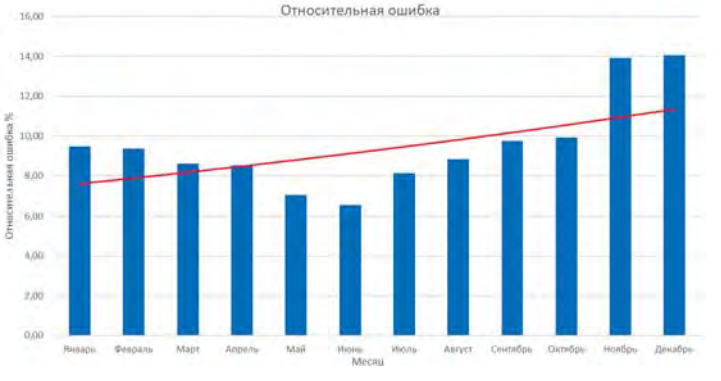

Рис. 10. Относительная ошибка прогноза ПЭС

Обсуждение результатов

В результате выполненных исследований, получена модель на основе алгоритма машинного обучения Random Forest способная выполнять прогнозирование полного электронного содержания с относительной погрешностью менее 10%.

В результате эксперимента также получена оценка точности прогноза ПЭС на каждый месяц 2020 года (табл. 2). Полученные результаты следует сравнить с другими средствами моделирования и прогнозирования ионосферы. На данный момент это ионосферные модели, используемые глобальными навигационными системами GPS, Глонасс, Galileo и другие более точные модели ионосферы. В статье [24] авторы получили относительную ошибку для моделей NeQuick (Galileo) и Klobuchar (GPS) порядка 30-36%. Относительная ошибка модели IGS-GIM составила 16%, а для MODIP-GIM порядка 4-5%. В работе [25] авторы приводят относительную ошибку для модели Klobuchar 8-11%, для модели BDGIM (Beidou) 4-8% и для модели NTCM-BC порядка 4%.

Сравнивая полученные данные прогнозирования с приведенными выше точностями ионосферных моделей видно, что прогнозирование ПЭС на основе машинного обучения соответствует по точности моделям Klobuchar и Nequick, а при прогнозировании на небольшой промежуток времени вперёд может достигать точности сравнимую с моделью BDGIM.

Таблица 2

Результаты оценки точности обученной модели

Месяц	СКО (TECU)	%	Месяц	СКО (TECU)	%
Январь	0,47	9,48	Июль	0,75	8,12
Февраль	0,58	9,37	Август	0,82	8,81
Март	0,64	8,59	Сентябрь	0,71	9,75
Апрель	0,66	8,53	Октябрь	0,85	9,91
Май	0,73	7,07	Ноябрь	1,38	13,91
Июнь	0,68	6,56	Декабрь	1,14	14,06

Заключение

На данный момент разработанная модель прогнозирования ПЭС позволяет получить значения ПЭС на довольно продолжительное время вперед с точность сопоставимой с точность моделей Klobuchar и NeQuick. Однако модель требует дальнейшего расширения объёма данных, расширения временных промежутков данных обучения и перехода к пространственному прогнозу ПЭС.

Подобная модель на основе машинного обучения может в дальнейшем использоваться для передачи данных в системах радиолокации и радиосвязи для уменьшения влияния ионосферных эффектов. Текущие результаты могут быть использованы как основа для создания новых усовершенствованных моделей. Кроме того, применение данного подхода к прогнозированию ионосферы может позволить прогнозировать параметры ионосферы для больших областей, и строить ионосферные карты на часы и дни вперёд.

Литература

1. *Куприянов А.О., Майоров А.А., Непоклонов В.Б., Давлатов Р.А., Печерица Д.С., Морозов Д.А.* Оценка влияния инструментальных погрешностей навигационного приемника на точность определения параметров ионосферы // Известия вузов «Геодезия и аэрофотосъемка» 2015. №6. С. 31-35.

2. *Куприянов А.О., Морозов Д.А.* Экспериментальный мониторинг ионосферы с применение мультисистемой ГНСС-аппаратуры // Известия вузов «Геодезия и аэрофотосъемка» 2016. №1. С. 29-33.
3. *Куприянов А.О., Тихонов В.В., Морозов Д.А., Перминов А.Ю.* Оперативный мониторинг параметров ионосферы в локальной области по результатам мультичастотных ГНСС-измерений // Изв. вузов «Геодезия и аэрофотосъемка». 2018. Т. 62. № 6. С. 616-623. DOI: 10.30533/0536-101X-2018-62-6-616-623
4. *Sarker I.H.* Ai-driven cybersecurity: an overview, security intelligence modeling and research directions // SN Comput Sci. 2021.
5. Sarker I.H., Hoque M.M., MdK Uddin, Tawfeeq A. Mobile data science and intelligent apps: concepts, ai-based modeling and research directions // Mob Netw Appl. C. 1-19, 2020.
6. *Sarker I.H., Kayes ASM, Badsha S., Alqahtani H., Watters P., Ng A.* Cybersecurity data science: an overview from machine learning perspective // J Big Data. 2020. №7(1). С. 1-29.
7. *Sarker I.H., Watters P., Kayes ASM. E Ślusarczyk B.* Industry 4.0: Are we ready? // Polish J Manag Stud. №17, 2018.
8. [Электронный ресурс]// URL: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение (дата обращения: 01.08.2022)
9. *Колесников А.А., Кикин П.М, Комиссарова Е.В., Касьянова Е.Л.* Использование технологий машинного обучения при решении геоинформационных задач. // ИНТЕРКАРТО. ИНТЕРГИС. №2. 2018. С. 371-384.
10. *Omid Memarian Sorkhabi.* Deep learning in geodesy // Computer sciences. 2021. URL: https://doi.org/10.21203/rs.3.rs-446466/v2
11. URL: https://www.jetbrains.com/pycharm/ (дата обращения: 01.08.2022)
12. URL: https://www.anaconda.com/products/individual (дата обращения: 01.08.2022)
13. URL: https://scikit-learn.org/stable/index.html (дата обращения: 01.08.2022)
14. URL: https://omniweb.gsfc.nasa.gov/ (дата обращения: 01.08.2022)
15. URL: https://izmiran.ru/ionosphere/moscow/text/ (дата обращения: 01.08.2022)
16. *Stefan Schaer, Werner Gurtner.* IONEX: The IONosphere Map EXchange Format Version 1.1. URL: http://ftp.aiub.unibe.ch/ionex/draft/ionex11.pdf
17. *Ho, Tin Kam.* Random Decision Forests // 3rd International Conference on Document Analysis and Recognition. Montreal. QC. 2016. С. 278-282.
18. *Breiman, L., Friedman, J., Stone, C. J., and Olshen, R. A.* Classification and Regression Trees // Boca Raton, FL: CRC press. URL: https://doi.org/10.1201/9781315139470
19. *Shannon C. E.* A mathematical theory of communication // ACM SIGMOBILE Mobile Computing and Communications Review 5. 2001. С. 3-55.
20. *Ho, T. K.* Random decision forests // 3rd International Conference on Document Analysis and Recognition. 1995. С. 278-282. Piscataway, NJ: IEEE.
21. *Breiman L.* Random forests // Machine Learning. №45. С. 5-32. 2 .
22. *Azad A. Mansoori, Parvaiz A. Khan, Purushottam Bhawre, A. K. Gwal, P. K. Purohit.* Variability of TEC at mid latitude with solar activity during the solar cycle 23 and 24 2013 // IEEE International Conference on Space Science and Communication (IconSpace). 2013. Melaka. Malaysia.
23. URL: https://www.swpc.noaa.gov/products/solar-cycle-progression.
24. *Rovira-Garcia A., Juan J.M., Sanz J., Gonz´alez-Casado G., Ib´a˜nez D.* Accuracy of Ionospheric Models used in GNSS and SBAS: Methodology and Analysis // Journal of Geodesy. № 90. С. 229-240. 2016
25. *Chao Yang, Jing Guo , Tao Geng , Qile Zhao, Kecai Jiang, Xin Xie and Yifei Lv.* Assessment and Comparison of Broadcast Ionospheric Models: NTCM-BC, BDGIM, and Klobuchar // Remote Sens. № 12. С. 1215. 2020.

PREDICTION OF THE TOTAL ELECTRONIC CONTENT OF THE IONOSPHERE BASED ON MACHINE LEARNING ALGORITHMS

DMITRII ZAMOGILNYI
Moscow, Russia, dmt.zam@gmail.com

KEYWORDS: *total electron content, GNSS, ionosphere, machine learning, random forest.*

ABSTRACT

Introduction. The paper presents and describes the technology of applying the machine learning algorithm in predicting the vertical total electron content of the ionosphere. The ionospheric error is one of the most significant sources of pseudorange measurement errors from GNSS signals. Increasing every year requirements for the accuracy of positioning and navigation by GNSS signals leads to the need to develop new methods to reduce the impact of various measurement errors, including the ionospheric error. At present, ionospheric models of various types are used for ionospheric correction of measurements. The currently widely used ionospheric models do not allow a significant increase in the accuracy of positioning based on GNSS signals. At the moment, the creation of a new effective method for modeling and forecasting the ionosphere that meets modern requirements for positioning accuracy is an important and urgent task. **The purpose of this work** is to create a methodology for modeling and predicting the total electron content of the ionosphere using machine learning algorithms. Machine learning is currently a fairly common and popular method for solving problems of classification, recognition and prediction. **The method** has been used for many years in medicine, robotics, industry, finance and many other branches of modern science and economics. To achieve this goal, it is necessary to solve a number of tasks. First of all, you need to select and collect data for training the model, then you need to select a machine learning method and hyperparameters for the selected method. Next, it is necessary to perform TEC prediction based on the trained model and evaluate the accuracy of the results obtained. comparison of the obtained results with the accuracy of other existing models It is shown that machine learning does a good job of predicting full electronic content. **The resulting** trained model makes it possible to obtain a forecast with an accuracy comparable to the accuracy of the Klobuchar, NeQuick models, and in some cases much more accurate.

REFERENCES

1. Kupriyanov A.O., Majorov A.A., Nepoklonov V.B., Davlatov R.A., Pecherica D.S., Morozov D.A. Ocenka vliyaniya instrumental'nyh pogreshnostej navigacionnogo priemnika na tochnost' opredeleniya parametrov ionosfery. *Izvestiya vuzov "Geodeziya i aerofotosemka".* 2015. No.6, pp. 31-35.

2. Kupriyanov A.O, Morozov D.A. Investigational ionosphere monitoring using multisystnm GNSS equipment. *Izvestiya vuzov "Geodeziya i aerofotosemka".* 2016. No.1, pp. 29-33.

3. Kupriyanov A.O., Tikhonov V.V., Morozov D.A., Perminov A.Y. Operational monitoring of the parameters of the ionosphere in the local area using the results of multifrequency GNSS-measurements. *Izv. vuzov "Geodeziya i aerofotos"emka"*. 2018. Vol. 62. No. 6, pp. 616-623. DOI: 10.30533/0536-101X-2018-62-6-616-623

4. Sarker I.H. Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Comput Sci*. 2021.

5. Sarker I.H., Hoque M.M., MdK Uddin, Tawfeeq A. Mobile data science and intelligent apps: concepts, ai-based modeling and research directions. *Mob Netw Appl,* pp. 1-19, 2020.

6. Sarker I.H., Kayes ASM, Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. *J Big Data*. 2020. No. 7(1), pp.1-29.

7. Sarker I.H., Watters P, Kayes ASM. Elusarczyk B. Industry 4.0: Are we ready? *Polish J Manag Stud*. No.17, 2018.

8. URL: http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение (accessed:: 01.08.2022).

9. Kolesnikov A.A., Kikin P.M., Komissarova E.V., Kasyanova E.L. The use of machine learning technologies in solving geoinformatic problems. Interkarto. Interdis. No. 2. 2018, pp. 371-384.

10. Omid Memarian Sorkhabi Deep learning in geodesy// Computer sciences. 2021. URL: https://doi.org/10.21203/rs.3.rs-446466/v2

11. URL: https://www.jetbrains.com/pycharm/ (accessed: 01.08.2022).

12. URL: https://www.anaconda.com/products/individual (accessed: 01.08.2022).

13. URL: https://scikit-learn.org/stable/index.html (accessed: 01.08.2022).

14. URL: https://omniweb.gsfc.nasa.gov/ (accessed: 01.08.2022)

15. URL: https://izmiran.ru/ionosphere/moscow/text/ (accessed: 01.08.2022).

16. Stefan Schaer, Werner Gurtner IONEX: The IONosphere Map EXchange Format Version 1.1 URL: http://ftp.aiub.unibe.ch/ionex/draft/ionex11.pdf (accessed: 01.08.2022).

17. Ho, Tin Kam. Random Decision Forests. *3rd International Conference on Document Analysis and Recognition*. Montreal. QC, 1995, pp. 14-1.

18. Breiman L., Friedman J., Stone C. J., Olshen R. A. Classification and Regression Trees. *Boca Raton, FL: CRC press*. URL: https://doi.org/10.1201/9781315139470.

19. Shannon C. E. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review 5*. 2001, pp. 3-55.

20. Ho T. K. Random decision forests. *3rd International Conference on Document Analysis and Recognition*. IEEE. 1995, pp. 278-282.

21. Breiman L. Random forests.*Machine Learning*. No.45, pp. 5-32. 2001.

22. Mansoori A.A., Khan P.A., Bhawre Purushottam, Gwal A. K., Purohit P. K. Variability of TEC at mid latitude with solar activity during the solar cycle 23 and 24 2013. *IEEE International Conference on Space Science and Communication (IconSpace)*. 2013. Melaka. Malaysia.

23. URL: https://www.swpc.noaa.gov/products/solar-cycle-progression. (accessed: 01.08.2022).

24. Rovira-Garcia A., Juan J.M., Sanz J., Gonzalez-Casado G., Ibanez D. Accuracy of Ionospheric Models used in GNSS and SBAS: Methodology and Analysis. *Journal of Geodesy*. No. 90, pp. 229-240. 2016.

25. Chao Yang, Jing Guo, Tao Geng, Qile Zhao, Kecai Jiang, Xin Xie and Yifei Lv Assessment and Comparison of Broadcast Ionospheric Models: NTCM-BC, BDGIM, and Klobuchar. *Remote Sens*. No. 12. P. 1215. 2020.

INFORMATION ABOUT AUTHOR:

Dmitrii Zamogilnyi, Lecturer of the Department of Applied Geodesy of the Moscow State University of Geodesy and Cartography, Moscow, Russia

For citation: Zamogilnyi D. Prediction of the total electronic content of the ionosphere based on machine learning algorithms. H&ES Reserch. 2022. Vol. 14. No 4. P. 39-46. doi: 10.36724/2409-5419-2022-14-4-39-46 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-47-53

ПОСТКВАНТОВЫЕ АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ИХ ИСПОЛЬЗОВАНИЕ В РАСПРЕДЕЛЕННОМ РЕЕСТРЕ

МОСКВИН
Владимир Сергеевич[1]

БОГАТЫРЕВ
Владимир Анатольевич[2]

АННОТАЦИЯ

Введение. Блокчейн является современной, широко распространенной, активно развивающейся технологией.Блокчейн наиболее востребован и распространен в финансовых технологиях и инструментах банковской и биржевой сферы, активно внедряется в государственном секторе, в торговле, производстве, здравоохранении, общественных и социальных услугах. Создание систем на основе технологии блокчейн является перспективным направлением современных исследований и разработок. Блокчейн – это надежный и безопасный способ хранения данных о транзакциях, предоставляющий возможности проверки целостности. Сегодня технология блокчейн широко распространена во всем мире, во многих сферах жизнедеятельности. В статье рассмотрены сущности и характеристики постквантовых алгоритмов электронной подписи на основе алгебраических решеток. **Цель** данной работы – изучение и сравнение основных характеристик существующих алгоритмов постквантовой цифровой подписи, оценка применимости в технологии блокчейн. **Научная новизна** работы состоит в применении новой методики оценки к алгоритмам цифровой подписи, применительно к использованию для технологии распределенного реестра, в дополнение к сравнительному анализу. **Результаы исследований.** Проведен сравнительный анализ алгоритмов по условным и безусловным критериями. Определены преимущества и недостатки существующих криптографических алгоритмов, принципы и специфика функционирования технологии блокчейн, а так же возможность применения постквантовых алгоритмов при формировании подписи блоков.

Сведения об авторах:

[1] аспирант, ФГБОУ ВПО "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики", moskvin.kvant@gmail.com

[2] профессор, доктор технических наук, ФГБОУ ВПО "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики"

КЛЮЧЕВЫЕ СЛОВА: *постквантовая криптография, защита информации, блокчейн, CRYSTHAL-DILITHIUM, FALCON, qTesla, электронная подпись, сравнительный анализ.*

Для цитирования: Москвин В.С., Богатырев В.А. Постквантовые алгоритмы электронной цифровой подписи и их использование в распределенном реестре // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 47-53. doi: 10.36724/2409-5419-2022-14-4-47-53

Введение

Блокчейн (block chain – цепь из блоков) является современной, широко распространенной, активно развивающейся технологией. Универсальность и надежность технологии позволяет применять ее повсеместно, в различных сферах жизнедеятельности [1]. Блокчейн наиболее востребован и распространен в финансовых технологиях и инструментах банковской и биржевой сферы, активно внедряется в государственном секторе, в торговле, производстве, здравоохранении, общественных и социальных услугах [2]. Хранение данных в блокчейне, в децентрализованной и распределенной сети, называемой распределенный реестр, обеспечивает высокий уровень доверия и надежности [3, 4].

Технология блокчейн позволяет создавать прозрачную, децентрализованную, экономичную среду, в которой каждая транзакция может быть проверена, а журналы аудита могут быть доступны для проверки всем участникам.

Блокчейн использует электронные цифровые подписи для аутентификации транзакций и подписания выпущенных блоков. Для того, чтобы успешно выполнить транзакцию, пользователь должен предоставить доказательство, что он обладает правом выполнять транзакции с объектом. Каждый узел в распределенной сети проверит отправленную транзакцию, электронную подпись и согласует результаты выполнения с остальными узлами сети.

Критичным составным элементом, гарантирующим безопасность блокчейна, является электронная цифровая подпись. Надежность наиболее распространенных в настоящее время схем цифровой подписи основана на ограничении вычислительной мощности классического компьютера при выполнении некоторых математических операций, таких как факторизация больших целых чисел или вычисление дискретного логарифма больших целых чисел. Появление мощных суперкомпьютеров и квантовых компьютеров поставило под угрозу безопасность классического шифрования. Развитие науки привело к созданию новых схем цифровой подписи, поскольку основные используемые в настоящее время, RSA и ECDSA, не являются квантовоустойчивыми..

Целью данной работы является изучение и сравнение основных характеристик существующих алгоритмов постквантовой цифровой подписи, оценка применимости в технологии блокчейн.

Научная новизна работы состоит в применении новой методики оценки к алгоритмам цифровой подписи, применительно к использованию для технологии распределенного реестра, в дополнение к сравнительному анализу.

Обзор проблемы постквантовой криптографии

Появление квантового компьютера достаточной мощности, способно фундаментально повлиять на способы решения некоторых вычислительных задач. Квантовые вычисления будут угрожать общепринятым, широко распространенным криптографическим алгоритмам, ставя под угрозу протоколы связи, алгоритмы аутентификации, схемы цифровых подписей и неизменность записей распределенного реестра, об этом утверждается во многих статьях [5-10].

Квантовые компьютеры целенаправленно исследуются и создаются субъектами национальных государств для взлома современной криптографии, возникновение угроз системам на основе технологии блокчейн – лишь вопрос времени [11].

Угроза применения квантового компьютера для атаки на систему, работающую на основе технологии блокчейн, ставит под вопрос основные достоинства технологии – неизменность, необратимость, безопасность и надежность. Именно благодаря этим качествам, технология блокчейн вызывает доверие. Нарушение ключевых принципов, на которых построен, например, весь рынок криптовалют, вызовет каскадный финансовый эффект. Согласно Block Research, “Общая капитализация крипторынка в 2021 году также достигла рекордных 3 трлн долларов после повторного пересечения 1 трлн долларов в январе и 2 трлн долларов в мае” [12], что наглядно демонстрирует глобальную ценность технологии блокчейн.

По результатам исследований Института Хадсона, успешная атака на криптовалюту, такую как биткоин, с применением квантового компьютера, будет иметь разрушительные последствия для владельцев криптовалют [13]. Последствия такой атаки могут привести к краху экономики в целом, из-за высокого уровня капитализации рынков, связанных с технологией блокчейн. Для систем, построенных на основе технологии блокчейн, критически важно применить квантовоустойчивые криптографические алгоритмы.

Квантовый компьютер работает иначе, чем классические компьютеры, которые широко распространены и активно используются сегодня. Работа квантового компьютера основана на процессах квантовой природы, таких как квантовая запутанность и квантовый параллелизм. В отличие от классического процессора, квантовый процессор может находиться во множестве состояний одновременно и все вычислительные операции применяются ко всем состояниям. При решении определенных задач, такой процессор имеет значительно большую производительность, чем современные классические процессоры [14].

Алгоритмы Шора и Гровера

Одним из примеров таких задач является вычисление дискретных логарифмов и факторизация больших целых чисел. Сложность выполнения таких расчетов лежит в основе надежности и безопасности алгоритмов с открытым ключом ECDSA (цифровая подпись на эллиптических кривых) и RSA (Ривест-Шамир-Адлеман). Использование классических компьютеров для решения таких задач занимает слишком много времени, даже при использовании ферм графических процессоров [15]. Применение алгоритма Шора [16] для нахождения простых множителей целого числа, будет иметь полиномиальную сложность в квантовых компьютерах, а не экспоненциальную, как в классических, что значительно сокращает надежность криптографических алгоритмов [17].

Алгоритм Гровера [16] сокращает пространство поиска симметричных ключей и хэшей простым перебором, эффективно уменьшая длину ключа при применении алгоритмов, таких как AES (Advanced Encryption Standard), в два раза. Простое решение для борьбы с такой угрозой состоит в

увеличении количества битов, используемых в хеш-функции или алгоритме симметричного шифрования.

Ключевое различие между алгоритмами Гровера и Шора заключается в том, что алгоритм Гровера представляет большую угрозу для криптографического хеширования и хранимых данных, в то время как алгоритм

Шора представляет угрозу средствам аутентификации пользователей и узлов сети распределенного реестра.

Квантовые компьютеры теперь стали научным фактом. Достижения последних двух лет показали, что квантовые компьютеры, достаточно мощные, чтобы превзойти классические компьютеры, могут появиться уже через несколько лет. Используя алгоритм Шора, квантовый компьютер сможет вычислить криптографические ключи, связанные с любым публичным адресом в распределенном реестре, или выполнить атаку посредника (англ. man in the middle), изменив данные при передаче. Реализация таких угроз подорвала бы доверие к технологии, это позволит масштабно взламывать любые узлы и адреса распределенного реестра.

Используя коллизионную атаку с применением алгоритма Гровера, можно легко взломать криптографическое хеширование, используемое в электронных цифровых подписях. Алгоритм Гровера позволяет найти два различных входных сигнала, которые дают одинаковое хэш-значение. Такой метод позволяет выполнить подмену исходных данных, сохранив, при этом, оригинальную цифровую подпись, которая применяется для гарантии защиты от изменения. В результате доверие к системам на основе технологии блокчейн исчезает, поскольку данные могут быть незаметно фальсифицированы.

Сравнительный анализ постквантовых криптографических схем цифровой подписи

Для предотвращения угроз безопасности и целостности данных, связанных с развитием квантовых компьютеров, научное сообщество разрабатывает алгоритмы постквантовой криптографической подписи.

Основные схемы постквантовой подписи можно разделить на следующие категории:

1. риптография, основанная на проблеме декодирования случайного линейного кода;
2. Криптография, основанная на решетках и сложности задачи поиска кратчайшего вектора;
3. Многомерная криптография, основанная на решении многомерных квадратных уравнений;
4. Подписи на основе хэшей, безопасность которых основана на устойчивости криптографических хеш-функций к прообразу и второму прообразу.

На сегодняшний день известно несколько алгоритмов электронной подписи, например такие как: CRYSTALS-Dilithium, FALCON, qTESLA, GeMSS, LUOV, MQDSS, Picnic, Rainbow и SPHINCS+ и др. [18].

Целью этой работы является сравнение трех алгоритмов которые основаны на алгебраических решетках и рассмотрение основных компонентов этих подписей.

В работе предлагается сравнить три подписи по трем параметрам:

– бе опасность/устойчивость,
– технические требования к эксплуатации,
– з щищенность от атак.

Алгоритм цифровой подписи представляет собой набор следующих трех алгоритмов: алгоритма генерации ключей, алгоритм подписания данных и алгоритм проверки подписи.

Цифровые подписи применительно к распределенному реестру могут быть уязвимы к атакам в будущем, так как подписанные данные могут храниться в сети десятки лет, при этом закрытый ключ, которым подписывались данные, невозможно заменить. Это означает, что компрометация такого ключа или цифровой подписи приведет к искажению данных, независимо от того, произойдет это сейчас, или через 10 лет. В таких условиях имеет смысл рассматривать только алгоритмы цифровой подписи, обладающие наивысшим уровнем защищенности. В данной статье рассматриваются только алгоритмы наивысшего, пятого уровня защищенности.

Технические требования к эксплуатации для распределенного реестра это, прежде всего, размер открытого ключа, размер закрытого ключа, размер подписи, скорость генерации ключей, скорость создания подписи, скорость проверки подписи.

К дополнительным характеристикам, учитываемым при оценке алгоритмов цифровой подписи, следует отнести простоту технической реализации алгоритма, объем и сложность программного кода, возможность реализации на малопроизводительных устройствах и другие особенности. Оценка алгоритмов выполнена при помощи сравнительного анализа и специально разработанной модели оценки.

CRYSTALS-Dilithium.

Безопасность / устойчивость: защита алгоритма цифровой подписи Dilithium основывается на сложности поиска кратчайшего вектора решетки. Конструкция Dilithium базируется на парадигме Фиата-Шамира с прерываниями и использует выборку отбраковки для компактности и безопасности. Криптоанализ сводится к решению задач обучения с ошибками в кольце (Module Learning with Errors - MLWE) и задач решения для коротких целых чисел (Module Short Integer Solution – MSIS).

Основная новизна алгоритма Dilithium по мнению авторов заключается в том, что размер открытого ключа сокращается в 2,5 раза за счет увеличения подписи на 150 байт. Так же в целях сокращения времени вычислений и уменьшения размеров ключей и подписей, используется битная упаковка. Чтобы быть более эффективным, Dilithium использует равномерное распределение вместо традиционного распределения Гаусса.

Технико-эксплуатационные требования: Dilithium предлагает достаточно высокую производительность и сравнительно прост для реализации, может быть эффективно реализован на малоресурсных устройствах, имеет небольшой размер ключа.

Защищенность от атак: наиболее эффективные атаки связаны с поиском коротких векторов в некоторых решетках. Самым известным алгоритмом поиска очень коротких ненулевых векторов в евклидовых решетках является алгоритм Block-Korkine-Zolotarev (BKZ), предложен Schnorr и Euchner в 1991 году [19].

Алгоритм Dilithium устойчив к такого рода атакам. Кроме того, стойкость алгоритма доказана в квантовой модели QROM (Quantum Random Oracle Model), в которой атакующий имеет квантовый доступ к случайному оракулу, то есть может запрашивать значения оракула для сообщений в квантовой суперпозиции.

Следует отметить, что существуют и другие атаки, но для данного криптографического алгоритма, атаки с использованием семейства алгоритмов BKW и Arora-Ge [20] не эффективны.

FALCON.

Безопасность/устойчивость: алгоритм Falcon имеет два ключевых составляющих элемента – решетки NTRU и быстрое преобразование Фурье. Стойкость алгоритма основывается на сложности поиска кратчайшего вектора решетки. Криптоанализ сводится к задаче поиска коротких целых чисел (Short Integer Solution – SIS) на NTRU-решетках.

Алгоритм нацелен на высокую эффективность и высокий уровень безопасности. Основная новинка – это очень быстрый рекурсивный алгоритм сэмплирование целых чисел стандартного распределения Гаусса для решеток, который использует структуру данных в виде дерева.

Технико-эксплуатационные требования: алгоритм использует NTRU решетку, характеризуется компактностью и скоростью работы, самую короткую длину ключа и самую высокую скорость проверки [15]. Однако Falcon требует больших затрат на генерацию ключа, поскольку ему приходится решать уравнение NTRU. Алгоритм основан на очень сложных методах дискретизации Фурье и требует арифметики с плавающей запятой, которая не поддерживается многими устройствами, кроме того, значительно усложняется анализ стойкости к атакам по сторонним каналам. Главным недостатком этого алгоритма является сложная программная и аппаратная реализация, недоступность для малоресурсных устройств. Реализация алгоритма в виде программного кода может содержать несколько тысяч строк кода.

Защищенность от атак: сэмплирование стандартного распределения Гаусса гарантирует минимальную утечку информации о секретном ключе вплоть до практически бесконечного количества подписей. Атаки, характерные для алгоритмов на решетках малоэффективны, однако, необходимы доработки алгоритма, для повышения устойчивости к атакам по сторонним каналам.

qTESLA.

Безопасность/Устойчивость: алгоритм qTESLA имеет высокий уровень защиты, основанный на сложности задачи обучения с ошибками в кольце (Ring learning with errors – R-LWE).

Технико-эксплуатационные требования: qTESLA спроектирован так, чтобы его было легко реализовать, и особое внимание уделяется наиболее часто используемым функциям схемы подписи, а именно подписи и проверке. В частности, сэмплирование целых чисел стандартного распределения Гаусса, наиболее сложная часть алгоритма подписи на основе решетки, относится исключительно к генерации ключей. Простая конструкция алгоритма предоставляет возможность выбора уровня безопасности при помощи наборов параметров, не изменяя, при этом компактной реализации алгоритма. Авторская реализация, написанная на языке C и поддерживающая все наборы параметров qTESLA, состоит всего из 300 строк кода.

Защищенность от атак: стойкость алгоритма доказана в квантовой модели QROM (Quantum Random Oracle Model). Более того, алгоритм позволяет выбирать параметры в соответствии с требованиями безопасности и защищенности, таким образом, повышать производительность, при этом сохраняя безопасность на требуемом уровне. qTESLA обеспечивает защиту от атак по времени и по сторонним каналам. Кроме того, он защищен от атак с использованием шифра подстановки [21, 22].

Сравнение рассмотренных алгоритмов

Проведем формальное сравнение характеристик рассмотренных алгоритмов, для этого приведем сводную таблицу, основанную на открытых спецификациях алгоритмов и их реализациях [23, 24, 25]. Измерение производительности выполнялось на компьютере с процессором Intel® Core® i5-8259U с 2.3 GHz при отключенном аппаратном ускорении. Данные о количестве процессорных циклов основаны на опубликованных результатах тестов библиотеки публичных реализаций постквантовой криптографии LIBOQS [26], измерение осуществлялось при помощи выполнения выбранной операции для каждого из алгоритмов, в течение фиксированного времени (10 секунд), результирующий показатель производительности усреднялся.

Таблица 1

Сравнительные характеристики алгоритмов

Алгоритм	Уровень защищенности	Устойчивость (битовая)		Размер в байтах			Количество процессорных циклов		
		Классическая	Квантовая	Закрытый ключ	Открытый ключ	Подпись	Генерация ключей	Подписание	Проверка
Dilithium	5	252	229	4864	2592	4595	**233195**	**445370**	**219604**
Falcon	5	273	248	**1793**	**2305**	**1330**	62556394	1656627	283565
qTesla	5	**284**	**261**	4640	5024	3520	24197000	5688300	990600

Качественное сравнение алгоритмов на основании характеристик выполнено на основании оценки набора алгоритмов с применением весовых коэффициентов.

При оценке характеристик следует учитывать объективный опыт и характеристики существующих распределенных реестров, например, существующая с 2007 года сеть Биткойн достигла общего размера базы в 430 Гб при общем количестве транзакций – более 769 миллионов [27]. Для подписания транзакций в сети Биткойн используется алгоритм ECDSA, размер закрытого ключа – 256 бит, а соответствующего ему открытого ключа – 512 бит, подпись занимает чуть более 70 байт [28]. В среднем в сети обрабатывается от 4 до 7 транзакций в секунду.

Интегральный показатель эффективности рассматриваемых алгоритмов задается на основе среднего линейного отклонения взвешенных значений каждой характеристики. Большее значение означает более высокую оценку в соответствии с

выбранными весовыми коэффициентами. Знак весового коэффициента отвечает за то, влияет ли повышение показателя в положительную или в отрицательную сторону (положительный весовой коэффициент – увеличение значения характеристики положительно влияет на общую оценку алгоритма, отрицательный весовой коэффициент – наоборот).

Оценка выполняется по формуле:

$$S = \frac{\sum_i d_i k_i}{\sum_i |k_i|},$$

где d_i – нормированное отклонение от среднего характеристики с индексом i, вычисляемое по формуле

$$d_i = \frac{x_i - \bar{x}}{\bar{x}},$$

здесь x_i – значение характеристики с индексом i, среднее значение характеристики:

$$\bar{x} = \sum_i x_i,$$

k_i – весовой коэффициент характеристики с индексом i.

С учетом описанных ранее особенностей реализации алгоритмов цифровых подписей с точки зрения применения в распределенном реестре, предложены следующие весовые коэффициенты для характеристик:

1. Для битовой устойчивости, как классической, так и квантовой – коэффициент 1;

2. Для размеров обоих ключей и размера подписи – коэффициент -1;

3. Для ко чества процессорных циклов – коэффициент -1.

По описанным характеристикам приведем финальный вычисленный результат оценки алгоритмов, округленный до трех знаков после запятой:

1. Dilithium получил оценку 0,214, в основном, благодаря высокой скорости генерации, подписания и проверки подписи.

2. Falcon получил оценку 0,132, благодаря минимальным размерам подписи среди всех рассмотренных алгоритмов.

3. qTesla получил оценку -0,346, алгоритм имеет наиболее высокий уровень битовой устойчивости, в остальных характеристиках уступает другим алгоритмам.

Согласно описанной формуле оценки и определенным весовым коэффициентам, алгоритм Dilithium набрал наибольшее количество баллов и признан наилучшим в соответствии с выбранными критериями оценки.

Выводы

На современном этапе развития постквантовых криптографических алгоритмов можно утверждать только о некоторых преимуществах и недостатках алгоритмов, в сравнении с другими алгоритмами, и оценивать возможность их широкого применения в качестве постквантовых стандартов.

В дальнейших исследованиях разработанных криптографических алгоритмов могут быть обнаружены новые уязвимости и новые векторы атак, как с применением классических компьютеров, так и с применением квантовых компьютеров и новых алгоритмов.

На наш взгляд, наиболее проработанным и безопасным алгоритмом является CRYSTALS-Dilithium с более высокими показателями производительности и эффективности.

Эти показатели имеют решающее значение при выборе алгоритма формирования подписи в цепочке блоков распределенного реестра.

Алгоритм Falcon имеет наименьшие размеры ключей и подписей, а также, стандартное распределение Гаусса, используемое в алгоритме, гарантирует минимальную утечку информации. При этом, алгоритм остается уязвимым для атак по сторонним каналам.

Основным преимуществом алгоритма qTesla является использование стандартного распределения Гаусса только во время генерации ключей, что делает алгоритм проще, быстрее и помогает избежать ошибок.

У разработчиков систем на основе технологии блокчейн есть возможность выбрать оптимальные методы защиты от атак квантовых вычислений, применив безопасные алгоритмы постквантовой криптографии. Исследования показали, что выбранные алгоритмы обладают высокой устойчивостью как классических компьютеров, так и квантовых и могут быть использованы в технологии распределенного реестра для обеспечения требуемых уровней безопасности и надежности, повышения уровня доверия к системе.

Литература

1. *Лоран Л.* Блокчейн от А до Я. Все о технологии десятилетия // Бомбора. 2018. С. 19-24.

2. *Тапскотт А., Тапскотт Д.* Технология Блокчейн. То, что движет финансовой революцией сегодня // Эксмо. 2018. С. 53-57.

3. *Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V.* Redundant Servicing of a Flow of Heterogeneous Requests Critical to the Total Waiting Time During the Multi-path Passage of a Sequence of Info-Communication Nodes // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2020. Vol. 12563, pp. 100-112.

4. *Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V.* Redundant multipath service of a flow heterogeneous in delay criticality with defined node passage paths // Journal of Physics: Conference Series. 2021. Vol. 1864. No. 1, pp. 012094.

5. *Шемякина М. А.* Анализ использования квантовых технологий в криптографии // Международный журнал гуманитарных и естественных наук. 2019. №. 5-4. С. 59-62.

6. *Шемякина М. А.* Использование квантовых технологий в информационной безопасности // Modem Science. 2019. № 11-4. С. 281-284.

7. *Борисова Е. В.* Описание базовых математических моделей в квантовой криптографии // Вестник Рязанского государственного радиотехнического университета. 2021. №. 75. С. 113-120.

8. *Суханов Е. Э., Штанг К. С., Алешко Р. А.* Блокчейн и квантовые вычисления // Синергия Наук. 2017. №. 14. С. 547-550.

9. *Киселенко В. А.* Квантовый компьютер как потенциальная угроза стойкости систем криптографической защиты информации // Академический вестник войск национальной гвардии Российской Федерации. 2019. №. 2. С. 60-62.

10. *Ласкус А. С.* Угрозы безопасности технологии блокчейн // Актуальные вопросы информационной безопасности и защиты информации. 2021. С. 48-54.

11. *Кириченко Е. А.* Квантовое превосходство как угроза кибербезопасности и постквантовые методы криптографии // Вестник ИМСИТ. 2021. № 1. С. 37-39.

12. *Петров А. А.* Криптовалютный рынок и его перспективы (2 часть) // Россия: тенденции и перспективы развития. №. 17-1. С. 496-509.

13. *Herman A., Friedson I.* Quantum computing: how to address the national security risk // Hudson Institute, August 6, 2018, p. 8; National Academics of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects.

14. *Афанасьев И.А., Малахов С. В.* Принцип работы квантового компьютера // Инновации. Наука. Образование. 2021. №. 34. С. 1109-1114.

15. *Маковейчук Я. Т., Петренко А. С., Петренко С. А.* Квантовый алгоритм криптоанализа системы ассиметричного шифрования RSA // Информационные системы и технологии в моделировании и управлении. 2021. С. 199-204.

16. *Лежинский М. В., Мокряков А. В.* Алгоритмы шифрования, устойчивые ко взлому в условии квантового превосходства // Сборник научных трудов кафедры прикладной математики и программирования по итогам работы постоянно действующего семинара "Теория систем". 2021. С. 141-147.

17. *Шемякина М. А.* Квантовые вычисления. Моделирование квантовых алгоритмов на классическом компьютере // ББК 1 Н 34. 2019. С. 90.

18. *Комарова А. В., Коробейников А. Г.* Анализ основных существующих пост-квантовых подходов и схем электронной подписи // Вопросы кибербезопасности. 2019. №. 2 (30). С. 58-68.

19. *Haque M. M., Pieprzyk J.* Preprocessing optimisation: revisiting recursive-BKZ lattice reduction algorithm // IET Information Security. 2018. Т. 12. №. 6. С. 551-557.

20. *Гаража А. А.* и др. Об использовании библиотек полностью гомоморфного шифрования // International Journal of Open Information Technologies. 2021. Т. 9. №. 3. С. 11-22.

21. Campbell Sr R. Evaluation of post-quantum distributed ledger cryptography // The Journal of The British Blockchain Association. 2019. Т. 2. №. 1. С. 7679.

22. *Soni D.* et al. qTESLA // Hardware Architectures for Post-Quantum Digital Signature Schemes. Springer, Cham, 2021. С. 43-63.

23. *Bai S., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D.* CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1) // Technical report 08.02.2021. URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (дата обращения: 15.10.22).

24. *Fouque P.A., Hoffstein J., Kirchner P., Lyubashevsky V., Pornin T., Prest T., Ricosset T., Seiler G., Whyte W., Zhang Z.* Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Specification v1.2 // Technical report. 01.10.2020. URL: https://falcon-sign.info/falcon.pdf (дата обращения: 15.10.22).

25. *Bindel N., Akleylek S., Alkim E., Barreto P., Buchmann J., Eaton E., Gutoski G., Kramer J., Longa P., Polat H., Ricardini J., Zanon G.* Submission to NIST's post-quantum project (2nd round): lattice-based digital signature scheme qTESLA // Technical report. 26.04.2019. URL: https://qtesla.org/wp-content/uploads/2019/04/qTESLA_round2_04.26.2019.pdf (дата обращения: 15.10.22).

26. Open Quantum Safe algorithm performance visualizations //SIG performance. 11.10.2022. URL: https://openquantumsafe.org/benchmarking/visualization/speed_sig.html (дата обращения: 15.10.22).

27. Blockchain metrics // Blockchain.com. 15.10.2022. URL: https://www.blockchain.com/explorer/charts/n-transactions-total (дата обращения: 15.10.22).

28. Nakov S. Practical Cryptography for Developers //Practical Cryptography for Developers 01.11.2022. URL: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (дата обращения: 15.10.22).

POST-QUANTUM DIGITAL SIGNING ALGORITHMS AND THEIR APPLICATION IN DISTRIBUTED REGISTRY

VLADIMIR S. MOSKVIN
Saint Petersburg, Russia, moskvin.kvant@gmail.com

VLADIMIR A. BOGATYREV
Saint Petersburg, Russia

KEYWORDS: *post-quantum cryptography, information security, blockchain, CRYSTAL-DILITHIUM, FALCON, qTesla, electronic signature, comparative analysis.*

ABSTRACT

Introduction: The creation of systems based on blockchain technology is a promising area of modern research and development. Blockchain is a reliable and secure way to store transaction data, providing integrity verification capabilities. Today, blockchain technology is widely spread all over the world, in many spheres of life. The article considers the essence and characteristics of post-quantum electronic signature algorithms based on algebraic lattices and provides a comparative analysis of algorithms by conditional and unconditional criteria. **Results.** The advantages and disadvantages of existing cryptographic algorithms, the principles and specifics of the functioning of blockchain technology, as well as the possibility of using post-quantum algorithms in the formation of block signatures are determined.

REFERENCES

1. Laurent L. Blockchain from A to Z. All about the technology of the decade. Bombora. 2018, pp. 19-24.

2. Tapscott A., Tapscott D. Blockchain technology. What drives the financial revolution today. Eksmo. 2018, pp. 53-57.

3. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Redundant Servicing of a Flow of Heterogeneous Requests Critical to the Total Waiting Time During the Multi-path Passage of a Sequence of Info-Communication Nodes. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020. Vol. 12563, pp. 100-112.

4. Bogatyrev V.A., Bogatyrev A.V., Bogatyrev S.V. Redundant multi-path service of a flow heterogeneous in delay criticality with defined node passage paths. *Journal of Physics: Conference Series*. 2021, Vol. 1864, No. 1, pp. 012094.

5. Shemyakina M. A. Analysis of the use of quantum technologies in cryptography. *International Journal of the Humanities and Natural Sciences*. 2019. No. 5-4, pp. 59-62.6.

6. Shemyakina M. A. The use of quantum technologies in information security. *Modem Science*. 2019. No. 11-4., pp. 281-284.

7. Borisova E. V. Description of basic mathematical models in quantum cryptography. *Bulletin of the Ryazan State Radio Engineering University*. 2021. No. 75, pp. 113-120.

8. Sukhanov E. E., Shtang K. S., Aleshko R. A. Blockchain and quantum computing. *Synergy of Sciences*. 2017. No. 14, pp. 547-550.

9. Kiselenko V. A. Quantum computer as a potential threat to the stability of cryptographic information protection systems. *Academic Bulletin of the National Guard Troops of the Russian Federation*. 2019. No. 2, pp. 60-62.

10. Laskus A. S. Threats to the security of blockchain technology. *Actual issues of information security and information protection*. 2021, pp. 48-54.

11. Kirichenko E. A. Quantum superiority as a threat to cybersecurity and post-quantum methods of cryptography. *Bulletin of IMSIT*. 2021. Nno. 1, pp. 37-39.

12. Petrov A. A. Cryptocurrency market and its prospects (part 2). Russia: trends and development prospects. No. 17-1, pp. 496-509.

13. Herman A., Friedson I. Quantum computing: how to address the national security risk. *Hudson Institute*, August 6, 2018, p. 8; National Academics of Sciences, Engineering, and Medicine, Quantum Computing: Progress and Prospects.

14. Afanasiev I. A., Malakhov S. V. The principle of operation of a quantum computer. *Innovations. The science. Education*. 2021. No. 34, pp. 1109-1114.

15. Makoveichuk Ya. T., Petrenko A. S., Petrenko S. A. Quantum algorithm for cryptanalysis of RSA asymmetric encryption system. *Information systems and technologies in modeling and control*. 2021, pp. 199-204.

16. Lezhinsky M. V., Mokryakov A. V. Encryption algorithms resistant to cracking in the condition of quantum superiority. *Collection of scientific papers of the Department of Applied Mathematics and Programming based on the results of the work of the permanent seminar "Theory of Systems"*. 2021, pp. 141-147.

17. M. A. Shemyakina, Quantum Computing. Modeling of quantum algorithms on a classical computer. *BBK 1 H 34*. - 019, pp. 90.18.

18. Komarova A. V., Korobeinikov A. G. Analysis of the main existing post-quantum approaches and electronic signature schemes. *Issues of cybersecurity*. 2019. No. 2 (30), pp. 58-68.

19. Haque M. M., Pieprzyk J. Preprocessing optimisation: revisiting recursive-BKZ lattice reduction algorithm. *IET Information Security*. 2018. Vol. 12. No. 6, pp. 551-557.

20. Garazha A. A. et al. On the use of fully homomorphic encryption libraries. *International Journal of Open Information Technologies*. 2021. Vol. 9. No. 3, pp. 11-22.

20. Campbell Sr R. Evaluation of post-quantum distributed ledger cryptography. *The Journal of The British Blockchain Association*. 2019. Vol. 2. No. 1, pp. 7679.

22. Soni D. et al. qTESLA. *Hardware Architectures for Post-Quantum Digital Signature Schemes*. Springer, Cham, 2021, pp. 43-63.

23. Bai S., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehl? D. CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1). Technical report 08.02.2021. URL: https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf (date of application: 15.10.22).

24. Fouque P.A., Hoffstein J., Kirchner P., Lyubashevsky V., Pornin T., Prest T., Ricosset T., Seiler G., Whyte W., Zhang Z. Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Specification v1.2.Technical report. 01.10.2020. URL: https://falcon-sign.info/falcon.pdf (date of application: 15.10.22).

25. Bindel N., Akleylek S., Alkim E., Barreto P., Buchmann J., Eaton E., Gutoski G., Kramer J., Longa P., Polat H., Ricardini J., Zanon G. Submission to NIST's post-quantum project (2nd round): lattice-based digital signature scheme qTESLA. Technical report. 26.04.2019. URL: https://qtesla.org/wp-content/uploads/2019/04/qTESLA_round2_04.26.2019.pdf (date of application: 15.10.22).

26. Open Quantum Safe algorithm performance visualizations. SIG performance. 11.10.2022. URL: https://openquantumsafe.org/benchmarking/visualization/speed_sig.html (date of application: 15.10.22).

27. Blockchain metrics. Blockchain.com. 15.10.2022. URL: https://www.blockchain.com/explorer/charts/n-transactions-total (date of application: 15.10.22).

28. Nakov S. Practical Cryptography for Developers. Practical Cryptography for Developers 01.11.2022. URL: https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages (date of application: 15.10.22).

INFORMATION ABOUT AUTHORS:

Vladimir S. Moskvin, graduate student, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia

Vladimir A. Bogatyrev, Doctor, Tech., Professor, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), Saint Petersburg, Russia

For citation: Moskvin V.S., Bogatyrev V.A. Post-quantum digital signing algorithms and their application in distributed registry. *H&ES Reserch*. 2022. Vol. 14. No 4. P. 47-53. doi: 10.36724/2409-5419-2021-14-4-47-53 (In Rus)

doi: 10.36724/2409-5419-2022-14-4-54-64

СОЗДАНИЕ И ИНТЕГРАЦИЯ ЦИФРОВОГО ДВОЙНИКА

СУРИМОВА
Валерия Александровна[1]

СКОРОДУМОВА
Елена Александровна[2]

АННОТАЦИЯ

Введение. Интеллектуальные услуги жизненного цикла, наряду с принятием других стратегий интеллектуального производства, демонстрируют значительный потенциал для повышения производительности и конкурентоспособности предприятий. Становится очевидной потребность в высококачественных моделях процессов и программных представлений физического оборудования, которые особенно подробно отражают эволюцию своих физических аналогов. Технология цифровых двойников может обеспечить благодатную почву для разработки приложений жизненного цикла на основе Интернета вещей. В данной работе предлагается программный подход к процессу разработки цифрового двойника. **Цель** данной работы состоит в изучении методов создания программных фреймворков в контексте технологии цифровых двойников, а также изучение процесса создания и интеграции цифровых двойников и разработка собственного инструмента. Рассматриваются существующие методы создания двойников и описывается библиотека на Python, разработанная самостоятельно. В работе используются методы категории исследования в действии и философия Agile разработки. **Методы.** Выбор методологии при поиске ответов на вопросы, возникающие при изучении методов усовершенствования цифровых двойников, в основном относится к категории исследований в действии. В данной работе исследование в действии используется как качественный инструмент, хорошо подходящий для ситуаций, когда исследователь стремится достичь двух различных целей, а именно: решить современную проблему, с которой сталкивается организация; внести вклад в пул знаний, который впоследствии может быть использован другими людьми для решения задач того же класса проблем. **Результаты.** Созданная библиотека поддерживает два режима получения данных: с помощью периодических запросов к базе данных и TCP-сокет соединение. Эксперименты, проведённые в рамках работы, позволяют сделать вывод о том, что библиотека уже сейчас может быть использована в качестве инструмента создания цифрового двойника и его интеграции.

Сведения об авторах:

[1] студент, Московский Технический Университет Связи и Информатики, Москва, Россия, surimova.lera@mail.ru

[2] к.ф.м.н, Московский Технический Университет Связи и Информатики, доцент, Москва, Россия, eas@mtuci.ru

КЛЮЧЕВЫЕ СЛОВА: *цифровой двойник, нейронные сети, совместная симуляция, большие данные, Python.*

Для цитирования: Суримова В.А., Скородумова В.А. Создание и интеграция цифрового двойника // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 4. С. 54-64. doi: 10.36724/2409-5419-2022-14-4-54-64

Введение

Промышленная парадигма постепенно смещается от ориентированной на продукт к ориентированной на услуги. С точки зрения производителя это означает, что потоки доходов могут быть расширены, чтобы охватить всю жизненную цепочку продукта, включая проектирование, производство, доставку, эксплуатационное использование и вывод из эксплуатации.

Интеллектуальные услуги жизненного цикла, наряду с принятием других стратегий интеллектуального производства, демонстрируют значительный потенциал для повышения производительности и конкурентоспособности предприятий. Становится очевидной потребность в высококачественных моделях процессов и программных представлений физического оборудования, которые особенно подробно отражают эволюцию своих физических аналогов. Часто моделирование цифровых двойников также необходимо дополнить данными датчиков реального мира в режиме реального времени, чтобы отразить изменения, происходящие в целевой системе с течением времени. Поэтому технология цифровых двойников может обеспечить благодатную почву для разработки приложений жизненного цикла на основе Интернета вещей.

В данной работе предлагается программный подход к процессу разработки цифрового двойника.

Постановка задачи и методология

Настоящая работа мотивирована недавними разработками в тесно связанных областях в сфере интеллектуальных промышленных услуг, а именно искусственного интеллекта и глубокого обучения. Мы рассмотрим концепцию создания и интеграции цифровых двойников путем синтеза набора функций цифровых двойников на основе обзора литературы. Также обсудим сопоставление этих функций с функциональными требованиями предполагаемой программной среды, которая облегчила бы создание цифровых двойников. Наконец, будет разработана конструктивная методология исследования.

Предпосылки

Практики гибкой разработки программного обеспечения активно развиваются с 1990-х годов, и сегодня они почти заменили традиционную модель. В целом, они имеют больший успех по сравнению с традиционными методами, благодаря их потенциалу постепенного создания ценности для клиентов в быстрых циклах разработки. Самые ранние внедрения гибких методов по времени примерно совпадают с введением первых широко распространенных объектно-ориентированных языков программирования, таких как C++ (впервые появился в 1983 г.) и Java (1996г.). Этот факт поддерживает идею взаимосвязи между ними. Можно сделать вывод, что наличие высокопроизводительных инструментов может, по крайней мере косвенно, способствовать внедрению высокопроизводительных промышленных методов и наоборот.

Цель данной работы состоит в изучении методов создания программных фреймворков в контексте технологии цифровых двойников. Хотя аналогичные идеи предлагались ранее, термин «цифровой двойник» впервые упоминается в статье Глэссгена и Штаргеля, написанной по заказу НАСА и ВВС США [1]. Основные выводы из современных разработок ([1]-[5]) можно резюмировать в следующем списке особенностей цифровых двойников:

- *Репрезентативность:* каждый цифровой двойник – это цифровой артефакт, которому соответствует парный физический артефакт. Как правило, можно сделать надежные выводы о поведении физической системы, наблюдая за реакцией цифрового двойника на сигналы искусственного возбуждения.
- *Актуальность:* существование цифрового двойника в самом общем случае должно распространяться на весь жизненный цикл его физического аналога. Сам двойник и/или инкапсулирующий промежуточный уровень должны отражать изменения, происходящие в течение жизненного цикла.
- *Возможность проверки:* в любое время любой атрибут, связанный с цифровым двойником, должен быть легко доступен соответствующим уполномоченным агентом. Это можно рассматривать как принцип прозрачности, когда раскрыты входные и выходные сигналы цифровых двойников, а также внутреннее состояние модуля симуляции, которое может быть трудно измерить обычными средствами соответствующего физического оборудования.

С высокой степенью абстракции сложный цифровой двойник может быть реализован как набор программных агентов, взаимодействующих с артефактами в физической или цифровой области. Соответственно, любая структура, которая создана с целью поддержки построения таких конфигураций, должна иметь возможность надлежащим образом управлять этими сложными соединениями «многие ко многим». Для удобства использования необходимо учитывать, что задействованные физические/цифровые артефакты могут быть доступны с помощью различных технологий, например, REST API [6], запросов к базе данных SQL/NoSQL или более сложного протокола связи IoT, такого как FMI [7] или MQTT [8].

Так как цифровой двойник должен существовать на каждом этапе вместе с физическим продуктом, возникают сложности в разработке доступной в каждый момент времени вычислительной инфраструктуры для конкретных этапов. Даже если рассматривать более реалистичный вариант использования цифрового двойника только в течение срока службы продукта, необходимо будет решить проблемы, касающиеся устойчивости и отказоустойчивости.

При разработке приложений цифровых двойников также необходимо учитывать понятие расширяемости. Когда срок службы продукта может составлять десятки лет, вполне возможно, что к физическому продукту будут добавлены надстройки, которые не могут быть адекватно воспроизведены в исходных экспериментальных рамках двойника. Следовательно, в идеале структура цифрового двойника должна обеспечивать удобные средства для внесения корректировок в экспериментальную основу и добавления но-

вых компонентов модели по мере развития физического аналога. Дополнительным моментом проектирования является то, что ориентированный на пользователя принцип необходим для того, чтобы такое программное обеспечение приобрело значительную популярность. Поэтому программное обеспечение должно быть интуитивно понятным, чтобы обеспечивать быстрое создание прототипов, а также достаточно гибким для обеспечения возможности расширения и развертывания для реальных приложений.

Методология исследования

Выбор методологии при поиске ответов на вопросы, возникающие при изучении методов усовершенствования цифровых двойников, в основном относится к категории исследований в действии. В данной работе исследование в действии используется как качественный инструмент, хорошо подходящий для ситуаций, когда исследователь стремится достичь двух различных целей, а именно: решить современную проблему, с которой сталкивается организация; внести вклад в пул знаний, который впоследствии может быть использован другими людьми для решения задач того же класса проблем.

Ярвинен [5] предложил рассматривать исследование в действии как подкласс исследовательских подходов к построению/оценке артефактов, в которых этапы построения и оценки выполняются циклически. В области исследований науки дизайна существует устоявшаяся идея о том, что простой процесс создания вещей и наблюдения за их работой, иногда даже постфактум, имеет большой потенциал как для развития прямого технологического прогресса, так и расширения базы научных знаний. В данной работе конструктивный подход выбран с целью получения более глубокого понимания проектирования и проведения экспериментов с цифровыми двойниками в контексте различных процессов непрерывного времени. Основная ценность данной работы заключается в создании прототипа минимально жизнеспособного продукта (minimum viable product, MVP) программной среды, которая поддерживает эту цель.

В частности, предлагаемое решение будет представлять собой объектно-ориентированную библиотеку, написанную на Python, которая направлена на создание абстракции для различных функций цифровых двойников низкого уровня. Далее следует отметить, что подход к исследованию циклического построения артефактов/оценки артефактов, очевидно, сродни различным Agile [9] методам разработки программного обеспечения (например, Scrum и т.п.). Таким образом, данный метод является подходящим выбором для практической реализации нашей задачи, которая по существу сводится к довольно стандартному проекту разработки программного обеспечения.

Выбранный подход дополнительно обоснован наблюдением за взаимосвязью между цифровыми двойниками и некоторыми из наиболее интересных современных исследовательских тем в области науки о данных. Сегодня инженеры-программисты все чаще практикуют машинное обучение (ML), глубокое обучение (DL) и искусственный интеллект (AI). Это связано с созданием современных библиотек глубокого обучения с открытым исходным кодом (например, Tensorflow, PyTorch, Keras), которые доступны для широкого круга разработчиков с точки зрения их уровня абстракции. Поскольку технологии ML / DL / AI играют решающую роль в некоторых из наиболее интересных приложений цифровых двойников будущего (например, для профилактического обслуживания), вполне вероятно, что часть будущих разработчиков будет участвовать в проектах в обеих областях. Отсюда возникает понятие согласованности инструментов. Идея заключается в том, что повышение производительности может быть достигнуто, если программные интерфейсы в обоих доменах будут, по крайней мере приблизительно, поддерживать аналогичные рабочие процессы. Насколько нам известно, попыток реализовать такие инструменты было совсем немного и открытых сведений очень мало.

В ходе данной работы мы сформулируем исследовательскую проблему, установим теоретическую основу, а также рассмотрим основные характеристики разработанного программного обеспечения и, наконец, оценим его производительность и проанализируем результаты. Эмпирическая часть работы была выполнена с использованием итерационных практик. Следуя философии Agile разработки, сосредоточим внимание на результатах и их применимости.

Цифровой двойник

Было установлено, что процесс симуляции заключается в наблюдении за поведением динамической модели во времени в контексте заданной экспериментальной системы. Поэтому можно представить экспериментальный фрейм, имеющий своего рода отображение на сегменте временной шкалы в жизненном цикле моделируемой физической системы. В более широком смысле также возможны сценарии симуляции, в которых весь жизненный цикл физической системы является экспериментальной структурой. Подобные концепции симуляции в контексте статьи называются цифровыми двойниками.

Чтобы проиллюстрировать концепцию, рассмотрим процесс проектирования и производства физического продукта, например, автомобиля или космического корабля. В зависимости от конкретной отрасли свойства отдельных конечных продуктов, выходящих из заводского конвейера, будут иметь некоторую степень вариации. Это может быть связано либо с целенаправленными настройками, навязанными конечным потребителем, предполагаемой миссией и условиями эксплуатации продукта, либо с небольшими неконтролируемыми колебаниями, происходящими в производственном процессе. Наряду с созданием материального продукта в вычислительной среде может быть создан его программный аналог, цифровой двойник этого уникального продукта. Таким образом, семантический вид этого цифрового двойника должен, насколько это возможно, отражать вариации, связанные с процессом проектирования и производства.

Поскольку современные системы проектирования и производства уже в значительной степени оцифрованы, каждая уникальная реализация продукта в физическом мире оставляет за собой след в киберсфере; цифровую тень, которая

включает все созданные во время реализации данные об операциях, условиях, процессах и т.д. Цифровая тень отдельного экземпляра продукта затем может быть связана с цифровой мастер-моделью – еще одним цифровым артефактом, состоящим из данных и функций, общих для всех экземпляров данного класса продукта. Таким образом рождается новый цифровой двойник.

Оснащенный моделями, которые могут симулировать различные подсистемы, созданный цифровой двойник теперь должен иметь возможность «испытать» каждое возможное событие, с которым его физический аналог может столкнуться в течение своей жизни. Сюда могут входить рабочие условия, которые изначально не рассматривались во время создания первоначального дизайна продукта. При этом набор симуляций, составляющий вычислительную часть цифрового двойника, постоянно получает данные датчиков, полученные от физического устройства. В контексте промышленных систем, склонных к отказам компонентов, это может позволить разработать приложения профилактического обслуживания, прогнозирования срока службы компонентов и даже динамическую активацию различных механизмов самовосстановления.

Как было упомянуто выше, цифровой двойник обладает исключительными свойствами: быть чрезвычайно точным и всегда актуальным. Наиболее важно то, что представление о цифровом двойнике, как об эквиваленте некоторого физического объекта, выделено в обоих определениях. Программное обеспечение, в отличие от физических машин, может быть спроектировано таким образом, чтобы пользователи могли свободно наблюдать за внутренним состоянием выполнения в любой момент времени, не влияя на сам процесс. Ясно, что в целом то же самое нельзя сказать о физических машинах, что дает еще один аргумент в пользу использования цифровых двойников.

Концепцию цифрового двойника можно рассматривать как расширение временного окна симуляции до всего жизненного цикла продукта. В то время как традиционно моделирование рассматривалось в качестве инструмента в основном для проектных операций, парадигма цифрового двойника позволяет использовать возможности симуляции на этапах поставки, эксплуатации и даже вывода из эксплуатации. Таким образом, мы видим, как роль симуляции развивалась за последние десятилетия (рис. 1).

Рис. 1. Эволюция роли симуляции

Описание программной среды, способной размещать приложения цифрового двойника, может быть реализовано путем определения двух различных классов агентов, а именно:

- *Агенты процесса*: сущности, которые взаимодействуют с данными процесса физических объектов или процессов в общем, и переводят эти данные в промежуточную форму, интерпретируемую другими агентами, и из неё.
- *Агенты симуляции:* объекты, которые взаимодействуют с модулями симуляции и переводят свои данные в промежуточную форму и обратно.

Здесь цифровой двойник можно интерпретировать как отношение RDT между набором агентов процесса P и набором агентов симуляции S:

$$R_{DT} = \{(p,s) \mid (p,s) \in P \times S,$$

s потребляет данные, произведенные в p}

Очевидно, что упрощенное определение, данное в уравнении, не охватывает всего пространства возможных взаимосвязей между модулями совместной симуляции в S. В общем сценарии совместной симуляции очевидно, что агенты моделирования могут получать не только данные от агентов процесса P, но и от других агентов моделирования. Точно так же опускаются подходы, ориентированные на управление в S. Тем не менее, с учетом этих ограничений, данное уравнение помогает проиллюстрировать концепцию, которая используется в процессе создания простого цифрового двойника.

Создание простого цифрового двойника

В этом разделе мы покажем, как создать простой, но функциональный цифровой двойник на Python. В качестве физического объекта рассмотрим аккумулятор. Цифровой двойник позволит нам анализировать и прогнозировать поведение аккумулятора, и его можно интегрировать в любой рабочий процесс управления виртуальными объектами.

Перед началом работы с данными была проведена предварительная подготовка. Предобработка состояла из 4 этапов:

- импорт необходимых библиотек;
- импорт набора данных;
- обработка пустых значений;
- кодирование категориальных данных;
- тестовый и тренировочный наборы.

В набор данных, с которым мы будем работать, входят такие показатели аккумулятора как напряжение, температура и др. Наиболее интересным параметром является ёмкость аккумулятора, которую мы будем использовать для иллюстрации работы двойника. Также в датасет входят временные метки, тип аккумулятора и его название.

Описание модели

Ожидается, что «цифровой двойник» будет реагировать на входные переменные так же, как и его «физический двойник». Для этого в виртуальный объект нужно интегрировать модель. Самая важная особенность цифрового двойника - это модель, которая может имитировать «физическое» поведение в цифровом контексте.

Аккумуляторы с истекшим сроком службы обычно предлагают только 80% от их номинальной максимальной емкости. Это ухудшение можно записать следующим образом, используя одну из эмпирических моделей:

$$L = 1 - (1 - L')e^{f_d},$$

где L – срок службы аккумулятора, L' – начальный срок службы батареи, а f_d – линеаризованная скорость снижения эффективности за единицу времени и за цикл.

Эта скорость может быть записана как функция от времени t, глубины цикла разряда δ, среднего за цикл состояния заряда σ и температуры элемента T_c:

$$f_d = f_d(t, \delta, \sigma, T_c) \cdot$$

Наша модель должна прогнозировать время автономной работы на основе полученной информации.

Для создания цифрового двойника будем использовать реальные данные НАСА о циклах зарядки-разрядки аккумуляторов (наборы данных об износе литий-ионных аккумуляторов). Прежде чем мы начнем, мы заменим переменную L (время автономной работы) на C (емкость аккумулятора) [10]. Мы получим следующее уравнение емкости:

$$C = C_0 e^{f_d}.$$

Здесь C – емкость аккумулятора, C_0 – начальная емкость аккумулятора. Для f_d будем использовать следующее приближение:

$$f_d = k\frac{iT_c}{t_i},$$

где i – цикл заряда-разряда, Tc – температура, измеренная в элементе во время цикла, t_i – время разряда, и k - эмпирическая константа со значением 0,13 [10].

Сгруппируем данные по циклам и изобразим график сравнения нашей модели и реальных данных. Результат этого шага представлен на рисунке 2.

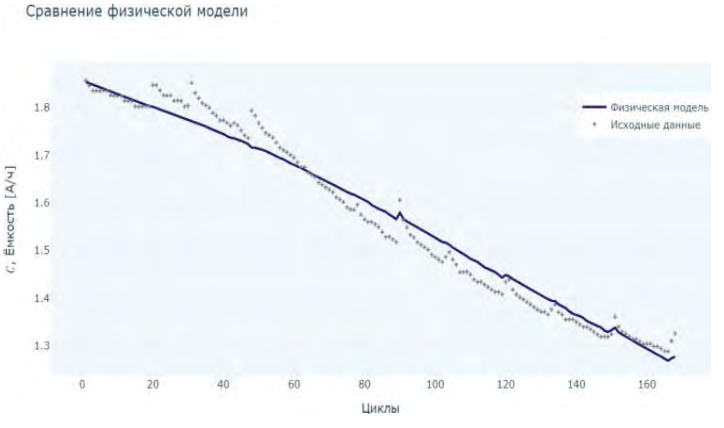

Рис. 2. График сравнения модели и реальности

Для оценки точности полученной модели можно посчитать Mean Absolute Error (MAE – Средняя абсолютная ошибка) [11]. Средняя абсолютная ошибка является мерой ошибки между реальными наблюдениями и смоделированными значениями. Полученный результат MAE = 0,004 позволяет сказать, что точность достаточно высока.

Применение нейронных сетей

Для усовершенствования нашей модели применим нейронную сеть (см. рис. 3).

Рассмотрим несколько типов нейронных сетей и оценим, какие из них наилучшим образом усовершенствуют нашу модель.

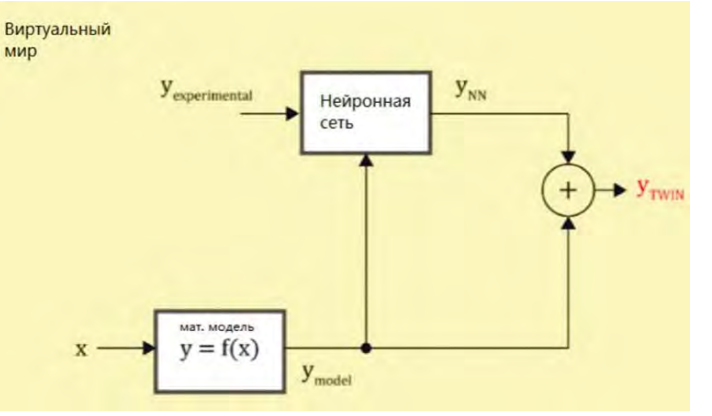

Рис. 3. Создание цифрового двойника

Многослойный перцептрон

Самым простым и наиболее часто используемым вариантом нейронной сети является полносвязная сеть или многослойный перцептрон. Создадим цифровой двойник с её помощью.

Воспользуемся функцией Dense из библиотеки Keras, которая создает полностью связанный слой нейронной сети, автоматически инициализируя веса как смещения.

Для иллюстрации обучения нейронной сети выведем график сравнения MAE (рис. 4). На данном графике мы видим значения MAE для тренировочного набора данных и для проверочного (validation set). Они показывают, что наша нейронная сеть не переучена и хорошо описывает данные, с которыми ещё не работала, так как уровень тренировочной и проверочной MAE находится в одном диапазоне. Также сравним показания смоделированной ёмкости и тренировочной ёмкости нейросети (рис. 5).

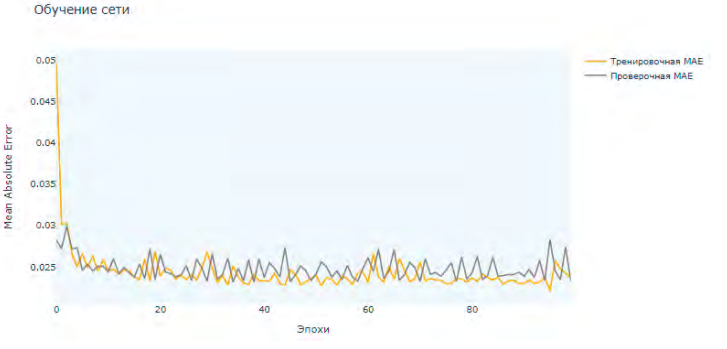

Рис. 4. Сравнение MAE

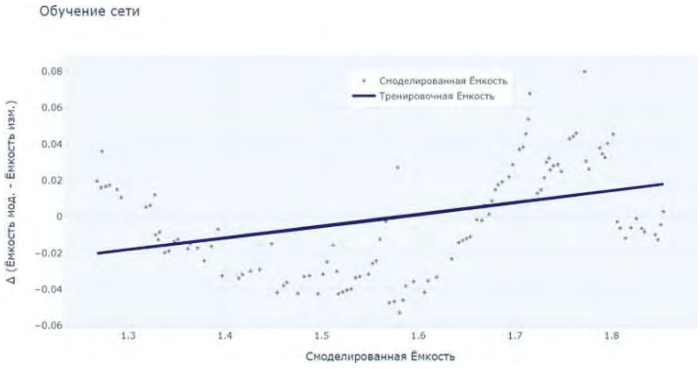

Рис. 5. Сравнение результатов модели с экспериментальными результатами

Как видно из рисунка 5, нейронная сеть получает базовое понимание различий между построенной математической моделью и экспериментальными результатами. Теперь можно добавить эти знания к нашей математической модели для её усовершенствования.

Далее мы можем сравнить нашу математическую модель (смоделированная емкость), реальные данные (наблюдаемая емкость) и модель нашего цифрового двойника (рис. 6).

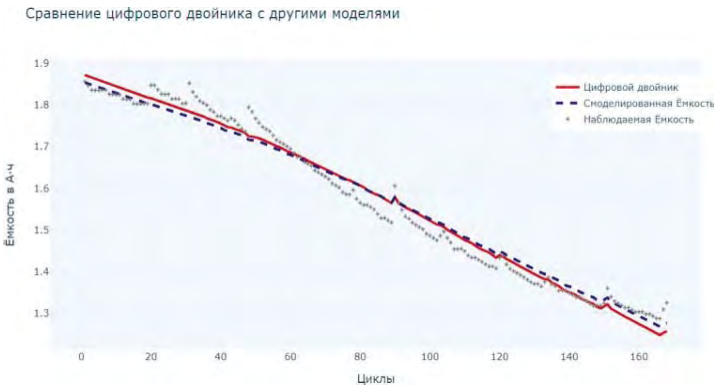

Рис. 6. Сравнение моделей

На рисунке 6 показано, как цифровой двойник улучшил нашу модель. Его преимущество заключается в том, что он позволяет использовать полуэмпирическую математическую модель и уточнять ее с помощью экспериментальных данных. Он имеет преимущества перед обеими моделями: особенно математической, поскольку она может быть улучшена, и моделью ML, поскольку двойник является более обобщённым (поэтому может быть применен, например, к другому аккумулятору, получая лучшую точность, чем при использовании только модели ML).

С помощью цифрового двойника мы можем строить прогнозы относительно работы аккумулятора. Результат представлен на рис. 7. Пунктирными линиями на графике изображены предсказанные значения ёмкости математической модели (синий цвет) и цифрового двойника (красный цвет). Мы видим, что предсказанная двойником емкость меньше, чем смоделированная ёмкость.

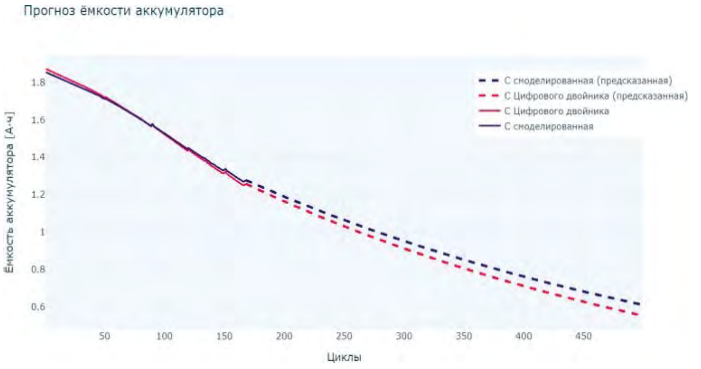

Рис. 7. Прогноз двойника и математической модели

Рекуррентная сеть LSTM

Часто для работы с последовательными данными используют рекуррентные нейронные сети, которые также называют нейронными сетями с обратной связью. Недостатком рекуррентных сетей является то, что элементы обрабатываются поочерёдно, что ведёт к большим затратам памяти. Поэтому была создана такая нейронная сеть как длинная цепь элементов краткосрочной памяти (LSTM – Long short-term memory) [12]. LSTM позволяет передавать информацию, пропуская большую часть обработки текущего элемента и быстрее переходить к следующему. Это даёт возможность сохранять память для более длинных последовательностей.

Выведем соответствующие графики сравнения MAE, сравнения цифрового двойника с другими моделями и график прогноза для модели с LSTM (рис. 8-10).

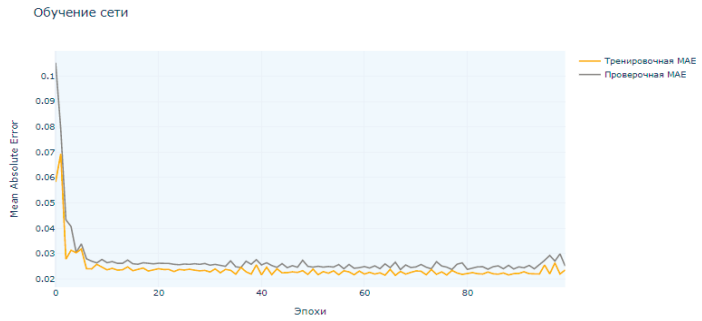

Рис. 8. Сравнение тренировочной и проверочной MAE для LSTM

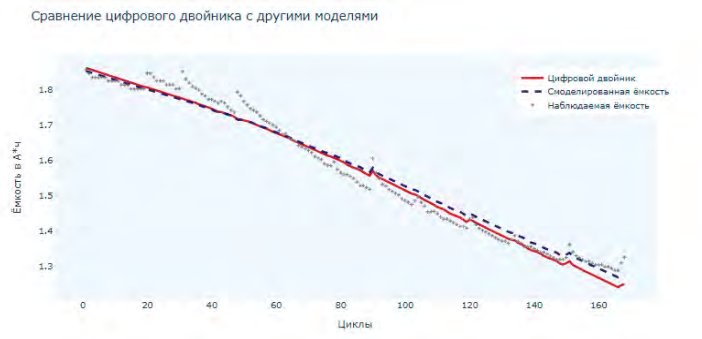

Рис. 9. Сравнение цифрового двойника LSTM с другими моделями

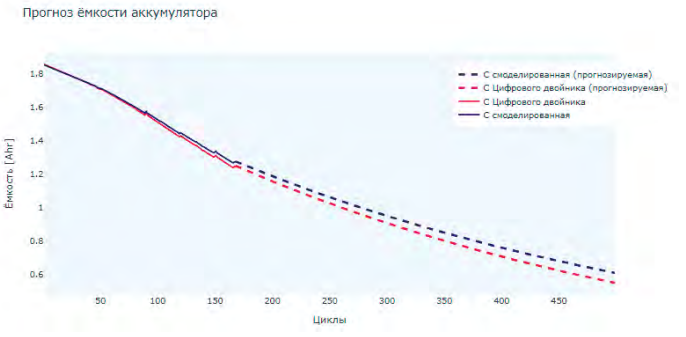

Рис. 10. Прогноз ёмкости с использованием LSTM

Очевидно, результаты, полученные с помощью нейронной сети LSTM, не имеют глобальных отличий от значений цифрового двойника, основанного на многослойном перцептроне. Однако, можно заметить, что разница между проверочной и тренировочной MAE для LSTM немного выше. Также мы видим, что в начале прогнозируемого отрезка емкость данного цифрового двойника принимает значения меньше, чем значения двойника с полносвязной сетью.

Трансформер

В предыдущем разделе были рассмотрены основные простые нейронные сети, которые обычно применяют для работы с последовательными данными, и временными рядами, в частности. Далее применим другую нейронную сеть, которую обычно используют для работы с текстом и языками – трансформер. Его архитектура представлена на рисунке 11.

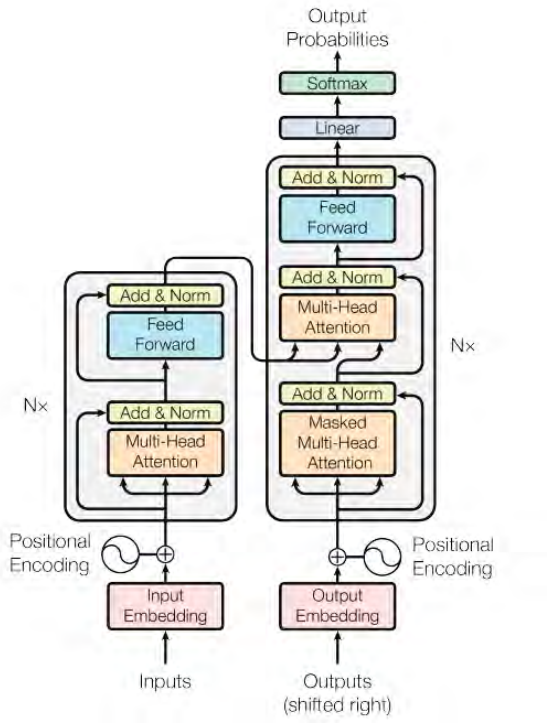

Рис. 11. Архитектура трансформера

Multi-head attention – это одна из самых примечательных частей архитектуры, которая отличает трансформер от других видов нейронных сетей. Это специальный новый слой, который дает возможность каждому входному вектору взаимодействовать с другими элементами через механизм внимания (Attention mechanism), вместо передачи скрытого представления (hidden state) как в RNN (Recurrent neural network – рекуррентная нейронная сеть**)**.

В трансформере модуль внимания повторяет свои вычисления несколько раз параллельно. Каждый из них называется Attention Head. Модуль внимания разбивает свои параметры «Запрос», «Ключ» и «Значение» по N-путям и передает каждое разбиение независимо через отдельную «голову». Затем все эти похожие вычисления объединяются для получения окончательной оценки внимания. Этот процесс называется «многоголовым вниманием» и дает трансформеру больше возможностей для кодирования множества взаимосвязей и нюансов для каждого элемента. Для модуля multi-head attention нами была создана специальная функция. Также к каждому исходному вектору в трансформере применяется нейронная сеть с прямой связью.

Помимо того, что нам необходимо задать векторы входной последовательности для реализации цифрового двойника с помощью трансформера, нам нужно иметь представление о значимости позиций элементов в последовательности. Для этого мы использовали функции синуса и косинуса.

Рассмотрим графики для полученной модели (рис. 12-13). По графикам можно заметить, что показатели трансформера немного отличаются от показателей остальных нейронных сетей. Это связано с тем, что обычно их применяют для более объёмных наборов данных. Показатели проверочной MAE заметно выше, чем показатели предыдущих двойников, а значения емкости ниже смоделированных и реальных.

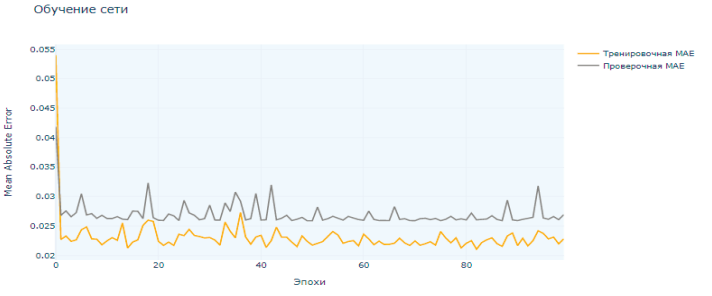

Рис. 12. Сравнение MAE для трансформера

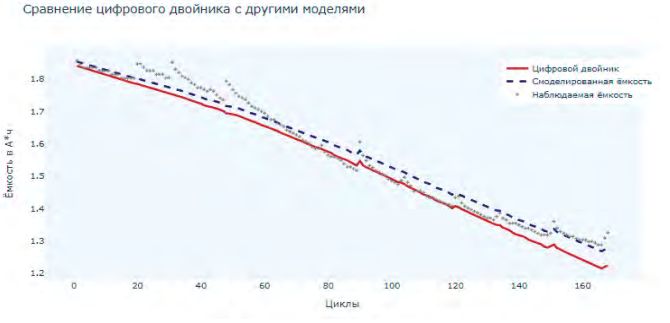

Рис. 13. Сравнение цифрового двойника трансформера с другими моделями

Таким образом, мы рассмотрели процесс создания простого цифрового двойника с помощью трёх различных нейронных сетей: многослойного перцептрона, LSTM и трансформера. Самым простым в применении является многослойный перцептрон. Данная нейронная сеть также показала высокую точность предсказаний. Цифровой двойник с LSTM и полносвязная сеть продемонстрировали практически одинаковые результаты, однако, если нам важно более эффективно использовать память, подходящим выбором будет нейронная сеть LSTM. В случае, когда важна скорость обучения и наилучшая эффективность работы модели, стоит выбирать нейронную сеть трансформер, так как вычисления в этой модели выполняются параллельно.

Библиотека для совместной симуляции

В этой главе описываются основные результаты эмпирической части работы.

В ходе работы был разработан прототип библиотеки цифровых двойников Python под названием DTSimulator. Данная библиотека – это инструмент интеграции цифрового двойника, который может быть использован для любых физических объектов. Библиотека является минимально жизнеспособным продуктом в том смысле, что она охватывает основные функции вместе с соответствующими модульными тестами, но еще не была тщательно проверена на интеграцию для всех возможных сценариев использования. Архитектура программного обеспечения полностью основана на подходе объектно-ориентированного программирования (ООП), так что классы высокого уровня могут быть легко расширены для поддержки еще большего количества различных типов входных потоков и моделей.

Архитектурабиблиотеки основывается на совместной работе трех различных классов:

- Источники данных (класс MeasurementStreamHandler), представляющие физические активы и исходящие от них потоки данных процесса.
- Потребители данных (класс ModelHandler), представляющие модели цифровых активов, которые имитируют или делают выводы о поведении соответствующих источников данных.
- Человек-оператор.

Предлагаемый MVP обеспечивает решение проблемы лаконичного построения конвейеров данных в режиме онлайн между источниками данных и потребителями данных, обеспечивая необходимые формальные преобразования на этом пути (рис. 14).

Рис. 14. Схема DTSimulator

Между источниками данных (физическими активами, на основе которых производятся измерения) и моделями активов потребителей данных существует взаимосвязь «многие ко многим». В терминах ООП эти отношения строятся с помощью отдельной сущности Experiment, которая, помимо прочего, отвечает за хранение маршрутов данных от измерений к моделям для данного вызова (рис. 15).

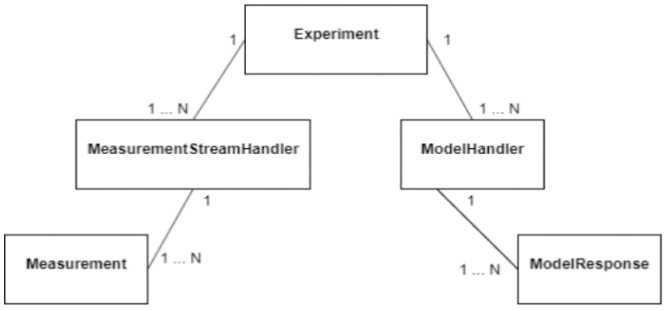

Рис. 15. Диаграмма классов уровня спецификации

В DTSimulator все данные существуют в одном из двух возможных форматов:

1) объект Measurment, который обозначает структуру данных с меткой времени, полученную от физического актива.
2) объект ModelResponse, который аналогичным образом обозначает структуру данных с меткой времени, полученную от цифрового актива.

Для каждого объекта Measurement, который создается из данных, полученных от физического объекта, в парном цифровом объекте создается ровно один объект ModelResponse. Measurement и ModelResponse представляют собой коллекции "ключ-значение".

В библиотеке существуют следующие категории ключей:

- *Ключи ввода (input_keys):* ключи в объекте Measurement, которые ожидаются в качестве входных данных вModelHandler.
- *Целевые ключи (target_keys):* ключи, которыебудут выведены из экземпляра ModelHandler в объект ModelResponse.
- *Контрольные ключи (control_keys):* ключи в Measurement, используемые в качестве проверочной переменной для выходных данных ModelHandler.
- *Ключ временной отметки (timestamp_keys):* ключ, обозначающий момент создания соответствующего экземпляра Measurement или ModelResponse.

На уровне реализации MeasurementStreamHandler и ModelHandler являются родительскими классами. На рисунке 16 показана иерархия наследования MeasurementStreamHandler.

MeasurementStreamPoller используется при получении данных измерений с помощью периодических запросов к базе данных. IncomingMeasurementListener применяется для случая TCP-сокет соединения.

Аналогичная иерархическая структура присутствует в классе ModelHandler (рис. 17).

Ключевыми на временной шкале эксперимента DTSimulator являются моменты, когда возвращается объект ModelResponse. На этом этапе содержимое ModelResponse записывается во внешний файл в виде значений, разделенных запятыми, в следующем порядке:

timestamp, input_keys, target_keys, control_keys

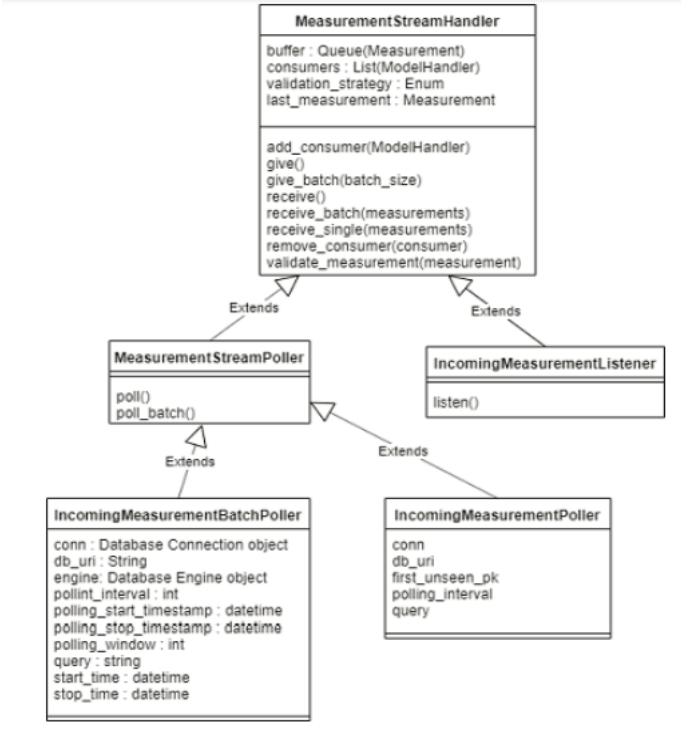

Рис. 16. Иерархия MeasurementStreamHandler

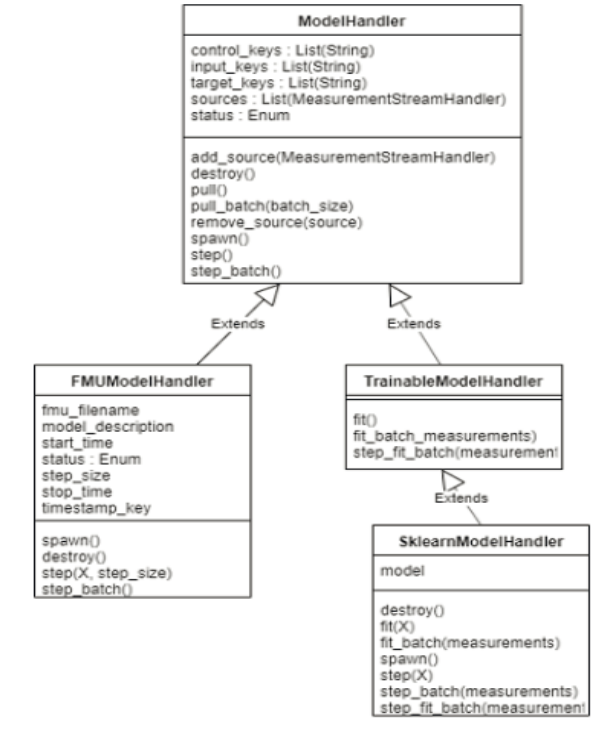

Рис. 17. Иерархия ModelHandler

Реальные данные часто содержат ошибки измерений или пустые значения. Для обработки значений Nonев библиотеке есть специальный функционал, основанный на идее возвращения к последнему значимому значению.

Пример использования библиотеки

Рассмотрим решение задачи прогнозирования мощности двигателя с помощью созданной библиотеки. Для демонстрации работы библиотеки воспользуемся данными испытаний на выбросы внедорожных дизельных двигателей [13].

Необработанные данные представлены в виде матрицы 1238x3, где первый столбец соответствует прошедшему времени в секундах, второй столбец – нормализованной частоте вращения двигателя (в процентах от максимума), а третий столбец соответствует нормализованному крутящему моменту двигателя (в процентах от максимума).

Выходная мощность поршневого двигателя определяется как произведение угловой скорости и крутящего момента:

$$P_{out}\left[B\right] = \omega\left[\frac{рад}{с}\right] \cdot T\left[Нм\right],$$

где

$$\omega\left[\frac{рад}{с}\right] = \frac{\pi}{60}\left[с^{-1}\right] \cdot 2\pi \cdot$$

Здесь n – скорость вращения, выраженная в оборотах в минуту (об/мин).

Временной ряд мощности вычисляется с использованием данных уравнений и добавления случайного гауссова шума с нулевым средним значением и стандартным отклонением 5 кВт.

В соответствии с архитектурой DTSimulator эксперимент состоит в периодическом опросе базы данных на наличие новых данных, и всякий раз, когда новые данные становятся доступными, они передаются подключенной модели. Однако, поскольку в этом случае необработанные данные находятся в простом CSV-файле, был разработан отдельный механизм для моделирования периодических измерений, записываемых в базу данных.

Цель эксперимента состоит в том, чтобы отслеживать входящие данные и делать выводы. Этот процесс довольно прост с использованием встроенных методов, содержащихся в классах ModelHandler. Когда код запущен, экземпляр симуляции активируется программно, и пользователь может просмотреть результаты моделирования в окне плоттера в реальном времени. В итоге результаты сохраняются в выходной CSV-файл для последующего изучения и/или последующей обработки с помощью произвольных инструментов. На рисунке 22 показан график окончательных результатов, полученных в среде симуляции.

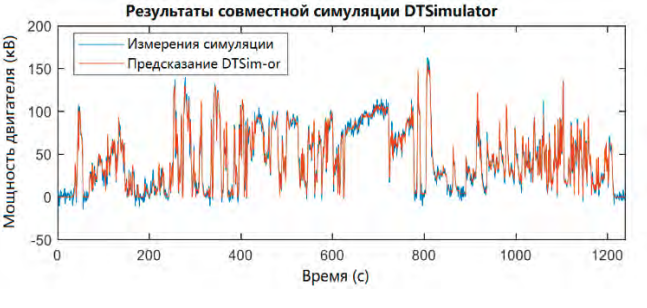

Рис. 18. Результаты эксперимента DTSimulator один-к-одному

На графике мы видим результат совместной симуляции – мы одновременно получаем измерения мощности двигателя и предсказанные показатели DTSimulator.

Заключение

Цель данной статьи заключалась в изучении и разработке инструментов для создания, проведения и оценки экспериментов с цифровыми двойниками. После изучения методов создания простейшего двойника с помощью различных нейронных сетей, разработана библиотека для создания цифровых двойников и реализации процесса совместной симуляции.

Созданная библиотека поддерживает два режима получения данных: с помощью периодических запросов к базе данных и TCP-сокет соединение. Эксперименты, проведённые в рамках работы, позволяют сделать вывод о том, что библиотека уже сейчас может быть использована в качестве инструмента создания цифрового двойника и его интеграции.

Поскольку срок службы физических активов может достигать большого количества лет, остаются открытыми вопросы, касающиеся устойчивости и отказоустойчивости. Будущие исследования должны рассмотреть возможность проверки поведения библиотеки путем проведения длительного эксперимента с цифровым двойником, возможного введения искусственных аномальных ситуаций, которые могут помешать процессу, и обеспечения достаточной надежности системы для восстановления после этих аномалий.

Литература

1. *Glaessgen E., Stargel D.* The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles // 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference – Special Session on the Digital Twin, 2012, pp. 1-14.

2. *Пономарев К.С., Феофанов А.Н.* Цифровой двойник производства как инструмент цифровизации технологических процессов предприятия // Актуальные тренды и перспективы развития науки, техники, технологий: сборник научных трудов по материалам Международной научно-практической конференции / Под общ. ред. Е. П. Ткачевой. Белгород: ООО Агентство перспективных научных исследований (АПНИ), 2019. С. 141-144.

3. *Фюер Ц., Вейсманн Ц.* Преимущества “цифрового двойника” // CAD/CAM/CAE Observer. 2017. №5 (113). С. 50-53 // Радиопромышленность. 2015. № 4. С. 56-64.

4. *Ponomarev K., Kudryashov N., Popelnukha N., Potekhin V.* Main principals and issues of digital twin development for complex technological processes // Ann. DAAAM Proc. Int. DAAAM Symp., pp. 523-528, 2017.

5. *Järvinen P.* Research Questions Guiding Selection of an Appropriate Research Method PerttiJärvinen Research Questions Guiding Selection of an Appropriate Research Method // Proceedings of European Conference on Information Systems 2000, 3-5 July, 2000.

6. Richardson L., Ruby S. RESTful Web Services. O'Reilly Media, Inc., 2008.

7. *Martin Otter, HildingElmqvist, TorstenBlochwitz, Jakob-Mauss, Andreas Junghanns, Hans Olsson.* Functional MockupInterface-Overview, 2010.

8. *Naik N.* Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP // Proc. IEEE Int. Syst. Eng. Symp. (ISSE), Oct. 2017, pp. 1-7.

9. *Beck K.* et al. Manifesto for Agile Software Development. Manifesto for Agile Software Development, 2001. URL: http://www.agilemanifesto.org/.

10. Xu Bolun, Oudalov Alexandre, Ulbig Andreas, Andersson Göran, Kirschen D.s. Modeling of Lithium-Ion Battery Degradation for Cell Life Assessment // IEEE TransactionsonSmartGrid. 99. 2016. 1-1. 10.1109/TSG.2016.2578950.

11. Willmott Cort J., Matsuura, Kenji, Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance // Climate Research. December 19, 2005, no. 30, pp. 79-80.

12. *Olah C.* Understanding LSTM Networks, 2015. URL: http://colah.github.io/posts/2015-08-Understanding-LSTMs/

13. Dieselnet. Nonroad Transient Cycle (NRTC). 2019. URL: https://www.dieselnet.com/standards/cycles/nrtc.php.

DIGITAL TWIN CREATION AND INTEGRATION

VALERIA A. SURIMOVA,
Moscow, Russia, surimova.lera@mail.ru

ELENA A. SKORODUMOVA,
Moscow, Russia, eas@mtuci.ru

KEYWORDS: *Digital Twin, Neural Networks, Collaborative Simulation, Big Data, Python*

ABSTRACT

Introduction. Smart lifecycle services, along with the adoption of other smart manufacturing strategies, show significant potential to increase the productivity and competitiveness of enterprises. There is a clear need for high-quality process models and software representations of physical hardware that reflect the evolution of their physical counterparts in particular detail. Digital twin technology can provide fertile ground for the development of IoT-based lifecycle applications. This paper proposes a software approach to the process of developing a digital twin. **The purpose of this work** is to study the methods of creating software frameworks in the context of digital twin technology, as well as to study the process of creating and integrating digital twins and developing our own tool. Existing methods for creating twins are considered and a self-developed Python library is described. The work uses the methods of the category of research in action and the philosophy of Agile development. **Methods.** The choice of methodology in seeking answers to questions that arise when studying methods for improving digital twins mainly falls into the category of research in action. In this paper, research in action is used as a qualitative tool, well suited to situations where the researcher seeks to achieve two different goals, namely: to solve a contemporary problem faced by the organization; contribute to a pool of knowledge that can later be used by other people to solve problems in the same class of problems. **Results.** Created library supports two modes of data retrieval: using periodic database queries and TCP socket connection. The experiments carried out as part of the work allow us to conclude that the library can already be used as a tool for creating a digital twin and its integration.

REFERENCES

1. Glaessgen E., Stargel D., "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles," *53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference – Special Session on the Digital Twin*, 2012, pp. 1-14.

2. Ponomarev K.S., Feofanov A.N. Digital twin of production as a tool for digitalization of technological processes of an enterprise. *Actual trends and prospects for the development of science, technology, technology: a collection of scientific papers based on the materials of the International Scientific and Practical Conference*. Belgorod: LLC Agency for Advanced Scientific Research (APNI), 2019, pp. 141-144.

3. Fuer Z., Weismann Z. The advantages of the "digital twin". *CAD / CAM / CAE Observer*. 2017. No. 5 (113), pp. 50-53; *Radio industry*. 2015. No. 4, pp. 56-64.

4. Ponomarev K., Kudryashov N., Popelnukha N., Potekhin V., "Main principals and issues of digital twin development for complex technological processes," *Ann. DAAAM Proc. Int. DAAAM Symp*., pp. 523-528, 2017.

5. Jarvinen P., "Research Questions Guiding Selection of an Appropriate Research Method Pertti Jarvinen Research Questions Guiding Selection of an Appropriate Research Method," *Proceedings of European Conference on Information Systems,* 2000, 3-5 July, 2000.

6. Richardson L., Ruby S., "RESTful Web Services,"O'Reilly Media, Inc., 2008.

7. Martin Otter, Hilding Elmqvist, Torsten Blochwitz, JakobMauss, Andreas Junghanns, Hans Olsson, "Functional MockupInterface-Overview", 2010.

8. Naik N., "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," *Proc. IEEE Int. Syst. Eng. Symp. (ISSE)*, Oct. 2017, pp. 1-7.

9. Beck K. et al., "Manifesto for Agile Software Development," Manifesto for Agile Software Development, 2001. URL: http://www.agilemanifesto.org/.

10. Xu Bolun, Oudalov Alexandre, Ulbig Andreas, Andersson Goran, Kirschen D.s. (2016). Modeling of Lithium-Ion Battery Degradation for Cell Life Assessment. *IEEE Transactionson Smart Grid*. 99. 1-1. 10.1109/TSG.2016.2578950.

11. Willmott Cort J., Matsuura Kenji (December 19, 2005). "Advantages of the mean absolute error (MAE) over the root mean square error (RMSE) in assessing average model performance". *Climate Research*. No. 30, pp. 79-80.

12. Olah C., "Understanding LSTM Networks," 2015. URL:http://colah.github.io/posts/2015-08-Understanding-LSTMs/

13. Dieselnet, "Nonroad Transient Cycle (NRTC)," 2019. URL:https://www.dieselnet.com/standards/cycles/nrtc.php.

INFORMATION ABOUT AUTHORS:

Valeria A. Surimova, Moscow Technical University of Communications and Informatics, student, Moscow, Russias, urimova.lera@mail.ru

Elena A. Skorodumova, Moscow Technical University of Communications and Informatics, Associate Professor, Ph.D., Moscow,

For citation: Surimova V.A., Skorodumova E.A. Digital twin creation and integration. H&ES Reserch. 2022. Vol. 14. No 4. P. 54-64. doi: 10.36724/2409-5419-2022-14-4-54-64 (In Rus)