

№ 2⁺⁰
2024 [72]

ИЗВЕСТИЯ

научно-технический журнал
ИНСТИТУТА ИНЖЕНЕРНОЙ ФИЗИКИ



27 апреля
День основания
Института



В НОМЕРЕ

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

2 Васильев В.В., Шахов Д.С.

Концепция неразъемного центроплана крыла из полимерных композиционных материалов

7 Порядина Д.А., Кучменко Т.А., Бузакин И.С.

Аутоидентификация автомобильных топлив по результатам полного анализа с применением метода главных компонент

10 Захаров В.Л., Смирнов Д.В., Демин И.В., Казаков Р.Р.

Анализ особенностей безопасной эксплуатации энергетического оборудования в частях космических войск

РАДИОТЕХНИКА И СВЯЗЬ

15 Шиманов С.Н., Крикунов А.А., Франков С.В.

Влияние диффузности метрик маршрутизаторов на оптимальность решения задачи маршрутизации в сети связи с коммутацией пакетов

22 Алаторцев А.И., Подвигин С.В., Бакмаев С.М.-К.

Модель квантового повторителя на азотной вакансии в монокристалле алмаза, как перспективное направление для реализации защищенных квантовых сетей

26 Зеленевский В.В., Зеленевский Ю.В., Попов А.В., Дурнов А.С., Наконечный А.Б.

Статистический анализ способов повышения помехоустойчивости систем передачи данных

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

31 Таганов Н.С., Бессонов М.А.

Построение почтового анализатора DLP системы на основе ключевых слов

39 Руденко Э.М., Семикина Е.В.

Методика расчета эйлеровых и гамильтоновых маршрутов для БПЛА с помощью редукции

45 Шолохов А.В., Лычагов А.С., Карпов К.В.

Определение факта нахождения подвижного объекта на участке цифровой карты дороги

49 Коломбет В.А., Лесных В.Н., Елистратов А.В.

Перспектива исследования психоактивных веществ в биофизическом психоанализе

57 Дараган А.Д., Ефремов А.А., Клементьев Е.Г., Руденко Э.М., Семикина Е.В.

Целевые функции маршрутов на эйлеровых и гамильтоновых графах

62 Абуд Б., Гончаров В.В.

Эффективность шифрования изображений с использованием AES и эллиптических кривых: экспериментальная оценка

71 Смуров С.В., Волков Г.Г.

Унитарные симметрии в партонной динамике протона

79 Атакищев О.И., Грибунин В.Г., Комаров И.Д., Борисенко А.Ю., Ермакова Ю.С.

Методика обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стеганографического анализа передаваемой информации

86 Пушкарева Е.Ю., Пискулин И.В.

Методика синтеза следящей системы управления движением перспективного РТК ВН в режиме автономного наведения

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И РОБОТОТЕХНИКА

92 Бугаков А.И., Шульга М.М.

Выбор и интеграция признаков для непрерывной адаптивной многофакторной аутентификации пользователя смартфона

ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

97 Лесных В.В., Зверев И.А.

Творческая интерпретация научных фактов как элемент подготовки инженерных и научных кадров (опыт создания научно-исторического квеста)

НАУЧНЫЕ ОБЗОРЫ • НАУЧНЫЕ РЕЦЕНЗИИ • ОТЗЫВЫ

104 Емелин Н.М.

Тенденции развития наукоградов как территорий с высоким научно-технологическим потенциалом

107 Куприянов А.И.

120 лет радиоэлектронной борьбы: история, современность, перспективы

112 СОБЫТИЯ

113 AUTHORS

115 ЭТИКА НАУЧНЫХ ПУБЛИКАЦИЙ

116 ТРЕБОВАНИЯ К АВТОРАМ СТАТЕЙ

Научно-технический журнал

**ИЗВЕСТИЯ
Института инженерной физики
№2 (72) 2024**

Издается с апреля 2006 г. Выходит ежеквартально

ISSN 2073-8110

Включен в «Перечень ВАК»

по научным специальностям:

- 2.2.11. Информационно-измерительные и управляющие системы
- 2.2.15. Системы, сети и устройства телекоммуникаций
- 2.3.1. Системный анализ, управление и обработка информации
- 2.3.6. Методы и системы защиты информации, информационная безопасность

Относится к категории К-2 (в соответствии с Распределением журналов по категориям (письмо ВАК от 06.12.2022 № 02-1198)).

Главный редактор,
председатель редакционного совета
и редакционной коллегии

Алексей Николаевич Царьков

Президент АНО «Институт инженерной физики»,
заслуженный деятель науки РФ,
доктор технических наук, профессор

Редакционный совет

Геннадий Иванович Азаров

главный научный сотрудник ФГУП «16 ЦНИИИ МО РФ»
заслуженный деятель науки РФ, заслуженный
изобретатель РФ, лауреат Государственной
премии РФ, лауреат премии Правительства РФ,
доктор технических наук, профессор

Сергей Владимирович Дворянkin

начальник департамента Государственной
корпорации «РОСТЕХ» ОАО КРЭТ,
доктор технических наук, профессор

Николай Михайлович Емелин

главный научный сотрудник
ФГБУ НТИМИ,
заслуженный деятель науки и техники РСФСР,
доктор технических наук, профессор

Валерий Иванович Николаев

научный референт ОАО «Концерн «Созвездие»,
лауреат Государственной премии СССР,
лауреат премии Правительства РФ,
доктор технических наук, профессор

Владимир Георгиевич Редько

заместитель руководителя
Центра оптико-нейронных технологий
НИИ системных исследований РАН,
доктор физико-математических наук

Юрий Александрович Романенко

старший научный сотрудник
филиала ВА РВСН им. Петра Великого (г. Серпухов)
заслуженный деятель науки РФ,
доктор технических наук, профессор

Анатолий Васильевич Тодосийчук

главный научный сотрудник Центра научно-
информационных исследований по науке,
образованию и технологиям Института научной
информации по общественным наукам РАН, почетный
работник науки и техники РФ, доктор экономических
наук, профессор

Игорь Анатольевич Шеремет

заместитель директора Российского фонда
фундаментальных исследований по науке,
академик РАН, доктор технических наук, профессор

Редакционная коллегия

Олег Николаевич Андрух

почетный работник науки и техники РФ,
кандидат технических наук, доцент

Борис Фёдорович Безродный

доктор технических наук, профессор

Сергей Борисович Беркович

почетный геодезист РФ

доктор технических наук, профессор

Владимир Эрнестович Бородай

лауреат Государственной премии СССР,

кандидат технических наук,

старший научный сотрудник

Игорь Александрович Бугаков

заслуженный изобретатель РФ,

почетный работник науки и техники РФ,

доктор технических наук, профессор

Вадим Геннадьевич Грибунин

почетный работник науки и техники РФ,

доктор технических наук, доцент

Сергей Григорьевич Данилюк

доктор технических наук, профессор

Владимир Владимирович Зеленевский

почетный работник науки и техники РФ,

доктор технических наук, профессор

Николай Николаевич Казаков

член Союза писателей России

выпускающий редактор

Олег Павлович Кузнецов

кандидат технических наук, доцент

Александр Ильич Куприянов

доктор технических наук, профессор

Анатолий Викторович Мазин

доктор технических наук, профессор

Алексей Сергеевич Марков

доктор технических наук,

старший научный сотрудник

Дмитрий Геннадьевич Митрофанов

заслуженный изобретатель РФ,

доктор технических наук, профессор

Роман Леонидович Мусатов

кандидат технических наук

заместитель главного редактора

Игорь Николаевич Оков

доктор технических наук, профессор

Владимир Петрович Пашинцев

заслуженный работник высшей школы РФ,

доктор технических наук, профессор

Дмитрий Вячеславович Смирнов

почетный работник науки и техники РФ,

доктор технических наук, доцент

Сергей Владимирович Смуров

почетный работник науки и техники РФ,

доктор технических наук, профессор

Валерий Николаевич Умников

доктор технических наук, профессор

Владимир Анатольевич Цимбал

заслуженный деятель науки РФ,

доктор технических наук, профессор

Сергей Николаевич Шиманов

почетный работник высшего профессионального

образования РФ, почетный радист РФ,

доктор технических наук, профессор



Алексей Николаевич Царьков

Президент Института инженерной физики

заслуженный деятель науки РФ

доктор технических наук, профессор

почетный гражданин города Серпухова

Дорогие друзья, уважаемые коллеги!
27 апреля Институту инженерной физики
исполняется 31 год!

Поздравляю всех коллег, единомышленников,
партнеров с Днем рождения Института!

За более чем три десятилетия мы вместе своим трудом, профессионализмом и опытом сделали наш Институт стабильным авторитетным предприятием оборонно-промышленного комплекса России, передовым научно-производственным центром Московской области, градообразующим предприятием городского округа Серпухов. На сегодняшний день Институт достиг значительных успехов в проведении научно-исследовательских и опытно-конструкторских работ, наши ученые занимаются разработкой и внедрением высокотехнологичных инноваций на мировом уровне в интересах развития науки и техники, для укрепления обороноспособности нашей страны. Институт постоянно улучшает качество оказываемых населению услуг в области проектирования, инсталляции и обслуживания систем связи и технических систем безопасности. Используя передовые технологии обучения и организации учебного процесса, Институт успешно реализует интеграцию науки и образования.

Важно, что наш коллектив профессионалов не останавливается на достигнутом – Институт постоянно наращивает научно-производственный и материально-технический потенциал. Мы идем в ногу со временем, в каждом направлении достигаем стабильных лучших результатов. Понимая, что развитие – залог успеха, мы осваиваем новые направления научных исследований и разработок, готовим научные кадры, модернизируем научно-производственную базу, повышаем качество услуг.

Постоянно строится, наращивает мощности Технопарк в сфере высоких технологий «ТехноИнноватика», в этом заслуга всего нашего коллектива и резидентов. Мы говорим слова благодарности инвесторам, Главе и администрации г.о. Серпухова за помощь и поддержку в развитии Технопарка в сфере высоких технологий как одного из важнейших центров будущего наукограда Большой Серпухов. Впереди большие перспективы, много планов и работы на благо развития нашего региона.

Коллектив Института проводит общественную, патриотическую, духовно-просветительскую работу, занимается благотворительностью, оказывает поддержку военнослужащим в зоне СВО и членам их семей. Считаю это нашим общим важным делом.

В День образования Института выражаю сердечную благодарность тем, с кем начинали создавать Институт, тем, кто сегодня вкладывает свой труд, талант, знания и опыт в его развитие и процветание! Желаю нашему коллективу идти только вперед в научной, производственной, образовательной деятельности, новых достижений и успехов на благо нашей Родины!

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

УДК 629.7.021



КОНЦЕПЦИЯ НЕРАЗЪЕМНОГО ЦЕНТРОПЛАНА КРЫЛА ИЗ ПОЛИМЕРНЫХ КОМПОЗИЦИОННЫХ МАТЕРИАЛОВ THE DESIGN CONCEPT OF AN ALL-IN-ONE CENTER WINGBOX MADE OF POLYMER COMPOSITE MATERIALS

Валентин Владимирович Васильев

кандидат технических наук, доцент

МАИ (НИУ)

Адрес: 125993, Москва, Волоколамское шоссе, д. 4

Тел.: +7(495)556-90-11

Денис Сергеевич Шахов

студент

филиал МАИ (НИУ) «Стрела»

Адрес: 140181, Московская обл.,

г. Жуковский, ул. Жуковского, д. 8

Тел.: +7(926)728-24-52

E-mail: denshakhov911@yandex.ru

Аннотация

Приводится описание конструкции и отдельных технологических процессов производства неразъемного центроплана крыла самолета из полимерных композиционных материалов. Отмечаются характерные преимущества и недостатки предлагаемой конструкции, по сравнению с существующими конструкциями.

Ключевые слова: центроплан крыла самолета, полимерные композиционные материалы, неразъемная конструкция, технология производства, выкладка, намотка

Summary

A description of a structure and individual technological processes for the production of the all-in-one center wing box made of polymer composite materials is proposed. Typical advantages and disadvantages of the proposed design are noted, compared with existing ones.

Keywords: center wing box, polymer composite materials, an all-in-one airframe structure, technology of manufacturing, lay-up, filament wending.

Улучшение качества проектирования в авиационной промышленности может быть достигнуто созданием научно-технического задела по перспективным направлениям за счет использования в разработке проекта результатов опережающих НИОКР [1].

Одним из наиболее перспективных направлений проектирования, применительно к гражданской авиации, является эффективное внедрение полимерных композиционных материалов (ПКМ) в конструкции высоконагруженных агрегатов планера самолета. Интерес к нему обусловлен высокими, по сравнению с традиционными металлическими сплавами, значениями удельной прочности и удельной жесткости

данской авиации, является эффективное внедрение полимерных композиционных материалов (ПКМ) в конструкции высоконагруженных агрегатов планера самолета. Интерес к нему обусловлен высокими, по сравнению с традиционными металлическими сплавами, значениями удельной прочности и удельной жесткости

Таблица 1

Качественное равенство физико-механических свойств металлических сплавов и волокон слоистых ПКМ вдоль волокна [2,3]

Материал	Свойства				
	ρ	σ_c	E	σ_c/ρ	E/ρ
	г/см ³	ГПа	ГПа	(м ² /с ²)×10 ⁶	(м ² /с ²)×10 ⁶
Алюминиевые сплавы	2,7	0,4-0,6	7,2	0,15	27
Титановые сплавы	4,5	1,1-1,3	11	0,16	24,5
Высокопрочные стали	7,8	1,2-1,4	21	0,14	27
Стеклопластики	1,5-2	0,7-2	22,1-58	0,5-1	15-30
Углепластики	1,8-2,2	1,1-2,5	22,1-58	0,7-2	40-80

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

армирующих волокон и созданных на их основе ПКМ (характеристики приведены в *таблице 1*).

Необходимость упрощения процедуры сертификации типа новых воздушных судов обусловила внедрение ПКМ в авиационные конструкции по концепции «black metal», заключающейся в прямой замене металлических элементов на композитные с их незначительной модификацией [2]. Данный подход не позволил добиться существенного снижения массы готовых изделий и определил особенность современного проек-

тирования конструкций из ПКМ – совместное создание материала и конструкции. Наиболее актуальными направлениями создания конструкций из ПКМ считаются [4]:

- применение безавтоклавных технологий формования;
- широкая автоматизация и минимизация числа производственных операций;
- переход от терморепактивных связующих к термопластичным.

Так, при создании самолета МС-21 впервые



Рис. 1. Центроплан самолета МС-21 [5]

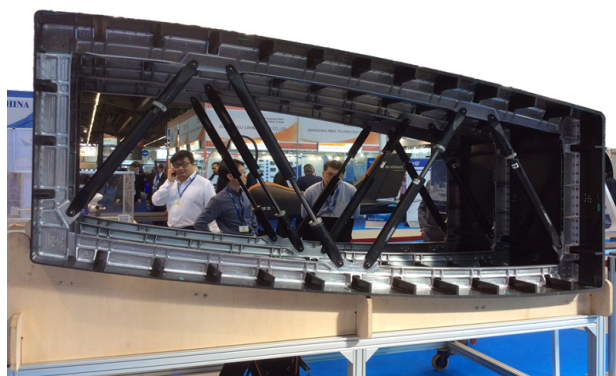


Рис. 2. Демонстратор технологии композитного центроплана Airbus Technocentre Nantes [6]

в практике отечественного самолетостроения были получены крупногабаритные подкрепленные панели, созданные за один производственный цикл с помощью технологии VARTM (вакуумной инфузии). Эти панели затем собирают в крупногабаритные агрегаты. Центроплан самолета МС-21 изображен на *рисунке 1* [5].

Корпорацией Airbus в 2019 году был представлен прототип неразъемного кессона центроплана из ПКМ (*рисунком 2*). Агрегат планировался к применению на обновленном самолете А320 [6].

Анизотропия и вариация механических свойств; критический характер критерия проч-

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ности на межслойный сдвиг; низкая ударная вязкость конструкционных углепластиков задают особенности проектирования силовых элементов конструкций из ПКМ: введение дополнительного коэффициента безопасности $f_{доп}=1,25-2,0$; существенное снижение допускаемых напряжений в конструкции ввиду необходимости неразрушающего контроля и др. [7].

Предлагаемая концепция конструкции центроплана базируется на выполнении каркаса панелей и стенок центроплана из углепластиковых типовых подборок швеллерного сечения (рисунк 3), с последующей намоткой дополнительных слоев обшивки поверх каркаса и далее совместным полным отверждением для формирования неразъемной конструкции [8].

Схема конструктивно-технологического членения каркаса центроплана (рисунк 4) позволяет разделить каркас на составляющие для удобства сборки. Сборка осуществляется последовательно-параллельным методом.

Поперечный набор центроплана состоит из силовой и рядовых нервюр (рисунк 5). Силовая нервюра находится в плоскости симметрии центроплана и выполнена фрезерованием из плиты высокоресурсного алюминиевого сплава 1163Т.

Рядовые нервюры представляют собой ферменную конструкцию из поясов, жестких узлов и стержней, также изготавливаются из сплава

1163Т. Пояса представляют собой прессованные профили, к которым с помощью болтовых соединений присоединяют жесткие узлы и стержни по принципу «ухо-вилка». Сборка нервюр осуществляется с фиксацией внешнего контура.

Принципиальная схема технологического процесса производства типовых швеллерных элементов панелей и стенок центроплана состоит из следующих операций:

- 1) на поверхность оснастки осуществляется автоматизированная выкладка сухих лент стекло- и углеволокна с ориентацией слоев $0^\circ, \pm 45^\circ, 90^\circ$;
- 2) формируется технологический пакет (преформа, пленочное связующее, разделительные и дренажные слои, вакуумный мешок и т.д.);
- 3) проводится формование с неполным отверждением по RFI-технологии в термокамере под действием вакуума.

Технология автоматизированной выкладки из ПКМ применяется при производстве силовых элементов крыла самолета МС-21. Устройства для выкладки и оснастки изображены на рисунке 6.

Слой стекловолокна наносится для защиты от гальванической коррозии металлических элементов нервюр и крепежа при контакте с углепластиком. Для исключения сверления отверстий в отформованных элементах предлагается наличие на поверхности оснастки штифтовых элементов малого диаметра для формирования отверстий путем раздвижки волокон. Полученные элементы панелей и стенок из ПКМ пропитываются пленочным связующим и подвергаются неполному отверждению для последующего придания элементам формы теоретического контура при сборке.

Сборка панелей и стенок, изображенных на рисунках 7 и 8 осуществляется в сборочных устройствах с фиксацией по внешнему контуру. Торцевые поверхности склеиваются, а в заранее

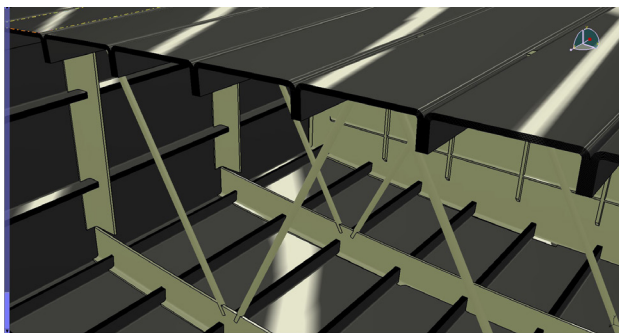


Рис. 3. Конструкция каркаса центроплана из типовых элементов швеллерного сечения

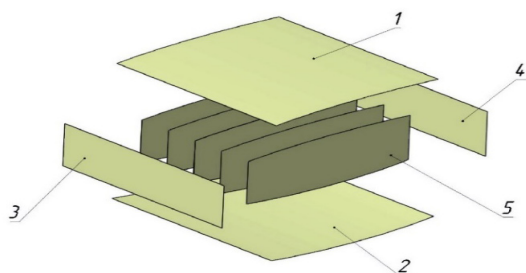


Рис. 4. Схема технологического членения каркаса центроплана: 1 – верхняя панель; 2 – нижняя панель; 3 – передняя стенка; 4 – задняя стенка; 5 – нервюры.

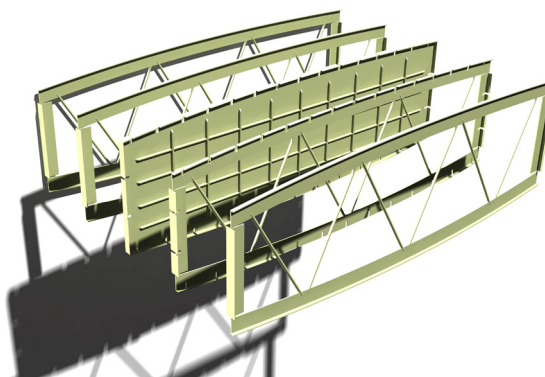


Рис. 5. Нервюры центроплана

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

отформованные отверстия помещаются иглы, образуя клееегольчатые соединения.

Особенность полученных конструкций панелей и стенок состоит в наличии пустот, образующихся за счет технологических радиусов укладки лент, как показано на *рисунке 9*. В эти пустоты помещают заранее изготовленные по их форме жгуты из дисперсного (сферопластик или пенопласт) или непрерывного волокнистого наполнителя (однонаправленные ленты и ткани), полученные по технологии экструзии, пултрузии, скручиванием из ленты, выкладкой или объемным плетением.

Далее производится перенос полученного каркаса на установку для намотки внешнего слоя обшивки. Намотка производится «сухим» методом. На финальном этапе производится полное отверждение полученной конструкции, упрощенно изображенной на *рисунке 10*, в термокамере.

К преимуществам предлагаемой конструкции относятся:

- отработанная технология автоматизированной выкладки;
- увеличенная скорость пропитки волокон по RFI-технологии (пропитка пленочным связующим), большая точность изготовления и меньшая вариация механических свойств получаемых изделий по сравнению с инфузионной технологией [11];
- исключение операций сверления отверстий в композитных элементах, что повышает прочность конструкции на межслойный сдвиг и смятие;
- унификация оснастки для производства типовых швеллерных элементов.

Предлагаемая конструкция неразъемного центроплана из ПКМ, базирующаяся, с одной стороны, на использовании типовых подборок продольных элементов швеллерного сечения и



Рис. 6. Автоматизированная выкладка углеволокна на оснастку на примере производства лонжерона крыла самолета МС-21 [9]

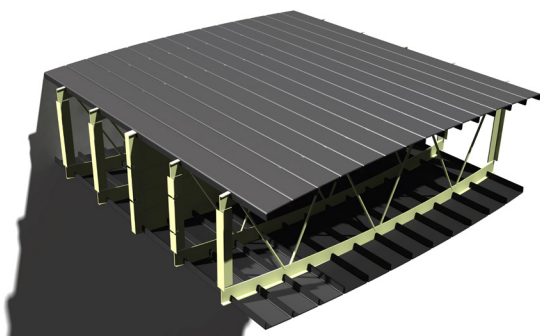


Рис. 7. Панели центроплана

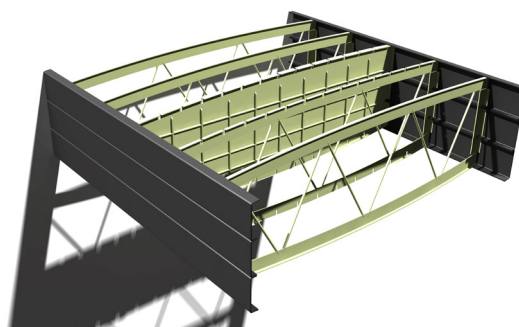


Рис. 8. Стенки центроплана

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

на отработанных и проверенных конструктивно-технологических приемах работы с ПКМ – с другой. Данная концепция обещает уменьшить количество проблемных вопросов изготовления и эксплуатации конструкций. В первую очередь это достигается исключением сверления отверстий в ПКМ для соединения элементов конструкции в единое целое и связанной с этим возможностью повышения расчетных напряжений, снижения массы, упрощения изготовления.

Литература

1. Проектирование самолетов / под ред. М.А. Погосяна. 5-е изд., перераб. и доп. М.: Инновационное машиностроение, 2018. 864 с.
2. Гришин В.И., Дзюба А.С., Дударьков Ю.И. Прочность и устойчивость элементов и соединений авиационных конструкций из композитов. М.: Издат. физ.-мат. лит-ры, 2013. 272 с.
3. Ендогур А.И. Проектирование авиационных конструкций. Проектирование конструкций деталей и узлов: Уч. пособ. М.: Изд-во МАИ-ПРИНТ, 2009. 540 с.
4. Славин А.В. Перспективы применения полимерных композиционных материалов в авиационных конструкциях в 2025-2035 гг. (обзор) / А.В. Славин, К.И. Донецкий, А.В. Хрульков // Труды ВИАМ, 2022. № 11(117). С. 81-92.
5. Центроплан для сборки фюзеляжа нового российского пассажирского самолета МС-21 доставили на Иркутский авиазавод. [Электронный ресурс] // CompMechLab – разработка и применение цифровых двойников (digital twin), цифровое проектирование, CAD/CAE\CAM\CAO\NPC технологии. URL: <https://fea.ru/news/6141> (дата обращения: 22.12.2023).
6. Gardiner G. The path to OOA wings with minimal fasteners [Электронный ресурс] // CompositesWorld. 2021. URL: <https://www.compositesworld.com/articles/the-path-to-ooa-wings-with-minimal-fasteners> (дата обращения: 10.09.2021).
7. Шахов Д.С. Высоконагруженные агрегаты планера самолета из полимерных композиционных материалов: особенности конструкции и проблемы создания / Авиация России: прошлое, настоящее, будущее: Материалы IV научно-практической конференции филиала «Стрела» МАИ в г.о. Жуковский (30 ноября-1 декабря 2020 г.). Жуковский, 2021. 316 с.
8. Шахов Д.С. Концепция конструкции неразъемного центроплана крыла из ПКМ / Авиация России: прошлое, настоящее, будущее: Материалы VI научно-практической конференции филиала «Стрела» МАИ, Жуковский 24-25 ноября 2022 г. // Филиал «Стрела» МАИ (НИУ). Жуковский: Филиал «Стрела» МАИ, 2023. 388с.
9. МС-21 – лайнер с «черным» крылом [Электронный ресурс] // Авиация России. 2016. URL: <https://aviation21.ru/ms-21-layner-s-chyornym-krylom/> (дата обращения: 22.12.2023).
10. Дудченко А.А. Оптимальное проектирование элементов авиационных конструкций из композиционных материалов: Уч. пособ. М.: Изд-во МАИ, 2002. 84 с.
11. Особенности изготовления ПКМ методом RFI / М.М. Григорьев, Д.И. Коган, О.Н. Твердая, Н.Н. Панина // Труды ВИАМ, 2013. № 4. С. 3.

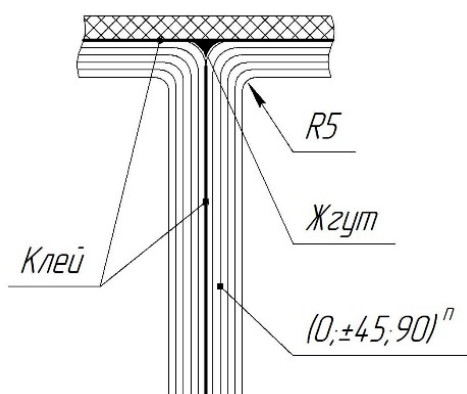


Рис. 9. Сечение панели обшивки с учетом заполняющего жгута [10]

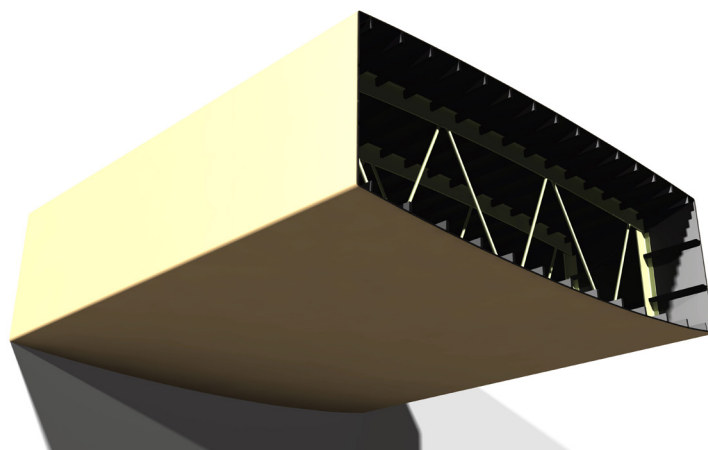


Рис. 10. Модель центроплана без крепежных элементов

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

543.42:665.753.4

АУТОИДЕНТИФИКАЦИЯ АВТОМОБИЛЬНЫХ ТОПЛИВ ПО РЕЗУЛЬТАТАМ ПОЛНОГО АНАЛИЗА С ПРИМЕНЕНИЕМ МЕТОДА ГЛАВНЫХ КОМПОНЕНТ¹ AUTO-IDENTIFICATION OF AUTOMOTIVE FUELS BASED ON THE RESULTS OF THE FULL ANALYSIS USING THE PRINCIPAL COMPONENT METHOD

Дарья Александровна Порядина

кандидат химических наук
преподаватель кафедры
«Материаловедения и ремонта вооружения»
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: +7 (977) 261-83-65
E-mail: sibilda1@yandex.ru

Татьяна Анатольевна Кучменко

доктор химических наук, профессор
заведующая кафедрой
«Физической и аналитической химии»
ФГБОУ ВО «Воронежский государственный
университет инженерных технологий»
Адрес: 394036, г. Воронеж,
проспект Революции, д. 19
Тел.: +7 (920) 422-77-25
E-mail: tak1907@yandex.ru

Иван Сергеевич Бузакин

курсант 5 курса факультета №1
«Стартовых и технических комплексов»
филиал ВА РВСН им. Петра Великого
(г. Серпухов)

Аннотация

В статье показана возможность применения метода главных компонент для идентификации вида автомобильных топлив (зимнее дизельное топливо, летнее дизельное топливо, керосин) по результатам полного анализа физико-химических показателей качества.

Ключевые слова: дизельное топливо, керосины, аутоидентификация, метод главных компонент, стандартные физико-химические показатели качества.

Summary

The article shows the possibility of using the method of main components to identify the type of automotive fuels (winter diesel fuel, summer diesel fuel, kerosene) based on the results of a complete analysis of physico-chemical quality indicators.

Keywords: diesel fuel, kerosene, auto-identification, principal component method, standard physical and chemical quality indicators.

В настоящее время идентификацию автомобильных топлив (бензины и дизельное топливо различных марок) проводят по величине октанового числа. Показатель «октановое число» определяется двумя методами – моторным и исследовательским [1].

Моторный метод определения октанового числа бензинов проводится на крупногабаритной и дорогостоящей установке, имитирующей действительный автомобильный двигатель, в котором происходит сжигание исследуемого образца с определением количества теплоты. Такое определение проводят только в аккредитованных лабораториях.

Исследовательский метод проводится в лабо-

ратории, путем полной перегонки исследуемого образца до сухого остатка, определению контрольных точек кривой разгонки; определению плотности и кинематической вязкости и последующим расчетом по эмпирической формуле [2]. Допускается различие между результатами моторного и исследовательского метода 5-6 единиц.

Для аутоидентификации видов дизельного топлива (летнее, зимнее, арктическое и всесезонного) необходимо определять температуру замерзания, температуру помутнения, температуру вспышки образцов [3]. Это показатели полного (арбитражного) анализа, которые определяются только в лабораториях.

В режиме на месте аутоидентификация авто-

¹ Работа выполнена в рамках программы «УМНИК» договор № 18814 ГУ/2023 от 26.09.2023 г.

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

мобильных топлив невозможна существующими методиками.

В настоящее время активно развивается новый раздел аналитической химии – хемометрика. Цель хемометрики – получение химических данных с помощью математических методов обработки и добычи данных [4].

В рамках гранта УМНИК разрабатывается портативное устройство на пьезосенсоах для аутоидентификации видов топлива и определения воды в дизельных топливах в режиме на месте. В соответствии с календарным планом на первом этапе оценивается возможность аутоидентификации видов дизельных топлив по результатам полного анализа.

Цель работы: оценить возможность аутоидентификации видов дизельных топлив по результатам полного анализа с применением метода главных компонент.

В качестве объектов исследования выбраны 26 образцов летнего дизельного топлива марки Л-0,2-62 и 25 образцов зимнего дизельного топлива марки ДТ З-0,2 минус 35, 1 проба керосина различных производителей различных производителей, выработанных по ГОСТ 305-82 [3].

Провели исследование образцов дизельного топлива на соответствие ГОСТ 305-82 по стандартным физико-химическим показателям качества: цетановое число (ЦЧ), плотность при 20°C (ρ , г/см³), фракционный состав – температура перегонки 50% топлива (Тп 50%, °C), температура перегонки 96 % топлива (Тп 96%, °C), кинематическая вязкость (ν , мм/с²), температура вспышки

(Т всп, °C), температура помутнения (Тпом, °C), температура замерзания (Тз, °C), кислотность (К, мг/100мл), содержание фактических смол (ФС, мг/100мл), ГОСТ 305-82 [5].

Для моделирования многомерных данных выборки топлив применялся метод главных компонент (МГК). Моделирование осуществлялось в программном обеспечении THE UNSCRAMBLER X V.10.4 (Норвегия, Осло).

В МГК моделировании участвовали 52 пробы топлив и 10 установленных параметров.

При построении модели по всем имеющимся данным установлено, что первые две главных компоненты объясняют 79% хранящейся в выборке информации. При этом пробы значительно разбиваются на три группы: летнее топливо, зимнее топливо и керосин (рисунки 1).

При этом установлено, то параметр цетановое число оказывает наименьшее влияние на разделение проб на классы в соответствии с их видом.

При исключении данного параметра при построении модели процент объясненной дисперсии увеличивается до 85% (рисунки 2).

Проследим возможность разбиения проб на группы внутри уже установленных групп: «летнее топливо», «зимнее топливо» (рисунки 3, 4).

При МГК моделировании летних и зимних топлив, установили, что наибольшее влияние на разбиение проб на группы оказывают такие параметры, как: температура 50% перегонки, температура 96% перегонки, Т вспышки в закрытом тигле, °C.

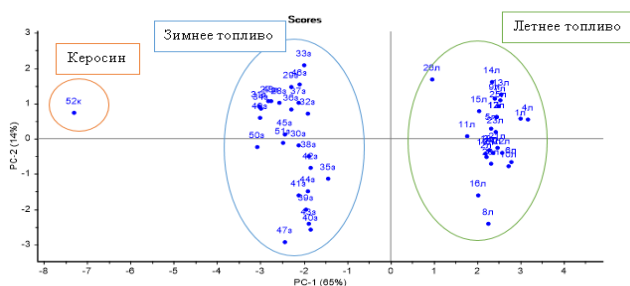


Рис. 1. График счетов проб топлив

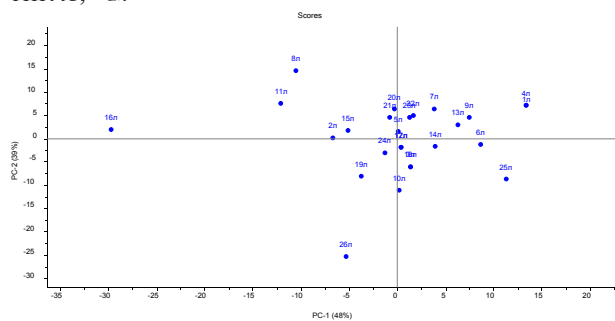


Рис. 3. График счетов летнего топлива

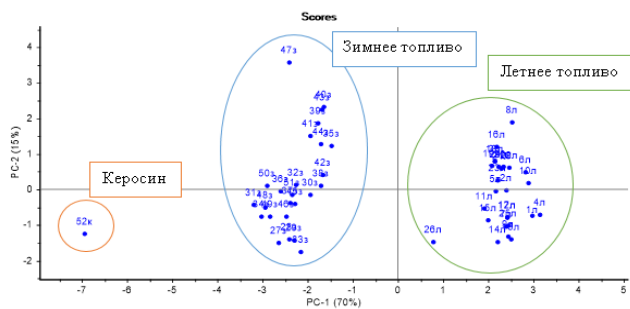


Рис. 2. График счетов проб топлив (исключен параметр «цетановое число»)

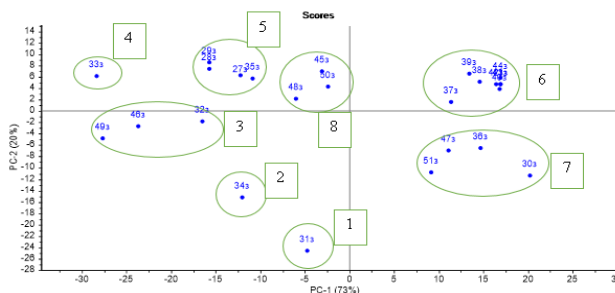


Рис. 4. График счетов зимнего топлива

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

Значительно выделяются из всей совокупности 16 л, 26 л, 8 л и 11 л имеют схожие характеристики (состав), аналогично 1 л и 4 л имеют максимально схожие характеристики. Остальные пробы относятся к одной группе по выбранным параметрам сравнения.

Применение в качестве входных параметров для метода главных компонент 10 параметров – стандартных физико-химических показателей качества дизельных топлив, позволяет решать задачи идентификации вида топлив – летнее дизельное топливо ДТ Л-0,2-62, зимнее дизельное топливо ДТ З-0,2 минус 35, керосин. Однако не позволяет решать задачи определения фальсификации, добавление керосина в пробу летнего дизельного топлива для улучшения его эксплуатационных свойств.

Дальнейшее исследование предполагается продолжить в направлении создания портативного устройства малого объема погружного типа. Измерительными элементами являются 4 пьезосенсора с разными покрытиями.

Такое устройство позволит без пробоподготовки, дополнительных операций, в малом объеме пробы, в течение 1-2 минут, бесконтактно, по составу газовой фазы оценить основные пока-

затели качества – содержание воды, соединений серы и кислотность.

Применение новых показателей аналитической информации позволит решать задачи аутоидентификации дизельных топлив при добавлении керосина.

Литература

1. ГОСТ 511-2022 Топливо для двигателей. Моторный метод определения октанового числа. М.: Российский институт стандартизации, 2023. 18 с.
2. ГОСТ 8226-2022 Топливо для двигателей. Исследовательский метод определения октанового числа. М.: Российский институт стандартизации, 2023. 35 с.
3. ГОСТ 305-2013 Топливо дизельное. Технические условия. М.: Издательство стандартов, 2013. 10 с.
4. Родионова О.Е. Хемометрический подход к исследованию больших массивов химических данных // Российский химический журнал, 2006. Т.1. №2. С. 128-129.
5. Сафонов Л.С., Ушаков А.И. Автомобильные топлива: Химотология. Эксплуатационные свойства. СПб.: НПИКЦ, 2002. 264 с.



ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ



УДК 658.58

АНАЛИЗ ОСОБЕННОСТЕЙ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ ЭНЕРГЕТИЧЕСКОГО ОБОРУДОВАНИЯ В ЧАСТЯХ КОСМИЧЕСКИХ ВОЙСК ANALYSIS OF THE FEATURES OF SAFE OPERATION OF POWER EQUIPMENT IN SPACE FORCE UNITS

Владимир Леонидович Захаров

доктор военных наук, профессор
действительный член АВН
профессор кафедры
ФГБОУ ВО МАИ (НИУ)
Адрес: 125993, Москва,
Волоколамское шоссе, д. 4
Тел.: +7 (905) 566-17-94
E-mail: varahas@yandex.ru

Дмитрий Вячеславович Смирнов

почетный работник науки и техники РФ
доктор технических наук, доцент
действительный член АИИ
профессор кафедры
ФГБОУ ВО МАИ (НИУ)
Первый Вице-президент Института
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл.,
г. Серпухов, Большой Ударный пер., д. 1а
Тел.: +7 (4967) 35-31-93
E-mail: dv_smr@iifmail.ru

Иван Вячеславович Демин

начальник эксплуатационного отделения
отдела энергетического обеспечения
базы обеспечения учебного процесса
ВКА имени А.Ф. Можайского
Адрес: 197198, Санкт-Петербург,
ул. Ждановская, д. 13
Тел.: 8 (911) 791-56-08

Рафаэль Рамисович Казаков

кандидат технических наук
заместитель начальника кафедры
«Тактики частей и подразделений
ракетно-космической обороны»
ВКА им. А.Ф. Можайского
Адрес: 197198, Санкт-Петербург,
ул. Ждановская, д. 13
Тел.: +7 (911) 223-59-67
E-mail: xoxlov1984@bk.ru

Аннотация

Определено понятие ситуации и нештатной ситуации в процессе эксплуатации энергетического оборудования. Рассмотрены основные причины возникновения нештатных ситуаций, представлены классификация нештатных ситуаций и статистика отказов на воздушных линиях электропередач различных объектов космических войск.

Ключевые слова: космические войска, система электроснабжения, энергетическое оборудование, объекты космических войск, нештатная ситуация, отказы элементов системы.

Summary

The concept of situation and emergency situation during the operation of power equipment is defined. The main causes of emergency situations are considered, the classification of emergency situations and statistics of failures on overhead power lines of various space forces facilities are presented.

Keywords: space forces, power supply system, power equipment, space forces facilities, emergency situation, failures of system elements.

Введение

Космические войска (КВ) являются одним из наиболее молодых родов войск. Выполняемые КВ задачи обширны, начиная от наблюдения за космическими объектами в околоземном космическом пространстве и заканчивая обеспечением наращивания орбитальной группировки космических средств в интересах страны.

Одной из важнейших составляющих поддержания вооружения КВ в готовности к применению по назначению является их непрерывное и бесперебойное обеспечение электроэнергией

заданных параметров качества, для чего каждый объект оборудован стационарной системой электроснабжения (СЭС).

СЭС включает в себя внешнюю, внутреннюю и автономную системы электроснабжения. В целом они составляют единый электротехнический комплекс объекта. Основу этого комплекса образует энергетическое оборудование (ЭО).

Все СЭС рассматриваемых объектов созданы по индивидуальным проектам. Каждый электротехнический комплекс имеет отличный от остальных по составу и мощности набор

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

потребителей. Объекты размещены в различных географических, климатических, экономических районах, следствием чего являются существенные различия условий эксплуатации их ЭО.

Ввиду особенностей территориального размещения ЭО практически не защищено от внешних воздействий, а также подвержено непосредственному влиянию факторов окружающей среды и применению противником различного рода подавляющих средств [1].

Особенности эксплуатации энергетического оборудования объектов

В ходе эксплуатации объектов ЭО возникают различные ситуации. Под ситуацией понимается совокупность состояний элементов системы эксплуатации ЭО и внешней среды, связанных между собой различными отношениями в рассматриваемый момент времени [2].

В зависимости от объекта управления ситуации делятся на: технические ситуации, возникающие в процессе управления техническими средствами; организационные ситуации, возникающие в процессе управления подчиненным л/с; организационно-технические ситуации, возникающие в процессе управления

техническими системами и л/с совместно.

Все ситуации делятся на штатные, т.е. предусмотренные эксплуатационной документацией, алгоритмами и программами штатного функционирования, и нештатные ситуации (НС). Под НС будем понимать ситуацию, не предусмотренную эксплуатационной документацией, программой и алгоритмами функционирования.

Все вышесказанное подтверждает актуальность исследований по обеспечению безопасной эксплуатации энергетического оборудования в частях.

Классификация нештатных ситуаций

НС могут быть классифицированы следующим образом:

1. По источнику воздействия:

- внешний источник воздействия (взаимодействие с другими системами, воздействие внешней среды). К внешним причинам относятся техногенные, природные, социально-экономические возмущения;

- внутренний источник возникновения (отказы элементов систем, ошибки обслуживающего л/с, т.е. технические, технологические, организационные и индивидуально-психологические факторы).



Рис. 1. Классификация НС



Рис. 2. Источники неопределенности описания НС

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

2. По динамике развития:

- статические (не развивающиеся);
- динамические (развивающиеся);

3. По последствиям:

- не критические (угрозы нарушения работоспособности оборудования нет);
- критические (угрожающие нарушением работоспособности агрегатов и систем);
- катастрофические (нарушение работоспособности агрегатов и систем, повлекшее за собой гибель λ/c);
- послеаварийные.

Схематично это можно представить [3] (рисунки 1).

Источники неопределенности описания НС приводятся на рисунке 2.

Описание нештатных ситуаций зависит от источников информации:

- неизвестность информации о решаемой задаче – полное или почти полное отсутствие какой-либо информации;
- недостоверность информации – возникает при неполном и (или) недостаточном сборе данных о событии; понимание о происходящих процессах формируется на основе приближенных моделей, а не на реально происходящих событиях; описание происходящих событий происходит размыто (не конкретизировано);
- неоднозначность информации – ситуация, возникающая при невозможности однозначно охарактеризовать происходящий процесс, в следствие чего прийти однознач-

но к одному решению невозможно.

Отказы элементов ЭО классифицируются по следующим признакам (рисунки 3).

Из представленной на рисунке 3 классификации нужно обратить внимание на последствия возникновения неисправностей и способы возможного их устранения, как наиболее актуальные в настоящее время. Вследствие постепенного старения техники и образцов вооружения не зависимо от видов и родов войск, все больше элементов и узлов ВВСТ подвергается отказам, зачастую связанными с их моральным и физическим износом. Зачастую отказавший элемент (узел) удается привести в работоспособное состояние силами расчета в кратчайшие сроки, но иногда возникают ситуации в результате которых происходит отказ всего изделия, что существенно сказывается на выполнении целевой задачи, или даже может привести к ее срыву.

По причинам возникновения НС на объектах ЭО могут быть классифицированы следующим образом (рисунки 4).

Из представленной классификации нештатных ситуаций необходимо выделить наиболее важные факторы, оказывающие влияние на энергетическое оборудование:

- неуправляемые природные воздействия – влияющие на ЭО посредством различных техногенных факторов;
- нерасчетные изменения параметров окружающей среды – влияющие на ЭО посредством изменения климатических явлений.

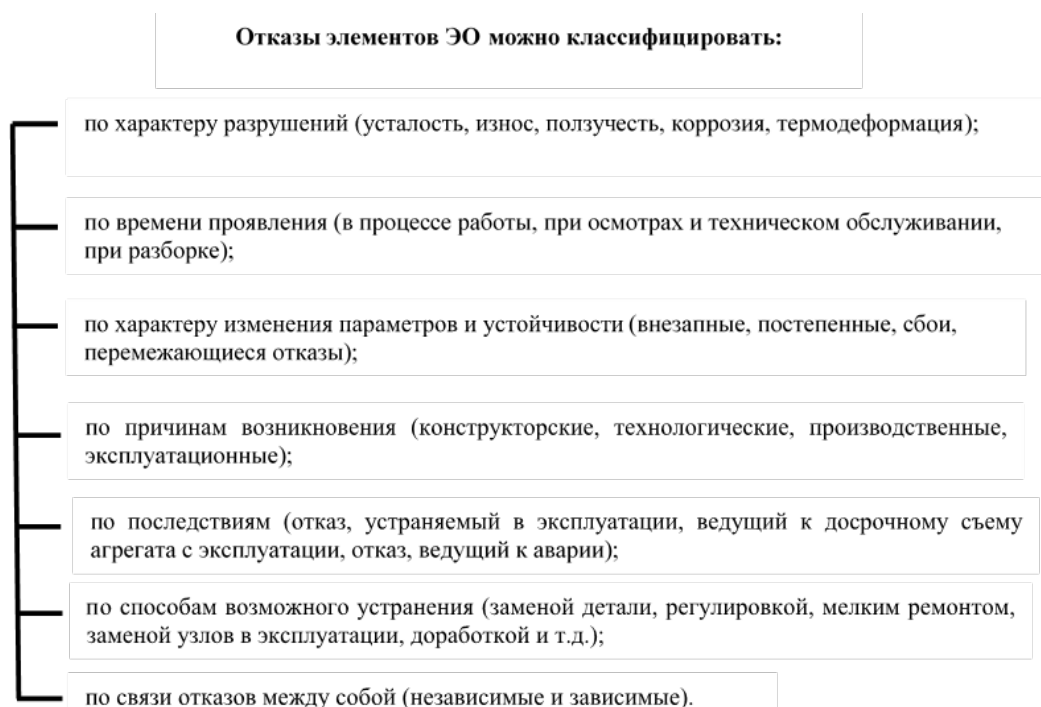


Рис. 3. Классификация отказов элементов ЭО

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

Нештатные ситуации в процессе функционирования энергетического оборудования

Во многих случаях причиной НС на объектах ЭО КВ являются отказы оборудования, возникновение которых зачастую вызвано сильным старением эксплуатируемого оборудования и низким качеством элементной базы. Особо опасной считается ситуация, когда посредством отказов отдельных узлов выходит из строя весь объект. На *рисунке 5* представлены различные виды отказов в ЭО.

Длительные сроки эксплуатации ЭО при отсутствии капитального ремонта и реконструкции приводят к тому, что увеличивается количество нештатных ситуаций, сопровождающихся частичным или полным прекращением снабжения потребителей электроэнергией. Это, в свою очередь, снижает надежность выполнения задач, выполняемых объектами.

При возникновении нештатных ситуаций и выходе из строя некоторого оборудования объекта в качестве последствий могут выступать:

- запрет на применение определенной группы режимов эксплуатации, связанных с данным объектом ЭО;
- запрет на применение определенного сочетания режимов эксплуатации;

тания режимов эксплуатации;

- запрет на использование некоторых видов ресурсов и т.п.

Основными причинами отказов являются износ, старение оборудования и ошибки персонала. Использование новых средств могло бы в большей мере решить эту проблему, однако высокая стоимость, длительный срок исследований и разработки не позволяют этого сделать.

В *таблице 1* представлен подробный анализ основных отказов на воздушных линиях электропередач на объектах и станциях.

В *таблице 1* представлены варианты отказов на космодромах и частях ПРН с указанием причин возникновения, количества и основных узлов. К наиболее серьезным можно отнести:

- отказ привода выключателя вследствие короткого замыкания в катушке управления;
- набросы посторонних предметов на шины;
- разрушение межфазной изоляции вследствие старения кабельной линии.

Рассмотренные выше отказы встречаются наиболее часто (от 9 до 12), но наиболее опасным является длительное время восстановления работ, которое достигает 16 ч/часов. Это может привести к срыву выполнения задачи.

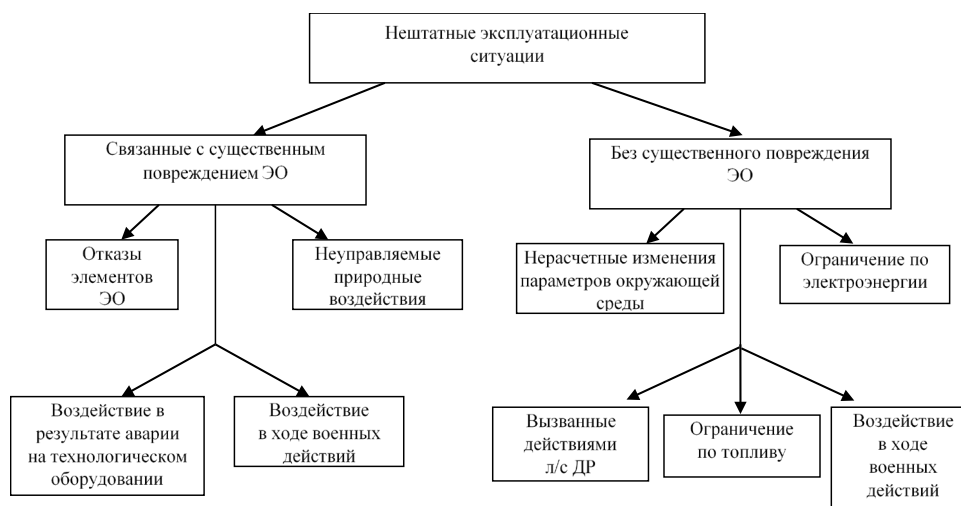


Рис. 4. Классификация НС по причинам их возникновения

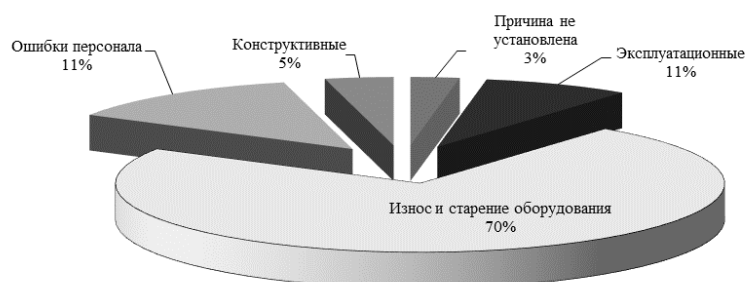


Рис. 5. Причины возникновения отказов в ЭО

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

Таблица 1
Отказы на воздушных линиях электропередач

Место аварии	Тип оборудования	Описание отказа	Количество отказов	Среднее время восстановления чел/час	Последствия
1	2	3	4	5	6
объект	ВВ-10	Разрушение опорного изолятора колонки отделителя с последующим самопроизвольным включением выключателя и разрушением полюса	4	18	Перебой в электроснабжении объекта
объект	ВВ-110	Падение дугогасительных камер из-за разрушения их рубашек	2	11	Перебой в электроснабжении объекта
объект	ВВ-110	Разрушение дугогасительной камеры в момент отключения выключателя	3	15	Перебой в электроснабжении объекта
объект	ВМ-10	Разрушение и возгорание шунта дугогасительной камеры из-за заклинивания её подвижного контакта	2	8	Перебой в электроснабжении объекта
Отказы в закрытых распределительных устройствах 10 кВ					
Станции	яч. 10 кВ	Отказ привода выключателя вследствие короткого замыкания в катушке управления	12	9	Обесточивание ТА станции
Станции	Система сборных шин	Набросы посторонних предметов на шины	11	16	Срыв выполнения задачи
Станции объекты	яч. 10 кВ	Короткое замыкание при ошибочном включении заземляющих ножей разъединителя	4	15	Срыв выполнения боевой задачи
Станции	СВиКВ	Ложное срабатывание устройств релейной защиты и автоматики (РЗА), отказы во вторичных цепях	8	4	Нарушение температурно-влажностного режима
Отказы в подстанциях КТП-1000/10-0.4 кВ с РУ-0.4 кВ					
Станции	A137	Разрушение автомата вследствие короткого замыкания при перекосе контактов	7	4	Обесточивание ТА станции
Станции	АВМ-20СВ	Отказ привода автоматического выключателя по причине короткого замыкания в катушке управления	5	6	Срыв выполнения задачи
Отказы кабельных линий ЭП					
Станции объекты	Кабельная линия	Пробой и короткое замыкание в соединительных муфтах кабельных линий	7	14	Перебой в электроснабжении объекта
объекты	Кабельная линия	Разрушение межфазной изоляции вследствие старения кабельной линии	9	13	Перебой в электроснабжении объекта

Заключение

Из анализа следует, что нештатные ситуации ЭО объектов КВ могут приводить к срыву выполнения задачи, крупному материальному ущербу, разрушениям и гибели личного состава. В самом общем случае НС приводят к снижению эффективности эксплуатации ЭО объектов КВ. Частыми причинами отказов являются износ и старение оборудования, а также ошибки персонала. Наиболее выигрышным решением данного вопроса является проведение более тщательного анализа возникновения отказов на конкретных образцах вооружения КВ и их дальнейшая модернизация с целью улучшения надежности и стабильности работы изделия.

Литература

1. Фролов Ю.М. Электроснабжение промышленных предприятий: уч. пособ. для вузов. М.: Юрайт, 2023. 351 с.
2. Аварии и катастрофы. Предупреждение и ликвидация последствий. Кн.3. М.: Изд-во Ассоциации строительных вузов, 1998. 413 с.
3. Парфенов И.И. Искусственный интеллект в управлении организационно-техническими системами / И.И. Парфенов, М.Я. Парфенова, В.И. Глинкин // Вопросы управления и проектирования в информационных и кибернетических системах. Уфа: Уфимский гос. авиа. тех. ун-т, 1997. С.30-40.
4. Касобов Л.С. Эксплуатация электрооборудования: уч. пособ. / Л.С. Касоболов, Ю.Е. Немихин, Ф.Е. Тарасов. Екатеринбург: УрФУ, 2016. 219 с.

УДК.004.057.4

ВЛИЯНИЕ ДИФФУЗНОСТИ МЕТРИК МАРШРУТИЗАТОРОВ НА ОПТИМАЛЬНОСТЬ РЕШЕНИЯ ЗАДАЧИ МАРШРУТИЗАЦИИ В СЕТИ СВЯЗИ С КОММУТАЦИЕЙ ПАКЕТОВ THE INFLUENCE OF THE DIFFUSENESS OF ROUTER METRICS ON THE OPTIMAL SOLUTION OF THE ROUTING PROBLEM IN A PACKET-SWITCHED COMMUNICATION NETWORK

Сергей Николаевич Шиманов

почетный работник ВПО РФ

почетный радист РФ

доктор технических наук, профессор

профессор кафедры

филиал ВА РВСН им. Петра Великого (г. Серпухов)

ведущий научный сотрудник

АНО «Институт инженерной физики»

Адрес: 142210, Московская обл.,

г. Серпухов, Большой ударный пер., д. 1а

Тел.: 8 (4967) 35-31-93

Алексей Александрович Крикунов

кандидат технических наук

докторант

филиал ВА РВСН им. Петра Великого

(г. Серпухов)

Адрес: 142210, Московская обл.,

г. Серпухов, ул. Бригадная, д. 17

Сергей Викторович Франков

начальник отдела АСУ

АНО «Институт инженерной физики»

Адрес: 142210, Московская обл.,

г. Серпухов, Большой ударный пер., д. 1а

Тел.: 8 (4967) 35-31-93

Аннотация

В статье на основе представления стохастического процесса изменения метрик маршрутизаторов в виде обобщённого винеровского процесса и решения соответствующего уравнения Фоккера-Планка получена зависимость изменения математического ожидания метрик маршрутизаторов в промежутках между их обновлениями, учёт которой позволяет сохранить оптимальность решения задачи маршрутизации на сети связи.

Ключевые слова: инфокоммуникационная сеть, метрика маршрутизатора, стохастический процесс, стохастические дифференциальные уравнения.

Summary

In the article, based on the representation of the stochastic process of changing router metrics in the form of a generalized Wiener process and solving the corresponding Fokker-Planck equation, the dependence of the change in the mathematical expectation of router metrics in the intervals between their updates is obtained, taking into account which allows us to maintain the optimal solution of the routing problem on a communication network.

Keywords: infocommunication network, router metric, stochastic process, stochastic differential equations.

В настоящее время подавляющее большинство инфокоммуникационных систем (ИКС) базируется на сетевых технологиях, в основе которых лежит интегрированное использование пропускной способности отдельных линий и каналов связи для передачи конкретного цифрового сообщения различных информационных направлений. Данный эффект достигается применением методов коммутации пакетов в совокупности с их эффективной маршрутизацией по организованным в сети межузловым каналам связи.

Выбор оптимальных маршрутов, как правило, осуществляется с помощью различных критериев, базирующихся на метриках, представляющих собой частные или комплексные показатели качества текущего информационного

обмена в информационных направлениях сети.

Очевидно, что качество решения задачи маршрутизации напрямую зависит от степени актуальности имеющихся метрик.

Особенностью современных ИКС является значительная стохастическая динамика изменения их состояния [1]. Это обусловлено целым рядом случайных факторов. Последние можно разделить на два класса: внутренних условий функционирования сети и внешних воздействий на сеть.

К внутренним факторам можно отнести:

- в первую очередь случайный характер самого информационного трафика – время передачи цифровых сообщений и их объём по тем или иным информационным направлениям сети носит случайный характер, то есть представля-

ет собой случайный процесс, таким образом, на сети имеет место взаимодействие (наложение) определённого количества случайных процессов;

- изменение динамики информационного обмена, под которой следует понимать существенное (чувствительное для сети) стохастическое изменение параметров, указанных выше случайных процессов;

- стохастическое или плановое изменение топологии сети, связанное как с мобильностью абонентов и элементов ИКС, так и с конечной надёжностью коммуникационного оборудования узлов сети;

- и т.д.

Под внешними воздействиями будем понимать деструктивные воздействия, как на отдельные элементы сети, так и на сеть в целом непреднамеренного (например, техногенного) характера и преднамеренного (различные информационные атаки или физическое воздействие) характера.

Очевидно, что всё вышеперечисленное приводит к потере актуальности метрик на узлах сети во временном масштабе.

Для поддержания актуальности в протоколах маршрутизации, используемых в конкретной ИКС, как правило, предусматривается периодическое обновление значений метрики путём обмена служебной информацией между маршрутизаторами, или периодического (или по необходимости) зондирования состояния сети. Однако эти процедуры связаны с загрузкой сети дополнительной служебной информацией, причём, чем выше поддержание актуальности метрик, тем больше служебная нагрузка на сеть, что в свою очередь снижает качество информационного обмена в ИКС в условиях ограниченной пропускной способности каналов сети.

Для оптимального управления данным процессом необходимо уметь прогнозировать устаревание метрик во времени. В [2,3] делались попытки эмпирического подбора функций распределения метрик и их изменения во времени. Так в [3] рассмотрен муравьиный алгоритм определения значений метрик и предложен статистический критерий их оценки. Однако данный подход требует дополнительного, хотя и не большого, обмена сетевой информацией между узлами сети. В [4] рассматривался эмпирический подход моделирования функций распределения метрик на основе двухпараметрического гамма-распределения $\Gamma(k, \theta)$ с изменяющимися во времени параметрами. Для этого предполагалось, что со временем метрика сети становится случайной величиной, параметры функции рас-

пределения которой (математическое ожидание и стандартное отклонение) зависят от времени.

Большинство моделей информационного обмена в ИКС основываются на свойстве марковости стохастического процесса функционирования последней [5]. Это разновидность стохастического процесса, в котором будущие значения переменной (в нашем случае значения метрик маршрутизаторов) зависит только от её текущего значения. Все предшествующие значения переменной игнорируются. Марковское свойство означает, что распределение вероятностей значений метрик маршрутизаторов в конкретный момент времени в будущем не зависит от траектории изменения их значений в прошлом. Данное свойство можно интерпретировать как свойство слабой эффективности, согласно которому значение метрики, фиксируемое в данный момент, содержит в себе всю информацию о её предыдущих значениях (траектории). Если бы это условие не выполнялось, то анализ графиков предыдущих значений метрик позволил бы техническому специалисту с высокой степенью достоверности предсказывать их будущие значения и, основываясь на этом, существенно повышать эффективность информационного обмена в ИКС.

С другой стороны не сложно предположить, что поскольку степень неопределённости метрики возрастает со временем, то растёт и её стандартное отклонение (имеем аналог второго начала термодинамики – неубывание энтропии изолированной системы). Кроме того с учётом перечисленного выше достаточно большого числа случайных факторов, определяющих возникающую неопределённость можно допустить, что изменение последней носит характер нормального распределения. Пусть за единицу времени (назовём её «стандартным» интервалом, далее просто интервалом, который принимается в соответствие с характером случайного процесса) изменение неопределённости метрики описывается функцией $\phi(0,1)$ нормального распределения с математическим ожиданием равным 0 и стандартным отклонением – 1. Тогда изменение метрики за два интервала описывается суммой двух нормальных распределений с нулевыми математическими ожиданиями и единичными стандартными отклонениями. Поскольку метрика является марковской величиной, то эти распределения не зависят друг от друга. Складывая два независимых нормальных распределения, мы получаем нормальное распределение, математическое ожидание и дисперсия которого равны суммам математических ожиданий и дисперсий каждого. Таким образом, математи-

ческое ожидание изменения метрики на протяжении двух интервалов остаётся равным нулю, а дисперсия равна 2. Следовательно, стохастическая неопределённость метрики через два интервала определяется случайной величиной с распределением вероятностей $\phi(0, \sqrt{2})$. Несложно получить, что за n интервалов времени данная функция примет вид $\phi(0, \sqrt{n})$. Очевидно, что за время равное половине интервала – $\phi(0, \sqrt{0.5})$, четверти – $\phi(0, \sqrt{0.25})$ и т.д. В общем случае можно записать, что изменение метрики на протяжении временного периода, имеющего длину T (в единицах интервалов), описывается распределением вероятностей $\phi(0, \sqrt{T})$. В частности, изменение метрики за очень короткий промежуток времени, имеющий длину ΔT , описывается распределением $\phi(0, \sqrt{\Delta T})$. Очевидно, что при $\Delta T \rightarrow 0$ мы имеем детерминированное значение метрики, фиксируемое в момент очередной её коррекции, принимаемый за начальный отсчёт времени.

Следует заметить, что квадратные корни в этих выражениях обусловлены тем, что в силу марковости процесса в нём складываются дисперсии, а не стандартные отклонения.

В теории случайных процессов процесс, которому подчиняется значение метрики, называется *винеровским* (Wiener process) [6]. Он представляет собой частный случай марковского стохастического процесса, когда математическое ожидание изменений метрики равно нулю, а её дисперсия равна 1. Следует заметить, что данный процесс находит широкое применение в различных областях науки: физике, биологии, экономике и т.д., что говорит о его общности с законами существования нашего мира.

Подводя итог вышеприведённым рассуждениям, можно констатировать, что метрика маршрутизатора μ в промежутках между её коррекциями подчиняется винеровскому процессу, поскольку она обладает следующими двумя свойствами:

1. Изменение $\Delta\mu$ на протяжении малого промежутка времени Δt удовлетворяет равенству

$$\Delta\mu = \varepsilon\sqrt{\Delta t}, \quad (1)$$

где ε – случайная величина, подчиняющаяся стандартному нормальному распределению $\phi(0, 1)$. Переходя к бесконечно малым, получаем

$$dW = \varepsilon(\sqrt{\Delta t} \rightarrow 0). \quad (2)$$

2. Величины $\Delta\mu$ на двух малых промежутках времени Δt являются независимыми.

Из первого свойства следует, что изменение метрик маршрутизаторов имеет нормальное распределение с математическим ожиданием равным нулю и стандартным отклонением $\sqrt{\Delta t}$. В геометрической интерпретации это означает, что огибающее семейство всех реализаций такого случайного процесса будут иметь параболический вид (*рисунок 1*).

Отдельно следует отметить, что поскольку изменение $\Delta\mu$ за время Δt пропорционально $\sqrt{\Delta t}$, то когда величина Δt становится очень малой, число $\sqrt{\Delta t}$ намного больше, чем Δt . Последнее определяет следующие интригующие свойства винеровского процесса: его траектория носит «скачкообразный – зубчатый» характер, то есть на любом конечном промежутке времени она имеет бесконечную длину, а в связи с этим ожидаемое количество совпадений значений метрики с любым конкретным значением из области допустимых значений на любом конечном промежутке времени является бесконечным.

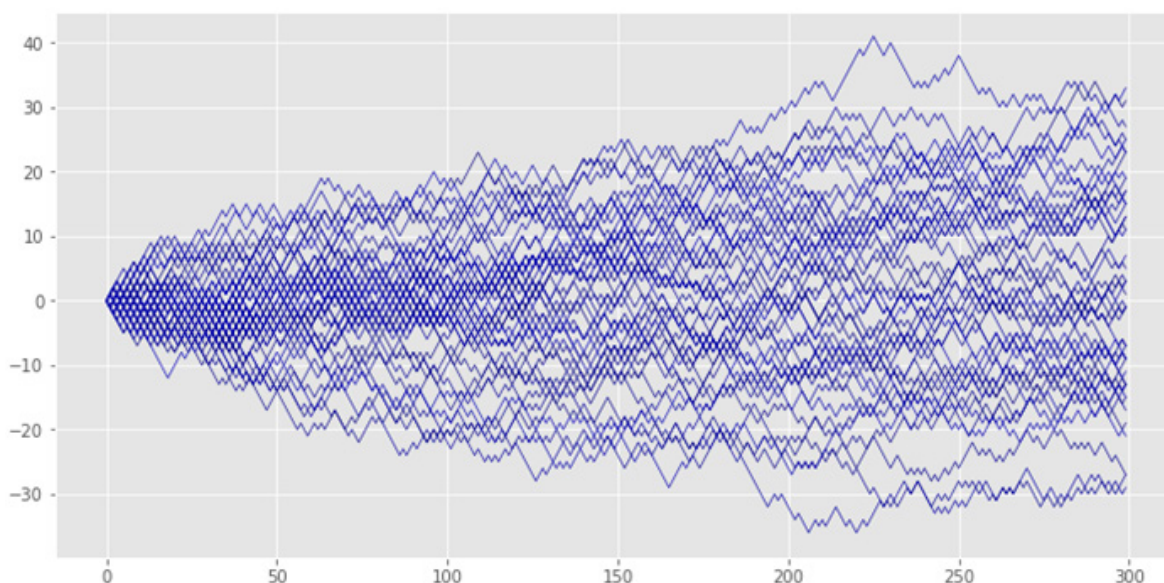


Рис. 1. Винеровские реализации приращений метрики маршрутизатора

Второе свойство – свойство независимости означает, что метрика подчиняется марковскому процессу.

Рассмотрим изменение метрики μ на протяжении достаточно большого интервала времени T . Обозначим его как разность между текущим неизвестным значением и последним фиксируемым значением: $\mu(T) - \mu(0)$. Указанную разность можно представить в виде суммы изменения переменной μ на протяжении N относительно малых промежутков времени длиной Δt , где $N = \frac{T}{\Delta t}$.

Тогда с учётом (1)

$$\mu(T) - \mu(0) = \sum_{i=1}^N \varepsilon_i \cdot \sqrt{\Delta t}, \quad (3)$$

где ε_i , $i = \overline{1, N}$ – случайные величины, имеющие распределение вероятностей $\phi(0,1)$. Учитывая свойство независимости приращений винеровского процесса, получаем, что $\mu(T) - \mu(0)$ имеет нормальное распределение, математическое ожидание которого равно нулю, дисперсия равна $N \cdot \Delta t = T$, а стандартное отклонение – \sqrt{T} .

Уравнения (1), (2) и (3) описывают процесс изменения (увеличения) неопределённости какой-либо метрики маршрутизатора во времени. Случайный процесс изменения самих значений метрик в этом случае может быть представлен как обобщённый винеровский процесс [7], описываемый дифференциальным уравнением вида

$$d\mu = u \cdot dt + D \cdot dW, \quad (4)$$

где dW – стандартный винеровский процесс (2). Константы u и D называются: u – коэффициент сноса, определяющий дрейф математического ожидания процесса в единицу времени; D – коэффициент диффузии, скорость нарастания неопределённости в единицу времени (изменение стандартного отклонения процесса на интервале Δt равна $D\Delta t$).

Если значения u и D являются функциями μ и t , то уравнение (4) принимает вид:

$$d\mu = u(\mu, t) \cdot dt + D(\mu, t) \cdot dW. \quad (5)$$

Процесс, описываемый данным уравнением, называют стохастическим процессом Ито [6].

Поскольку (5) описывает стохастический процесс изменения метрики во времени, то представляет интерес нахождение динамической (в смысле зависящей от времени) функции плотности вероятности значений метрики $f(\mu, t)$ в момент t на множестве её допустимых значений M . Для этого воспользуемся марковским свойством, рассматриваемого процесса.

Пусть для каждой пары значений $\mu, \mu' \in M$ и для любых двух моментов времени t и t' определена условная вероятность $P[\mu', t' | \mu, t]$ значения метрики μ' в момент t' при условии, что в

момент t её значение было μ . Будем рассматривать однонаправленный процесс $t' > t$, то есть прямую эволюцию процесса. Примем крайнее по времени значение обновления метрики за начальное распределение $f(\mu, t)_{t=0} = f_0(\mu_0)$, заданное, например, в виде δ -функции:

$$\delta(\mu - \mu_0, t_0) = \begin{cases} 0, & \text{при } -\infty < \mu < \mu_0, \\ \rightarrow \infty, & \text{при } \mu = \mu_0, \\ 0, & \text{при } \mu_0 < \mu < \infty. \end{cases} \quad (6)$$

При этом предполагается, что

$$\int_{-\infty}^{\infty} \delta(\mu - \mu_0, t_0) d\mu = 1.$$

Тогда эволюция процесса на конечном интервале τ с учётом уравнения Колмогорова-Смолуховского-Чепмена [8] будет описываться условной вероятностью

$$P[\mu', t + \tau | \mu_0, t_0] = \int P[\mu, t + \tau | \mu', t'] \cdot P[\mu', t' | \mu_0, t_0] d\mu'. \quad (7)$$

Поскольку величина t' в (7) принята произвольной, лежащей в пределах больше t_0 и меньше $t + \tau$, то в дальнейшем будем считать $t' = t$, то есть

$$P[\mu, t + \tau | \mu_0, t_0] = \int P[\mu, t + \tau | \mu', t] \cdot P[\mu', t | \mu_0, t_0] d\mu'. \quad (8)$$

Переходя к характеристической функции (Фурье-образу) $P[\mu, t + \tau | \mu', t]$, используя разложение показательной функции в степенной ряд и выполнив обратное преобразование уравнение (8) может быть представлено в следующем виде [9]:

$$P[\mu, t + \tau | \mu_0, t_0] = P[\mu, t | \mu_0, t_0] + \sum_{n=1}^{\infty} \frac{(-1)^n}{n!} \frac{\partial^n}{\partial \mu^n} (m_n(\mu, t; \tau) P[\mu, t | \mu_0, t_0]), \quad (9)$$

где $m_n(\mu, t, \tau)$ – условные моменты n -го порядка метрики μ .

Из разложения (9) можно получить скорость изменения условной вероятности перехода по времени t :

$$\begin{aligned} \frac{\partial P[\mu, t | \mu_0, t_0]}{\partial t} &= \lim_{\tau \rightarrow +0} \frac{P[\mu, t + \tau | \mu_0, t_0] - P[\mu, t | \mu_0, t_0]}{\tau} = \\ &= \lim_{\tau \rightarrow +0} \sum_{n=1}^{\infty} \frac{(-1)^n}{n!} \frac{\partial^n}{\partial \mu^n} \left(\frac{m_n(\mu, t; \tau)}{\tau} P[\mu, t | \mu_0, t_0] \right) \end{aligned} \quad (10)$$

Поскольку в соответствии с (5) рассматриваемый стохастический процесс является диффузионным, то для него достаточно, чтобы отличными от нуля были только первые два момента, которые обозначим как $u(\mu, t)$ называемый коэффициентом сноса и $D(\mu, t)$ – коэффициент диффузии [8].

Тогда уравнение (10) принимает вид:

$$\frac{\partial P[\mu, t | \mu_0, t_0]}{\partial t} = -\frac{\partial}{\partial \mu} (u(\mu, t) P[\mu, t | \mu_0, t_0]) + \frac{1}{2} \frac{\partial^2}{\partial \mu^2} (D(\mu, t) P[\mu, t | \mu_0, t_0]) \quad (11)$$

С учётом того, что

$$f(\mu, t) = \int P(\mu', t | \mu, t) f(\mu', t) d\mu',$$

из (11) получаем одномерное уравнение Фоккера-Планка (УФП), описывающее изменение плотности распределения метрики в промежутках между её обновлениями на маршрутизаторах ИКС:

$$\frac{\partial f(\mu, t)}{\partial t} = -\frac{\partial}{\partial \mu} (u(\mu, t) f(\mu, t)) + \frac{1}{2} \frac{\partial^2}{\partial \mu^2} (D(\mu, t) f(\mu, t)). \quad (12)$$

Несложно заметить покомпонентную схожесть уравнений (5) и (12). Последнее подтверждает, что дифференциальное уравнение Фокера-Планка описывает изменение плотности вероятности метрики представленного в (5) процесса Ито.

Уравнение Фокера-Планка является дифференциальным уравнением в частных производных. В общем виде оно имеет бесконечное множество решений. Конкретное решение Коши может быть найдено (пусть даже численным методом) только для чётко определённых начальных и граничных условий. Кроме того, поскольку решение представляет собой функцию плотности распределения, то оно дополнительно должно удовлетворять условию нормировки:

$$\int_{\text{ОДЗ}\mu} f(\mu, t) d\mu = 1. \quad (13)$$

Вернёмся к определению плотности распределения неопределённости метрик. Для этого будем считать, что на интервале обновления коэффициент сноса метрики равен нулю, а диффузия постоянна. Тогда дифференциальное уравнение (12) примет вид:

$$\frac{\partial f(\mu, t)}{\partial t} = \frac{D}{2} \frac{\partial^2 f(\mu, t)}{\partial \mu^2}. \quad (14)$$

Как было отмечено выше, частное решение такого уравнения может быть получено для конкретных граничных и начальных условий. Так, например, одно из первых решений такого уравнения для броуновского движения частицы на неограниченной координате x при начальном значении $x=0$ было получено более 100 лет назад А. Эйнштейном [10].

В качестве имеющихся в нашем распоряжении граничных условий можно рассмотреть следующие:

- величина метрики не может быть отрицательной – $\mu_{\min} > 0$, поскольку, как правило, все они являются положительными физическими

величинами;

- максимальное значение метрики не может превышать некоторого значения – $\mu_{\max} > \mu_{\min}$, при превышении которого данное направление на узле связи считается не работоспособным;

- искомая плотность вероятности $f(\mu, t)$ на границах области допустимых значений ($\mu_{\min} \leq \mu \leq \mu_{\max}$) не стремится к нулю и, следовательно, удовлетворяет условию границ второго рода

$$\left(\frac{\partial f(\mu, t)}{\partial \mu} \right)_{\mu=\mu_{\max}}^{\mu=\mu_{\min}} = 0, \quad (15)$$

Данное допущение согласуется с допущением относительного постоянства трафика в ИКС;

- искомая плотность вероятности $f(\mu, t)$ должна удовлетворять условию нормировки вероятностей (13).

В качестве начального условия естественно принять, что начальное значение метрики соответствует последнему значению, установленному сетевым протоколом

$$\mu_{t=0} = \mu_{\text{прот}} = \mu_0. \quad (16)$$

В этом случае начальная плотность распределения определяется через дельта-функцию (6).

Поскольку решение дифференциального уравнения (14) математически представляет собой разложение искомой функции в ряд Фурье, то использование δ -функции в качестве начальных условий требует удержания в сумме ряда очень большого числа слагаемых, что затрудняет вычислительные процедуры анализа $f(\mu, t)$.

Для получения более комфортного в вычислительном смысле результата воспользуемся интервальными начальными условиями. Будем считать, что протокольное значение метрики μ_0 известно с определённой очень малой, но конечной точностью $\Delta\mu_0$, то есть начальная метрика равномерно распределена на интервале

$$[\mu_0 - \Delta\mu_0, \mu_0 + \Delta\mu_0]. \quad (17)$$

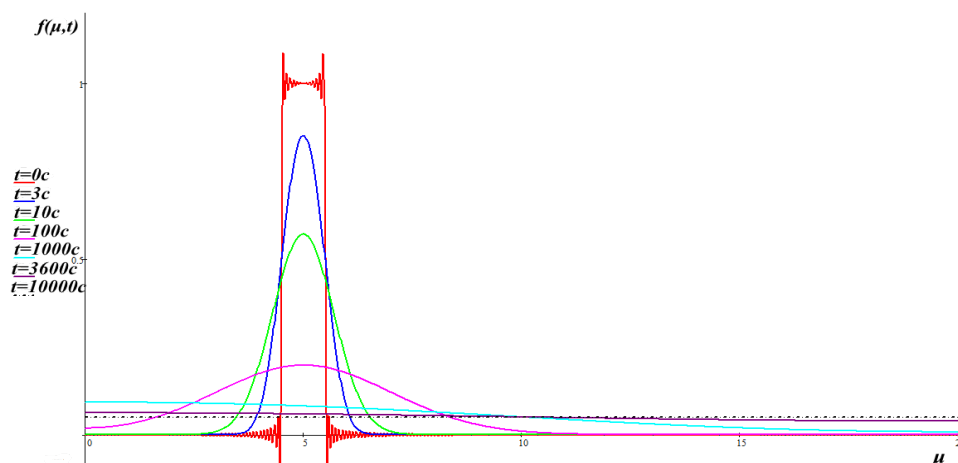


Рис. 2. Изменение плотности распределения μ от t

В этом случае начальная плотность распределения имеет вид:

$$f(\mu, 0) = \begin{cases} 0, & \text{при } 0 \leq \mu \leq \mu_0 - \Delta\mu_0, \\ \frac{1}{2\Delta\mu_0}, & \text{при } \mu_0 - \Delta\mu_0 < \mu < \mu_0 + \Delta\mu_0, \\ 0, & \text{при } \mu_0 + \Delta\mu_0 \leq \mu \leq \mu_{\max}. \end{cases} \quad (18)$$

С учётом перечисленных выше начальных (17, 18) и граничных условий (15), а также условия нормировки (13) решение дифференциального уравнения (14) имеет следующий вид:

$$f(\mu, t) = \frac{1}{\mu_{\max}} + \frac{1}{\mu_{\max}} \sum_k \exp(-\lambda_k^2 Dt) \frac{\sin[\lambda_k(\mu_0 + \Delta\mu_0)] - \sin[\lambda_k(\mu_0 - \Delta\mu_0)]}{\Delta\mu_0 \lambda_k} \cos(\lambda_k \mu), \quad (19)$$

где $\lambda_k = \frac{k\pi}{\mu_{\max}}$ – собственные числа решения уравнения (19). По сути, сумма второго слагаемого (19) представляет собой ненормированное решение дифференциального уравнения (14) в виде разложения Фурье по собственным функциям – $\cos(\lambda_k \mu)$.

На рисунке 2 приведено численное моделирование плотности распределения метрики – $f(\mu, t)$ для различных интервалов времени после её последнего обновления. Для моделирования были приняты следующие исходные данные: $\mu = [0, \mu_{\max}]$, $\mu_{\max} = 20$, $\mu_0 = 5$, $\Delta\mu_0 = 0,5$, $D = 0,02$, число компонент суммы $k = 1 \dots 500$. Такое ограничение суммы приводит к эффекту Гиббса, что наблюдается на графике для $t = 0$ с. Данный эффект связан с разложением в ряд Фурье кусочно-непрерывной функции (18). Для его уменьшения необходимо увеличение числа компонент суммы в (19), что существенно увеличивает вычислительные расходы при численном моделировании. Данный эффект практически исчезает уже при незначительном увеличении модельного времени t (например при $t = 3$ с), и, следовательно, практически не сказывается на анализе полученных результатов. Исходные данные носят относительный характер, то есть используются

для численного моделирования с целью наглядности восприятия изменения неопределённости метрики во времени (плотности распределения $f(\mu, t)$). Анализ полученных для различных временных интервалов функций плотности распределения μ показывает изменение возможных значений метрики от кусочно-детерминированной с заданной степенью точности $\Delta\mu_0$ при $t = 0$ с до максимально неопределённой с равномерным распределением на всём множестве допустимых значений при $t = 10000$ с.

С точки зрения процесса управления маршрутизацией интерес представляет не сама плотность распределения метрик, а значение их математического ожидания:

$$M_\mu(t) = \langle \mu \rangle_t = \int_0^{\mu_{\max}} \mu f(\mu, t) d\mu = \frac{\mu_{\max}}{2} \left\{ 1 + 2 \sum_k \exp(-\lambda_k^2 Dt) \frac{\sin[\lambda_k(\mu_0 + \Delta\mu_0)] - \sin[\lambda_k(\mu_0 - \Delta\mu_0)]}{\Delta\mu_0 \lambda_k} \frac{[(-1)^k - 1]}{(k\pi)^2} \right\}. \quad (20)$$

Можно проверить, что при $t = 0$ сумма второго слагаемого в скобках, представляющая ряд Фурье, сворачивается в $\left(\frac{\mu_0}{\mu_{\max}} - \frac{1}{2}\right)$, вследствие чего

$$M_\mu(t=0) = \langle \mu \rangle_0 = \mu_0,$$

а поскольку при $t \rightarrow \infty$ экспонента $\exp(-\lambda_k^2 Dt) \rightarrow 0$, то

$$M_\mu(t \rightarrow \infty) = \langle \mu \rangle_\infty = \frac{\mu_{\max}}{2},$$

что соответствует математическому ожиданию равномерного распределения на интервале $[0, \mu_{\max}]$. Таким образом, граничные результаты $\langle \mu \rangle_t$ соответствуют начальным и граничным условиям стохастической диффузии метрик.

Парадоксальность зависимости (20) заключается в том, что уравнение (14) для которого получены решения (19) и соответственно (20) предполагает постоянство математического ожидания стохастического процесса изменения метрик – коэффициент сноса $u(\mu, t)$ УФП (12) был принят равным нулю. Однако диффузная неопределённость на ограниченном множестве допустимых значений меняет математическое ожидание процесса даже при нулевом сносе.

На рисунке 3 приведены графики изменения математического ожидания метрик при различных начальных значениях μ_0 и коэффициентах диффузии D .

Из приведённых графических зависимостей математического ожидания метрик видно, что с течением времени они нелинейно стремятся к среднему по области допустимых значений, при этом средняя скорость их изменения существенно зависит от коэффициента диффузии процесса – D . В связи с этим начальное ранжирование метрик на маршрутизаторе после их очередного обновления может не сохраняться в промежутках между обновлениями, что в свою очередь

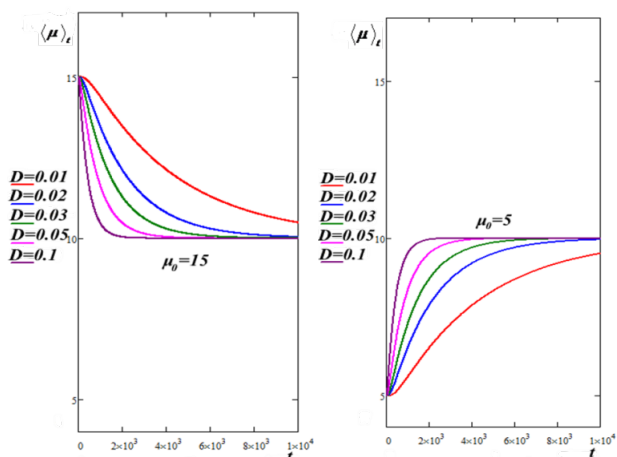


Рис. 3. Изменение математического ожидания метрик

приведёт к не оптимальности решения задачи маршрутизации.

Так на *рисунке 4* приведён пример изменения во времени метрик (математических ожиданий метрик) трёх направлений маршрутизатора после их последнего обновления. Начальные значения метрик:

$$\mu_{01}=4; \mu_{02}=7; \mu_{03}=16.$$

Коэффициенты диффузии направлений:

$$D_1=0,06; D_2=0,02; D_3=0,03.$$

Если в качестве метрики принять среднее время передачи пакета по сети до абонента при выборе того или иного направления, то начальное ранжирование направлений (сразу после обновления метрик) имеет вид: [1;2;3]. Учёт нарастания неопределённости, приведённый на графиках, показывает, что в момент времени t^* ранжирование метрик меняется на [2;1;3], то есть приоритетным становится второе направление. Не сложно заметить, что по истечению достаточно большого времени в условиях диффузии метрик все направления передачи пакета становятся равноценными.

Коэффициент диффузии конкретной метрики на конкретном маршрутизаторе может быть статистически оценён по предыстории процесса её обновления. При этом такая статистическая оценка будет интегрально учитывать действие на ИКС всего множества внутренних и внешних возмущающих факторов, что исключает необходимость построения моделей их воздействия. Хотя справедливости ради следует заметить, что последнее утверждение в условиях нулевого сноса и "отражающих" граничных условий (15) справедливо лишь при допущении относительной стационарности процесса функционирования ИКС.

Таким образом, учёт стохастической диффузии метрик маршрутизаторов позволил выявить новое свойство: а именно *изменение метрик (в*

смысле их математического ожидания) во времени на интервале их обновления, зависящее от коэффициента диффузии. Полученная зависимость (20) может быть использована в алгоритмах маршрутизаторов ИКС с целью оптимального решения задачи маршрутизации пакетов и снижения служебной нагрузки на сеть за счёт увеличения интервалов обновления метрик.

Литература

1. Шиманов С.Н., Дёмочкин Е.А. Технологии Mesh-сети. Типы и протоколы маршрутизации Mesh-сетей // Труды Российского научно-технического общества радиотехники, электроники и связи им. А.С. Попова. Серия: Научная сессия, посвящённая Дню радио. Вып. LXX. М.: «Информпресс-94», 2015. С.232.
2. Шиманов С.Н., Кирдяшов Ф.Г. Научно-методический подход к моделированию процесса функционирования сети связи с коммутацией пакетов на сетевом уровне // Информационные технологии в проектировании и производстве, 2008. №1. С.75-77.
3. Шиманов С.Н., Ковальков Д.А., Дёмочкин Е.А. Особенности использования вероятностно-статистического алгоритма маршрутизации в самоорганизующихся Mesh-сетях // Труды Российского научно-технического общества радиотехники, электроники и связи им. А.С. Попова. Серия: Научная сессия, посвящённая Дню радио. Вып. LXXI. М.: 2016. С.530-533.
4. Шиманов С.Н., Франков С.В., Дёмочкин Е.А., Рыженков В.А. Вероятностная маршрутизация в Mesh-сетях с быстроменяющейся топологией // Известия Института инженерной физики, 2019. №1(51). С.22-27.
5. Цимбал В.А. Информационный обмен в сетях передачи данных. Марковский подход. Монография. М.: Вузовская книга, 2014. 144 с.
6. Гординер К.В. Стохастические методы в естественных науках: Пер. с англ. М.: Мир, 1986. 526 с.
7. Босов А.Д., Орлов Ю.Н. Эмпирическое уравнение Фоккера-Планка для прогнозирования нестационарных временных рядов // Препринты ИПМ им. М.В.Келдыша, 2013. № 3. 30 с.
8. Королюк В.С., Портенко Н.И., Скороход А.В., Турбин А.Ф. Справочник по теории вероятностей и математической статистике. М.: Наука, 1985. 640 с.
9. Тихонов В.И., Миронов М.А. Марковские процессы. М.: Сов. радио, 1977. 488 с.
10. Эйнштейн А. О движении взвешенных в покоящейся жидкости частиц, требуемом молекулярно-кинетической теорией теплоты / В кн.: Эйнштейн А., Смолуховский М. Броуновское движение. М.-Л.: ОНТИ, 1936. С. 13-27.

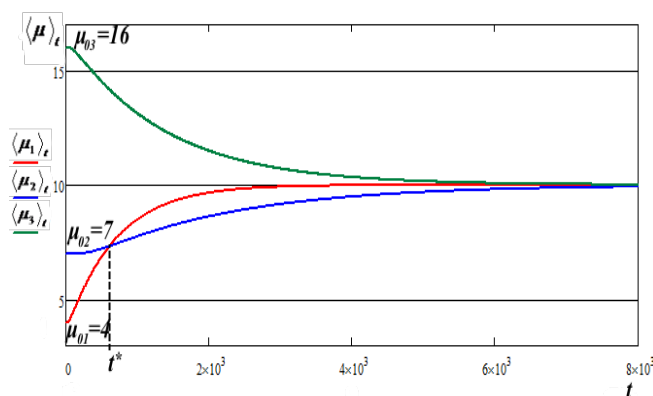


Рис. 4. Изменение ранжирования направлений маршрутизатора



УДК 530.145+539.184+654.026

МОДЕЛЬ КВАНТОВОГО ПОВТОРИТЕЛЯ НА АЗОТНОЙ ВАКАНСИИ В МОНОКРИСТАЛЛЕ АЛМАЗА, КАК ПЕРСПЕКТИВНОЕ НАПРАВЛЕНИЕ ДЛЯ РЕАЛИЗАЦИИ ЗАЩИЩЕННЫХ КВАНТОВЫХ СЕТЕЙ MODEL OF A QUANTUM REPEATER BASED ON A NITROGEN VACANCY IN A DIAMOND SINGLE CRYSTAL AS A PROMISING DIRECTION FOR THE IMPLEMENTATION OF SECURE QUANTUM NETWORKS

Алексей Игоревич Алаторцев
доктор технических наук
начальник управления системных исследований
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл.,
г. Серпухов, Большой Ударный пер., д. 1а
Тел.: 8 (903) 183-94-86
E-mail: alexalat@yandex.ru

Сергей Владимирович Подвигин
кандидат технических наук
начальник лаборатории
квантовых информационных технологий
АНО «Институт инженерной физики»
Тел.: +7 (929) 540-24-54
E-mail: svp.r@bk.ru

Сабир Магомед-Кадиевич Бакмаев
кандидат физико-математических наук
ведущий научный сотрудник
управления системных исследований
АНО «Институт инженерной физики»
Тел.: 8 (962) 908-48-42
E-mail: sabir20021@yandex.ru

Аннотация

В данной статье предлагается модель квантового повторителя на базе азотной вакансии в монокристалле алмаза. Данная модель основана на последних достижениях в области исследований спин-фотонных интерфейсов, способных функционировать при комнатных температурах. Азотная вакансия использует в качестве кубита памяти ядро углерода ^{13}C и находится в полости алмаза, образующей оптический резонатор. Модули квантовых повторителей соединены волоконно-оптическим кабелем. Планируемая архитектура может быть реализована в перспективных квантовых сетях.

Ключевые слова: квантовая запутанность, абсолютно защищенная информация, NV-центры, квантовый повторитель, оптический резонатор.

Summary

In this article we propose quantum repeater model based on the nitrogen-vacancy center in diamond crystal. Our model based of resent progress towards non-cryogenic spin-photon interface. Every repeater node consists from an optical cavity containing negative charged nitrogen-vacancy center, with one nuclear spin ^{13}C as memory qubit. The quantum repeater modules connected via optical fiber. Proposal architecture should realize quantum information networks in future.

Keywords: quantum entanglement, absolutely secure information, NV-centers, quantum repeater, optical resonator.

Феномен квантовой запутанности является хорошей основой для множества прикладных применений, таких как: распределенные квантовые вычисления, защищенные протоколы для передачи конфиденциальной информации, высокочувствительные измерения магнитных полей и т.д. [1].

Крайне важным параметром для надежной реализации вышеперечисленных задач является соотношение запутанного состояния к состоянию декогеренции, демонстрирующее какое количество запутанных состояний сохранится с течением времени вне процесса их генерации.

В многочисленных работах по экспериментальной проверке передачи запутанных кубитов на расстояния, реализованных на основе захваченных ионов, наблюдалась значительная потеря фотонов, находящихся в запутанном состоянии. Главной причиной потерь информации является нестабильность квантовых состояний кубитов из-за воздействий различных факторов, таких как: тепловые флуктуации атомов окружающих ион, воздействие электрических полей, вызванных внутренними механическими напряжениями внутри кристалла, воздействие магнитных полей, вызванными движением

ем орбитальных электронов и т.д. Относительно успешная передача информации с помощью запутанных фотонов была осуществлена при охлаждении квантовой ячейки до сверхнизких температур. Поскольку запутанные состояния дублировать невозможно по причине ограничений, налагаемой теоремой о клонировании из квантовой механики, то единственным на данный момент решением является использование квантовых повторителей.

Основная концепция, предлагаемая в статье, заключается в использовании в качестве кандидата для реализации квантового повторителя [2] дефекта в монокристаллическом алмазе, состоящего из атома азота и вакантного места в виде отсутствующего атома углерода (далее NV-центра).

Особый интерес представляют два варианта практической реализации квантового повторителя в виде двухкубитных устройств. В первом случае – система, состоящая из изотопа углерода ^{13}C и электронов, а во втором случае – система, состоящая из изотопа азота ^{15}N и электронов [3]. В обоих случаях один из электронов NV-центра предполагается использовать в качестве операционного кубита, а ядро изотопа – в качестве кубита «долговременной» памяти. В нашем случае наиболее интересен первый вариант, поскольку концентрация изотопа углерода в монокристалле алмаза примерно в три раза выше концентрации изотопа азота и, следовательно, подходящие для квантовых повторителей NV-центры будут чаще распространены.

В квантовом повторителе на основе NV-центра можно управлять поляризацией спина электрона и спином изотопа ядра. Спин электрона позволяет реализовать запутанное состояние фотона со спином изотопа ядра углерода,

который используется как кубит памяти для последующей передачи фотона в запутанном состоянии по оптическому кабелю [4].

Конструкция квантового повторителя состоит из следующих компонентов: квантовой ячейки; детектора одиночных фотонов (ОФД); светоделителя пучка фотонов; поляризационного светоделителя фотонов (ПСД); формирователя состояний Белла; преобразователя когерентного излучения. Квантовая ячейка представляет собой микрополость с NV-центром в монокристалле алмаза, которую можно использовать как оптический микрорезонатор высокой добротности для осуществления тонкой подстройки частоты инициирующего лазерного импульса.

Структурная схема генерации удаленной запутанности представлена на рисунке 1.

Система образует запутанность между двумя сопряженными узлами. Микрорезонатор модуля настроен так, что он отражает входящий фотон когда электрон NV-центра находится в состоянии $|0\rangle$.

Генерация запутанности NV-центра начинается с подготовки спинов электронов в состоянии:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \quad (1)$$

Далее формируются запутанные пары соответствующие состояниям Белла, состоящие из телекоммуникационного фотона и фотона NV-центра:

$$|\Psi_{ent}\rangle = \frac{1}{\sqrt{2}}[|HV\rangle - |VH\rangle]. \quad (2)$$

Здесь H и V – горизонтальные и вертикальные поляризации спина фотона. Запутанные фотоны далее передаются по оптическому каналу между двумя узлами. В передающей части квантового повторителя фотоны с помощью ПСД расщепляются по горизонтальным и вертикальным проекциям спина. Вертикальная

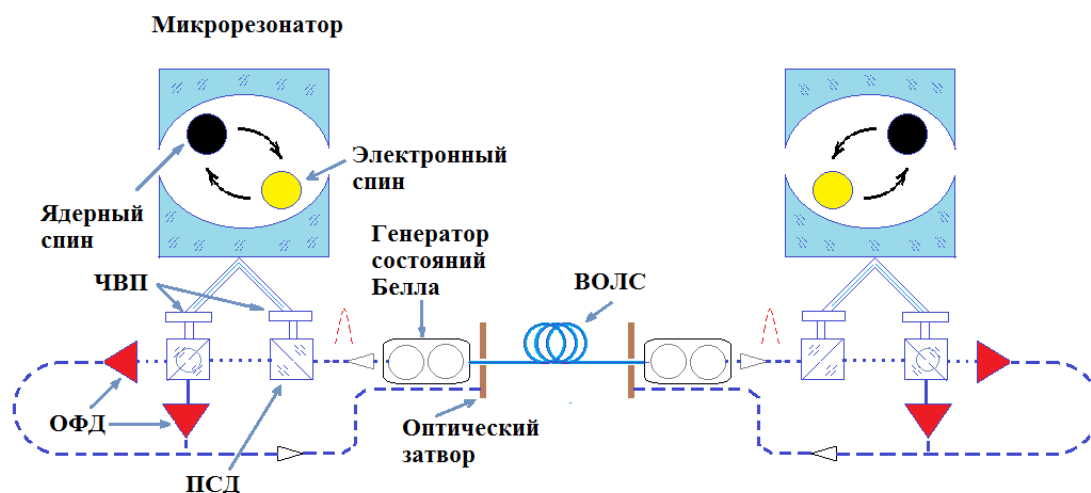


Рис. 1. Схема генерации запутанности между двумя квантовыми узлами, соединенными волоконно-оптическим кабелем

мода поляризации поворачивается на $+45^\circ$ с помощью четвертьволновой пластины (ЧВП) и взаимодействует с NV-центром.

Сдвиговой π -импульс фотона воздействует на NV-центр – если электрон NV-центра находится в $|0\rangle$ -состоянии или отражается от микрорезонатора – если электрон NV-центра находится в $|+1\rangle$ -состоянии. Мода поляризации отраженного фотона поворачивается на -45° с помощью ЧВП и смешивается в ПСД с фотоном с горизонтальной поляризацией. На этом этапе состояние фотона измеряется ОФД.

Детектирование фотона NV-центра означает, что спин электрона NV-центра в модуле отправителя находится в запутанном состоянии с телекоммуникационным фотоном. В дальнейшем выполняются две операции: телекоммуникационный фотон передается по волоконно-оптической линии связи (ВОЛС); состояние спина электрона NV-центра передается спину ядра изотопа ^{13}C .

Телекоммуникационный фотон, попавший в оптический канал, передается по ВОЛС в приемный узел вместе с результатом измерения первого фотона. По прибытии фотона в удаленном приемном узле происходят две последовательные операции: временной интервал фотона преобразуется в его поляризацию; ПСД разделяет фотоны на моды с вертикальными и горизонтальными поляризациями. С помощью ЧВП спин фотона с вертикальной поляризацией поворачивается на $+45^\circ$ и взаимодействует с NV-центром в приемном модуле, находящемся в $|+1\rangle$ -состоянии. Далее этот фотон смешивается во втором ПСД и результат его поляризации измеряется в ОФД. Результирующее состояние, зависящее от успешного результата измерения:

$$R(t) = \frac{1+e^{-t_2}}{2} |\psi_{-}\rangle\langle\psi_{-}| + \frac{1-e^{-t_2}}{2} |\psi_{+}\rangle\langle\psi_{+}|, \quad (3)$$

где $|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |\pm 1\rangle) \pm \frac{1}{\sqrt{2}}(|0\rangle - |\pm 1\rangle)$;
 t_2 – время когерентного состояния.

Для описания динамики процессов, спиновый гамильтониан одиночного NV-центра в основном состоянии представим в виде:

$$H_{NV} = \hbar(D\sigma_z^2 + E[\sigma_x^2 + \sigma_y^2] + g_e\mu_b B\sigma_z) - \hbar g_n\mu_n B I_z + \hbar g A_{||} S_z I_z + \frac{1}{2} \hbar A_{\perp} (S_+ I_- + S_- I_+), \quad (4)$$

где $D/2n=2,84$ ГГц – тензор расщепления спиновых состояний в нулевом магнитном поле;
 $D/2n \sim 10$ МГц – тензор расщепления при нулевом электростатическом поле;

$g_e\mu_b B$ – расщепление, индуцированное магнитным полем;

σ_{xyz} – обобщенные матрицы Паули;

S_+ и S_- – операторы, проецирующие спин соответственно вверх и вниз;

μ_b – магнетон Бора;

$g_2 = 2.0$ – электронный g -фактор;

$B \sim 20$ мТл – внешнее магнитное поле;

\hbar – постоянная Планка.

При воздействии СВЧ-импульса частотой ω_0 на систему $^{13}\text{C}+NV$ оператор Гамильтона описывает процесс как:

$$H_{\text{эфф}} = \hbar\omega_A |1\rangle\langle 1| + \hbar\omega_B |2\rangle\langle 2| + H_{\text{вз}}, \quad (5)$$

где ω_A и ω_B – частоты квантовых переходов;

$H_{\text{вз}} = -[Ed]$;

$E = v \sin(\omega_j t + \varphi)$ – напряженность электрического поля;

d – оператор дипольного момента:

$$d = \sum_k d_k (\sigma_k^+ + \sigma_k^-), \quad (6)$$

где $d_k (k=a,b,c)$ – матричные элементы соответствующие переходам между энергетическими уровнями.

При поглощении импульса квантовое состояние системы меняется со временем, а изменение квантового состояния осциллирует с частотой Раби:

$$\frac{d\psi}{dt} = -\Omega_k (\sigma_k^- e^{i\varphi} + \sigma_k^+ e^{-i\varphi}) |\psi\rangle, \quad (7)$$

где соответственно $\Omega_k = -\frac{v d_k}{2\hbar}$.

В зависимости от длительности инициирующего импульса фотона квантовая система эволюционирует следующим образом:

• при воздействии $\pi/2$ -импульса:

$$|\psi_0\rangle \rightarrow |\psi_0\rangle + \frac{1}{\sqrt{2}} e^{-i\theta} |\psi_1\rangle, \quad |\psi_1\rangle \rightarrow |\psi_1\rangle - \frac{1}{\sqrt{2}} e^{i\theta} |\psi_0\rangle; \quad (8)$$

• при воздействии π -импульса:

$$|\psi_0\rangle \rightarrow e^{-i\theta} |\psi_1\rangle, \quad |\psi_1\rangle \rightarrow e^{i\theta} |\psi_0\rangle; \quad (9)$$

• при воздействии 2π -импульса:

$$|\psi_0\rangle \rightarrow -|\psi_0\rangle, \quad |\psi_1\rangle \rightarrow -|\psi_1\rangle. \quad (10)$$

Генерация запутанных состояний между узлами квантовой сети

Для генераций запутанных состояний используется схема интерферометра Маха-Цендера. Вначале в каждом из NV-центров электрон подготавливается в состоянии $(|0\rangle + |1\rangle)/\sqrt{2}$. Добиться этого можно с помощью лазерного $\pi/2$ импульса фокусируемого на системе $^{13}\text{C}+NV$. В результате волновую функцию совместного электронного состояния обоих NV-центров можно записать в виде:

$$|\psi\rangle_{22} = \frac{1}{\sqrt{2}} (|0\rangle_1 + |1\rangle_1) \cdot \frac{1}{\sqrt{2}} (|0\rangle_2 + |1\rangle_2) = \frac{1}{2} (|00\rangle_{12} + |10\rangle_{12} + |01\rangle_{12} + |11\rangle_{12}). \quad (11)$$

Тогда фотонный импульс попадает в интерферометр, который в свою очередь отделяет запутанные состояния. В итоге суперпозиция состояний обоих NV-центров примет вид:

$$|\psi\rangle_{int} = \frac{1}{\sqrt{2}} (|01\rangle_{12} + |10\rangle_{12}), \quad (12)$$

что соответствует максимально запутанному состоянию.

После создания запутанных состояний между двумя электронными кубитами, необходимо произвести запись в кубиты памяти, в качестве которых используется ядро изотопа углерода ^{13}C . Электронный кубит должен не только производить запись, но и считывать состояния ядра:

$$|1\rangle_e \rightarrow |\uparrow\rangle_c, \quad |0\rangle_e \rightarrow |\downarrow\rangle_c.$$

Предварительная инициация ядра (проекция вектора спина вниз) производится с помощью последовательных $n/2$ -импульсов. Согласно выражениям (8) при воздействии трех последовательных n, n_2, n_c -импульсов, которые устанавливают начальные значения фаз ϕ_1, ϕ_2, ϕ_c , квантовая система перейдет из состояния:

$$|\psi\rangle = (\psi_{e1}|0\rangle + \psi_{e2}|1\rangle)(\psi_{n1}|\downarrow\rangle + \psi_{n2}|\uparrow\rangle) \quad (13)$$

в состояние:

$$|\psi'\rangle = \psi_{e1}|0\rangle(\psi_{n1}|\downarrow\rangle + \psi_{e2}e^{i(\phi_c+\phi_2)}|\uparrow\rangle) + \\ + |\psi_{e2}|0\rangle(\psi_{n1}|\downarrow\rangle - \psi_{e2}e^{i(\phi_c-\phi_1+2\phi_2)}|\uparrow\rangle), \quad (14)$$

где разность фаз равна $\phi_1 + \phi_2 = \frac{\pi}{2} + \pi n$, $n \in \mathbb{Z}$.

При этом запись в кубит памяти будет выглядеть следующим образом:

$$\psi_{e1}|0\rangle + \psi_{e2}|1\rangle \rightarrow |\psi'\rangle_e \psi_{n1}|\downarrow\rangle + \psi_{e2}e^{i\phi}\psi_{n2}|\uparrow\rangle \quad (15)$$

где $\phi = \phi_c + \phi_2$.

Таким образом, с помощью последовательных $n/2$ -импульсов создается суперпозиция спиновых состояний:

$$|\psi_0\rangle \rightarrow (|\psi_0\rangle + e^{-i\phi}|\psi_1\rangle)/\sqrt{2} \\ |\psi_1\rangle \rightarrow (|\psi_0\rangle - e^{i\phi}|\psi_1\rangle)/\sqrt{2}, \quad (16)$$

которая позволяет реализовать квантовый по-

вторитель на азотной вакансии в монокристалле алмаза.

Заключение

Таким образом, квантовые повторители позволяют обмениваться запутанными состояниями между узлами квантовых сетей и тем самым существенно увеличить расстояния для передачи абсолютно защищенной информации. Предполагается, что рассматриваемая в данной статье модель квантового повторителя будет функционировать без охлаждения до сверхнизких температур. При этом использование высокодобротных оптических резонаторов в структуре монокристалла алмаза позволит существенно снизить влияние внешних полей на квантовые состояния NV-центра и тем самым повысить устойчивость передачи информации.

Литература

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М: Мир, 2006. 824 с.
2. Смуров С.В., Волков Г.Г. Особенности квантовых состояний NV-центров в нелокальности запутанности и телепортации // Известия Института инженерной физики, 2023. № 2 (68). С.49-58.
3. Bukach A.A., Kilin S.Ya. Optics and Spectroscopy, 2007. Vol. 103, № 2. Pp. 202-209.
4. Nemoto K. et al. Photonic Architecture for Scalable Quantum Information Processing in Diamond. Phys. RevX 4, 031022 (2014).
5. Nemoto K. et al. Photonic Quantum Networks formed from NV – centers. Sci. Rep. 6, 26284; doi: 10.1038/srep26284 (2016).



СТАТИСТИЧЕСКИЙ АНАЛИЗ СПОСОБОВ ПОВЫШЕНИЯ ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ STATISTICAL ANALYSIS OF WAYS TO INCREASE THE NOISE IMMUNITY OF DATA TRANSMISSION SYSTEMS

Владимир Владимирович Зеленецкий
почётный работник науки и техники РФ
доктор технических наук, профессор
профессор кафедры
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл., г. Серпухов,
ул. Бригадная, д. 17
Тел.: 8 (905) 548-48-54
E-mail: Zelenevsky.Vladimir@gmail.com

Юрий Владимирович Зеленецкий
доктор технических наук, доцент
научный сотрудник
ВА РВСН им. Петра Великого
Адрес: 143900, Московская обл.,
г. Балашиха, ул. Карбышева, д. 8
Тел.: 8 (903) 721-12-61
E-mail: sys1434@mail.ru.

Александр Владимирович Попов
адъюнкт кафедры
филиал ВА РВСН им. Петра Великого
(г. Серпухов)
Тел.: 8 (4967) 72-19-11

Артем Сергеевич Дурнов
соискатель ученой степени
кандидата технических наук
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл., г. Серпухов,
Большой Ударный пер., д. 1а
Тел.: 8 (4967) 35-31-93

Андрей Борисович Наконечный
научный сотрудник
АНО «Институт инженерной физики»

Аннотация

В статье представлены систематизированные оценки помехоустойчивости системы передачи данных при различных способах кодирования исходных сообщений (двоичные циклические коды, недвоичные эквидистантные коды, двоичные коды с мажоритарным декодированием) с применением кодового уплотнения данных и расширения спектра сигнала.

Ключевые слова: битовое отношение сигнал/шум, отношение мощности помехи и сигнала, битовая вероятность ошибки, вероятность ошибочного доведения кодограммы база сигнала, ортогональные сигналы, циклические коды, недвоичные эквидистантные коды.

Summary

The article presents systematic estimates of the noise immunity of a data transmission system with various methods of encoding source messages (binary cyclic codes, non-binary equidistant codes, binary codes with majority decoding) using code compaction of data and signal spectrum expansion

Keywords: bit signal-to-noise ratio, interference and signal power ratio, bit error probability, probability of erroneous completion of the codogram of the signal base, orthogonal signals, cyclic codes, non-binary equidistant codes.

Известные системы радиосвязи [6,7] используют сигнал с ОФМ и расширенным спектром по закону ПСП (длина ПСП определяет базу сигнала B). При воздействии на вход радиоприёмника стационарной гармонической помехи средняя вероятность битовой ошибки P_b (помехоустойчивость радиоприёмника сигнала с ОФМ и расширенным спектром) определяется выражением [7]:

$$P_b \approx 0,5643 \int_0^{\infty} e^{-t^2} dt, \quad (1)$$

$$\left(\frac{1 + P_{II}}{h_b^2 P_{r,B}} \right)^{-0,5}$$

где h_b^2 – битовое отношение сигнал/шум на входе

первой решающей схемы радиоприёмника; P_{II}/P_C – отношение мощностей помехи и полезного сигнала на входе радиоприёмника.

Характер зависимостей $P_b = f(h_b^2)$ для различных значений B и P_{II}/P_C представлен в *таблице 1*.

Анализ результатов, представленных в *таблице 1*, показывает:

- при $B = const$ ($B = 1023$) с увеличением P_{II}/P_C вероятность P_b увеличивается (для $h_b^2 = 15$ при $P_{II}/P_C = 75$ вероятность $P_b = 7,846 \cdot 10^{-5}$, а при $P_{II}/P_C = 300$ вероятность $P_b = 9,207 \cdot 10^{-3}$);

- при $B = const$ с увеличением P_{II}/P_C наступает

Таблица 1
Зависимость $P_b=f(h^2b)$ для различных значений B и P_{Π}/P_C

$B=1023$	$P_{\Pi}/P_C=75$	h_b^2	5	10	15	20	50	100
		P_b	$3,415 \cdot 10^{-3}$	$3,407 \cdot 10^{-4}$	$7,846 \cdot 10^{-5}$	$2,822 \cdot 10^{-5}$	$1,832 \cdot 10^{-6}$	$4,804 \cdot 10^{-7}$
	$P_{\Pi}/P_C=300$	h_b^2	5	10	15	20	50	100
		P_b	0,022	0,012	$9,207 \cdot 10^{-3}$	$7,894 \cdot 10^{-3}$	$5,757 \cdot 10^{-3}$	$5,114 \cdot 10^{-3}$
$B=2047$	$P_{\Pi}/P_C=300$	h_b^2	5	10	15	20	50	100
		P_b	$8,148 \cdot 10^{-3}$	$2,199 \cdot 10^{-3}$	$1,097 \cdot 10^{-3}$	$7,118 \cdot 10^{-4}$	$2,649 \cdot 10^{-4}$	$1,757 \cdot 10^{-4}$

пороговый эффект, при котором увеличение h_b^2 практически не влияет на уменьшение вероятности P_b :

- увеличение $B=const$ ($B=2047$) позволяет уменьшить вероятность P_b (повысить помехоустойчивость), например, при $P_{\Pi}/P_C=300$ для $B=1023$, $h_b^2=15$ вероятность $P_b=9,207 \cdot 10^{-3}$, а для $B=2047$, $h_b^2=15$ значение $P_b=1,093 \cdot 10^{-3}$.

Однако увеличение базы сигнала с целью повышения помехоустойчивости приводит к прямопропорциональному росту скорости передачи двоичных символов в канале передачи данных (расширению требуемой полосы пропускания) или к увеличению времени передачи данных от оконечной аппаратуры (уменьшению скорости передачи данных оконечной аппаратурой), так как полоса пропускания канала радиосвязи фиксирована.

Применение кодирования данных блочными двоичными циклическими кодами (n, k, d_{\min}) , где n – длина кодовой комбинации, k – число информационных символов в кодовой комбинации, d_{\min} – минимальное кодовое расстояние с последующим кодовым уплотнением двоичных символов ортогональными последовательностями позволяет получить более высокие показатели помехоустойчивости [1,2,6]. Такая схема передачи данных реализует каскадное кодирование данных. Структурная схема системы радиосвязи в этом случае будет иметь вид (рисунк 1).

На рисунке 1 обозначены:

КУ – блок кодирующего устройства [1,2];

БКУ – блок кодового уплотнения [5];

М – модулятор сигнала [3,5];

ГОС – генератор ортогональных сигналов [3,5];

ГПСП – генератор псевдослучайной последовательности [6];

ГПОС – генератор полярных ортогональных сигналов [6];

СВС – система временной синхронизации [5];

СДМ – сужающий демодулятор [5];

КД – корреляционный декодер [5];

ДКУ – блок декодирующего устройства [1,2].

Зададимся параметрами кодов и сигналов.

Длина передаваемой кодограммы $N=120$ двоичных символов.

Блок КУ будет использовать коды, которые имеют разную скорость кодирования, а именно [1,2]:

1) блочный циклический код с параметрами $n=63, k=30, d_{\min}=13$, который имеет скорость кодирования $k/n=30/63 \approx 0,5$ и позволяет гарантированно исправлять 6 двоичных ошибок;

2) блочный циклический код с $n=63, k=10, d_{\min}=27$, который имеет скорость кодирования $k/n=10/63 \approx 0,16$ и позволяет гарантированно исправлять 13 двоичных ошибок;

3) блочный циклический код с $n=127, k=22, d_{\min}=47$, исправляющий 23 двоичные ошибки.

Блок кодового уплотнения данных будет использовать ортогональные последовательности с длиной $W=8,16,32,64$. Генератор псевдослучайной последовательности формирует дискретный сигнал с базой $B=1024$, равной длине ПСП. Модулятор формирует сигнал с относительной фазовой манипуляцией (ОФМ) и расширенным спектром сигнала по закону ПСП.

Математические выражения, которые позволяют получить статистические характеристики декодирования данных при воздействии на вход радиоприёмника узкополосной гармониче-

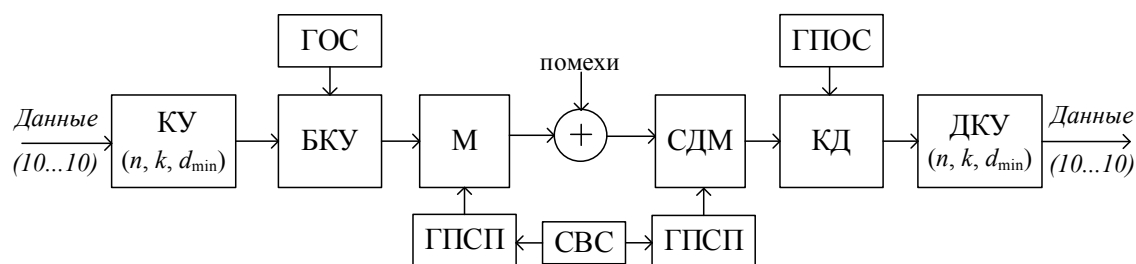


Рис. 1. Структурная схема системы радиосвязи с каскадным кодированием данных

ской помехи и аддитивного гауссовского шума следующие:

- вероятность ошибочного доведения кодограммы до получателя P_1

$$P_1 = 1 - (1 - P_2)^{N/k}, \quad (2)$$

- вероятность ошибочного декодирования кодовой комбинации P_2

$$P_2 = \sum_{i=t+1}^n C_n^i P^i (1-P)^{n-i}; \quad (3)$$

- вероятность битовой ошибки на выходе корреляционного декодера (на входе блока ДКУ) равна [5]:

$$P_3 = 0,5 \left[1 - (1 - P_{b1})^W \right], \quad (4)$$

где $P_{b1} = 0,5643 \int_0^{\left(\frac{1}{Wb_b^2} \frac{P_{II}}{P_c B}\right)^{-0,5}} e^{-0,5t^2} dt$.

В таблице 2 представлены численные значения оценки вероятностей P_1, P_2, P_3 и соответствующие им значения h_b^2 при различных W .

Анализ результатов, представленных в таблице 2, показывает:

- при одинаковых параметрах сигнала ($W=const, B=const$), неизменных значениях $P_{II}/P_c = 75$ блочный двоичный циклический код (63,10,27) позволяет обеспечить требования по вероятности ошибочного доведения кодограммы ($P_1=const$) с меньшими энергетическими затратами h_b^2 по отношению к коду (63,30,13);

- для кода (63,30,13) существует оптимальное значение параметра W (длина ортогональной последовательности), при которой требуется минимальное значение h_b^2 для фиксированно-

го значения вероятности P_1 (в частности, для $P_1 \geq 10^{-5}$ значение $W=32$);

- для кодов (63,10,27) и (127,22,48) увеличение параметра W способствует уменьшению значения h_b^2 при $P_1=const$ и увеличению скорости передачи данных источником.

Так как код (63,10,27) имеет энергетические преимущества по отношению к коду кодов (63,30,13), то представляет интерес оценка помехоустойчивости двоичного ортогонального кода (64,6,32), который можно декодировать по методу максимального правдоподобия и получить дополнительный выигрыш в помехоустойчивости [6]:

$$P_2 = 1 - (P_4 + P_5 + P_6),$$

где $P_4 = \sum_{i=0}^t C_n^i P_3^i (1-P_3)^{n-i}; n=64; t = \frac{32-P_3}{2} = 15;$

$$P_5 = \sum_{s=t+1}^{d_{\min}} C_n^s P_3^s (1-P_3)^{n-s} \prod_{S=0}^{s-1} \left(1 - \frac{C_n^S C_{n/2}^{s-S}}{C_n^{s-S}} \right)^{2^{s-1}}; k=6; d_{\min}=32;$$

$$P_6 = \sum_{i=d_{\min}+1}^{n-1} C_n^i P_3^i \prod_{S=0}^{i-1} \left(1 - \frac{C_n^{i-d_{\min}+S} C_{n/2}^{d_{\min}-S}}{C_n^{d_{\min}-S}} \right)^{2^{i-1}} (1-P_3)^{n-1}.$$

Оценки вероятностей P_1, P_2, P_3 , отношения h_b^2 для $P_{II}/P_c = 75; B=1024, W=1, W=8, W=16, W=32, W=64$ представлены в таблице 3.

Сравнивая оценки вероятностей P_3 , отношения h_b^2 при $P_1=const$ для ортогонального кода (64,6,32), которые представлены в таблице 3, и циклического кода (63,10,27), представленные в таблице 2, можно сделать однозначные выводы в пользу кода (64,6,32). Более того, увеличивая длину кода (127,22,48) при пороговом декодиро-

Таблица 2
Статистические характеристики декодирования

Блочный код (63,30,13); $t_u=6; P_{II}/P_c=75; B=1023$							
P_1	P_2	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$	$h_b^2 (W=16)$	$h_b^2 (W=32)$	$h_b^2 (W=64)$
10^{-4}	$3,09 \cdot 10^{-5}$	0,0141	2,911	2,812	2,133	1,795	1,98
10^{-5}	$3,09 \cdot 10^{-6}$	0,00982	3,404	3,48	2,754	2,57	4,32
10^{-6}	$3,083 \cdot 10^{-7}$	0,00698	3,873	4,345	3,66	4,055	75
Блочный код (63,10,27); $t_u=13; P_{II}/P_c=75; B=1023$							
P_1	P_2	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$	$h_b^2 (W=16)$	$h_b^2 (W=32)$	$h_b^2 (W=64)$
10^{-4}	10^{-5}	0,0565	1,38	1,31	0,938	0,682	0,518
10^{-5}	10^{-6}	0,047	1,556	1,449	1,04	0,762	0,59
10^{-6}	10^{-7}	0,039	1,754	1,61	1,154	0,857	0,678
10^{-7}	10^{-8}	0,033	1,923	1,76	1,27	0,95	0,773
Блочный код (127,22,47); $t_u=23; P_{II}/P_c=75; B=1023$							
P_1	P_2	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$	$h_b^2 (W=16)$	$h_b^2 (W=32)$	
10^{-4}	$1,754 \cdot 10^{-5}$	0,0738	1,236	1,13	0,811	0,586	
10^{-5}	$1,7 \cdot 10^{-6}$	0,0643	1,393	1,219	0,875	0,632	
10^{-6}	$1,694 \cdot 10^{-7}$	0,056	1,542	1,315	0,944	0,687	
10^{-7}	$1,69 \cdot 10^{-8}$	0,04966	1,71	1,41	1,005	0,7413	

Таблица 3
Статистические характеристики декодирования ортогонального кода (64,6,32)

P_1	P_2	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$	$h_b^2 (W=16)$	$h_b^2 (W=32)$	$h_b^2 (W=64)$
10^{-4}	$5,14 \cdot 10^{-6}$	0,116	0,7516	0,857	0,624	0,448	0,324
10^{-5}	$5,14 \cdot 10^{-7}$	0,0982	0,8872	0,951	0,687	0,4932	0,359
10^{-6}	$5,12 \cdot 10^{-8}$	0,0832	1,028	1,05	0,757	0,543	0,4
10^{-7}	$5,12 \cdot 10^{-9}$	0,0714	1,17	1,146	0,822	0,594	0,442

вании, не удастся получить лучшие результаты декодирования.

На практике часто используется мажоритарная обработка двоичных символов кодовой комбинации, которая передается несколько раз. Покажем, что в этом случае при фиксированном времени передачи (фиксированной энергии сигнала на передачу нескольких повторов кодовой комбинации) эффект может быть отрицательным. Например, при использовании совершенного кода Голея (24,12,8) на одной передаче получают следующие результаты (таблица 4) для $P_{II}/P_C=75; B=1024$.

При 5-кратной передаче кода (24,12,8) для $P_{II}/P_C=75; B=1024$ результаты следующие (таблица 5).

В таблице 5 вероятность $P_{M=5}$ рассчитана по выражению

$$P_{M=5} = \sum_{i=\frac{5+1}{2}}^5 C_5^i P_3^i (1-P_3)^{5-i}. \quad (5)$$

Анализ результатов, представленных в таблицах 4 и 5, позволяет сделать следующие выводы:

Таблица 4

Декодирование кода (24,12,8) на одной передаче

P_1	P_2	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$
10^{-4}	10^{-5}	$5,97 \cdot 10^{-3}$	4,093	1,271
10^{-5}	10^{-6}	$3,31 \cdot 10^{-3}$	5,058	1,746
10^{-6}	10^{-7}	$1,85 \cdot 10^{-3}$	6,0814	2,399
10^{-7}	10^{-8}	$1,04 \cdot 10^{-3}$	7,24	3,34

Таблица 5

Декодирование кода (24,12,8) при 5-кратных повторах

P_1	P_2	$h_b^2 (W=1)$	$h_b^2 (W=8)$	P_3	$P_{M=5}$
$9,22 \cdot 10^{-5}$	$9,22 \cdot 10^{-6}$	$4,093/5=0,986$	1,0257	0,0871	0,0058
$6,43 \cdot 10^{-5}$	$6,43 \cdot 10^{-5}$	$5,058/5=1,0116$	1,047	0,0843	0,0053
$5,26 \cdot 10^{-6}$	$5,26 \cdot 10^{-7}$	$6,0814/5=1,2163$	1,186	0,0678	0,0028
$3,27 \cdot 10^{-7}$	$3,27 \cdot 10^{-8}$	$7,24/5=1,448$	1,352	0,053	0,014

Таблица 6

Оценки параметров декодирования кода (11,1,11)

P_1	P_2	P_q	P_3	$h_b^2 (W=1)$	$h_b^2 (W=8)$
10^{-4}	$6,73 \cdot 10^{-6}$	0,177	0,0885	0,973	1,0116
10^{-5}	$6,714 \cdot 10^{-7}$	0,136	0,068	1,213	1,18
10^{-6}	$6,7 \cdot 10^{-8}$	0,105	0,05025	1,5	1,4
10^{-7}	$6,68 \cdot 10^{-9}$	0,08	0,04	1,7219	1,574

- если требования по вероятности доведения кодограммы $P_1 > 10^{-4}$, то повторы кодовой комбинации с последующей мажоритарной обработкой на приёмной стороне дают положительный эффект;

- при $P_1 < 10^{-4}$ декодирование кода (24,12,8) на одной передаче дает лучшие результаты, что объясняется более высоким значением h_b^2 ;

- применение кодового уплотнения данных ($W=8$) позволяет обеспечить заданные требования по вероятности $P_1 < 10^{-5}$ при меньших значениях h_b^2 , а скорость передачи данных увеличивается в W раз.

Применение эквидистантных недвоичных кодов, у которых основание кода $q=256$, длина кодовой комбинации N_q равна кодовому расстоянию D_q для любой пары кодовых комбинаций, позволяет исправлять пакет двоичных ошибок. Для таких кодов вероятность ошибочного декодирования кодовой комбинации P_2 равна [5]

$$P_2 = \sum_{i=T_b+1}^{N_q} C_{N_q}^i P_q^i (1-P_q)^{N_q-i}, \quad (6)$$

где P_q – вероятность ошибочного приёма недвоичного символа кода, равная для сигнала с расширенным спектром $2P_b$, а для систем с кодовым уплотнением данных $P_q = 2P_b$; $T_u = \left\lceil \frac{D+1}{2} \right\rceil$.

В таблице 6 представлены значения вероятностей P_1, P_2, P_q, P_3 , отношений h_b^2 для сигналов с параметрами: $W=1$ при $P_{II}/P_C=75; B=1024; W=8$

при $P_{\pi}/P_c=75$; $B=1024$ и эквидистантного кода с параметрами $N_q=D_q=11$, $q=256$, который переносит $\log_2 256=8$ двоичных символов.

Анализ таблицы 6 показывает:

- при $P_1=10^{-4}$ кодовое уплотнение данных ($W=8$) требует большего значения h_b^2 по сравнению с традиционным способом передачи сигнала с расширенным спектром (энергетический проигрыш составляет $1,0116/0,973=1,04 \approx 0,17$ дБ), однако скорость передачи данных источником увеличивается в 8 раз;

- при $P_1 \leq 10^{-5}$ кодовое уплотнение данных позволяет получить энергетический выигрыш кодирования (для $P_1=10^{-7}$ выигрыш равен $1,7219/1,574=1,094 \approx 0,39$ дБ);

- длина пакета двоичных ошибок, который будет исправлен таким каскадным кодом, равна $T_{\pi} = WT_{\pi} = 6 \cdot 8 = 48$ дв. символов.

Двоичные коды (64,6,32), (63,10,27), (127,22,48) такие пакеты ошибок исправить не могут.

Однако для недвоичного кода ($q=256$) можно использовать кодовое уплотнение только с параметром $W=8$.

Поэтому целесообразно оценить эффективность представленных способов кодирования данных. В качестве показателя эффективности кодирования данных будем использовать выражение [4]:

$$P = 10 \lg \frac{Wk}{n} \frac{P_3}{h_b^2} \text{ при } P_1 = f(W, \frac{k}{n}, P_3, h_b^2) = const.$$

Результаты оценки показателя P представлены в таблице 7.

Анализ результатов, представленных в таблице 7, позволяет сделать следующие выводы:

- использование коротких блочных кодов типа (24,12,8) с целью упрощения процесса декодирования и повторов кодовых комбинаций положительного результата не дает (5-кратный повтор кодовых комбинаций кода (24,12,8) уступает по показателю эффективности блочному коду (127,22,47), хотя эквивалентная избыточность остается неизменной);

- наилучшие результаты по показателю эффективности P при $P_1=const$ имеет двоичный ор-

тогональный код (63,6,32) при его декодировании по методу максимального правдоподобия, однако такой код не может исправлять пакеты ошибок $T_{\pi} > 15$ двоичных символов;

- недвоичный код ($N_q=11$, $K_q=1$, $D_q=11$, $q=256$) по показателю эффективности уступает двоичному ортогональному коду (64,6,32), двоичным циклическим кодам (63,10,27), (127,22,47), коду Голя с 5-кратными повторами комбинаций, но его достоинство в том, что длина пакета исправляемых ошибок $T_{\pi}=48$ двоичных символов.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение, 2-е изд: пер с англ. М.: ООО «И.Д.Вильямс», 2017. 1100 с.
2. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. 774 с.
3. Зеленецкий В.В., Зеленецкий Ю.В., Егоров В.В., Наконечный А.Б. Математическая модель имитозащищенного канала передачи данных стеганографическими способами // Известия Института инженерной физики, 2022. №2(64). С. 20-23.
4. Зеленецкий В.В., Зеленецкий Ю.В., Егоров В.В., Наконечный А.Б. Эффективность методов кодирования данных в системах радиосвязи // Известия Института инженерной физики, 2022. №3(65). С. 15-19.
5. Зеленецкий В.В., Зеленецкий Ю.В., Егоров В.В., Наконечный А.Б. Методика оценки помехоустойчивости радиоканала с кодовым уплотнением данных и расширенным спектром при воздействии импульсной помехи // Известия Института инженерной физики, 2022. №4(66). С. 28-34.
6. Зеленецкий Ю.В. Методы информационно-статистического анализа и алгебраического синтеза в конечном поле корректирующих кодов систем телекоммуникаций повышенной помехозащищенности с широкополосным доступом: дисс. на соиск. уч. степ. докт. тех. наук. Серпухов: МОУ «ИИФ», 2014. 322 с.
7. Борисов В.И., Зинчук В.М., Лимарев А.Е., Шестопапов В.И. Помехозащищенность систем радиосвязи с расширением спектра прямой модуляцией ПСП. М.: «РадиоСофт», 2011. 548 с.

Таблица 7

Эффективность кодирования данных

Параметры кодирования ($n, k, B, W, P_{\pi}/P_c$)	$P_1=10^{-4}$	$P_1=10^{-7}$
24,12,1023,8,75	$P=-17,239$ дБ	$P=-29,217$ дБ
24, 12, 1023, 8, 75 (5 повторов)	$P=-11,68$ дБ	$P=-15,441$ дБ
127, 22, 1023, 8, 75	$P=-10,433$ дБ	$P=-13,115$ дБ
63, 10, 1023, 8, 75	$P=-12,045$ дБ	$P=-16,232$ дБ
11, 1, 1023, 8, 75	$P=-11,964$ дБ	$P=-17,332$ дБ
64, 6, 1023, 8, 75	$P=-9,935$ дБ	$P=-13,304$ дБ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056

ПОСТРОЕНИЕ ПОЧТОВОГО АНАЛИЗАТОРА DLP СИСТЕМЫ НА ОСНОВЕ КЛЮЧЕВЫХ СЛОВ BUILDING A DLP SYSTEM MAIL ANALYZER BASED ON KEYWORDS



Никита Сергеевич Таганов

магистрант
Московский технический университет
связи и информатики
Адрес: 111024, Москва, ул. Авиамоторная, д. 8а
Тел.: +7 (985) 232-39-18
E-mail: taganov2@mail.ru

Максим Александрович Бессонов

кандидат технических наук
Московский технический университет
связи и информатики
Адрес: 111024, Москва, ул. Авиамоторная, д. 8а
Тел.: +7 (977) 751-46-98
E-mail: m.a.bessonov@mtuci.ru

Аннотация

В статье представлен разбор системы предотвращения утечек информации в почтовых сообщениях (как части системы борьбы с внутренними нарушителями – DLP), базирующейся на комплексном методологическом подходе к анализу текстов и использованию передовых технологий машинного обучения. Освещены взаимодействие и взаимодействие различных модулей, включая метод цифровых отпечатков, регулярные выражения и тематическое моделирование (LDA), в целях обеспечения высокой эффективности в выявлении потенциальных угроз конфиденциальности информации.

Ключевые слова: тематическое моделирование, конфиденциальная информация, LDA, цифровые отпечатки, регулярные выражения, правила, почтовые сообщения.

Summary

This article presents an analysis of the system for preventing information leaks in emails, based on a comprehensive methodological approach to text analysis and the use of advanced machine learning technologies. The interaction and synergy of various modules, including the digital fingerprint method, regular expressions and thematic modeling (LDA), are highlighted in order to ensure high efficiency in identifying potential privacy threats.

Keywords: thematic modeling, confidential information, LDA, digital fingerprints, regular expressions, rules, mail messages.

Введение

В настоящее время, в связи с бурным развитием цифровых технологий, цифровизацией общества и государства, возникают все новые риски в области информационной безопасности. Особое внимание в данном контексте уделяется защите конфиденциальной информации в сфере электронной почты – с увеличением объема передаваемых данных возрастает риск утечек конфиденциальной информации.

С ростом объемов электронного общения и обмена данными через электронную почту возрастает потребность в надежных механизмах защиты конфиденциальной информации. В свете этих изменений становится актуальной задача создания системы, объединяющей разнообразные методы обнаружения утечек информации.

Целью статьи является представление интегрированного подхода к предотвращению уте-

чек конфиденциальной информации в сфере электронной почты.

Методы категоризации данных

Большое количество данных требует систематизации и классификации для более эффективного анализа и использования. Один из ключевых аспектов этого процесса – методы категоризации данных, которые включают несемантические, псевдосемантические и семантические подходы.

Несемантические методы представляют собой основные техники категоризации, основанные на структуре и формальных характеристиках данных. Ручная разметка, использование контекста хранения информации, программы-агенты и метод регулярных выражений – все эти методы включают в себя механическое или структурное разделение данных, что делает их удобными для простых операций классификации.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Псевдосемантические методы добавляют элемент смысла к процессу категоризации, используя лингвистический анализ и цифровые отпечатки. Лингвистический анализ позволяет учесть семантику языка и контекст слов, тогда как цифровые отпечатки позволяют идентифицировать уникальные характеристики данных. Эти методы поднимают уровень точности и полноты категоризации, учитывая смысловые аспекты информации.

Семантические методы представляют собой более сложный подход, в основе которого лежит понимание значения данных и их взаимосвязей. С использованием семантических методов, система может распознавать смысловые отношения между объектами и классифицировать данные на основе их значения, что делает этот метод наиболее продвинутым и интеллектуальным в сфере категоризации.

Эффективное сочетание этих методов позволяет создавать более точные и адаптированные системы категоризации данных, что является неотъемлемой частью современных информационных технологий.

В рамках данной статьи сосредоточимся на рассмотрении трех методов обнаружения конфиденциальной информации в документах. Каждый из этих методов представляет собой эффективный инструмент в борьбе с утечками данных, а именно: лингвистический анализ, метод цифровых отпечатков и метод регулярных выражений.

Лингвистический анализ

Первый метод, который мы рассмотрим – лингвистический анализ. Для анализа используется алгоритм LDA (Latent Dirichlet Allocation). LDA является статистической моделью, которая используется для выявления тематических паттернов в коллекции текстовых документов. Он основан на предположении, что каждый документ является смесью нескольких тем, а каждая тема, в свою очередь, является смесью слов. Используя LDA, возможно определить, какие слова связаны с конкретной темой и какие документы их содержат.

Данный алгоритм позволяет извлекать темы из набора текстовых документов, не имея априорной информации о тематике каждого документа. Он основывается на следующих предположениях: каждый документ представляет собой смесь нескольких тем, а каждая тема определяется распределением вероятностей над словами в словаре [1]. Таким образом, каждое слово в документе выбирается из вероятностного распределения тем, присутствующих в этом документе.

Алгоритм LDA можно описать следующим образом:

1. Инициализация: на первом шаге задаются количество тем и случайные распределения слов в каждой теме. Каждая тема представляет собой распределение слов, которые могут относиться к этой теме. Изначально эти распределения задаются случайно.

2. Для каждого слова в каждом документе выбирается тема с вероятностью, пропорциональной распределению слов в каждой теме. На этом шаге слова из документов рассматриваются по очереди, и для каждого слова выбирается тема с наибольшей вероятностью. Вероятность выбора темы определяется на основе распределения слов в каждой теме и распределения тем в каждом документе.

3. Используя выбранные темы для каждого слова в документе, обновляются распределения тем в каждом документе. После того, как для каждого слова была выбрана тема, производится обновление распределения тем в документе на основе выбранных тем для каждого слова. То есть, если для документа выбраны темы «наука» и «технологии», то вероятность наличия этих тем в данном документе будет увеличиваться.

4. Используя выбранные темы для каждого слова в каждой теме, обновляются распределения слов в каждой теме. После обновления распределений тем в каждом документе, производится обновление распределения слов в каждой теме на основе выбранных тем для каждого слова. То есть, если слово «компьютер» было выбрано для темы «технологии», то вероятность наличия этого слова в данной теме будет увеличиваться.

5. Шаги 2-4 повторяются до сходимости. После того, как произведены обновления на шагах 2-4, алгоритм проверяет, достигнута ли сходимость. Если нет, то производятся новые обновления.

6. После выполнения шагов 2-5 до достижения сходимости, LDA выдает результат в виде распределений тем в каждом документе и распределений слов в каждой теме [2].

Распределение тем в каждом документе показывает, какие темы присутствуют в документе и с какой вероятностью. Например, если анализируется коллекция документов, связанных с технологическими новинками, то документ, связанный с искусственным интеллектом, может иметь высокую вероятность темы «машинное обучение», а документ, связанный с новым смартфоном, может иметь высокую вероятность темы «мобильные устройства» [3]. Пример вывода матрицы вероятностей представлен в *таблице 1*.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Предобработка данных является важным этапом в анализе текстовых данных, так как именно на этом этапе происходит подготовка данных для последующего анализа [4]. Ниже приведены основные шаги предобработки данных

Удаление шума и выбросов. На данном этапе удаляются лишние символы, знаки препинания, стоп-слова (часто используемые слова, такие как «и», «в», «на» и т.д.), а также другие символы, которые не несут смысловой нагрузки. Также удаляются выбросы, то есть значения, которые значительно отличаются от среднего значения.

Токенизация. Токенизация – это процесс разделения текста на отдельные слова, называемые токенами. В результате токенизации каждое слово становится отдельным элементом данных, который может быть использован в дальнейшем анализе. Токенизация может быть выполнена путем разделения текста по пробелам или другими специальными символами [5].

Приведение к нижнему регистру. Для обеспечения единообразия и устранения различий между словами, написанными в разных реги-

страх, обычно выполняется приведение всех слов к нижнему регистру. Например, слова «Договор» и «договор» будут приведены к единому виду «договор».

Удаление стоп-слов. Стоп-слова – это часто встречающиеся слова, которые обычно не несут смысловой нагрузки и не влияют на результаты анализа. Они могут быть удалены из текста, чтобы уменьшить размер данных и улучшить производительность алгоритма. Примеры стоп-слов в русском языке включают «а», «в», «он», «к» и другие. Список стоп-слов может варьироваться в зависимости от конкретной задачи и языка [6].

Лемматизация и стемминг. Это процессы приведения слов к их базовой или корневой форме. Лемматизация выполняет более сложные преобразования, учитывая грамматические правила языка, в то время как стемминг просто обрезает слово до его основы без учета контекста. Например, слова могут быть приведены к основе с помощью лемматизации или стемминга (рисунк 1).

Удаление нерелевантных или редких слов. Иногда не все слова являются информативными

Таблица 1
Матрица вероятностей

	Topic0	Topic1	Topic2	Topic3	Topic4	Доминирующая тема
Doc0	0.32	0.00	0.24	0.00	0.43	4
Doc1	0.01	0.01	0.01	0.01	0.98	4
Doc2	0.35	0.01	0.28	0.01	0.35	0
Doc3	0.22	0.01	0.01	0.01	0.76	4
Doc4	0.01	0.01	0.24	0.01	0.74	4
...
Doc95	0.00	0.00	0.00	0.00	0.98	4
Doc96	0.00	0.00	0.00	0.00	0.98	4
Doc97	0.00	0.00	0.00	0.00	0.98	4
Doc98	0.00	0.00	0.00	0.00	0.98	4
Doc99	0.06	0.00	0.00	0.00	0.93	4

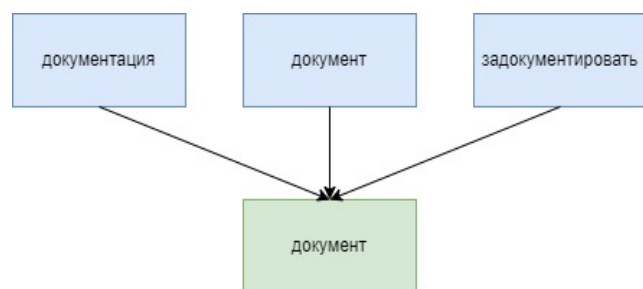


Рис. 1. Приведение к основе слова

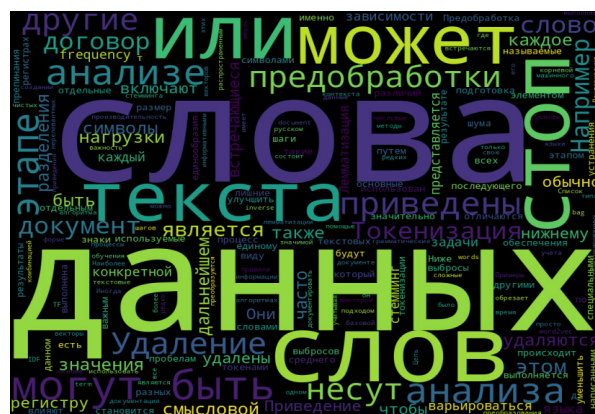


Рис. 2. Пример мешка слов

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

для анализа. Например, редко встречающиеся слова или слова, которые встречаются только в одном документе, могут быть удалены, так как они не несут значимой информации.

Векторизация текста. На этом этапе текстовые данные преобразуются в числовые векторы, чтобы их можно было использовать в алгоритмах машинного обучения. Наиболее распространенным подходом является мешок слов (bag of words) (рисунки 2), где каждое слово представляется вектором, а каждый документ представляется комбинацией векторов слов. Другие методы включают TF-IDF (term frequency-inverse document frequency) и word2vec [7].

Каждый из этих шагов предобработки данных имеет свою важность и может варьироваться в зависимости от конкретной задачи и типа данных. Цель предобработки данных состоит в создании чистых, структурированных и надежных данных, которые могут быть использованы в дальнейшем анализе и обработке.

В целом, LDA является мощным инструментом для анализа текстовой информации, который позволяет извлекать полезную информацию из большого количества документов. Однако важно помнить, что для достижения наилучших результатов, необходимо проводить анализ и корректировку параметров алгоритма, а также использовать дополнительные методы для обработки текстовой информации, такие как предобработка и очистка текста.

Цифровые отпечатки

Цифровые отпечатки (ЦО) в почтовом анализаторе DLP-системы используются для обнаружения конфиденциальной информации, такой как пароли, номера кредитных карт, социальные страховые номера и другие конфиденциальные данные в электронной почте и файловых вложениях. Цифровой отпечаток представляет собой хеш-функцию, которая создается из образца конфиденциальных данных, например, известного номера кредитной карты или паттер-

на символов, используемых в пароле [8].

При использовании цифровых отпечатков в DLP-системах, анализатор электронной почты сканирует сообщения и файловые вложения, чтобы определить, содержат ли они какие-либо конфиденциальные данные, соответствующие заданным шаблонам цифровых отпечатков. Если в сообщении или вложении обнаруживается совпадение с одним из цифровых отпечатков, анализатор электронной почты может применить соответствующую политику безопасности, например, отправить сообщение на дополнительную проверку или заблокировать его отправку.

Цифровые отпечатки могут использоваться в различных сценариях DLP, таких как контроль конфиденциальных данных в электронной почте, обнаружение утечек данных через сетевые протоколы, мониторинг использования USB-накопителей и других внешних устройств, а также при анализе активности пользователей в корпоративных системах.

ЦО могут быть созданы с помощью различных инструментов, включая специализированные программы, которые могут создавать отпечатки на основе заданных шаблонов. Однако, для того чтобы цифровые отпечатки были эффективны, необходимо тщательно подбирать шаблоны и контролировать их использование, чтобы исключить ложные срабатывания.

Регулярные выражения

Регулярные выражения (РВ) (Regular Expressions, или просто regex) – это синтаксические конструкции для поиска и манипулирования текстом в соответствии с определенным шаблоном. Используются они для обработки текста в различных задачах, включая поиск, замену, извлечение и фильтрацию.

Регулярные выражения состоят из символов, которые образуют паттерн для поиска или замены. Символы могут быть буквами, цифрами, специальными символами и комбинациями этих элементов (таблица 2).

Таблица 2
Шаблоны

Шаблон	Описание	Примеры
.	Один любой символ	&
\d	Любая цифра	9
\D	Любой символ кроме цифры	B
\s	Пробел, перенос строки, символ табуляции	" "
\S	Любой символ кроме пробела, переноса строки, символа табуляции	+
[a-z]	Любая буква от a до z	c
[0-9]	Любая цифра от 0 до 9	5
\w	Любая буква	a
\W	Любой символ кроме буквы	%

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Существует множество различных языков для создания регулярных выражений, однако наиболее распространенными являются POSIX и PCRE. Оба этих языка обладают широкими возможностями для создания регулярных выражений и позволяют настраивать правила поиска и фильтрации данных на основе широкого спектра шаблонов (таблица 3) [9]. Для примера было принято решение использовать PCRE, так как требуется обработка сложных сценариев, а он обладает более широким и мощным синтаксисом, чем POSIX.

Для использования регулярных выражений в данной сфере, понадобится определить типы данных, которые необходимо искать в почтовых сообщениях: номера телефонов, номера банковских карт, номера паспортов и другие конфиденциальные данные. Затем, с помощью специального языка, который поддерживается в почтовом анализаторе, необходимо создать регулярные выражения для поиска этих данных.

Для российских номеров телефонов можно использовать следующее регулярное выражение:

```
(+7|8)?\s?(?\d3)?\d3?[\s-]?\d{3}[\s-]?\d{2}[\s-]?\d{2}
```

Данное выражение будет находить номера телефонов в форматах:

1. +7 XXX XXX XX XX;
2. 8 XXX XXX XX XX;
3. XXX XXX XX XX;
4. XXX-XXX-XX-XX;
5. XXX.XXX.XX.XX;
6. XXX XXX XX XX.

Такое выражение позволит найти различные форматы российских номеров телефонов, в том числе с различными разделителями и с использованием различных кодов регионов. Однако необходимо учитывать, что данное выражение не является универсальным и может не нахо-

дить некоторые форматы номеров телефонов, а также учитывать возможность ложных срабатываний и принимать соответствующие меры для минимизации ошибок. Для этого можно использовать дополнительные правила фильтрации и проверки данных, которые позволят убедиться в точности результатов анализа.

В целом, использование регулярных выражений в почтовом анализаторе позволяет автоматизировать процесс обработки почтовых сообщений и обеспечить более точный и эффективный поиск конфиденциальных данных. Кроме того, регулярные выражения могут быть использованы для создания правил блокировки определенных типов данных, что позволяет предотвратить несанкционированный доступ к конфиденциальной информации. Для эффективного использования регулярных выражений необходимо постоянное обновление правил поиска и фильтрации данных.

Взаимодействие модулей

Метод цифровых отпечатков и регулярные выражения используются совместно для обеспечения более эффективного поиска конфиденциальной информации, передаваемой через почтовый сервис.

Когда регулярное выражение находит совпадение, сообщение считается подозрительным и отправляется на дополнительный анализ. В этом месте метод цифровых отпечатков используется для дополнительной проверки, действительно ли найденные данные являются конфиденциальными.

Использование только регулярных выражений не гарантирует, что найденная информация является конфиденциальной. Например, если мы ищем номера кредитных карт с помощью регулярного выражения, оно может также находить номера, которые не являются кредитными

Таблица 3
Примеры синтаксиса РВ

Регулярное выражение	Функция
<code>\b\d{16}\b</code>	Поиск 16-значных чисел (например, номера кредитных карт) в тексте, ограниченные границами слов (то есть, не содержащие других цифр).
<code>\b\d{9}\b</code>	Поиск 9-значных чисел (например, социальные номера) в тексте, ограниченные границами слов.
<code>\b[A-Z]{2}\d{4}\b</code>	Поиск номеров автомобильных номеров, состоящих из двух букв и четырех цифр.
<code>\b[0-9a-fA-F]{32}\b</code>	Поиск 32-значных хешей (например, MD5), представленные в шестнадцатеричной форме.
<code>\b([A-Za-z0-9_%.+]+@[A-Za-z0-9.-]+.[A-Za-z]{2,})\b</code>	Поиск адресов электронной почты в тексте.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

картами, но соответствуют шаблону, например, номера банковских счетов.

В этом случае метод цифровых отпечатков играет роль дополнительной проверки найденной информации. Если найденная информация является конфиденциальной, она может быть связана с соответствующим цифровым отпечатком. Если найденная информация не является конфиденциальной, то ее цифровой отпечаток будет отличаться от ожидаемого.

Каждая строка с найденной подозрительной информацией обрабатывается с помощью алгоритма хеширования. Полученный хэш-код сравнивается с базой данных хэш-кодов известных конфиденциальных данных. Если совпадение найдено, то строка блокируется как содержащая конфиденциальную информацию, если совпадения нет, то строка не является конфиденциальной и не подлежит блокировке. Подробная схема изображена на *рисунке 3*.

Таким образом, регулярные выражения находят предположительную конфиденциальную информацию, а цифровые отпечатки проверяют, действительно ли она является конфиденциальной. Это позволяет системе быстро и точно определять, содержит ли сообщение конфиденциальную информацию и принимать соответствующие меры, например, блокировку или предупреждение отправителя о наличии конфиденциальной информации в сообщении.

После прохождения двух вспомогательных модулей алгоритм LDA приступает к классификации данных независимо от вердикта. В случае выявления конфиденциальной информации предыдущими модулями, категоризация документа по-прежнему необходима для подтверждения факта передачи подобных данных. Также

проверка дополнит необходимыми данными log-файлы, чем в свою очередь может помочь администраторам безопасности. При отсутствии предупреждающих флагов о наличии секретной информации в передаваемом документе, LDA необходимо определить его тематику. В пример можно привести документ содержащий медицинские сведения. Система защиты от утечек данных должна следовать законодательным требованиям и нормам обработки медицинских сведений, установленным Федеральным законом 152-ФЗ «О персональных данных» и другими российскими законами и нормативными актами. При обнаружении передачи медицинских сведений, система сразу же заблокирует трансляцию и отправит сообщение ответственному лицу. Подобный документ может не содержать номера телефонов, банковских карт и т.п., но правильно определенная тематика предотвратит нарушение конфиденциальности.

По этой причине LDA является основным методом в системе. Он позволяет проводить анализ контекста текста и выявлять скрытые связи между словами и темами, которые могут указывать на наличие конфиденциальной информации. В то время как цифровые отпечатки и регулярные выражения могут помочь в обнаружении известных конфиденциальных данных, LDA позволяет находить скрытые связи, которые могут указывать на наличие неизвестных конфиденциальных данных.

Блок решающих правил

Построение решающих правил для системы предотвращения утечек информации требует внимательного анализа требований, классификации данных, анализа рисков и определения

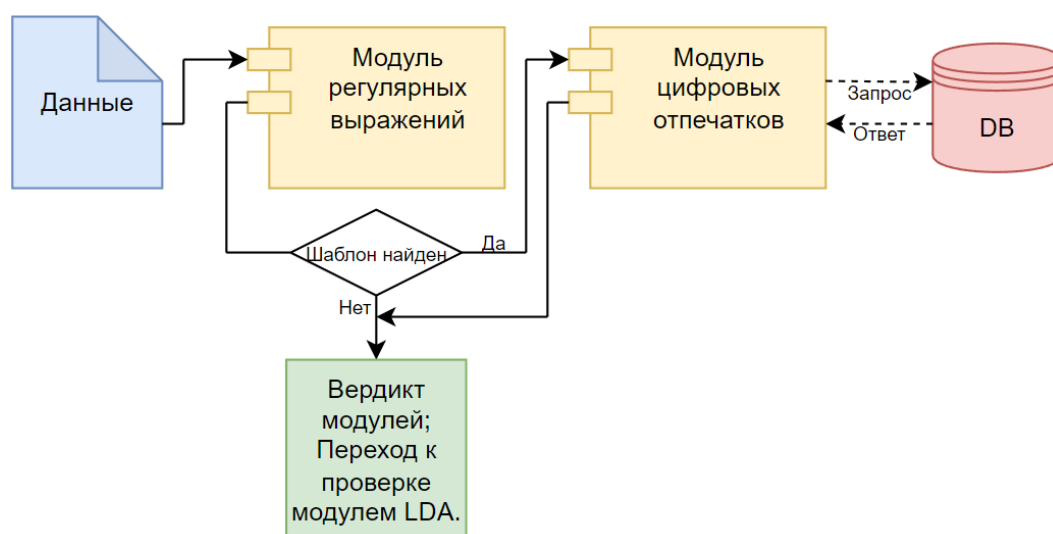


Рис. 3. Схема взаимодействия цифровых отпечатков и регулярных выражений

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

политик безопасности. Правильно настроенные правила позволят системе эффективно обнаруживать и предотвращать утечки конфиденциальной информации, а также реагировать на нарушения политик безопасности.

Рассмотрим схему принятия решения по входным данным. Каждый модуль на вход получает передаваемую информацию. После их обработки на выходе создается флаг, информирующий о наличии или отсутствии конфиденциальной информации, за исключением модуля регулярных выражений, он информирует только о потенциальной конфиденциальной информации. Структурная схема почтового сервиса с системой предотвращения утечек информации

изображена на *рисунке 4*.

По развернутой схеме флагов (*рисунок 5*) можно увидеть принцип реагирования системы на наличие потенциальной или действительной конфиденциальной информации, то есть когда флаги получают значение «true» на входе. Единственным случаем, когда анализатор допустит передачу документа, является наличие флага модуля регулярных выражений, при условии отсутствия флагов других модулей.

Вывод

Предложенная система объединяет преимущества различных методов, обеспечивая не только высокую точность обнаружения конфи-

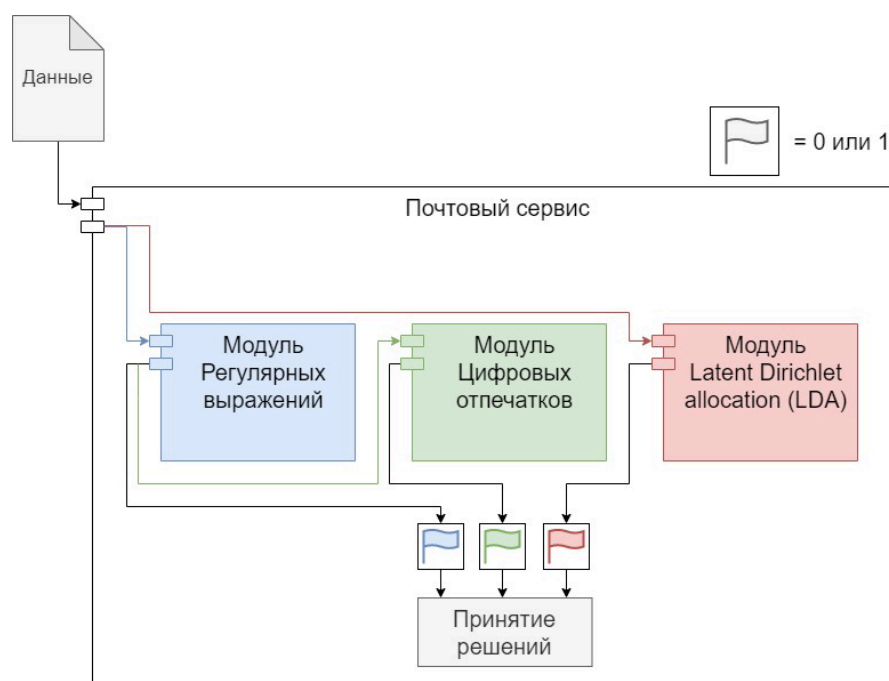


Рис. 4. Структурная схема почтового сервиса

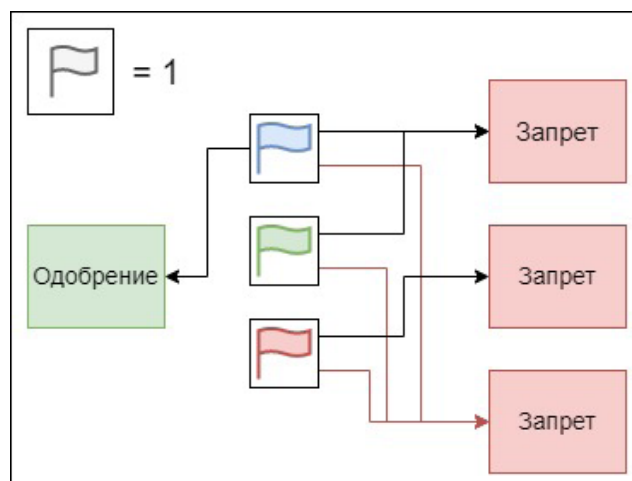


Рис. 5. Схема реагирования системы

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

денциальной информации, но и минимизацию ложных срабатываний. Интегрированный подход, представленный в данной статье, позволяет эффективно объединить цифровые отпечатки, регулярные выражения и алгоритм LDA для обеспечения высокоточного анализа электронных сообщений. Эта система позволяет быстро и точно выявлять потенциальные и фактические случаи утечек конфиденциальной информации, предупреждая от возможных нарушений безопасности.

Основываясь на данном подходе, будущие разработки в области обеспечения безопасности информации могут стремиться к созданию более сложных и интеллектуальных систем, способных адаптироваться к постоянно меняющимся угрозам. Это направление работы открывает перспективы для создания инновационных решений, гармонично сочетающих в себе точность, скорость и надежность в обеспечении безопасности электронной переписки.

Литература

1. Воронцов К.В. Алгоритм латентного размещения Дирихле для моделирования и кластеризации текстовых коллекций // Машинное обучение и анализ данных, 2014. Т.1. С.115-123.
2. Пирогов В.А., Сивков А.А., Фомичева М.М. Применение метода латентного размещения Дирихле в задачах кластеризации текстовых

данных // Информационно-управляющие системы, 2015. Т.2. С.22-26.

3. Blei D.M., Ng A.Y., Jordan M.I. Latent Dirichlet Allocation // Journal of Machine Learning Research, 2003. Vol.3. P.993-1022.

4. Gandomi A., Haider M. Beyond the hype: Big data concepts, methods, and analytics // International Journal of Information Management, 2015. Vol.35. № 2. P.137-144.

5. Королев В.Ю., Власов В.В. Методы предобработки данных в задачах анализа текстов // Информационные технологии и вычислительные системы, 2018. Т.3. С.113-122.

6. Гришкин А.А., Михалев А.Г. Методы предобработки данных в задачах анализа и построения прогнозных моделей // Научно-технический вестник информационных технологий, механики и оптики, 2016. Т.16. №2. С.376-383.

7. Семёнов И.Н. Методы предобработки данных в задачах исследования социальных сетей // Информатика и её применения, 2015. Т.9. №3. С.23-29.

8. Иванов А.А. Цифровые отпечатки и их применение в информационной безопасности // Труды Института системного программирования РАН, 2010. Т.18. С.277-290.

9. Виноградова Е. Н., Виноградов Ю. В. Алгоритмы построения решающих правил в задачах искусственного интеллекта // Искусственный интеллект и принятие решений, 2013. №2. С.35-44.



ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.039

МЕТОДИКА РАСЧЕТА ЭЙЛЕРОВЫХ И ГАМИЛЬТОНОВЫХ МАРШРУТОВ ДЛЯ БПЛА С ПОМОЩЬЮ РЕДУКЦИИ THE METHOD OF CALCULATING EULERIAN AND HAMILTONIAN ROUTES FOR UAVS USING REDUCTION

Эдуард Михайлович Руденко
кандидат технических наук
доцент кафедры математики
филиал ВА РВСН им. Петра Великого
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: +7 (916) 851-80-55
E-mail: eduard5529@yandex.ru

Елена Викторовна Семикина
преподаватель кафедры информатики
филиал ВА РВСН им. Петра Великого
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
E-mail: labinfo_serp@inbox.ru
Тел.: +7 (915) 064-50-74



Аннотация

В статье рассматривается методика расчета эйлеровых и гамильтоновых маршрутов на графах для обеспечения бортовых алгоритмов БПЛА оперативного решения задач на графах реперных точек на местности и организации различных схем мониторинга. Математическая модель задачи нахождения маршрутов включает в себя алгоритмы прямого перебора номеров реперных точек, генетический алгоритм минимизации целевой функции от целочисленных переменных номеров реперных точек, методы редукции графов большой размерности. В основе этих методов используется целевая функция графа, которая обнуляется только на эйлеровых или гамильтоновых маршрутах. Целевая функция (ЦФ) строится на основе теорем о единственном представлении математических величин в виде суммы или произведения [1,2]. На множестве всех эйлеровых маршрутов рассматривается задача нахождения маршрутов максимального и наибольшего мониторинга, на которых обеспечивается наиболее плотный мониторинг с интервалом одно ребро наибольшего количества БПЛА с соблюдением условий безопасности полета. Для нахождения эйлеровых и гамильтоновых маршрутов на графах с большим числом вершин и ребер применяется метод редукции по уменьшению их размерности и нахождения маршрутов на них, которые потом поднимаются до маршрутов исходных графов. Редукция не исключает полностью NP-алгоритмы по времени нахождения эйлеровых и гамильтоновых маршрутов, но позволяет отодвинуть эту границу в область графов большей размерности, обеспечивает получение ограниченного числа маршрутов для решения задач маршрутизации БПЛА.

Ключевые слова: граф реперных точек, эйлеровы и гамильтоновы маршруты, целевая функция графа, коды ребер и вершин графа, генетический алгоритм, редукция графа.

Summary

The article discusses the methodology for calculating Eulerian and Hamiltonian routes on graphs to provide on-board UAV algorithms for operational problem solving on graphs of reference points on the ground and the organization of various monitoring schemes. The mathematical model of the problem of finding routes includes algorithms for direct enumeration of reference point numbers, a genetic algorithm for minimizing the objective function of integer variables of reference point numbers, and methods for reducing graphs of large dimension. These methods are based on the graph objective function, which is zeroed only on Eulerian or Hamiltonian routes. The objective function (CF) is based on the theorems about the only representation of mathematical quantities in the form of a sum or product [1,2]. On the set of all Eulerian routes, the problem of finding the routes of maximum and greatest monitoring is considered, which provide the most dense monitoring with an interval of one edge of the largest number of UAVs in compliance with flight safety conditions. To find Eulerian and Hamiltonian routes on graphs with a large number of vertices and edges, a reduction method is used to reduce their dimension and find routes on them, which then rise to the routes of the original graphs. Reduction does not completely exclude NP-algorithms for the time of finding Eulerian and Hamiltonian routes, but it allows you to move this boundary into the area of graphs of higher dimension, provides a limited number of routes for solving UAV routing problems..

Keywords: fiducial point graph, optimal closed routes on a graph, objective function, codes of edges and vertices of a graph, genetic algorithm.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Математическая задача нахождения эйлеровых и гамильтоновых маршрутов

Для организации мониторинга между назначенными реперными точками (вершинами), соединенными ребрами, наибольшее применение находят эйлеровы или гамильтоновы графы. На эйлеровых графах (ЭГ) существуют замкнутые маршруты, проходящие один раз по каждому ребру, а на гамильтоновых графах (ГГ) существуют замкнутые маршруты, проходящие один раз через каждую вершину. Для графов с большим числом вершин и ребер, то есть на графах большой размерности, существует проблема нахождения эйлеровых или гамильтоновых маршрутов, которые обладают дополнительным свойством организации безопасного полета с интервалом одно ребро наибольшей группой БПЛА. Такие эйлеровы маршруты (ЭМ) называются маршрутами наибольшего мониторинга (МНМ). Наиболее простой способ их нахождения за-

Листинг 1

```

record = [ ]; % пустой массив
for i1 = 1:n % n – число вершин графа: n = |V|
    for i2 = 1:n
        .....
        for im = 1:n % m – число ребер графа: m = |E|
            X = [i1 i2 ..... im]; % аргумент ЦФ
            Y = YrabнениеVnEm(X); %ЦФ графа VnEm
            if Y == 0
                i0 = i0 + 1; % счетчик ЭМ
                [1 X 1] % ЭМ графа
                record = [record; [1 X 1]] % массив ЭМ
            end
        end
    end
    .....
end
end
i0 % число найденных ЭМ
record % массив ЭМ
t1 = toc % время перебора
    
```

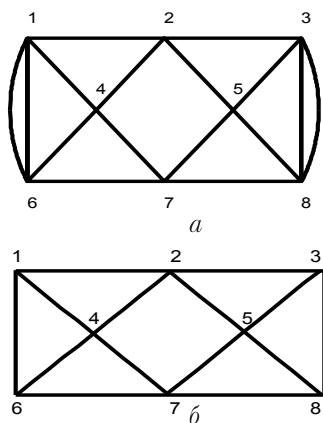


Рис. 1. Граф: а – ЭГ v_8e_{16} с кратными ребрами (1 6) и (3 8); б – ГГ v_8e_{14} с 8 вершинами и 14 ребрами

ключается в отборе их из множества всех эйлеровых маршрутов на данном графе. Сложность решения этой задачи состоит в том, что задача нахождения всех ЭМ является NP-проблемой, требующей неограниченно большого времени по алгоритму полного перебора, который позволяет в лексиграфическом порядке найти все ЭМ без пропусков на данном графе. На *листинге 1* приведён программный код метода полного перебора.

Программа полного перебора выполняет $n^m = |V|^{|E|}$ вычислений что составляет для уже небольших графов большое число. Так, если компьютер выполняет в секунду миллиард операций 10^9 , то для графа (*рисунок 1а*) с $|V| = 8$ и $|E| = 16$ потребуется время для перебора равное $8^{16}/10^9/3600 = 78,19$ часов. Для бытовых компьютеров этот расчёт может занять несколько лет [4,5].

Для гамильтонова графа на *рисунке 1б* число гамильтоновых маршрутов составляет всего 18 штук (*таблица 1*).

Время счета 53,96 секунды.

Ниже на *рисунке 2* представлены ГМ на графе ГГ v_8e_{14} . Девять маршрутов на *рисунке 2* надо прочитывать в двух направлениях: в прямом и обратном, и поэтому получается 18 ГМ.

Метод перебора позволил подсчитать все ГМ. По сравнению с числом ЭМ на графе v_8e_{16} (*рисунок 1а*) число ГМ значительно меньше.

Следовательно:

- метод перебора позволяет получить все эйлеровы и гамильтоновы маршруты на графах малой размерности за приемлемое время: секунды, минуты, часы или несколько суток;

- метод перебора не позволяет получить все эйлеровы и гамильтоновы маршруты на графах большой размерности при числе вершин $\#|V| > 7$ и ребер $\#|E| > 16$ из-за большого числа шагов $> 7^{16}$ и неприемлемо большого времени счета (задача NP).

На ЭМ и ГМ мониторинг БПЛА целесообразно назначать при организации движения змейкой друг за другом с интервалом одно или несколько ребер с соблюдением условий безопасного мониторинга (УБМ): не встречаться в одной вершине и на одном ребре. Это можно обеспечить с помощью выполнения требования проходить каждое ребро за одинаковое время, т.е. длинные ребра проходить с большей скоростью, а короткие – с меньшей скоростью [3]. При этом соблюдать дополнительное требование приходить в вершины приблизительно в одинаковые моменты времени, что обеспечивается прописыванием этих требований в полетном задании и организацией связи между БПЛА (или

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

с центром управления).

Требование непрерывности и полноты обследования территории, назначенной для мониторинга по ЭМ или по ГМ, может потребоваться большое число БПЛА, а это приводит к необходимости использовать такие маршруты, на которых возможно движение максимального (или наибольшего, т.е. самого большого количества) аппаратов с соблюдением УБМ. Это означает, что надо подсчитать или иметь насчитанные заранее маршруты максимального мониторинга (МММ) или маршруты наибольшего мониторинга (МНМ).

Как следует из работы [4], все гамильтоновы маршруты являются маршрутами наибольшего мониторинга и число БПЛА на ГМ равно числу вершин графа: $n_{\text{МНМ}} = |V|$.

Гарантированно получить МММ, а лучше МНМ, можно только если имеется возможность их выбрать из всего множества ЭМ графа реперов. Но получение всех ЭМ или ГМ на произвольном графе является в настоящее время нерешенной проблемой [6], которая решается для ЭГ или ГГ только небольшой размерности и только с помощью метода полного перебора..

Поэтому существует проблема нахождения

Таблица 1
Гамильтоновы маршруты на графе v8e14

1	1 2 3 5 8 7 4 6 1	7	1 4 2 3 5 8 7 6 1	13	1 6 4 7 5 8 3 2 1
2	1 2 3 5 8 7 6 4 1	8	1 4 2 3 8 5 7 6 1	14	1 6 4 7 8 3 5 2 1
3	1 2 3 8 5 7 4 6 1	9	1 4 2 5 3 8 7 6 1	15	1 6 4 7 8 5 3 2 1
4	1 2 3 8 5 7 6 4 1	10	1 4 6 7 5 8 3 2 1	16	1 6 7 5 8 3 2 4 1
5	1 2 5 3 8 7 4 6 1	11	1 4 6 7 8 3 5 2 1	17	1 6 7 8 3 5 2 4 1
6	1 2 5 3 8 7 6 4 1 . $m_6 = (1, 5, 3, 4, 6, 2, 1)$	12	1 4 6 7 8 5 3 2 1	18	1 6 7 8 5 3 2 4 1

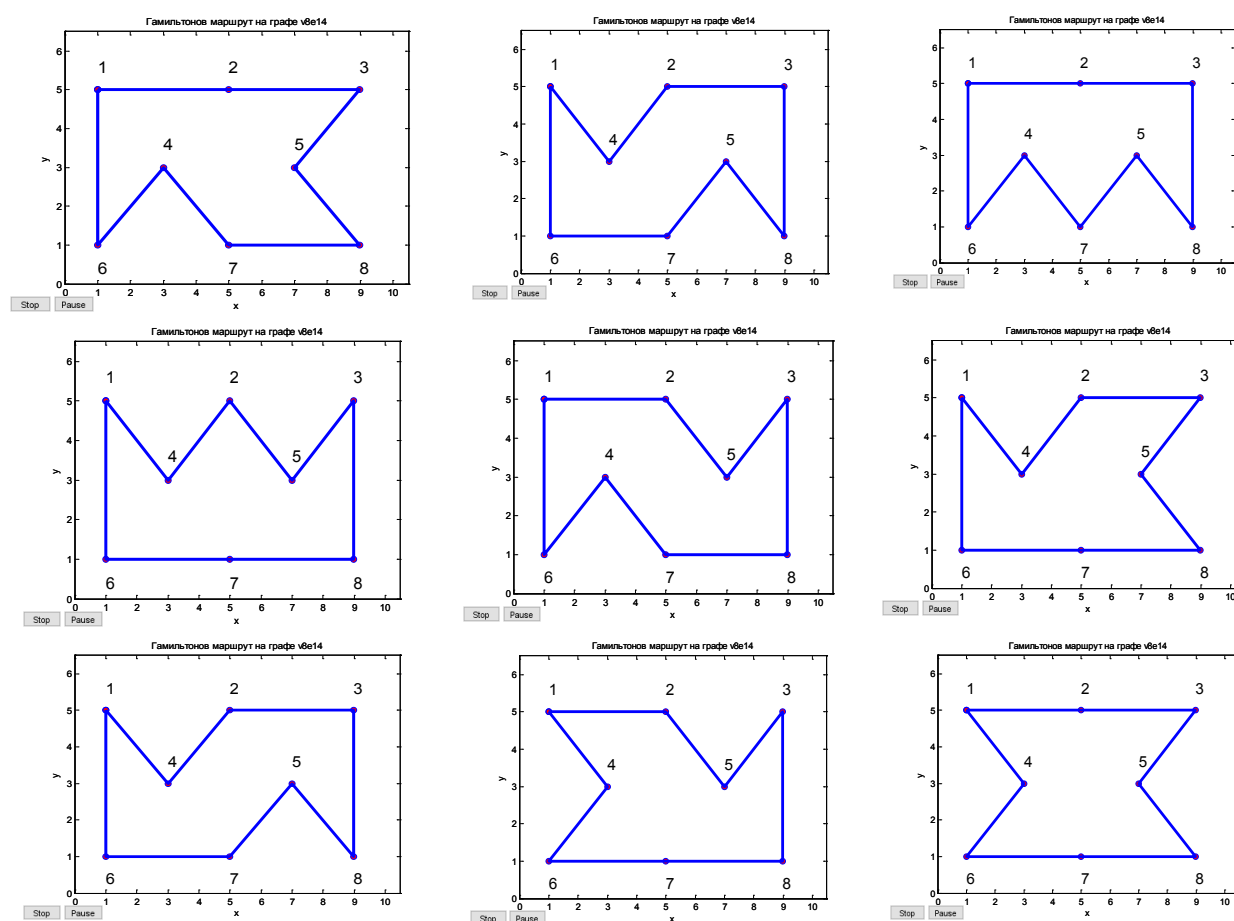


Рис. 2. Гамильтоновы маршруты на графе v8e14

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

маршрутов максимального и наибольшего мониторинга. В работе предложен метод, на основе которого разработана комплексная методика построения маршрутов на эйлеровых и гамильтоновых графах, значительно сокращающая время расчета до нескольких минут и часов.

Выводы:

- для организации безопасного движения группы БПЛА рассматривается граф реперов, на котором известны числа МММ и МНМ, БПЛА двигаются змейкой по эйлеровым или гамильтоновым маршрутам в количестве, не превосходящем указанное число МММ (МНМ);
- многообразие вариантов движения по графу напрямую зависит от множества эйлеровых или гамильтоновых маршрутов, которые насчитываются либо заблаговременно, либо в ходе движения;
- использование реперов на местности, образующих эйлеровы и гамильтоновы графы, является закономерно обоснованным из-за наличия у них десятков, сотен и тысяч маршрутов;
- решение проблемы нахождения большого количества эйлеровых или гамильтоновых маршрутов является актуальной прикладной за-

дачей организации различных вариантов применения БПЛА.

Метод редукции графа

Для построения ЭМ и ГМ может быть применен метод редукции. Рассмотрим определение и подсчет эйлеровых маршрутов на графе $v8e12$ (рисунки 3) с помощью редукции.

Граф $v8e12$ имеет горизонтальную и вертикальную оси симметрии и обладает горизонтальным и вертикальным автоморфизмом

$$\gamma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 8 & 4 & 2 & 7 & 6 & 3 \end{pmatrix}; \quad (1)$$

$$\gamma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 7 & 1 & 5 & 8 & 3 & 6 \end{pmatrix}.$$

В качестве графа первой редукции рассмотрим квадрат – граф $v4e4$ (рисунки 3б). На циклическом графе $v4e4$ существует два эйлеровых маршрута: (1 3 5 7 1), (1 7 5 3 1). Преобразуем граф $v4e4$ в граф промежуточной редукции графа $v4e8$ (рисунки 4).

На графе $v4e8$ существует 10 эйлеровых маршрутов, которые легко подсчитать. Первые пять маршрутов получаются при проходе в начале ребер графа в порядке возрастания номеров вершин с последующим возвращением назад:

$$\begin{aligned} & (1\ 2\ 4\ 5\ 1\ 2\ 4\ 5\ 1), (1\ 2\ 4\ 5\ 1\ 5\ 4\ 2\ 1), \\ & (1\ 2\ 4\ 5\ 4\ 2\ 1\ 5\ 1), \\ & (1\ 2\ 4\ 2\ 1\ 5\ 4\ 5\ 1), (1\ 2\ 1\ 5\ 4\ 2\ 4\ 5\ 1). \end{aligned} \quad (2)$$

В наборе ЭМ (2) имеется симметричный маршрут (1 2 4 5 1 5 4 2 1), для которого выполняется равенство

$$Y_{обр}(1\ 2\ 4\ 5\ 1\ 5\ 4\ 2\ 1) = (1\ 2\ 4\ 5\ 1\ 5\ 4\ 2\ 1).$$

Последующие четыре маршрута получаются обращением маршрутов (2) (операция инверсии) и добавлением нового маршрута:

$$\begin{aligned} & (1\ 5\ 4\ 2\ 1\ 2\ 1\ 5\ 4): \\ Y_{обр}(1\ 2\ 4\ 5\ 1\ 2\ 4\ 5\ 1) &= (1\ 5\ 4\ 2\ 1\ 5\ 4\ 2\ 1), \\ Y_{обр}(1\ 2\ 4\ 5\ 1\ 5\ 4\ 2\ 1) &= (1\ 5\ 1\ 2\ 4\ 5\ 4\ 2\ 1), \\ Y_{обр}(1\ 2\ 4\ 5\ 4\ 2\ 1\ 5\ 1) &= \\ &= (1\ 5\ 4\ 5\ 1\ 2\ 4\ 2\ 1), \\ Y_{обр}(1\ 2\ 1\ 5\ 4\ 2\ 4\ 5\ 1) &= (1\ 5\ 4\ 2\ 4\ 5\ 1\ 2\ 1), \\ & (1\ 5\ 4\ 2\ 1\ 2\ 1\ 5\ 4). \end{aligned} \quad (3)$$

Всего получим 10 различных маршрутов.

Рассмотрим следующую редукцию $v4e10$ (рисунки 4б), расположенную между графами $v4e8$ и $v8e12$. Маршруты на графе $v4e10$ получаются из маршрутов (2) и (3) графа $v4e8$ с помощью операции вставки номеров вершин 3 и 6. Вершина 3 должна быть вставлена один раз между вершинами 2 и 4, а вершина 6 один раз между 1 и 5. Вершина 3 в каждый маршрут из наборов (9) и (10) может быть вставлена двумя способами, так

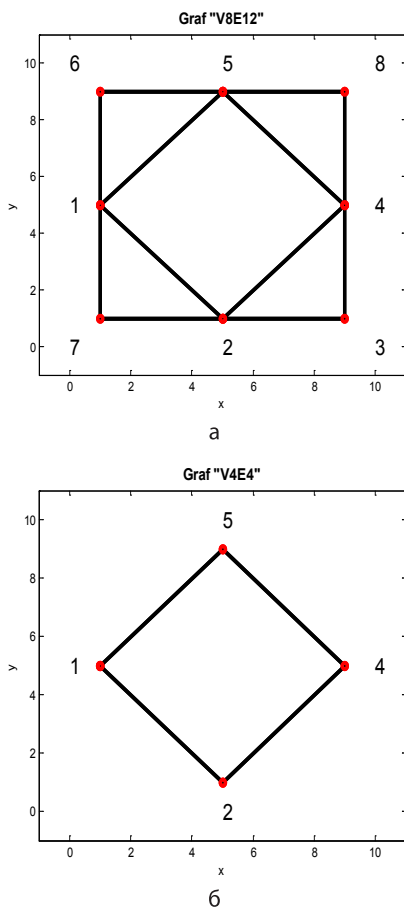


Рис. 3. Графы: а - $v8e12$ и его редукция б - $v4e4$

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

как кратность ребра (2 4) равна двум. При этом получим 20 маршрутов.

Аналогично вставка вершины 6 в полученные 20 маршрутов, порождает из каждого по два маршрута, так как ребро (1 5) имеет кратность два. Поэтому, проводя вставку, получим 40 маршрутов на графе $v4e10$, приведенные в таблице 2.

В таблице 2 полужирным шрифтом выделены номера вставленных вершин 3 и 6.

Если от графа $v6e10$ перейти к исходному графу $v8e12$ (рисунк 3а), то понадобится вставка номеров вершин 7 и 8 в кратные ребра (1 2) и (4 5),

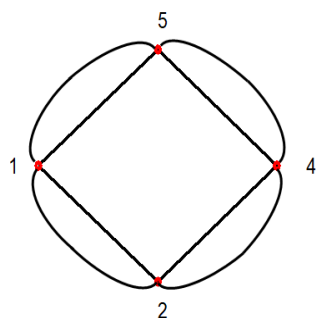
подобно тому как это было выполнено в таблице 2. В результате получим из 40 маршрутов графа $v6e10$ 160 ЭМ графа $v8e12$, которые приведены в таблице 3.

В таблице 3 полужирным шрифтом выделены номера вершины в ЭМ с номерами 6, 8, 12, 28, 47, 65, 70, 71, 94, 95, 100, 110, 135, 151, 155 и 159, которые являются маршрутами наибольшего мониторинга. Число таких ЭМ равно 16. Число маршрута наибольшего мониторинга на графе $v8e12$ равно $n_{\text{МММ}}=5$, которым помечены после тире ЭМ таблицы 3.

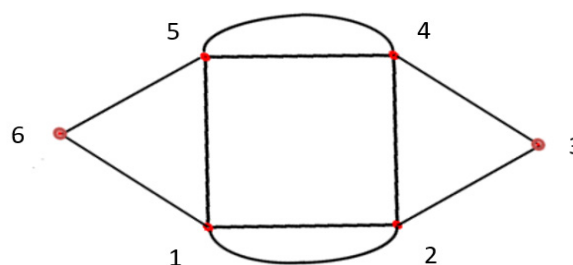
Таблица 2

Эйлеровы маршруты графа $v4e8$, преобразованные вставку вершин 3 и 6 в эйлеровы маршруты графа $v6e10$

	ЭМ графа $v4e8$	ЭМ графа $v6e10$
1	(1 2 4 5 1 2 4 5 1)	(1 2 3 4 5 6 1 2 4 5 1), (1 2 4 5 6 1 2 3 4 5 1), (1 2 3 4 5 1 2 4 5 6 1), (1 2 4 5 1 2 3 4 5 6 1)
2	(1 2 4 5 1 5 4 2 1)	(1 2 3 4 5 6 1 5 4 2 1), (1 2 4 5 6 1 5 4 3 2 1), (1 2 3 4 5 1 6 5 4 2 1), (1 2 4 5 1 6 5 4 3 2 1)
3	(1 2 4 5 4 2 1 5 1)	(1 2 3 4 5 4 2 1 6 5 1), (1 2 4 5 4 3 2 1 6 5 1), (1 2 3 4 5 4 2 1 5 6 1), (1 2 4 5 4 3 2 1 5 6 1)
4	(1 2 4 2 1 5 4 5 1)	(1 2 3 4 2 1 6 5 4 5 1), (1 2 4 3 2 1 6 5 4 5 1), (1 2 3 4 2 1 5 4 5 6 1), (1 2 4 3 2 1 5 4 5 6 1)
5	(1 2 1 5 4 2 4 5 1)	(1 2 1 6 5 4 3 2 4 5 1), (1 2 1 6 5 4 2 3 4 5 1), (1 2 1 5 4 3 2 4 5 6 1), (1 2 1 5 4 2 3 4 5 6 1)
6	(1 5 4 2 1 5 4 2 1)	(1 6 5 4 3 2 1 5 4 2 1), (1 6 5 4 2 1 5 4 3 2 1), (1 5 4 3 2 1 6 5 4 2 1), (1 5 4 2 1 6 5 4 3 2 1)
7	(1 5 4 2 1 2 1 5 4)	(1 2 3 4 5 6 1 5 4 2 1), (1 2 4 5 6 1 5 4 3 2 1), (1 2 3 4 5 1 6 5 4 2 1), (1 2 4 5 1 6 5 4 3 2 1)
8	(1 5 1 2 4 5 4 2 1)	(1 6 5 1 2 3 4 5 4 2 1), (1 6 5 1 2 4 5 4 3 2 1), (1 5 6 1 2 3 4 5 4 2 1), (1 5 6 1 2 4 5 4 3 2 1)
9	(1 5 4 5 1 2 4 2 1)	(1 6 5 4 5 1 2 3 4 2 1), (1 6 5 4 5 1 2 4 3 2 1), (1 5 4 5 6 1 2 3 4 2 1), (1 5 4 5 6 1 2 4 3 2 1)
10	(1 5 4 2 4 5 1 2 1)	(1 6 5 4 3 2 4 5 1 2 1), (1 6 5 4 2 3 4 5 1 2 1), (1 5 4 3 2 4 5 6 1 2 1), (1 5 4 2 3 4 5 6 1 2 1)



а – $v4e8$



б – $v6e10$

Рис. 4. Графы

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Таблица 3
Маршруты графа v8e12

№	ЭМ	№	ЭМ
1	1234271548561	81	1651234584271
2	1234271584561	82	1651234854271
3	1234271654851	83	1651245843271
4	1234271658451	84	1651248543271
5	1234516584271	85	1651723458421
6	1234517248561	86	1651723485421
7	1234561584271	87	1651724584321
8	1234561724851	88	1651724854321
9	1234584271561	89	1654215843271
10	1234584271651	90	1654217234851
11	1234851654271	91	1654234851271
12	1234851724561	92	1654234851721
13	1234854271561	93	1654271234851
14	1234854271651	94	1654271584321
15	1234856154271	95	1654321584271
16	1234856172451	96	1654321724851
17	1243271548561	97	1654324851271
18	1243271584561	98	1654324851721
19	1243271654851	99	1654327124851
20	1243271658451	100	1654327158421
21	1245165843271	101	1654851234271
22	1245172348561	102	1654851243271
23	1245615843271	103	1654851723421
24	1245617234851	104	1654851724321
25	1245843271561	105	1658421543271
26	1245843271651	106	1658421723451
27	1248516543271	107	1658423451271
28	1248517234561-5	108	1658423451721
29	1248543271561	109	1658427123451
30	1248543271651	110	1658427154321-5
31	1248561543271	111	1658432154271-4
32	1248561723451-4	112	1658432172451
33	1271542348561	113	1658432451271
34	1271543248561	114	1658432451721
35	1271584234561	115	1658432712451
36	1271584324561	116	1658432715421-4
37	1271654234851	117	1658451234271
38	1271654324851	118	1658451243271
39	1271658423451	119	1658451723421
40	1271658432451	120	1658451724321
41	1542165843271-4	121	1721542348561
42	1542172348561	122	1721543248561
43	1542348561271	123	1721584234561
44	1542348561721	124	1721584324561
45	1542712348561	125	1721654234851
46	1542716584321-4	126	1721654324851
47	1543216584271-5	127	1721658423451
48	1543217248561	128	1721658432451
49	1543248561271	129	1723421548561
50	1543248561721	130	1723421584561
51	1543271248561	131	1723421654851
52	1543271658421-4	132	1723421658451
53	1548561234271	133	1723451248561-4
54	1548561243271	134	1723451658421
55	1548561723421	135	1723456124851-5
56	1548561724321	136	1723456158421
57	1561234584271	137	1723458421561
58	1561234854271	138	1723458421651
59	1561245843271	139	1723485124561-4
60	1561248543271	140	1723485165421
61	1561723458421	141	1723485421561
62	1561723485421	142	1723485421651
63	1561724584321	143	1723485612451-4
64	1561724854321	144	1723485615421
65	1584216543271-5	145	1724321548561
66	1584217234561	146	1724321584561
67	1584234561271	147	1724321654851
68	1584234561721	148	1724321658451
69	1584271234561	149	1724512348561-4
70	1584271654321-5	150	1724516584321
71	1584321654271-5	151	1724561234851-5
72	1584321724561	152	1724561584321
73	1584324561271	153	1724584321561
74	1584324561721	154	1724584321651
75	1584327124561	155	1724851234561-5
76	1584327165421-4	156	1724851654321
77	1584561234271	157	1724854321561
78	1584561243271	158	1724854321651
79	1584561723421	159	1724856123451-5
80	1584561724321	160	1724856154321

(Окончание в следующем номере)

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 681.5.23

ОПРЕДЕЛЕНИЕ ФАКТА НАХОЖДЕНИЯ ПОДВИЖНОГО ОБЪЕКТА НА УЧАСТКЕ ЦИФРОВОЙ КАРТЫ ДОРОГИ DETERMINING WHETHER A MOVING OBJECT IS LOCATED ON A SECTION OF A DIGITAL ROAD MAP

Алексей Викторович Шолохов

доктор технических наук, профессор
профессор кафедры
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: 8 (924) 607-47-88
E-mail: monibwen@gmail.com

Александр Сергеевич Лычагов

кандидат технических наук
докторант
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: 8 (985) 135-48-38
E-mail: lichagov@rambler.ru

Константин Владимирович Карпов

адъюнкт
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: +7 (929) 538-37-69
E-mail: kkv_8@mail.ru

Аннотация

Рассматривается задача выбора участков цифровой карты, применяемых для уточнения местоположения подвижного объекта. В качестве теоретической основы решения задачи выбора участков цифровой карты дорог используется известный подход, применяемый при оптимальной обработке навигационной информации в условиях многоальтернативной модели сигналов с добавлением вероятности нахождения объекта на отрезке по информации от системы технического зрения.

Ключевые слова: навигация, навигационная система счисления пути, цифровая карта дороги, система технического зрения.

Summary

The problem of selecting sections of a digital map used to clarify the location of a moving object is considered. As a theoretical basis for solving the problem of choosing sections of a digital road map, a well-known approach is used for optimal processing of navigation information in a multi-alternative signal model with the addition of the probability of finding an object on a segment based on information from the vision system.

Keywords: navigation, dead reckoning navigation system, digital road map, technical vision system.

Введение

Одним из широко известных, наряду со спутниковыми сигналами, способом повышения точности функционирования автономных наземных навигационных систем (ННС) является способ привлечения информации о траектории движения объекта из цифровой модели местности, так называемой цифровой карте дороги (ЦКД) [1-6].

Среди методов, основанных на использовании ЦКД в целях коррекции ННС, в настоящее время выделяется три подхода, использующих

информацию о дорогах [4-6]: параметрический, прямолинейные отрезки и набор контрольных точек.

ЦКД может рассматриваться в качестве эталона при условии нахождения объекта на ней, однако в виду различных естественных причин таких как объезд различных препятствий, тип дороги (одна-, двух-, многополосная), люфт рулевого колеса и т.п., практически оказывается невозможно строгое движение по заданной траектории (осевой линии дороги). В результате возникает дополнительная методическая по-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

грешность присущая всем рассмотренным подходам – случайное боковое отклонение объекта от осевой линии дороги. Известны подходы, которые позволяют более точно найти оптимальные оценки навигационных параметров, однако при этом используется допущение о движении автомобиля по дороге, положение которой задается параметрами ЦКД. В работе [6] исследован вопрос обоснования допусков в задачах комплексной обработки информации и показана невозможность повышения точности оценок, получаемых в результате оптимальной обработки информации ННС и ЦКД, путем использования каких-либо допусков для распознавания нахождения подвижного объекта на ЦКД. Этим обуславливается необходимость использования дополнительных независимых от навигационной системы и цифровых карт источников информации о положении объекта на дороге.

Данные факторы обусловили решение дополнительной задачи для корректного привлечения информации ЦКД – задача определения (выбора) участка ЦКД.

Существующие варианты [4,5] решения данной задачи основываются на использовании косвенных признаков, по которым выбирается тот или иной участок цифровой карты, также не лишенных ряда недостатков. В связи с этим авторами предлагается использовать дополнительный источник информации – видеокамеру, который в совокупности с алгоритмами компьютерного зрения [7-9] более качественно решит поставленную задачу.

Особенности задачи определения участка ЦКД

Известное решение [5,6] задачи определения участка ЦКД основывается на рассмотрении параметров, характеризующих положение приборной точки относительно участка ЦКД и сравнении текущих значений дирекционного угла объекта с углами азимутальной ориентации участков ЦКД. Траектория движения объекта относится к k -му участку ЦКД с некоторой вероятностью P_k , при одновременном выполнении

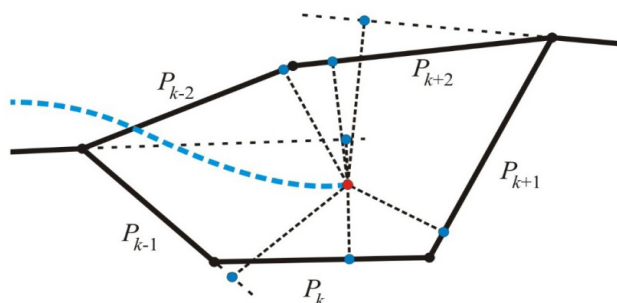


Рис. 1. Определение факта нахождения на отрезке ЦКД

трех условий (рисунк 1).

А. Проекция приборной точки на участок ЦКД, не выходит за его границы.

В. Расстояние между точкой приборной траектории и участком ЦКД не превышает заданной величины r^* .

С. Текущее значение дирекционного угла объекта соответствует углу азимутальной ориентации участка ЦКД.

Рассмотренные события будем полагать взаимно независимыми, что позволяет записать

$$P_k = P_A \cdot P_B \cdot P_C, \quad (1)$$

где P_A, P_B, P_C – вероятность исхода соответствующего события.

Вероятность P_A определяется выражением

$$P_A = P(\xi_i \geq 0) \cdot P(l - \xi_i \geq 0) = (1 - F_\xi(0)) \cdot (1 - F'_\xi(0)), \quad (2)$$

где $P()$ – вероятность события;

ξ – удаленность точки от конца отрезка;

l – длина отрезка;

F_ξ и F'_ξ – функции распределения ξ_i и $(l - \xi_i)$ соответственно, которые будем считать нормальными.

Опуская выкладки, связанные с выводом выражений для параметров указанных функций распределения, запишем

$$P_A = \frac{1}{4} \left(1 + \operatorname{erf} \left[\frac{m}{\sqrt{2 \cdot D}} \right] \right) \left(1 + \operatorname{erf} \left[\frac{l - m}{\sqrt{2 \cdot D}} \right] \right), \quad (3)$$

где $m = M[\mu_i] = (B_u - B_i) \cos \alpha - (L_u - L_i) \sin \alpha$;

μ_i – длина пройденного пути по i -му отрезку ЦКД

$D = D^{KT} + D_B \cos 2\alpha + D_L \sin 2\alpha - K \sin 2\alpha$;

D^{KT} – дисперсия погрешностей координат начала и конца отрезка ЦКД;

$M[\]$ – оператор математического ожидания;

$\operatorname{erf}()$ – функция ошибок;

D_B, D_L, K – элементы ковариационной матрицы вектора $[B_i^{HC} L_i^{HC}]$.

Вероятность P_B определяется выражением

$$P_B(r^*) = P(r^* \leq r_i \leq r^*) = \operatorname{erf} \left(\frac{r^*}{\sqrt{2D_r}} \right), \quad (4)$$

где $D_r = D_B \sin 2\alpha + D_L \cos 2\alpha - K \sin 2\alpha + D_i^K + D_r^{БШ}$;

D_i^K – дисперсия погрешностей координат участка ЦКД;

$D_r^{БШ}$ – дисперсия белого шума.

Аналогично вероятность P_C

$$P_C(\alpha^*) = \operatorname{erf} \left(\frac{\Delta \alpha}{\sqrt{2(D_{\alpha i} + \frac{2D^{KT}}{l^2})}} \right), \quad (5)$$

где $\Delta \alpha$ – невязка между измерительными данными и ЦКД;

$D_{\alpha i}$ – дисперсия дирекционного угла i -го участка ЦКД.

Таким образом, решение задачи сводится к определению номера участка ЦКД k , для которой значение P_k максимально

$$k^* = \arg \max_k P_k(P_A P_B P_C) \quad (6)$$

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Определение участка ЦКД с использованием СТЗ

Новизна предлагаемого подхода заключается в определении вероятности P_B как по информации ННС и ЦКД, так и по информации системы технического зрения (СТЗ) следующим образом.

При приближении к k -му участку ЦКД (рисунк 2) вычисляется вероятность P_{B1} на основе выражения (4), что с учетом полученных вероятностей P_A и P_C позволяет вычислить вероятность P_1

$$P_1 = P_A \cdot P_{B1} \cdot P_C \quad (7)$$

Если полученная вероятность ниже $P_{дон}$ допустимой, то ННС функционирует автономно – состояние Φ_1 (таблица 1). Осуществляется поиск «ближайшего» отрезка, информация от СТЗ не задействована.

Если вероятность P_1 выше допустимой, траектория движения подвижного объекта относится к k -му участку ЦКД и предполагается, что дорога должна находиться в зоне видимости камеры – состояние Φ_2 . СТЗ переходит в режим определения бокового отклонения [10,11].

На основе полученного от СТЗ значения бокового отклонения d_i и дисперсии его значения D_d вычисляется вероятность P_{B2} , которая определяется выражением

$$P_{B2}(d^*) = \text{erf}(d^* / \sqrt{2D_d}) \quad (8)$$

Вероятность нахождения на отрезке ЦКД P_2

Таблица 1
Таблица состояний

Состояние	$P_1 > P_{дон}$	$P_2 > P_{дон}$	Признак нахождения
Φ_1	0	0	0
Φ_2	1	0	0
Φ_3	1	1	1

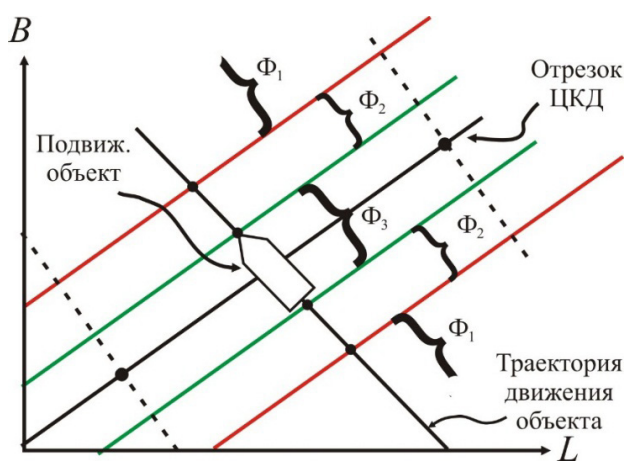


Рис. 2. Определение факта нахождения на отрезке ЦКД

в свою очередь определяется формулой

$$P_2 = P_A \cdot P_{B2} \cdot P_C \quad (9)$$

Таким образом, при выполнении условия $P_2 > P_{дон}$ формируется признак нахождения подвижного объекта на отрезке ЦКД.

Заключение

В работе рассматривается задача выбора участков цифровой карты дороги с использованием информации от СТЗ. Предложенный алгоритм позволяет определить факт нахождения на дороге и рассчитать вероятность нахождения объекта на участке ЦКД для дальнейшего использования отрезка ЦКД для коррекции выработываемых ННС параметров положения и ориентации подвижного объекта.

Литература

1. Беркович С.Б. Оценка эффективности использования геопространственных данных в задаче автономного определения координат наземной навигационной системой / С.Б. Беркович, Р.Р. Бикмаев, Н.И. Котов, А.И. Шахов, В.В. Устинов, А.В. Шолохов // Известия Института инженерной физики, 2021. №2(60). С.2-10.
2. Джанджгава Г.И. Навигация по геофизическим полям. Научно-методические материалы / Г.И. Джанджгава, Л.И. Августов. М.: ООО «Научтехлитиздат», 2018. 296 с.
3. Садеков Р.Н. Автомобильная навигационная система, корректируемая по цифровой карте дорог с использованием последовательных методов Монте-Карло / Р.Н. Садеков, А.В. Шолохов // XII Всероссийское совещание по проблемам управления ВСПУ-2014. Москва, 2014. С.3699-3705.
4. Шолохов А.В. Выбор участков цифровой карты дороги, привлекаемых для коррекции наземной навигационной системы / Ю.В. Черкашин, А.В. Шолохов // Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем: 21-я межвед. науч.-технич. конф.: сб. трудов. Ч.2. Серпухов: СВИ РВ, 2002. С.167-171.
5. Шолохов А.В. Коррекция наземных навигационных систем по цифровой карте дорог с учетом ее погрешностей // Навигация и управление движением: 5-я науч.-технич. конф. молодых ученых : сб. докл. СПб.: ЦНИИ «Электроприбор», 2004. С.227-233.
6. Шолохов А. В. Обоснование допусков в задачах комплексной обработки информации автомобильных навигационных систем и цифровых карт дорог / Р.И. Садеков, А.В. Шолохов // Известия Института инженерной физики, 2014. №2(32). С.61-65.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

7. Обработка изображений в авиационных системах технического зрения / Под ред. Л.Н. Костяшкина, М.Б. Никифорова. М.: ФИЗМАТЛИТ, 2016. 240 с.

8. Position, navigation and timing technologies in the 21st century, volume 2 / Y. Jade Morton [at all]. New Jersey : John Wiley & Sons, 2021. 896 p.

9. Бикмаев Р.Р. Особенности применения многочастотного фильтра в алгоритмах навигации подвижного наземного объекта интегрированного с системой технического зрения // Сборник докладов 4-й Всероссийской НТК «Навигация-2019», 2019. С. 58-67.

10. Лычагов А.С. Алгоритм определения бокового отклонения по информации системы технического зрения / А.С. Лычагов, Ю.С. Карасев,

А.Р. Коротков // XL Всероссийская научно-техническая конференция «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем»: сб. трудов. Ч. 2. Серпухов, 24-25 июня 2021, 2021. С. 129-133.

11. Карпов К. В. Алгоритм вычисления бокового отклонения на основе перспективного преобразования изображения / К.В. Карпов, А.С. Лычагов // Тр. XXXIX Межведомственная НТК «Развитие научно-технических аспектов методологии испытания и эксплуатации с целью повышения эффективности применения существующих средств и систем экспериментально-испытательной базы»: сб. трудов. Т. 2. Космодром «Плесецк» (г. Мирный), 2023. С. 144-149.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.896+159.964.22

ПЕРСПЕКТИВА ИССЛЕДОВАНИЯ ПСИХОАКТИВНЫХ ВЕЩЕСТВ В БИОФИЗИЧЕСКОМ ПСИХОАНАЛИЗЕ¹ THE PERSPECTIVE OF THE STUDY OF PSYCHOACTIVE SUBSTANCES IN BIOPHYSICAL PSYCHOANALYSIS

Валерий Александрович Коломбет
кандидат физико-математических наук
заведующий лабораторией
Институт теоретической и
экспериментальной биофизики РАН
Адрес: 142290, Московская обл.,
г. Пущино, ул. Институтская, д. 3
Тел.: +7(4967)73-92-62
E-mail: v.kolombet@rambler.ru

Вадим Николаевич Лесных
младший научный сотрудник
Институт теоретической и
экспериментальной биофизики РАН
E-mail: 1253vadim@mail.ru

Александр Владимирович Елистратов
ведущий инженер научного подразделения
Институт теоретической и
экспериментальной биофизики РАН
Тел.: +7 (4967) 73-94-64
E-mail: unenlagia@yandex.ru

Аннотация

В статье представлены результаты воздействия на мышление человека психоактивного вещества (ПАВ), выбранного из стандартного арсенала современной медицины. Новизна в том, что в данном случае это воздействие тестировалось посредством предложенного нами т.н. биофизического варианта психоаналитического метода свободных ассоциаций. Оказалось, что спектр словесных ассоциаций, возникающих на любую тему, ставшую объектом внимания, жёстко связан с настроением. При каждой смене объекта внимания происходит крупный скачок в соседнее состояние настроения. «Крупный» потому, что во всём диапазоне настроений доминирует лишь восьмерка таких состояний. В процессе тестирования волонтер записывает серию переключений своего настроения. Многомесячные серии таких тестов позволяют отслеживать изменения процессов мышления у человека, в том числе у человека с ментальными проблемами. Один такой пример подробно рассмотрен в статье. Он показал, в частности, что в процессе применения, выбранного ПАВ может возникать негативный эффект, вызванный, возможно, несоблюдением регламента. В более широкой перспективе использования этого подхода, возникает возможность уточнения свойств т.н. человеческого фактора, нередко проявляющегося в авариях и техногенных катастрофах. С другой стороны, понимание особенностей структуры естественного интеллекта человека может оказаться основой для применения в робототехнике и, возможно, в новых версиях искусственного интеллекта. Ну и, конечно, достаточно хорошо выражены перспективы использования этого подхода в медицине.

Ключевые слова: психоанализ, объект внимания, настроение, цепной вербальный тест.

Summary

The article presents the results of the impact on human thinking of a psychoactive substance (psychoactive substance) selected from the standard arsenal of modern medicine. The novelty is that in this case this effect was tested by means of the so-called biophysical variant of the psychoanalytic method of free associations proposed by us. It turned out that the range of verbal associations that arise on any topic that has become the object of attention is rigidly related to mood. With each change of the object of attention, there is a major leap into the neighboring state of mood. "Large" because only eight such states dominate the entire range of moods. During the testing process, the volunteer records a series of mood swings. A multi-month series of such tests allows you to track changes in human thinking processes, including in patients with mental problems. One such example is discussed in detail in the article. In particular, he showed that in the process of using the selected psychoactive substance, a negative effect may occur, possibly caused by non-compliance with the regulations. In the broader perspective of using this approach, it becomes possible to clarify the properties of the so-called human factor, which often manifests itself in accidents and man-made disasters. On the other hand, understanding the features of the structure of human natural intelligence may be the basis for application in robotics and, possibly, in new versions of artificial intelligence. And, of course, the prospects for using this approach in medicine are quite well expressed.

Keywords: psychoanalysis, object of attention, mood, chain verbal test.

¹ Работа выполнена в рамках Государственного задания № 075-00224-24-00.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Введение

Традиционные задачи, в частности, те, которые следуют из традиционного взгляда на природу т.н. человеческого фактора, на повышение возможностей робототехники и искусственного интеллекта, медицины и пр. пока ещё не учитывают достижений т.н. биофизического психоанализа [1,2]. Мы показали, что у человека ассоциации, возникающие к любому объекту внимания, тесно связаны с настроением, и при смене объекта внимания настроение изменяется крупным скачком.

Нам было интересно узнать, что в той части физиологии мышления, которая описывает именно феномен внимания, уже возникла идея о существовании в человеческом мозге двух отдельных сетей внимания – т.н. дорсальной и вентральной систем внимания – служащих для, соответственно, произвольного распределения внимания и переориентации внимания на неожиданные события, соответственно [3]. За последние годы эта идея вдохновила огромное количество исследований [4]. Независимо разработанный нами т.н. цепной вербальный тест вносит сюда свою существенную лепту. Алгоритм этого теста прост: выбирается любое слово и выписываются к нему слова-ассоциации. В какой-то момент времени эту серию ассоциаций прерывается и производится переход следующей серии ассоциаций, причём в качестве объекта ассоциаций теперь принимается последнее слово предыдущей серии и т.д.

Предполагается, что генерация серии ассоциаций отвечает работе первой сети внимания, а прерывание её работы понуждает включиться вторую сеть внимания. Резкое изменение на-

строения может быть своего рода храповиком, обеспечивающим необратимость процесса переключения сети внимания. Алгоритм цепного вербального теста заставляет снова включиться первую систему внимания, затем вторую и так далее по бесконечному циклу.

Технической аналогией здесь может быть серия положений вала шагового двигателя. На *рисунке 1* этот феномен оформлен в виде т.н. круга ментальных состояний. Безэмоциональные входное и выходное ментальные состояния, позволяющие на спокойном эмоциональном фоне отслеживать физическую реальность (это входное ментальное состояние «Бодрствование») и корректировать доступную часть физической реальности, изменяя своё поведение (это уже выходное ментальное состояние «Действие»), изображены как белый и черный сектора круга. Остальные ментальные состояния тесно связаны с памятью. Они покрашены на рисунке в разные цвета радуги и концентрируются возле центров положительных и отрицательных эмоций – желтого и синего секторов. Положительный центр/сектор помогает нам – самовоспроизводящимся автоматам [5] – размножиться, а отрицательный выжить. На *рисунке 1* положительный сектор и пара его соседей окрашены в теплые цвета: оранжевый, желтый и зеленый, а отрицательный и его ближайшие соседи окрашены в холодные цвета: голубой, синий и лиловый. По сути, этой простой картиной мы мало отличаемся от примитивных микроорганизмов, чей набор секторов можно покрасить в черный, белый, желтый и синий цвета; два последних – это известные положительный и отрицательный таксисы.

На *рисунке 2* представлены характерные

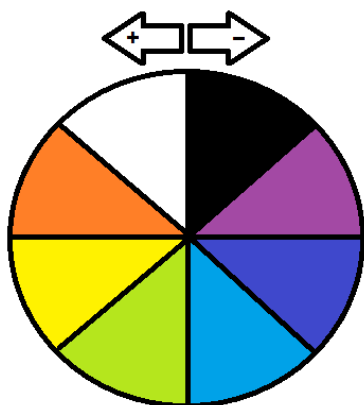


Рис. 1. Круг ментальных состояний. Безэмоциональные состояния представлены как два бесцветных сектора, остальные состояния – это сектора, окрашенные в различные цвета радуги; они связаны с эмоциями и, следовательно, с хорошим и плохим настроением разной интенсивности [6–12]. Максимумы эмоций помечены желтым и синим цветами

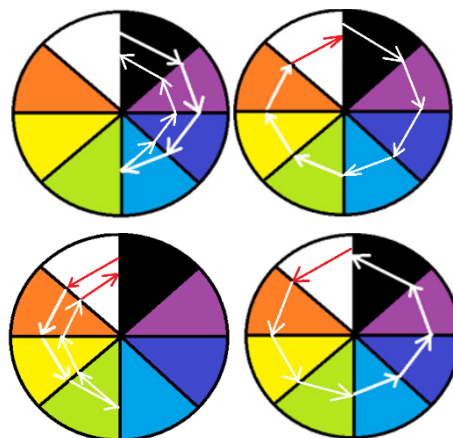


Рис. 2. Четверка характерных фрагментов **pipo**, **pipro**, **nino** и **pino**, выявляемых при сканировании мышления т.н. биофизическим вариантом психоаналитического метода свободных ассоциаций [6–12]. Серии стрелочек внутри кружков указывают на расположение и на направление переключений настроения

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

8-строчные блоки процесса мышления, которые легко выделить в результатах тестирования, и которые мы называем **pipo**, **nipo**, **nino** и **ripo**. Здесь буквы **p** и **n**, происходят от слов, соответственно, **positive** и **negative**, а буквы **i** и **o** от **in** и **out** (рисунк 2). Например, фрагмент – **po** – расшифровывается как **positive out**, т.е. как «находящийся в области центра положительного настроения, выходной фрагмент»). Символы + и – (таблица 2) указывают на присутствие «лишних» тем ассоциаций и на их недостаток.

Предметом этой статьи является прикладной

аспект применения биофизического варианта психоаналитического метода свободных ассоциаций – чувствительность этой техники к протеканию ментальных процессов у человека.

Результаты и обсуждение результатов

Картину своего собственного мышления в образах биофизического психоанализа каждый легко определит самостоятельно, используя, например, Интернет-ресурс [12]. Там приведена 300-страничная монография первого автора этой статьи, дающая подробное описание про-

Таблица 1

Раскрашенный как на *рисунке 1* пример результата тестирования (теста №520). Здесь добавлено разбиение теста на 8-строчные фрагменты (см. *рисунк 2*) и проставлены их коды. Слева – объекты внимания, в центре – ассоциации, раскрашенные в соответствии с *рисунком 1*, справа – коды фрагментов теста

		nino
Серый:	Невзрачный, неяркий, Осень ,	
Осень:	Промозглый, Знойкий,	
Знойкий:	Холодный, мокрый,	
мокрый:	Неприятный, Дождь, вода,	
вода:	Море, дождь ,	
дождь:	Зонт, Лужи,	
Лужи:	Дождь,	
Дождь:	Зонт, лужи,	
		nipo
лужи:	Гроза, Ливень,	
Ливень:	Сила, Зонт,	
Зонт:	Гроза, Слякоть,	
Слякоть:	Холод, Серость,	
Серость:	Осень, Зыбко,	
Зыбко:	Грустно, Ненадежно,	
Ненадежно:	Страшно, Неприятель,	
Неприятель:	Недоверие, Недруг,	
		nipo
Недруг:	Тяжесть, Брезгливо,	
Брезгливо:	Грязно, Неопратно,	
Неопратно:	Неряшливый, Неаккуратный,	
Неаккуратный:	Беспорядок,	
Беспорядок:	Голова,	
Голова:	Человек, Ум,	
Ум:	Друг,	
Друг:	Хорошо, Надежно,	
		ripo
Надежно:	Мост, Дружба,	
Дружба:	Тепло,	
Тепло:	Лето, Мама,	
Мама:	Любовь,	
Любовь:	Жизнь, Город, Животное,	
Животное:	Кролик,	
Кролик:	Счастье, Дом,	
Дом:	Семья, Я,	

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

		pero
Я:	Жизнь,	
Жизнь:	Непросто, Вкусно,	
Вкусно:	Сыр, Красота,	
Красота:	Искусство,	
Искусство:	Человек, Художник, Музей,	
Музей:	Вдохновение, Творчество,	
Творчество:	Ребенок, Талант,	
Талант:	Мысли, сумбур,	
		pero
сумбур:	Мысли, Беспорядочность,	
Беспорядочность:	Легкомыслие,	
Легкомыслие:	Легкость, Девушка ,	
Девушка:	Красота, Грация,	
Грация:	Кошка, Танец, Талант,	
Талант:	Удача, Победа,	
Победа:	Трудолюбие, Сила,	
Сила:	Природа, Разум,	
		nino
Разум:	Тайна, Наука,	
Наука:	Интересно, Загадка,	
Загадка:	Незнание,	
Незнание:	Недостаток, Отсутствие,	
Отсутствие:	Нужда, Лишение,	
Лишение:	Утрата, Несправедливость,	
Несправедливость:	Неопределенность, Общество,	
Общество:	Люди, Регламент,	
		nino
Регламент:	Привила, Закон,	
Закон:	Строгость, правда, упорядоченный,	
упорядоченный:	Строгий, Требование,	
Требование:	Неукоснительно,	
Неукоснительно:	Момент, Авария,	
Авария:	Срочно, Красный,	
Красный:	Предупреждение,	
Предупреждение:	Сигнал,	
		pero
Сигнал:	Звук, Движение,	
Движение:	Жизнь,	
Жизнь:	Жизнь,	
Жизнь:	Жизнь,	
Жизнь:	Солнце, Синий, Счастье, Природа,	
Природа:	Животные, Ресурс, Мощь,	
Мощь:	Природа, Явление, Время,	
Время:	Воспоминание	

цесса тестирования, а также множество примеров. На том же сайте приводится автоматизированный тест, который позволяет облегчить и стандартизировать процесс тестирования.

Примером результата тестирования здоро-

вого человека может быть *таблица 1* (см. также *рисунок 3*). Здесь можно отметить, во-первых, что и старт, и финиш тестирования приходятся на верхнюю точку окружности ментального круга, а, во-вторых, что отсутствие сбоев, т.е. помехо-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

защищённость процесса цепного вербального тестирования весьма хороша. Естественно предполагать, что эти ценные свойства совмещаются у ментально здорового человека.

Расшифровку этого теста можно представить в предельно сжатом виде в виде ментального кода

ninoninoniporiporiporiporiponinoninoporipo,

однако для удобочитаемости все экспериментально полученные ментальные коды, описывающие последовательности переключений настроения, прерываются пробелом в момент пересечения верхней точки ментального круга. В такой форме этот код принимает вид серии фрагментов: **nino nino nipo ripo ripo ripo nino nino ripo.**

На основе существующего сейчас компьютерного анализа тональности слов (в данном случае посредством метода VADER) накоплена следующая усредненная числовая оценка эмоционального содержания слов в этом тесте (рисунк 3). Вычисления были выполнены посредством приведенной ниже программы для численных оценок эмоционального содержания ассоциаций в тестах. Аналогичное представление уже не на одном тесте, а на множестве тестов (см. на рисунке 4). Для этого использован 35-дневный фрагмент серии ментальных кодов, извлечённый из многомесячной серии тестов одного волонтера (см. таблицу 2).

В примере таблицы 2 вполне достаточно информации для накопления удовлетворительных численных оценок по всем секторам ментально-

го круга (см. рисунок 4).

На четвертой (IV) и пятой (V) неделях однократного ежедневного тестирования у волонтера была выявлена правильная волнообразная форма кривой настроения. К рисунку добавлена также волна, полученная в результате усреднения по этим двум неделям.

На шестой неделе (VI) правильное волнообразное изменение настроения заметно нарушилось. Отчасти это стало следствием оскудения тестов в результате воздействия стандартного психоактивного препарата (волонтеру в начале VI недели в соответствующем медицинском учреждении был сделан плановый укол этого ПВА – галоперидола деканоата).

На седьмой (VII) и восьмой (VIII) неделях тестирования восстановилась правильная волнообразная форма кривой настроения. К этой части рисунка добавлена также волна, полученная в результате усреднения по этим двум неделям.

По вертикали представлена тональная оценка настроения, достигающая при предельно плохих ассоциациях значения -1 и при предельно хороших значения $+1$.

На рисунке 4 хорошо выражены ожидаемые экстремумы настроения в третьем и в шестом секторах. Изменение настроения в пятом-восьмом секторах ментограммы, искажившие правильную форму волны на VI неделе тестирования, можно попытаться связать с изменением состояния, вызванным введением препарата. Волны рисунка 4 накоплены по 35 тестам, коды которых представлены в таблице 2. Вычисления

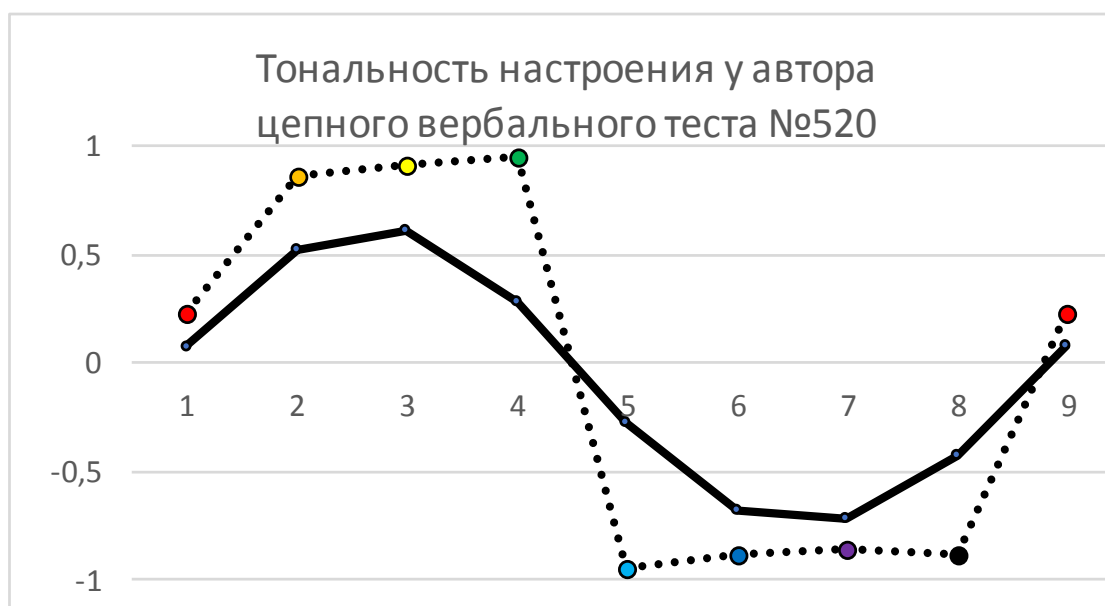


Рис. 3. Графическое представление тональности настроения в тесте №520 в различных секторах ментального круга у автора ментального кода **nino nino nipo ripo ripo ripo ripo nino nino ripo.** Сплошная линия – результат сглаживания экспериментальной зависимости

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Таблица 2

Пятинедельный фрагмент тестирования, выполненного большим волонтером в свободное время ежедневно с 18 декабря 2010 года по 28 апреля 2011 года. Жирным шрифтом выделены коды завершенных 8-строчных участков ментального процесса (см. рисунок 2). Они были востребованы для построения рисунков 4 и 5

Номер недели	Дата опыта	Код ментограммы
IV	08.01.2010	pi po pi--
	09.01.2010	--ni po pi no+++
	10.01.2010	pi po++ pi po+
	11.01.2010	--pino pi no pi
	12.01.2010	pi po pi no
	13.01.2010	pi no
	14.01.2010	pi po -pi no
V	15.01.2010	pi no pi no --
	16.01.2010	+++ ni no pi po ni po -
	17.01.2010	ni po - -pi no -- --ni po -
	18.01.2010	-po ni+
	19.01.2010	+ pi po ni no
	20.01.2010	+++ pi no+++++
	21.01.2010	+po pi po pi++
VI	22.01.2011	pi po ni no --
	23.01.2011	pi po pi po
	24.01.2011	pi po pi
	25.01.2011	po pi no ni no --
	26.01.2011	+ni no --
	27.01.2011	po po po po
	28.01.2011	no no no no
VII	29.01.2011	pi no+
	30.01.2011	+ ni po ni no
	31.01.2011	-ni po pi no ni+
	01.02.2011	ni po ni no -
	02.02.2011	-ni po pi no ni po
	03.02.2011	po ni po pi no++
	04.02.2011	++ ni no+++
VIII	05.02.2011	-pi no ni po -
	06.02.2011	-pi no ni po -
	07.02.2011	ni po pi no -
	08.02.2011	-no ni no ni
	09.02.2011	++++ pi po++++
	10.02.2011	+ ni po ni po
	11.02.2011	ni no pi po+

выполнены посредством программы на языке python, использующей метод VADER, итогом каждого вычисления мы выбрали обобщающее число с характеристикой «compound».

```
import nltk
from nltk.sentiment.vader import SentimentIntensityAnalyzer
```

```
# Инициализируем анализатор тональности
sid = SentimentIntensityAnalyzer()
```

```
# Список слов для анализа
```

```
words = ["Cars, Rabbit, Plastic, Teddy Bear, Toy Soldiers"]
```

```
# Проходимся по каждому слову, оцениваем его тональность и выводим результат
```

```
for word in words:
    ss = sid.polarity_scores(word)
    print(f»{word}: {ss}»)
```

Поскольку база данных, на которую опирается метод VADER, создана на английском языке, возникшие в тестах серии слов и выражений сначала переводились на английский, и только

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

потом вычислялись оценки эмоциональности.

Так как результаты IV и V недель тестирования сильно напоминают результаты VII и VIII недель тестирования, по этой четвёрке недель было выполнено усреднение, и этот усреднённый результат был сравнен с итогом VI недели тестирования (см. рисунок 5), когда больной находился под действием недавно введенного психоактивного препарата.

Поскольку использование этого психоактивного препарата является в данном примере периодическим процессом с 35-суточным периодом, то улучшить статистику картины VI недели тестирования позволит учет результатов последующих фрагментов опыта – двух имеющихся в наличии более поздних полных аналогов VI не-

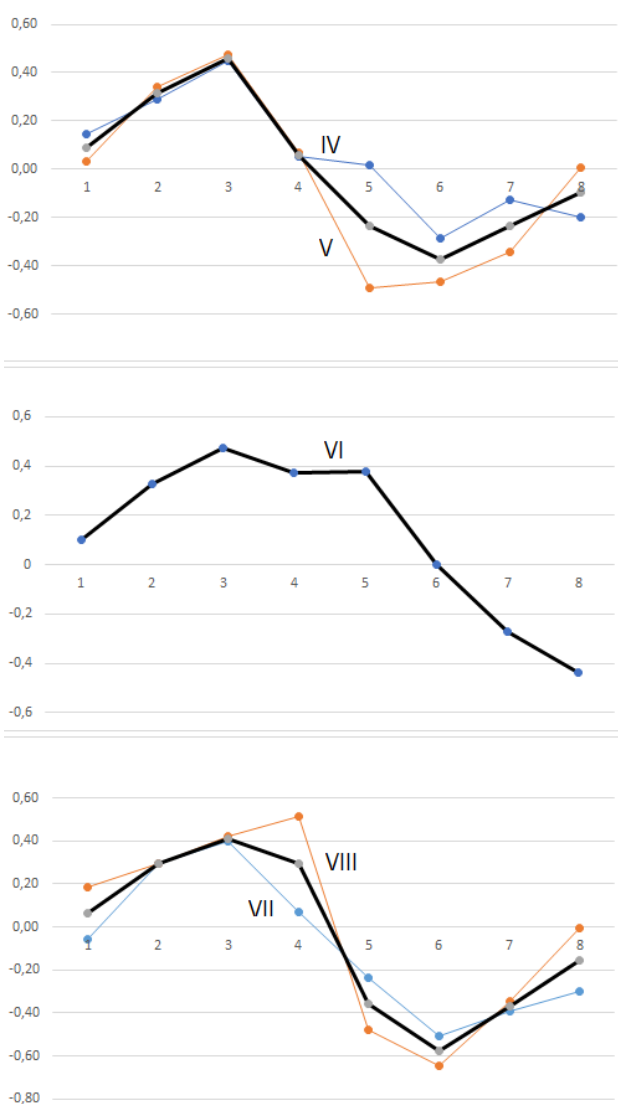


Рис. 4. Накопленные за неделю волны настроения вдоль восьмёрки секторов ментограммы. Таким образом, смещение фазы между соседними точками составляет 45 градусов дуги

дели (см. таблицы 3 и 4).

По мере улучшения статистики путем добавления аналогов VI недели был обнаружен стабильный, не зависящий от приёма лекарства минимальный уровень негативных эмоций в седьмом ментальном состоянии (рисунок 6). Он означает подавленное настроение, по-видимому, депрессию, слуховые феномены. В другие недели 5-недельного периода этого негативного явления нет.

По медицинским рекомендациям введение новых порций этого ПАВ положено через 2-4 недели, но волонтер регулярно затягивал этот интервал до 5 недель. Возможно, именно поэтому вместо ожидаемого «спокойного» минимума настроения в шестом секторе, после улучшения статистики VI недели минимум обнаружен уже в седьмом секторе.



Рис. 5. Сравнение результатов тестирования по VI, V, VII и VIII неделям, которые можно считать за контрольные, с результатами VI недели, когда больной подвергался влиянию новой порции психоактивного препарата. Оси как на рисунке 4

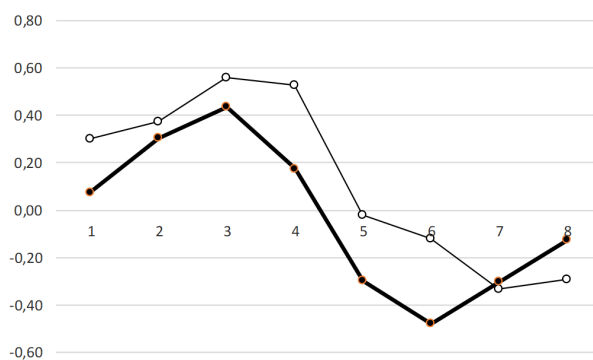


Рис. 6. Картина финальной модификации результата VI недели добавлением первого и второго аналогов этой недели (см. Таблицы 3 и 4), когда волонтер точно так же подвергался влиянию новых порций ПАВ. Для сравнения приведена нижняя кривая, построенная по остальным четырём неделям 5-недельного периода. Видны улучшения настроений в состояниях 1÷6. На состояние 7 галоперидол снова (ср. с рис.5) не повлиял. Оси как на рисунке 4

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Таблица 3

VIa – недельный фрагмент тестирования, первый аналог VI недели опыта

26.02.2011	no pipo++
27.02.2011	po nino pipo--
28.02.2011	po pi-
01.03.2011	pipo pipo--
02.03.2011	+po pipo--
03.03.2011	-nipo
04.03.2011	pipo

Таблица 4

VIb – недельный фрагмент тестирования, второй аналог VI недели опыта

02.04.2011	nipo+++
03.04.2011	pipo
04.04.2011	+nipo
05.04.2011	no pino+
06.04.2011	+pipo
07.04.2011	+pipo+
08.04.2011	+nino++

Выводы

Из приведенных примеров следует важный прикладной момент: можно сказать, что нами не только представлен новый способ описания мышления, но и опробован новый способ (практически, предложен экспресс-метод) исследования влияния на мышление человека самых различных препаратов из соответствующего медицинского арсенала.

Наше исследование важного частного случая психоактивных веществ – галоперидола деканоата – в очередной раз подтвердило высокую эффективность этого лекарства как средства, нормализующего процесс мышления. Об этом свидетельствует высокосимметричная форма кривой, накопленной по IV, V, VII и VIII неделям тестирования (см. рисунок 5).

Как должно быть ясно из материала статьи, для выполнения дальнейших исследований в этой области нужны заинтересованные лица, способные подобно нашему волонтеру дисциплинированно и, главное, безбоязненно выполнять ежедневное однократное тестирование в течение многих месяцев.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.

Соблюдение этических стандартов

Настоящая работа не содержит описания каких-либо исследований с использованием жи-

вотных в качестве объектов. Работа основывается на использовании материалов тестирования процесса мышления различных людей, но все эти материалы предложены, во-первых, добровольно и, во-вторых, инкогнито, то есть права на авторство не могут быть заявлены и доказаны. Этические стандарты соблюдены.

Литература

- Коломбет В.А., Лесных В.Н., Елистратов А.В.. Психодиагностика как биофизический метод // Известия Института инженерной физики, 2023. №4 (65). С.2-5.
- Коломбет В.А., Лесных В.Н., Коломбет В.В. Представление структуры естественного интеллекта в биофизическом психоанализе // Известия Института инженерной физики, 2024. №1(71). С.13-17.
- Corbetta M., Shulman G. L. Control of goal-directed and stimulus-driven attention in the brain // Nature Reviews Neuroscience, 2002. V. 3. P. 201-215.
- Vossel S., Geng J.J., Fink G.R. Dorsal and Ventral Attention Systems: Distinct Neural Circuits but Collaborative Roles // The Neuroscientist, 2013. V.20. Iss. 2. P.150-159.
- Коломбет В.А., Панчелюга В.А., Лесных В.Н. Самовоспроизводящиеся автоматы во вселенной: жизнь, универсальная система утраивающихся периодов, фундаментальные взаимодействия // Известия Института инженерной физики, 2022. №2(64). С.2-4.
- Коломбет В.А. Ментальные миры // Сознание и физическая реальность, 1997. Т. 2. №4. С. 15-24.
- Коломбет В.А. Трансфизические миры. В кн.: В.А. Коломбет. Трансфизические миры. Происхождение имен. М.: КРОН-ПРЕСС, 2001. С. 8-525.
- Коломбет В.А. «Синдром Стендаля» в свете гипнографии // Прикладная психология и психоанализ, 2003. №2. С. 11-27.
- Коломбет В.А. ВММ – вычислительная машина мозга // Вестник Калужского университета, 2006. №2. С. 21-29.
- Коломбет В.А. Введение в гипнографический психоанализ. М.: ООО Мэйлер, 2008. 240 с.
- Коломбет В.А., Лесных В.Н., Елистратов А.В., Тараненко А.М.. Базовый ментальный сценарий и его использование при оценке качества работы операторов сложных систем / XLI Всероссийская НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем». Филиал ВА РВСН (г. Серпухов), 2022. С. 63-67.
- Коломбет В.В. Сайт golosaVgolove.ru в сети Интернет.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.898

ЦЕЛЕВЫЕ ФУНКЦИИ МАРШРУТОВ НА ЭЙЛЕРОВЫХ И ГАМИЛЬТОНОВЫХ ГРАФАХ OBJECTIVE FUNCTIONS OF ROUTES ON EULERIAN AND HAMILTONIAN GRAPHS

Алексей Данилович Дараган

доктор технических наук
профессор кафедры
филиал ВА РВСН им. Петра Великого
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: +7 (4967) 72-19-11

Антон Алексеевич Ефремов

кандидат технических наук
заместитель начальника кафедры
филиал ВА РВСН им. Петра Великого

Егор Геннадьевич Клементьев

адъюнкт кафедры
филиал ВА РВСН им. Петра Великого

Эдуард Михайлович Руденко

кандидат технических наук
доцент кафедры математики
филиал ВА РВСН им. Петра Великого
Тел.: +7 (916) 851-80-55
E-mail: eduard5529@yandex.ru

Елена Викторовна Семикина

преподаватель кафедры информатики
филиал ВА РВСН им. Петра Великого
E-mail: labinfo_serp@inbox.ru
Тел.: +7 (915) 064-50-74

Аннотация

В статье рассматривается применение генетического алгоритма для поиска маршрутов на графе реперных точек на местности для нужд маршрутизации беспилотных летательных аппаратов. Реперы, как вершины, соединенные ребрами, образуют математические графы. Особое внимание заслуживают эйлеровы и гамильтоновы графы, на которых существует большое многообразие замкнутых маршрутов, проходящих один раз через каждое ребро или каждую вершину. Математическая задача поиска маршрутов на эйлеровых или гамильтоновых графах решается с помощью минимизации неотрицательной целевой функции от целочисленных переменных, меняющихся во множестве номеров вершин графа. Минимизация целевой функции проводится генетическим алгоритмом. Целевая функция строится на основе теорем о единственном представлении математических величин в виде суммы или произведения полиномиальных выражений, равных целым степеням различных оснований, которые используются для кодирования ребер эйлерова или вершин гамильтонова графа. Маршрутами являются аргументы целевой функции, которые обращают ее в нуль. В статье приводятся различные примеры целевых функций для решения задачи маршрутизации: целочисленные, рациональные, комплексные, трансцендентные, многочленные, векторные, матричные и другие типы, в основе построения которых лежит теорема об однозначном разложении.

Ключевые слова: беспилотный летательный аппарат, граф реперных точек на местности, математический граф эйлеров и гамильтонов, целевая функция, генетический алгоритм.

Summary

The article discusses the application of a genetic algorithm to find routes on a graph of reference points on the ground for the routing needs of unmanned aerial vehicles. Reference points, like vertices connected by edges, form mathematical graphs. Special attention should be paid to Eulerian and Hamiltonian graphs, on which there is a large variety of closed routes passing once through each edge or each vertex. The mathematical problem of finding routes on Eulerian or Hamiltonian graphs is solved by minimizing the non-negative objective function of integer variables varying in the set of vertex numbers of the graph. The minimization of the objective function is carried out by a genetic algorithm. The objective function is based on theorems about the only representation of mathematical quantities in the form of a sum or product of polynomial expressions equal to integer powers of various bases, which are used to encode the edges of an Eulerian or vertices of a Hamiltonian graph. The routes are the arguments of the target function, which turn it to zero. The article provides various examples of objective functions for solving the routing problem: integer, rational, complex, transcendental, polynomial, vector, matrix and other types, the construction of which is based on the theorem of unambiguous decomposition.

Keywords: unmanned aerial vehicle, graph of reference points on the ground, mathematical graph of Eulers and Hamiltons, objective function, genetic algorithm.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Организация патрулирования группой беспилотных летательных аппаратов (БПЛА) на контролируемой зоне с целью сбора информации на подстилающей сцене в формализованном виде сводится к определению маршрута или нескольких маршрутов на графе реперов на местности. Расчет маршрутов приводит к задаче маршрутизации на эквивалентном математическом графе [1]. Задачу поиска маршрутов на графе можно решить с помощью минимизации целевой функции (ЦФ) графа. В данной работе для минимизации ЦФ применяется генетический алгоритм (ГА) [2], который использует эволюционные механизмы отбора, скрещивания, мутации на особях или хромосомах, представляющих собой совокупность генов. В задаче поиска маршрута на графе генетическим алгоритмом в качестве генов рассматриваются номера вершин, а в качестве хромосом – наборы вершин графа, которые и являются одним из возможных решений задачи маршрутизации. Применение ГА позволяет находить различные типы маршрутов на графах: замкнутые, разомкнутые, маршруты для группового полета БПЛА. Существенную роль при этом сыграли теоретические исследования в построении целевых функций для оптимизационных задач на графах. В качестве примеров рассмотрим нахождение маршрутов на эйлеровых и гамильтоновых графах.

ЦФ на графах позволила связать алгебраическую и трансцендентную форму представления чисел в виде суммы или произведения уникальных кодов ребер или вершин, в которые они однозначно раскладываются. Построение ЦФ на основе теорем об однозначном разложении в сумму или произведение различных математических величин: чисел, многочленов, отношения многочленов, функций было положено в основу структуры ЦФ.

Целевая функция маршрута на графе должна обладать свойством: принимать нулевые значения только на наборах номеров вершин графа, являющимися маршрутами. Оптимизационная задача на эйлеровых или гамильтоновых графах (ЭГ или ГГ) по нахождению замкнутых маршрутов состоит не в том, чтобы подсчитать минимальное число ребер или вершин, а в том, чтобы найти сами множества маршрутов, т. е. найти если не все различные, то, по крайней мере, наибольшее их количество. Это позволяет сделать применение ГА в цикле по изменению значения фактора кроссовера, влияющего на формирование хромосом-наборов генов для построения из них маршрутов.

Так как ГА работает с хромосомами из номеров вершин

$$(v_1, \dots, v_p, v_{i+1}, \dots, v_n),$$

то для применения теорем об однозначном разложении в сумму:

$$s_1 + s_2 + \dots + s_{\#E} = A \quad (1)$$

или произведение

$$m_1 \cdot m_2 \cdot \dots \cdot m_{\#V} = M \quad (2)$$

применяется подпрограмма отображения каждого ребра e_i , как пары вершин, $e_i = (v_p, v_{i+1})$ в числа s_i или m_i для ЭГ или номера каждой вершины v_i в s_i или m_i в ГГ.

Числа s_i и m_i , как элементы однозначного разложения в сумму величины A или в произведение M , несут индивидуальную информацию о ребрах или вершинах графа и являются уникальными кодами в графе. Числа A и M являются аддитивным и мультипликативным кодом графа. Индексы $\#E$ и $\#V$ в разложениях (1) и (2) равны числу ребер и вершин в графе.

ЦФ ЭМ $m = (v_1, v_2, \dots, v_{\#E}, v_1)$ на графе, в аддитивной и мультипликативной форме имеют вид [3]:

$$Z_E(m) = \sum_{i=1}^{\#E} \text{cod}_E(v_i, v_{i+1}) - A_E = 0; \quad (3)$$

$$Z_E(m) = \prod_{i=1}^{\#E} \text{cod}_E(v_i, v_{i+1}) - M_E = 0, \quad (4)$$

где $\text{cod}_E(v_p, v_{i+1}) = s_i$ или m_i – аддитивный или мультипликативный коды ребра.

ЦФ ГМ $n = (v_1, v_2, \dots, v_{\#V}, v_1)$, имеют вид в аддитивной форме

$$Z_V(n) = \sum_{i=1}^{\#V+1} \text{cod}_V(v_i) - A_V = 0; \quad (5)$$

$$Z_E(n) = \sum_{i=1}^{\#V} \text{addweight}_E(v_i, v_{i+1}) - A_E = 0$$

и в мультипликативной форме:

$$Z_V(n) = \prod_{i=1}^{\#V+1} \text{cod}_V(v_i) - M_V = 0; \quad (6)$$

$$Z_E(n) = \prod_{i=1}^{\#V} \text{multweight}_E(v_i, v_{i+1}) - M_E = 0$$

где вторые соотношения $Z_E(n)$ в формулах (5) и (6) контролируют прохождение ГМ $n = (v_1, v_2, \dots, v_{\#V}, v_1)$, содержащего $\#V$ различных вершин, по ребрам графа. Веса ребер в формуле (5) являются тривиальными, т.е. равны между собой:

$$\text{addweight}_E(e_i) = \text{addweight}_E(v_p, v_{i+1}) = a, A_E = \#V \cdot a.$$

В формуле (6) аналогично имеем тривиальные веса:

$$\text{multweight}_E(e_i) = \text{multweight}_E(v_p, v_{i+1}) = a, M_E = a^{\#V}.$$

Природа чисел s_i или m_i и форма их представления влияет на тип ЦФ и решаемой оптимизационной задачи ГА. Если числа вещественные, то оптимизация проходит в рамках общей задачи математического программирования. Если числа целые, то оптимизационная задача решается как задача целочисленного программирования.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

В работе [4] рассматривался теоретико-числовой подход для построения ЦФ для ЭГ и ГГ.

Теоретико-числовые ЦФ строятся на основе основной теоремы арифметики об однозначном представлении целого, дробного рационального числа в виде произведения целых степеней различных простых чисел.

Рассмотрим множество типов ЦФ для простейшего графа $v4e6$ с кратной диагональю (рис. 1).

1. Поставим каждому ребру графа (рис. 1) числовой код. Например, ребру (1,2) поставим в соответствие значение кода, равное простому числу 2, (2,3)→3, (3, 4)→5, (4,1)→11, а ребру (2,4)→5.

В таком случае целая мультипликативная ЦФ ЭМ с кодами из простых чисел для графа $v4e6$ примет следующий вид

$$Z(x_1, x_2, \dots, x_{\#E+1}) = \text{abs} \left(\prod_{i=1}^6 (f(x_i, x_{i+1})) - 2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \right). \quad (7)$$

Цифра 5 стоит во 2-ой степени, так как, это ребро (2,4) в графе $v4e6$, имеет кратность 2. Следует отметить, что в качестве кодов ребер графа могут быть любые взаимно простые целые числа без общих множителей.

2. ЦФ ЭМ можно представить в дробной мультипликативной форме. Дробная ЦФ имеет следующий вид:

$$Z(x_1, x_2, \dots, x_{\#E+1}) = \text{abs} \left(\prod_{i=1}^6 (f(x_i, x_{i-1}) - 2^{-1} \cdot 3 \cdot 5^{-1} \cdot 7^2 \cdot 11^{-1}) \right). \quad (8)$$

3. Закодировать ребра графа $v4e6$ также можно следующим образом: ребра (1,2)→3⁰, (2,3)→3¹, (3,4)→3³, (4,1)→3¹, (2,4)→3². В таком случае, аддитивная 3-ическая ЦФ примет вид:

$$Z(x_1, x_2, \dots, x_{\#E+1}) = \text{abs} \left(\sum_{i=1}^6 (f(x_i, x_{i-1})) - 3^0 - 3^1 - 2 \cdot 3^2 - 3^3 - 3^4 \right). \quad (9)$$

Так как ребро (2,4) – кратные, то s -ическая ЦФ должна иметь основание $s > 2$.

Значение множителя 2 перед степенью 3², означает что ребро (2,4) является двойным.

Метод построения теоретико-числовых ЦФ базируется на использовании в качестве кодов ребер однозначное разложение чисел в произведение или сумму из теории чисел.

Подобными свойствами однозначного разложения обладают не только натуральные, целые, рациональные числа, но и многочленные функции от нескольких переменных x_1, x_2, \dots, x_n и

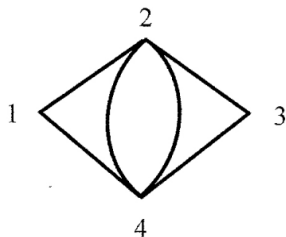


Рис. 1. Граф $v4e6$

их отношения.

Многочлены однозначно представляются в виде суммы одночленов, в виде произведения неприводимых сомножителей, а отношение многочленов также однозначно раскладывается в сумму элементарных дробей и в произведение несократимых и неприводимых множителей.

Использование ГА для минимизации ЦФ накладывает ограничение на форму представления информации только в числовом формате. Поэтому для применения основной теоремы алгебры об однозначном разложении многочленов и дробных многочленных функций в сумму или произведение и для кодирования ребер в виде чисел роль переменных x_1, x_2, \dots, x_k должны выполнять алгебраически независимые трансцендентные числа, то есть x_1, x_2, \dots, x_k , не быть корнями никакого многочлена с рациональными коэффициентами [5]. Выбор различных трансцендентных чисел $x=n$, $x=e$, $x=\sin x$, $x=\log_m k$ при $k \neq m^s$ или значений других трансцендентных функций могут быть использованы для подсчета маршрутов наравне с теоретико-числовыми ЦФ.

4. Если закодировать каждое ребро графа $v4e6$ следующим образом: ребро (1,2)→ $(x-\zeta_1)$, (2,3)→ $(x-\zeta_2)$, (2,4)→ $(x-\zeta_3)$, (3,4)→ $(x-\zeta_4)$, (4,1)→ $(x-\zeta_5)$, где ζ – некоторое алгебраическое число, то есть число, которое является корнем некоторого многочлена с рациональными коэффициентами, а x – трансцендентное число, то в таком случае, мультипликативная ЦФ ЭМ, состоящая из произведения несократимых и неприводимых множителей примет вид:

$$Z(x_1, x_2, \dots, x_{\#E}) = \text{abs} \left(\prod_{i=1}^6 f(x_i, x_{i-1}) - (x-\zeta_1)(x-\zeta_2)(x-\zeta_3)^2(x-\zeta_4)(x-\zeta_5) \right). \quad (10)$$

5. Если, закодировать каждое ребро графа элементарной дробью, например, (1,2)→ $a_1/(x-\zeta_1)$, (2,3)→ $a_2/(x-\zeta_2)$, (2,4)→ $a_3/(x-\zeta_3)$, (3,4)→ $a_4/(x-\zeta_4)$, (4,1)→ $a_5/(x-\zeta_5)$, где ζ_i – различные алгебраические числа, x – трансцендентное число, например, $x=n$. Тогда аддитивная трансцендентная ЦФ ЭМ может быть записана в виде суммы элементарных дробей:

$$Z(x_1, x_2, \dots, x_N) = \text{abs} \left(\sum_{i=1}^6 f(x_i, x_{i-1}) - \frac{a_1}{x-\zeta_1} - \frac{a_2}{x-\zeta_2} - \frac{2a_3}{x-\zeta_3} - \frac{a_4}{x-\zeta_4} - \frac{a_5}{x-\zeta_5} \right). \quad (11)$$

Также можно рассмотреть еще два типа множеств, которые могут быть использованы для кодирования ребер графа.

6. На примере графа $v4e6$ (рис. 1) рассмотрим случай, когда ребра кодируются элементами векторного пространства, которые по сложению являются моноидами с однозначным

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

разложением векторов по базису единичных векторов: $(1,2) \rightarrow (1,0,0,0,0)$, $(2,3) \rightarrow (0,1,0,0,0)$, $(2,4) \rightarrow (0,0,0,1,0)$, $(3,4) \rightarrow (0,0,1,0,0)$, $(4,1) \rightarrow (0,0,0,0,1)$, в таком случае, аддитивная форма записи векторной ЦФ ЭМ имеет вид:

$$Z(x_1, x_2, \dots, x_N) = abs(\sum_{i=1}^6 (f(x_i, x_{i-1}) - (1, 1, 2, 1, 1)) \quad (12)$$

7. Можно рассмотреть пример бесконечномерного пространства функций с базисом $\{\sin x, \sin 2x, \dots, \sin ix, \dots\}$, который представляет собой множество по сложению. Кодировка ребер графа $v4e6$ в таком случае выглядит следующим образом: $(1,2) \rightarrow \sin x$, $(2,3) \rightarrow \sin 2x$, $(2,4) \rightarrow \sin 3x$, $(3,4) \rightarrow \sin 4x$, $(4,1) \rightarrow \sin 5x$. Аддитивная форма трансцендентной ЦФ в виде отрезка ряда Фурье, примет следующий вид [6]:

$$Z(x_1, x_2, \dots, x_N) = abs(\sum_{i=1}^6 (f(x_i, x_{i-1}) - \sum_{i=1}^5 \sin ix - \sin 3x). \quad (13)$$

8. При фенотипе хромосом в виде квадратных матриц, ребра графа (рисунки 1) могут быть закодированы матрицами: $(1,2) \rightarrow [s00; 000]$, $(2,3) \rightarrow [0s^20; 000]$, $(2,4) \rightarrow [00s^3; 00]$; $(3,4) \rightarrow [000; s^400]$, $(4,1) \rightarrow [000; 0s0]$. ЦФ ЭМ графа $v4e6$ строится на основе однозначного разложения в сумму матриц. В таком случае, аддитивная форма матричной ЦФ примет, следующий вид:

$$Z(x_1, x_2, \dots, x_N) = abs(\prod_{i=1}^6 (f(x_i, x_{i-1}) - [s^2 s^2 s^3; s^4 s^5 0]). \quad (14)$$

9. Следующий вариант кодировки ребер графа $v4e6$ заключается в использовании в качестве кодов комплексных чисел, которыми являются корни многочлена $x^5 - 2 = 0$:

$$\zeta_n = \sqrt[5]{2} \cdot (\cos \frac{2\pi n}{5} + i \cdot \sin \frac{2\pi n}{5}), \quad n = 1, \dots, 5. \quad (15)$$

Кодировка ребер графа $v4e6$ проводится следующим образом: первому ребру $(1,2)$ ставится в соответствие число $(\pi - \zeta_1)$, остальным ребрам $(2,3) \rightarrow (\pi - \zeta_2)$, $(2,4) \rightarrow (\pi - \zeta_3)$, $(3,4) \rightarrow (\pi - \zeta_4)$, $(4,1) \rightarrow (\pi - \zeta_5)$. В таком случае мультипликативная форма ЦФ ЭМ станет комплексной трансцендентной и примет следующий вид:

$$Z(x_1, x_2, \dots, x_{\#E}) = abs(\prod_{i=1}^6 f(x_i, x_{i-1}) - \prod_{i=1}^5 (z - \zeta_i)^{a_i}), \quad (16)$$

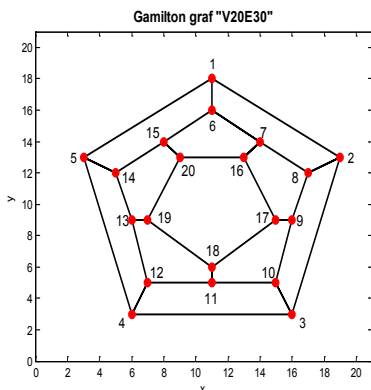


Рис. 2. Гамильтонов граф $v20e30$

где a_i – кратность ребра равна единице, кроме $a_3=2$; $z = \pi$ – трансцендентное число.

10. Аналогично, можно рассмотреть построение ЦФ для гамильтоновых графов. В качестве примера приведем поиск маршрутов на гамильтоновом графе $v20e30$ (рисунки 2).

Для поиска ГМ на графе Гамильтона $v20e30$ каждая вершина кодируется матрицей. Например, код для вершины 3 имеет вид:

$$s_3 = \begin{pmatrix} 0 & 0 & 2^9 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (17)$$

В свою очередь для вершины 19 код-матрица имеет следующий вид:

$$s_{19} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7^4 & 0 \end{pmatrix} \quad (18)$$

Аналогичным образом поступают и для остальных вершин.

Сумма кодов вершин ГГ $v20e30$ в таком случае, используя матричную запись согласно (5), имеет вид:

$$A_v = \begin{pmatrix} 2^3 & 2^4 & 2^5 & 2^9 & 2^{14} \\ 3^2 & 3^3 & 3^6 & 3^7 & 3^9 \\ 5 & 5^2 & 5^4 & 5^5 & 5^6 \\ 7 & 7^2 & 7^3 & 7^4 & 7^5 \end{pmatrix}. \quad (19)$$

ЦФ (5) будет представлять собой разницу сумм значений кодов вершин: $s_1, s_2, \dots, s_{\#V}$ ГМ и матрицы (19). В случае равенства двух составляющих данной разницы, делается вывод о том, что проверяемый маршрут является ГМ. Второе слагаемое ЦФ имеет вид (5) с тривиальными кодами.

В таблице 1 представлена часть найденных ГМ, которые представляют собой последовательность вершин.

Выводы

На основании исследований, проводимых в рамках ВНШ-303 (Системы искусственного интеллекта специального назначения), можно отметить:

- выбор типа целевой функции, влияет на время поиска маршрутов, например, для поиска маршрутов на графе $v7e12$, были разработаны программы поиска с использованием трансцендентной ЦФ и матричной. Результаты поиска показали, что время поиска 240 ЭМ в первом случае, практически в два раза превышает время поиска при использовании матричной ЦФ и составляет около 30 и 15 минут соответственно;
- при разработке программ поиска маршрутов для графов, размеры которых превышают

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

25 вершин, наблюдается нелинейный рост времени поиска (рисунк 3), а также снижение схожести процесса оптимизации.

Поэтому в рамках исследований ВНШ-303 необходимо совершенствование алгоритмов поиска маршрутов на графах большой размерности по снижению времени счета. Применительно к использованию группы БПЛА такой подход позволит в случае изменения условий патрулирования рассчитывать маршруты движения и планировать полет группы непосредственно на борту.

Литература

1. Дараган А.Д. Системы искусственного интеллекта. Монография / А.Д. Дараган, Э.М. Руденко, В.С. Залогин, А.А. Ефремов, А.С. Андреев, М.А. Финогенов, В.В. Чуринов. Серпухов: ФВА РВСН им. Петра Великого, 2020. 205 с.

2. Гладков Л.А. Генетические алгоритмы / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик; под ред. В.М. Курейчика. 2-е изд., испр и доп. М.: Физматлит, 2006. 320 с.

3. Дараган А. Д. Словарь-справочник. Искусственный интеллект в терминах и определениях / А.Д. Дараган, А.А. Ефремов, Е.В. Забегалин, В.С. Залогин, Э.М. Руденко, Е.В. Семикина, М.А. Финогенов. Серпухов: ФВА РВСН им. Петра Великого, 2023. 151 с.

4. Руденко Э.М., Семикина Е.В. Маршрутизация беспилотных летательных аппаратов, трансцендентные целевые функции графа и генетический алгоритм // Научные технологии в космических исследованиях Земли, 2021. Т.13. №1. С.4-14.

5. Гельфонд А.О. Трансцендентные и алгебраические числа. М.: URSS, 2019. 224 с.

6. Jacobson N. Basic algebra 1 (2nd ed.), Dover-2009.

Таблица 1
Гамильтоновы маршруты графа v20e30

№	Маршрут
1	1 6 7 8 9 17 16 20 15 14 5 4 12 13 19 18 11 10 3 2 1
2	1 6 7 16 17 18 11 12 13 19 20 15 14 5 4 3 10 9 8 2 1
3	1 5 14 15 20 19 13 12 4 3 2 8 9 10 11 18 17 16 7 6 1
4	1 5 14 15 20 19 13 12 4 3 2 8 9 10 11 18 17 16 7 6 1
5	1 5 4 12 11 18 19 13 14 15 20 16 17 9 10 3 2 8 7 6 1
6	1 6 15 20 19 18 11 10 9 17 16 7 8 2 3 4 12 13 14 5 1
7	1 5 14 13 19 18 17 9 10 11 12 4 3 2 8 7 16 20 15 6 1
8	1 2 8 7 6 15 14 13 12 11 18 19 20 16 17 9 10 3 4 5 1
9	1 5 14 13 19 20 15 6 7 16 17 18 11 12 4 3 10 9 8 2 1
10	1 2 3 10 9 8 7 16 17 18 11 12 4 5 14 13 19 20 15 6 1

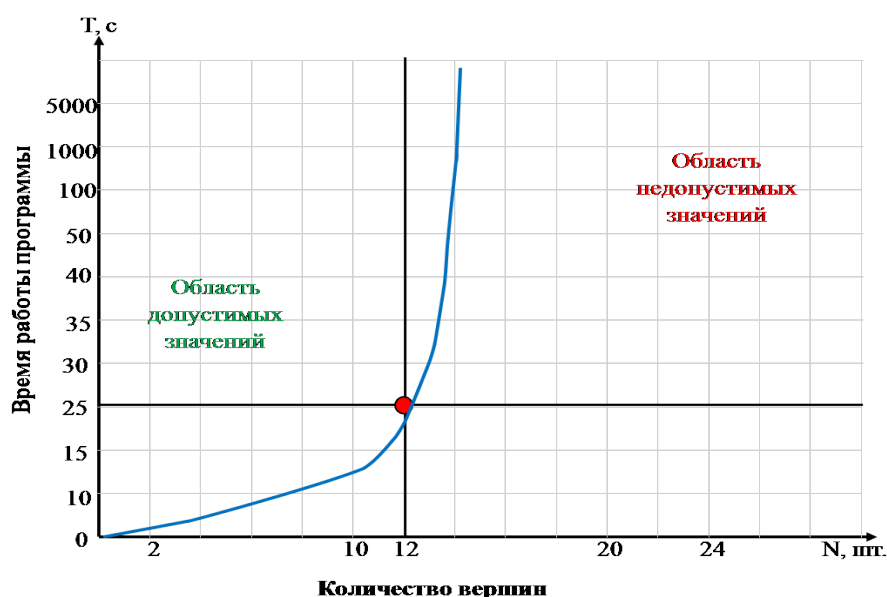


Рис. 3. График зависимости времени поиска от количества вершин

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056.55

ЭФФЕКТИВНОСТЬ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ AES И ЭЛЛИПТИЧЕСКИХ КРИВЫХ: ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА EFFICIENCY OF IMAGE ENCRYPTION USING AES AND ELLIPTIC CURVES: EXPERIMENTAL EVALUATION

Басель Абуд

аспирант кафедры МТС
Московский технический университет
связи и информатики (МТУСИ)
Адрес: 111024, Москва, ул. Авиамоторная, д. 8А
Тел: +7 (495) 957-77-31
E-mail: baselabood@Hotmail.com

Владимир Васильевич Гончаров

доктор технических наук, профессор
профессор кафедры МТС
МТУСИ
Адрес: 111024, Москва, ул. Авиамоторная, д. 8А
Тел: +7 (495) 957-77-31
E-mail: v_v_goncharov@mail.ru

Аннотация

Исследование направлено на разработку эффективной системы шифрования изображений, объединяющей алгоритмы Advanced Encryption Standard (AES) (расширенный стандарт шифрования) и Elliptical Encryption (ECC) (эллиптическое шифрование). В работе используется комплексный метод, включающий анализ различных режимов шифрования AES (ECB, CTR, CBC, CFB, OFB) в сочетании с ECC. Эксперименты проводились для сравнения качества изображения, устойчивости к статистическим атакам и эффективности вычислений. Определены оптимальные варианты шифрования для различных сценариев их использования, обеспечивая при этом высокую устойчивость к атакам при сохранении качества изображения. Результаты могут быть использованы в областях, требующих конфиденциальности и целостности визуальных данных, таких как медицинская диагностика, информационные системы и др.

Ключевые слова: шифрование изображений, анализ корреляции соседних пикселей (APCA), эллиптическая кривая Диффи-Хеллмана, Advanced Encryption Standard (AES), HKDF (HMAC-based Extract-and-Expand Key Derivation Function), режимы шифрования.

Summary

The study is aimed at developing an efficient image encryption system that combines Advanced Encryption Standard (AES) and Elliptical Encryption (ECC) algorithms. The research employs a comprehensive approach, including the analysis of various AES encryption modes (ECB, CTR, CBC, CFB, OFB) in conjunction with ECC. Experiments are conducted to compare image quality, resistance to statistical attacks, and computational efficiency. The study identifies optimal encryption methods for different usage scenarios, ensuring high resilience to attacks while preserving image quality. The findings can be applied in areas requiring confidentiality and integrity of visual data, such as medical diagnostics and information systems.

Keywords: Image encryption, Analysis of Pixel Correlation (APCA), Elliptic Curve Diffie-Hellman, Advanced Encryption Standard (AES), HKDF (HMAC-based Extract-and-Expand Key Derivation Function), encryption modes.

Введение

Шифрование данных, особенно изображений, имеет ключевое значение в обеспечении конфиденциальности передаваемых данных. Advanced Encryption Standard (AES) является широко используемым методом, однако его комбинация с эллиптической криптографией (ECC), существенно повышает их безопасность. В работе исследуется возможность совместного применения AES и ECC для защиты изображений с оценкой производительности и безопасности алгоритма. Режимы шифрования AES представлены с учетом их сочетания с ECC, даны их досто-

инства и недостатки. Исследование направлено на улучшение безопасности и эффективности шифрования изображений.

Краткий обзор исследований по шифрованию изображений с использованием AES и ECC

В статье [7] представлена гибридная система шифрования AES-ECC, где вначале генерируются пары ключей ECC, затем секретный ключ AES шифруется и передается с использованием ECC. Недостатком системы является использование асимметричного ECC для всего блока данных, что требует дополнительного времени

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

и неэффективно по энергопотреблению. В свою очередь в [8] предлагается шифрование на основе эллиптической кривой, эффективной в ограниченных интервалах, требующей больших вычислительных ресурсов.

В [9] рассматривается асимметричный ЕСС для каждого пикселя изображения с использованием генетического алгоритма, что требует значительных ресурсов. Последовательный метод гибридной криптосистемы ЕСС-AES, рассматриваемой в [10] для цветных изображений, замедляет обработку данных. Требует значительных ресурсов ЕСС для шифрования изображений с помощью матриц [11]. Применяемый комбинированный подход ЕСС и шифра Хилла [12] обладает высокой безопасностью, но требует значительно большего времени на шифрование.

Предлагаемые криптографические алгоритмы.

Эллиптическая криптография (ЭК) обеспечивает безопасность данных, используя точки на эллиптических кривых для шифрования и подписи. Экономия вычислительных ресурсов достигается за счет ассоциативности операций

сложения точек на кривой. Математический аспект криптосистемы на основе ЭК определяется уравнением эллиптической кривой [1]:

$$y^2 = x^3 + ax + b \pmod{p} \quad (1)$$

где a и b – коэффициенты кривой;

p – простое число;

точки (x, y) удовлетворяют уравнению.

Шифрование и подпись выполняются через операции умножения точек на кривой и вычисления дискретного логарифма, что делает систему устойчивой к атакам методом перебора [2].

Протокол ECDH (эллиптическая кривая Диффи-Хеллмана) обеспечивает безопасный обмен ключами через ненадежный канал, используя эллиптическую криптографию. Он устанавливает общий ключ без его прямой передачи, что делает его широко применимым в различных приложениях (рисунк 1 [3]).

В качестве второго алгоритма используется симметричный алгоритм шифрования AES-256 [4]. На рисунке 2 показаны порядок шифрования и дешифрования в соответствии с алгоритмом AES-256. Режимы работы AES, такие как ECB,



Рис. 1. Структура протокола ECDH



Рис. 2. Порядок шифрования и дешифрования AES-256

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Таблица 1

Значения энтропии, рассчитанные для серых слоев разного цвета трех предложенных изображений

Режим	Энтропия								
	Изображение 1 (256 × 256)			Изображение 2 (512 × 512)			Изображение 3 (1024 × 1024)		
	красный	зеленый	синий	красный	зеленый	синий	красный	зеленый	синий
ECB	7.99727	7.99743	7.99713	7.99922	7.99920	7.99913	7.99978	7.99980	7.99978
CTR	7.99721	7.99719	7.99700	7.99937	7.99917	7.99916	7.99980	7.99979	7.99980
CBC	7.99715	7.99742	7.99725	7.99933	7.99926	7.99928	7.99981	7.99980	7.99982
CFB	7.99740	7.99707	7.99689	7.99928	7.99927	7.99919	7.99980	7.99978	7.99978
OFB	7.99744	7.99728	7.99727	7.99928	7.99913	7.99928	7.99980	7.99979	7.99978

CBC, CTR, CFB и OFB, представляют собой различные способы применения AES к блокам данных [5,6]. На рисунках 3 и 4 показаны алгоритмы AES для различных режимов.

Предлагаемый объединенный алгоритм шифрования

На рисунке 5 показан порядок шифрования и дешифрования с использованием разработанного алгоритма.

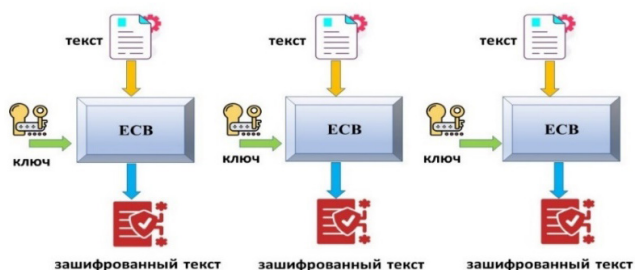


Рис. 3. Алгоритм шифрования AES-ECB

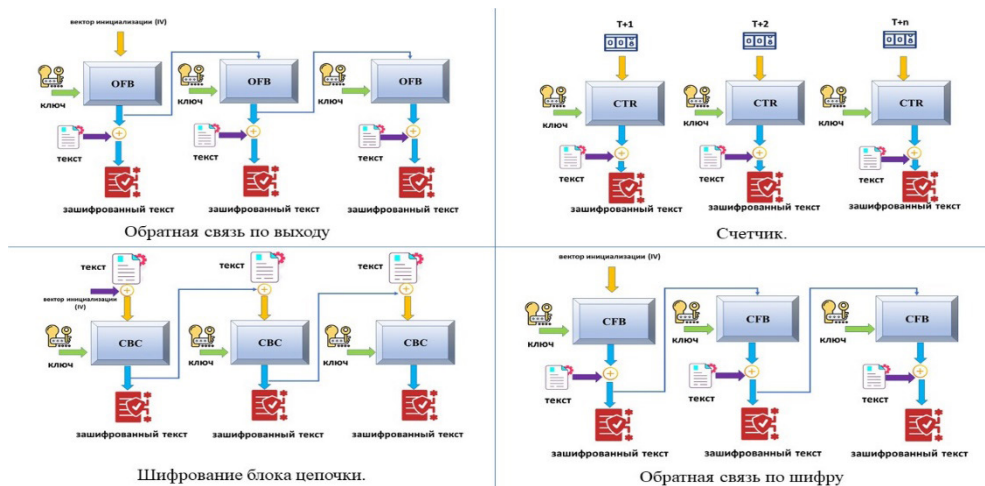


Рис. 4. Порядок шифрования AES в режимах, отличных от базового

Реализация предложенного алгоритма и результаты эксперимента

Предлагаемый алгоритм реализован с использованием языка Python через код Visual Studio на компьютере с Windows 11, процессором Intel core i7 и 8 ГБ ОЗУ. В качестве входных данных для кода используются 3 изображения PNG разных размеров, а именно: изображение 1 (256×256), изображение 2 (512×512) и изображение 3 (1024×1024). Размер основного блока установлен на 16 и предполагая, что значение $IV=b \times 00$ для моделей CBC–CFB–OFB. Также генерируются случайные ключи ECC (рисунк 6).

В криптографии и алгоритмах шифрования понятная серость может использоваться для оценки качества зашифрованных данных. Если зашифрованное изображение имеет хорошую понятную серость, это может свидетельствовать о том, что данные зашифрованы без потери информации и что оригинальное изображение может быть восстановлено с высокой степенью

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

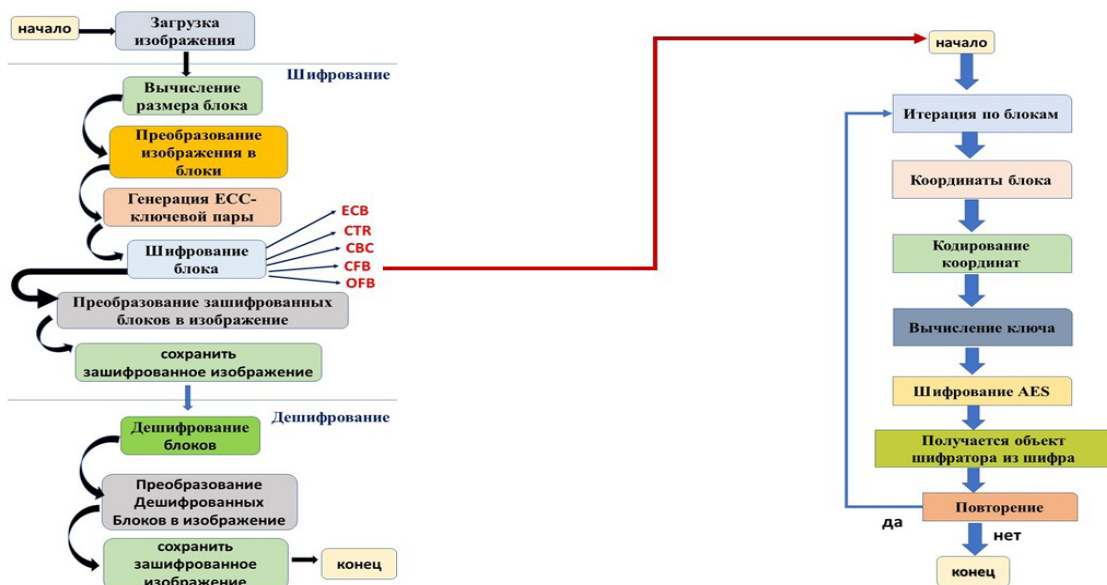
точности после расшифровки. Результаты расчета энтропии трех секретных изображений в пяти режимах шифрования представлены в *таблице 1*. В таблице показано, что значения энтропии (по К. Шеннону) многих зашифрованных изображений близки к 8. Это означает, что система обеспечивает высокий уровень случайности и непредсказуемости в зашифрованных данных, что делает их безопасными и защищенными от несанкционированного доступа.

В *таблице 2* представлены результаты шифрования предложенных изображений в каждой модели алгоритма AES, анализ гистограммы секретного изображения и зашифрованного изображения, а также среднего значения времени шифрования и дешифрования.

Из анализа результатов видно, что модель AES-CTR требует минимально возможного времени для шифрования и дешифрования, и это делает его лучшей моделью, если скорость является главным приоритетом. Необходимо отметить, что хищение информации об изображении

после ее шифрования невозможно, т.к. распределение RGB до кодирования принимает вид кривой разных значений, либо после кодирования принимает почти равную кривую для всех значений RGB.

Распределение значений пикселей изображений и корреляции соседних пикселей до и после шифрования с использованием пяти моделей AES представлены в *таблице 3*. Анализ результатов показал, что все модели, используемые для шифрования, удовлетворяют требованиям, так как плотность пикселей распределяется равномерно, а это затрудняет для неавторизованного пользователя выделение областей с максимальной и минимальной информацией для зашифрованных изображений. Вместе с тем результаты в таблице демонстрируют, что все модели подходят для кодирования с точки зрения корреляции соседних пикселей. Высокие значения корреляции указывают на сильную связь между соседними пикселями, что означает наличие повторяющихся узоров или структур на изображе-



Предлагаемый алгоритм шифрования и дешифрования изображений ECC-AES

процесс шифрования блока

Рис. 5. Предлагаемый алгоритм шифрования и дешифрования изображений ECC-AES с блоками шифрования

```

-----BEGIN PUBLIC KEY--
MFkwEWHKQZlzeCAQYIKOZlzeDAQCDQgAEo
3ZT/VZOVQ1HOMWOMKRsr7DMOC+2
VQlwt8fpNk+6CpBMfs26NwkqjRVjz9qdkggBFw
==nw3p51NW7La1RqPwh11y
-----END PUBLIC KEY-----
    
```

```

-----BEGIN PRIVATE KEY-
49AgEGCCqGSM49MIGHAgEAMBMGBuqGSM
Qyt1U3ZczlouZge6AwEHBGowawlBAQQg
hRANCAAT2KV707UN8CRFhR47u7EE3k2dXI8
jpp0anFfkRLgMg8blsnXXv4KgWNYs
yTXH3on4rkulfa4Gnhu83Ktiu8De+eonq1ZGLY
hTYYB0Aeqy2tgRYHuV
-----END PRIVATE KEY--
    
```

Открытый ключ ECC


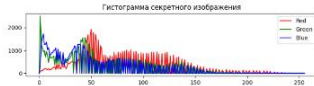

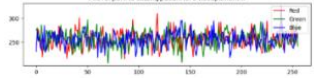

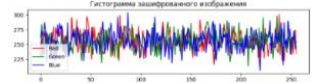

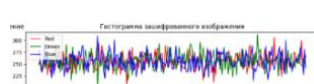

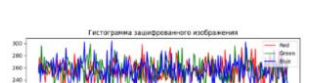



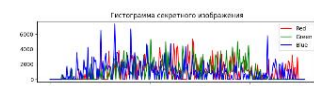
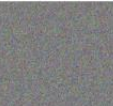
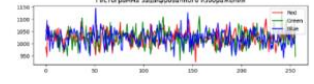

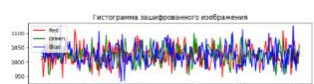
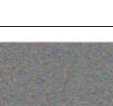
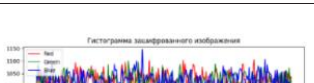
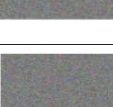



Закрытый ключ ECC

Рис. 6. Открытый и закрытый ключ ECC

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Таблица 2

Результаты шифрования на предложенных изображениях в каждом алгоритме AES

Предлагаемые изображения	Гистограмма секретного изображения	Зашифрованные изображения	Гистограмма зашифрованного изображения	Среднее время шифрования и дешифрования
Изображение 1 (256 × 256) 		Электронная кодовая книга. (ECB) 		0.367 секунды
		Счетчик. (CTR) 		0.2725 секунды
		Шифрование блока цепочки. (CBC) 		0.3195 секунды
		Обратная связь по шифру. (CFB) 		0.3275 секунды
		Обратная связь по выходу. (OFB) 		0.32 секунды
Изображение 2 (512 × 512) 		Электронная кодовая книга. (ECB) 		0.6905 секунды
		Счетчик. (CTR) 		0.623 секунды
		Шифрование блока цепочки. (CBC) 		0.767 секунды
		Обратная связь по шифру. (CFB) 		0.771 секунды
		Обратная связь по выходу. (OFB) 		0.7885 секунды

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ


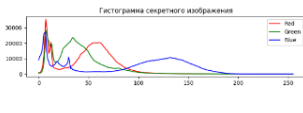

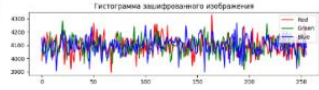

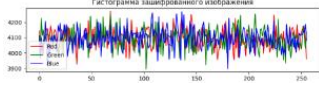

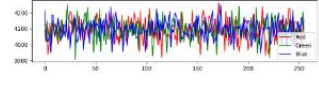

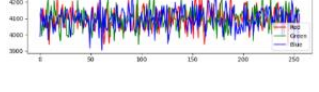
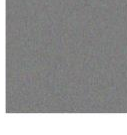
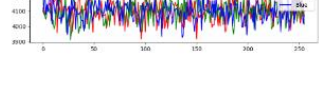

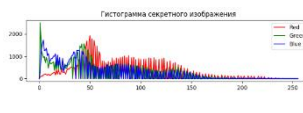

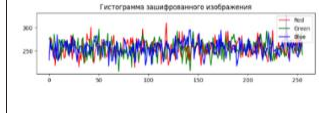

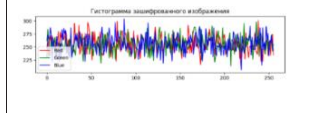

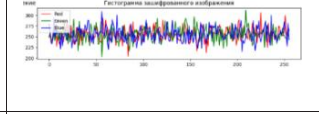

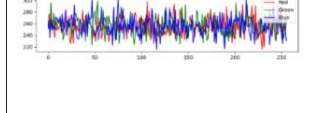
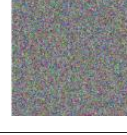
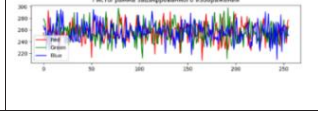
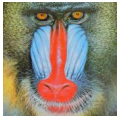
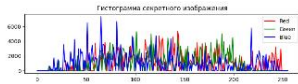

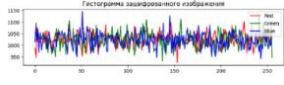

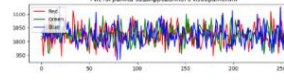

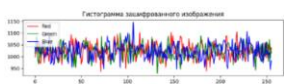

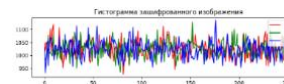

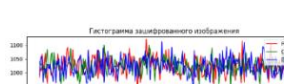

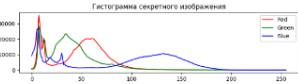

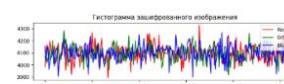

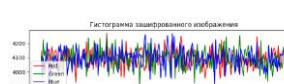

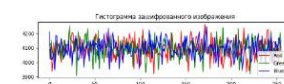



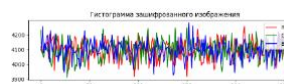
<p>Изображение 3 (1024 × 1024)</p> 		<p>Электронная кодовая книга. (ECB)</p> 		2.7605 секунды
		<p>Счетчик. (CTR)</p> 		2.675 секунды
		<p>Шифрование блока цепочки. (CBC)</p> 		3.155 секунды
		<p>Обратная связь по шифру. (CFB)</p> 		3.414 секунды
		<p>Обратная связь по выходу. (OFB)</p> 		3.16035 секунды

Таблица 3
Распределение пикселей по соответствующим изображениям

Предлагаемые изображения	Гистограмма секретного изображения	Зашифрованные изображения	Гистограмма зашифрованного изображения	Среднее время шифрования и дешифрования
<p>Изображение 1 (256 × 256)</p> 		<p>Электронная кодовая книга. (ECB)</p> 		0.367 секунды
		<p>Счетчик. (CTR)</p> 		0.2725 секунды
		<p>Шифрование блока цепочки. (CBC)</p> 		0.3195 секунды
		<p>Обратная связь по шифру. (CFB)</p> 		0.3275 секунды
		<p>Обратная связь по выходу. (OFB)</p> 		0.32 секунды

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

<p>Изображение 2 (512 × 512)</p> 		<p>Электронная кодовая книга. (ECB)</p> 		0.6905 секунды
		<p>Счетчик. (CTR)</p> 		0.623 секунды
		<p>Шифрование блока цепочки. (CBC)</p> 		0.767 секунды
		<p>Обратная связь по шифру. (CFB)</p> 		0.771 секунды
		<p>Обратная связь по выходу. (OFB)</p> 		0.7885 секунды
<p>Изображение 3 (1024 × 1024)</p> 		<p>Электронная кодовая книга. (ECB)</p> 		2.7605 секунды
		<p>Счетчик. (CTR)</p> 		2.675 секунды
		<p>Шифрование блока цепочки. (CBC)</p> 		3.155 секунды
		<p>Обратная связь по шифру. (CFB)</p> 		3.414 секунды
		<p>Обратная связь по выходу. (OFB)</p> 		3.16035 секунды

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

нии. С другой стороны, более низкие значения корреляции указывают на более случайное распределение значений пикселей, что является менее предсказуемым и более сложным изображением, как показывают результаты предыдущей таблицы. В *таблице 4* представлены параметры метрик оценки для шифрования изображений, рассчитанные между тремя секретными изображениями и теми же изображениями после их шифрования с помощью пяти этапов работы алгоритма AES. Результаты анализа таблицы показали, что для изображения размером (256×256) лучшими по значениям параметров оказались AES-CBC, AES-ECB и AES-CFB, в то время как остальные модели демонстрировали худшие результаты. Для изображения размером (512×512) наилучшими оказались AES-CTR, AES-CFB и AES-ECB, в то время как другие показали менее эффективные результаты. В случае изображения размером (1024×1024) – лидерами оказались AES-CFB, AES-CTR и AES-ECB, превосходя другие модели по значению соответствующих параметров, в то время как остальные модели демонстрировали более низкую производительность.

Анализируя среднее время шифрования и дешифрования, значения энтропии и предыдущие параметры метрик качества изображения для каждой модели, баллы будут распределены на основе этого анализа, при этом баллы распределяются в порядке от лучшего к худшему по трем изображениям для каждой модели, а затем баллы суммируются, чтобы показать общую сумму.

Заметим, что алгоритм AES-CFB, набравший 12 баллов, аналогичен AES-CTR, но немного превосходит его. Однако следует отметить, что с увеличением размера изображения увеличивается средняя скорость кодирования и декодирования, что может быть отрицательным фактором при оценке алгоритма с точки зрения скорости работы. В то время как AES-CBC и AES-ECB получили схожие оценки – 10 и 8 соответственно. Его можно эффективно использовать для обработки изображений небольшого размера, где указанные выше значения параметров показывают хорошие результаты. Однако по мере увеличения размера изображения оно становится менее эффективным как с точки зрения значений параметров, так и с точки зрения корреляции соседних пикселей и гистограмм. Хотя средняя скорость кодирования и декодирования хорошая, но она становится бесполезной при слабых значениях параметров. Алгоритм AES-OFB, набравший всего два балла, оказался худшим по всем параметрам.

Заключение

В работе проведен анализ гибридного алгоритма, объединяющего AES и эллиптическую кривую, на основе оценки пяти режимов AES для оптимального шифрования изображений по выбранным значениям показателей. Метрики включали гистограммы, взаимосвязь пикселей и энтропию зашифрованных изображений. Времена кодирования и декодирования рассчитаны и усреднены для каждого режима. Режимы CTR

Таблица 4
Оценка результатов шифрования и дешифрования изображений

Изображение	между секретным изображением и зашифрованным изображением					между секретным изображением и зашифрованным изображением					между секретным изображением и зашифрованным изображением				
	ECB	CTR	CBC	CFB	OFB	ECB	CTR	CBC	CFB	OFB	ECB	CTR	CBC	CFB	OFB
MSE	12160.30	12118.59	12161.18	12136.39	12129.18	8596.89	8601.22	8561.53	8584.54	8577.09	12169.29	12178.32	12154.27	12178.88	12152.01
PSNR	7.281	7.296	7.281	7.289	7.292	8.787	8.785	8.805	8.793	8.797	7.278	7.274	7.283	7.274	7.284
SSIM	0.0064, 0.0098	(0.0078, 0.01127)	(0.0074, 0.0114)	(0.0057, 0.0092)	(0.0062, 0.0099)	(0.0085, 0.0091)	(0.0075, 0.0082)	(0.0093, 0.0099)	(0.0087, 0.0094)	(0.0089, 0.0097)	(0.0067, 0.0106)	(0.0065, 0.0104)	(0.0063, 0.0102)	(0.0063, 0.0102)	(0.0064, 0.0104)
Корреляция	0.0011	0.0022	0.0046	-0.0013	0.0035	0.0000102	-0.0014	0.0020	-0.00097	0.00118	0.000974	-0.0011	0.000373	-0.000780	0.000909
MAE	127.658	127.537	127.356	127.393	127.314	127.592	127.449	127.5529	127.494	127.593	127.497	127.542	127.497	127.544	127.444
SC	207466	207160	207177	206889	206889	830303	828872	830281	828830	830151	332265	331907	332029	331974	331781
AD	127.358	127.445	127.733	127.626	127.626	127.407	127.589	127.426	127.492	127.415	127.499	127.459	127.511	127.458	127.543
MD	255	255	255	255	255	255	255	255	255	255	255	255	255	255	255

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

и СFB оказались наилучшими для изображений, но СВС и ЕСВ показали приемлемые результаты, особенно для небольших по объему изображений.

Литература

1. Рацеев С. М. Математические методы защиты информации: Учеб. пособ. для вузов. М.: Лань, 2023. С.392-394.
2. ГОСТ Р 34.10-2001. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
3. Черепнёв М.А., Грачева С.С. Решение задачи Диффи Хеллманна некоторых эллиптических кривых, удовлетворяющих ГОСТ34.10-2001 // Информационные технологии, 2020. Т.26. №3. С.159-168.
4. Архипова И.С. Криптографический алгоритм AES как средство защиты информации // Аллея науки, 2018. Т.6. № 4. С.83-87.
5. Спиричева Н.Р. Алгоритмы блочной криптографии. Екатеринбург: Изд-во Урал. ун-та, 2013. 78 с.
6. Лось А.Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: Учебник для вузов. М.: Юрайт, 2021. С.206-215.
7. Ganesh A R, Manikandan P N, Sethu SP, Sundararajan R, Pargunarajan K (2011) An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks. International conference on recent trends in information technology (ICRTIT). Chennai, Tamil Nadu. 1209-1214. <https://doi.org/10.1109/ICRTIT.2011.5972351>.
8. Anwar M.N.B., Hasan M., Hasan M.M., Loren J.Z., Hossain, S.T. Comparative Study of Cryptography Algorithms and Its' Applications. Int. J. Comput. Netw. Commun. Secur, 2019. 7, 96-103.
9. Shankar K., Eswaran P (2016) An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. Artificial intelligence and evolutionary computations in engineering systems. Adv intell syst comput, vol 394, pp 705-714. Springer, New Delhi. https://doi.org/10.1007/978-81-322-2656-7_64.
10. Toughi S, Fathi MH, Sekhavat YA (2017) An image encryption scheme based on elliptic curve Pseudo random and advanced encryption system. Signal Process 141:217-227. <https://doi.org/10.1016/j.sigpro.2017.06.010>.
11. Visu P., Sivakumar N., Kumaresan P., Babu S.Y., Ramesh P.S. Removing leaf petioles and auto locating apex base points using straight-line interpolation and bisection. Multimedia Tools Appl. 2020, 79, 5355-5369.
12. Dawahdeh Z.E., Yaakob S.N., Bin Othman R.R. A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. J. King Saud Univ. Comput. Inf. Sci. 2018, 30, 349-355. [CrossRef]

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 539.182

УНИТАРНЫЕ СИММЕТРИИ В ПАРТОННОЙ ДИНАМИКЕ ПРОТОНА UNITARY SYMMETRIES IN PARTON DYNAMICS OF THE PROTON

Сергей Владимирович Смуров
почетный работник науки и техники РФ
доктор технических наук, профессор
Первый Вице-президент Института –
Главный конструктор
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл.,
г. Серпухов, Большой Ударный пер., д. 1а
Тел.: +7 (4967) 35-31-93
E-mail: Svs_iif@mail.ru

Геннадий Германович Волков
доктор физико-математических наук,
профессор
старший научный сотрудник
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл.,
г. Серпухов, Большой Ударный пер., д. 1а
Тел.: +7 (4967) 35-31-93
E-mail: gennadii.volkov@rambler.ru



Аннотация

В данной статье мы обсуждаем возникновение и роль унитарных симметрий, как стандартных, связанных с инвариантностью квадратичных форм, так и расширенных, которые обуславливают инвариантность кубических форм, которые могут возникать в трех – частичной динамике партоннов.

Ключевые слова: квантовая хромодинамика, симметрии, алгебры, партон, протон, кварки, глюон, циклические комплексные числа, унитарность, многообразия, квантовая запутанность.

Summary

In this article we discuss the emergence and role of unitary symmetries, both standard ones associated with the invariance of quadratic forms, and extended ones that determine the invariance of cubic forms that can arise in three-partial parton dynamics.

Keywords: quantum chromodynamics, symmetries, algebras, parton, proton, quarks, gluon, cyclic complex numbers, unitarity, manifolds, quantum entanglement.

1. Эволюция ядерного щита в кварк-глюонную плазму

Теоретическая ядерная наука стремится понять и предсказать структуру, динамику и происхождение видимой материи во Вселенной. Вопросы, находящиеся на переднем крае теоретической ядерной науки, включают: Как кварки и глюоны удерживаются внутри протонов и нейтронов и необходим ли учет тройного взаимодействия 3-х кварков? Какие симметрии определяют внутренние свойства и динамику кварков и глюонов? Какова структура самих кварков? Как протоны и нейтроны связываются, образуя ядра, и каковы пределы стабильности, например в тяжелых ядрах типа уран-235 или плутоний 239? Как мы можем точно предсказать сложные ядерные реакции? Почему коллективное поведение возникает в квантовых системах многих тел? Как и где во Вселенной образовались химические элементы? Каковы фазы ядерной материи в экстремальных условиях?

В то время как в единой электрослабой теории с внутренней калибровочной группой

$SU(2)_C \times U(1)_Y$, спонтанной нарушенной в вакууме до $U(1)_{EM}$ симметрии, в которой переносчиками взаимодействия между заряженными кварками и лептонами являются нейтральные безмассовые фотоны и массивные векторные бозоны W_μ^\pm, Z_μ^0 , в квантовой хромодинамике (КХД) в рамках калибровочной группы $SU(3)_C$ взаимодействие между кварками, несущими цветовой заряд, обеспечивается обмена 8-ю безмассовыми глюонами G_μ^a , $a=1, \dots, 8$, несущими также цветовой заряд. Как следствие КХД на базе локальной калибровочной группы $SU(3)_C$, внутренняя структура нуклонов представляет собой сложную динамическую систему валентных кварков, погруженную в квантовое море виртуальных кварков, анти-кварков и глюонов, систему, не похожую ни на одну другую, наблюдавшуюся до сих пор в природе [1-3]. Дополнительная сложность этой системы заключается в необходимости учитывать еще спиновые степени свободы, кварк-глюонные орбитальные движения и две глобальные симметрии: $SU(2)_I$ -изотопическую и $SU(3)_H$ -«горизонтальную» сим-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

метрии [4-6], которые соответственно учитывают изотопические спины u - и d - кварков $I=1/2$ и нарушенную симметрию трех кварковых поколений $\{(ud),(c,s),(t,b)\}$.

В результате оказалось, что пространственно-временной спин протона $S=1/2$ не является простой суммой спинов валентных кварков, но включает еще и значительные вклады квантового моря партонов [3]. Масса нуклона также не является суммой составляющих только валентных кварков (которая близка к нулю), а нужно учитывать взаимодействия кварков, кварк-антикварк- и глюонного морей. Сравнивая массу нуклона (протон/нейтрон) с массами изотопического триплета пи-мезонов, которые включают два валентных кварка

$$\pi^+ \{u\bar{d}\}, \pi^0 \{1/\sqrt{2}(u\bar{u} - d\bar{d})\}, \pi^- \{d\bar{u}\},$$

возникает вопрос о необходимости учета возможности дополнительного гипотетического взаимодействия составляющих нуклон, например, 3-х частичных взаимодействий кварков [4-6].

Решение таких вопросов, связанных с динамикой кварк-глюонной структуры протона и нейтрона, которая приводит к конфайнменту цвета, предсказывает значения их спина и массы и дает универсальный механизм нуклон-нуклонных и ядерных взаимодействий – центральная цель ядерной науки.

Взаимодействия между кварками приводят к малоисследованной области материи, в которой глюоны доминируют в волновой функции ядра. Были замечены намеки на этот домен в ядерных столкновениях на RHIC и LHC, где ядра сталкиваются почти со скоростью света! Подобные результаты также были получены в ходе электрон-протонного рассеяния в экспериментах HERA [2-3]. КХД предсказывает, что при очень высоких плотностях и температурах, например, в ранней Вселенной сразу после Большого взрыва, сильно взаимодействующая материя превращается в кварк-глюонную плазму.

Соответствующие сильные цветовые поля лежат в основе многих плохо изученных новых явлений в КХД, такие как удержание цвета внутри нуклона, свойства кварк-глюонной плазмы и происхождения спина нуклона.

Быстро растущей областью исследований в ядерной физике является применение квантовой информатики, поскольку многие серьезные проблемы в области ЯФ требуют передовых и потенциально квантовых методов и технологий моделирования и зондирования. В частности, моделирование в исследованиях холодной и горячей КХД доказало свою эффективность в качестве основного подхода, основанного на первых принципах. Квантовое моделирование

фундаментально отличается от классического моделирования тем, что существует многомерное Гильбертово пространство квантовой системы многих тел, которое может быть более компактно закодировано в квантовые единицы, какими могут быть двумерные спиновые состояния кубиты и спины более высоких измерений, кудиты. Кроме того, вычисления можно распараллелить более эффективно, используя принципы суперпозиции и запутанности в квантовой физике.

В динамической кварк-глюонной структуре протона и нейтрона участвуют внутренние унитарные симметрии электромагнитного заряда $U(1_{EM})$, обуславливающая дробные заряды кварков, изотопическая $SU(2)$ -симметрия, связывающая u - и d - кварки в изотопический дублет, море кварк-анти-кварков различных флейворов проявляет нарушенную симметрию поколений $SU(3)_H$, динамика кварк-глюонных взаимодействий содержится в локальной калибровочной $SU(3^c)$ -симметрии. Спины кварков и глюонов соответствуют представлениям группы $SU(2)_l$ подгруппы $SL(2,C) \approx SU(2) \times SU(2)$, дважды накрывающей группу Лоренца $SO(1,3)$. Все эти упомянутые группы симметрий мы относим к бинарно унитарным, связанных с инвариантностью квадратичных форм $\psi\psi^*$ и парным взаимодействием кварков с калибровочными полями $\psi^* \Gamma_\mu \psi A_\mu$ [1]. Тернарная унитарность обуславливается появлением в теории кубических инвариантных форм, которые в физических процессах могут быть связаны с трех-частичными взаимодействиями типа $\Gamma_{ijk} \psi_i^* \psi_j^* \psi_k B_\mu$ [1,5]. Возникновение этих форм и выше мы обсуждаем в данной статье.

2. От симметрий атома водорода к симметрии протона

Наличие у кварков новой степени свободы – цвета привело к развитию фундаментальной теории сильных взаимодействий в рамках квантовой хромодинамики (КХД) с локальной калибровочной $SU(3^c)$ -группы.

Достаточно ли этой симметрии для квантования $SU(2)_l$ -изотопического дублета – протона-нейтрона с довольно сложной кварк-глюонной структурой? Здесь вполне уместно напомнить, что $SU(3)$ -группа Ли является 8-мерным многообразием! До сих пор в исследовании окружающего пространства-времени физики экспериментально смогли достигнуть только 4-х измерений, например, в релятивистской механике (СТО) получено множество результатов и объяснений явлений при скоростях, близких к скорости света или в СМ электрослабых взаи-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

модействий, базирующейся на пространственно-временной группе Лоренца $SO(3,1)$ (группе Пуанкаре). Полезно вспомнить тернистый путь к квантованию атома водорода, нерелятивистской системы, состоящей из одного протона и электрона, движущегося в Кулоновском поле протона. Как оказалось, такая простая система дополнительно к вращательной $SO(3)$ -симметрии имеет другую «скрытую» $SO(3)$ симметрию Лапласа-Рунге-Ленца, расширяя тем самым полную симметрию атома водорода до группы $SO(3) \times SO(3) \approx SO(4)$. Многообразие состояний частицы теперь выглядит как $R^3 \times R^3$, где первое R^3 дает положение r частицы, а второе R^3 дает импульс p частицы. Векторное поле $A_k: R^3 \times R^3 \rightarrow R^3$ становится эрмитовым (самосопряженным) оператором:

$$\vec{A} = \frac{1}{m} \vec{p} \times \vec{L} - k \frac{\vec{r}}{r},$$

где $\vec{L} = \vec{r} \times \vec{p}$, где $\vec{r}, \vec{p}, \vec{L}$ соответственно обозначают эрмитовы операторы положения, импульса и углового момента. С учетом гамильтониана $H = p^2/2m_e$ можно получить следующие коммутационные соотношения [7]:

$$\begin{aligned} [H, L_i] &= 0, [H, A_i] = 0 \\ [L_i, L_j] &= i\epsilon_{ijk} L_k, [L_i, A_j] = i\epsilon_{ijk} A_k \\ [A_i, A_j] &= i\epsilon_{ijk} L_k (2/m_e) H, \end{aligned} \quad (1)$$

которые с точностью до константы образуют алгебру $su(2) \oplus su(2) \approx so(4)$, то есть $V = \text{Span}\{L_i, T_k | i, k=1,2,3\}$ образует 6-мерное векторное пространство линейных комбинаций операторов L_i и T_k над полем вещественных чисел R . Эта алгебра Ли, которая порождает группу $SO(4)$ вращений в R^4 . Дальнейшее расширение группы $SO(4)$ до группы $SO(4) \times SU(2)$ возникает в результате суммирования орбитального момента и спина электрона в полный момент $J = L + S$. Набор наблюдаемых задается операторами H, L^2, J^2, J_z с собственными значениями $E, l(l+1), j(j+1), m$, соответственно [7]. Поэтому у нас есть основания некой «скрытой симметрии» атома водорода, которая будет выглядеть, как вращение в R^4 . Возникает вопрос, а почему бы в протон-нейтроне, кроме локальной калибровочной $SU(3^c)$ -симметрии, не могла бы возникнуть скрытая симметрия, которая помогла помочь решить все или часть проблем, упомянутых в начале статьи.

Структура $SU(3)$ представляет собой унитарную группу с восемью параметрами и, следовательно, имеет восемь независимых генераторов, которые являются бесследовыми и эрмитовыми 3×3 матрицами и, таким образом, может быть представлена в следующем виде:

$$T = \begin{pmatrix} \alpha & a^* & b^* \\ a & \beta & c^* \\ b & c & -\alpha - \beta \end{pmatrix} \quad (2)$$

Возможным набором генераторов являются 3×3 матрицы $T_a = \lambda_a/2$, $\text{Tr}(T_a) = 0$, $T_a^+ = T_a$ ($a=1, \dots, 8$), образующие алгебру $su(3)$, которые строятся из генераторов $I_k = 1/2 \sigma_k$ алгебры $su(2)$, 2×2 -матриц Паули σ_k ($k=1,2,3$), следующим образом:

$$\lambda_{1,2,3} = \begin{pmatrix} 0 & & \\ \sigma_{1,2,3} & & \\ 0 & & 0 \end{pmatrix}, \lambda_{4,5} = \begin{pmatrix} 0 & 0 & 1, -i \\ 0 & 0 & 0 \\ 1, i & 0 & 0 \end{pmatrix}, \lambda_{6,7} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & \sigma_{1,2} & \\ 0 & & 0 \end{pmatrix}, \lambda_8 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad (3)$$

$$\lambda_8 = 1/\sqrt{3}(\text{diag}(1, -1, 0) + 2(0, 1, -1)).$$

Представим произвольную бесследовую эрмитову $H = H^+$ 3×3 -матрицу в виде линейной комбинации 8-ми генераторов:

$$H(x_1, \dots, x_8) = \sum_{k=1, \dots, 8} x_k T_k, \{x_k\}, x_k \in R. \quad (4)$$

Тогда ее экспонента:

$$U(x_1, \dots, x_8) = e^{iH(x_1, \dots, x_8)}, \quad (5)$$

удовлетворяет условию унитарности: $UU^+ = 1_{3 \times 3}$. Связь детерминанта унитарной матрицы U со следом эрмитовой матрицы H ($\text{Tr} H = 0 \rightarrow \det U = 1$) следует из следующих соотношений:

$$\det e^{iH} = \det(U e^{iH} U^{-1}) = \det(e^{iH U^{-1} U}) = \det e^{iD};$$

$$D = \begin{pmatrix} \lambda_1 & & \\ & \dots & \\ & & \lambda_n \end{pmatrix}, \text{Tr} D = \sum_{k=1, \dots, n} \lambda_k = \text{Tr} H. \quad (6)$$

Добавив в разложение (4) элемент $x_0 \lambda_0$, λ_0 — единичная 3×3 матрица, H' (x_0, x_1, \dots, x_8) можно представить в виде эрмитовой матрицы:

$$H'(x_0, x_1, \dots, x_8) = \begin{pmatrix} x_0 + x_3 + 1/\sqrt{3}x_8 & x_1 + ix_2 & x_4 + ix_5 \\ x_1 - ix_2 & x_0 - x_3 + 1/\sqrt{3}x_8 & x_6 + ix_7 \\ x_4 - ix_5 & x_6 - ix_7 & x_0 - 1/\sqrt{3}x_8 \end{pmatrix}, \quad (7)$$

детерминант которой (для удобства $\sqrt{3}x_8 \rightarrow x_8' = x_8$) определяет кубическую поверхность $\det H' = F(x_0, \dots, x_8)$ в 9-мерном евклидовом пространстве R^9 :

$$F(x_0, \dots, x_8) = (x_0 + x_3 + x_8)(x_0 - x_3 + x_8)(x_0 - 2x_8) + x_1(x_4 x_5 + x_3 x_7) + x_2(x_5 x_6 - x_4 x_7) - (x_0 + x_3 + x_8)(x_6^2 + x_7^2) - (x_0 - x_3 + x_8)(x_4^2 + x_5^2) - (x_0 - 2x_8)(x_1^2 + x_2^2) \quad (8)$$

Сделаем следующие замены переменных:

$$\begin{aligned} x_6 &= y_0 - 1/2(y_1 + y_2), x_7 = \sqrt{3}/2(y_1 - y_2), r = x_0 + x_3 + x_8 = y_0 + y_1 + y_2 \\ x_4 &= s_0 - 1/2(s_1 + s_2), x_5 = \sqrt{3}/2(s_1 - s_2), r = x_0 - x_3 + x_8 = s_0 + s_1 + s_2 \\ x_1 &= t_0 - 1/2(t_1 + t_2), x_2 = y_0 - 1/2(y_1 + y_2), r = x_0 - 2x_8 = t_0 + t_1 + t_2 \end{aligned} \quad (9)$$

уравнение (8) можно привести к следующему виду (сравни [4-6]):

$$F = -(y_0^3 + y_1^3 + y_2^3 - 3y_0 y_1 y_2) - (s_0^3 + s_1^3 + s_2^3 - 3s_0 s_1 s_2) - (t_0^3 + t_1^3 + t_2^3 - 3t_0 t_1 t_2) + 3y_0(t_0 s_0 + t_1 s_1 + t_2 s_2) + 3y_1(t_0 s_1 + t_1 s_2 + t_2 s_0) + 3y_2(t_0 s_2 + t_1 s_0 + t_2 s_1) \quad (10)$$

В поисках новых видов многомерных пространств с необычными топологическими структурами и алгебраическими свойствами и группами симметрий довольно естественным кажется обращение к исследованию C_n -циклических комплексных (абелевых) и гиперкомплексных (неабелевых) чисел с $n > 2$.

Согласно абелевой C_n -циклической группе комплексификации евклидовых пространств R^n , на примере ряда $n=3,4, \dots, (n-1)$ параметрических гиперповерхностей, мы пришли к расши-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

рению понятий «унитарности» и «ортогональности» [4-6].

Переход к неабелевым случаям осуществляется увеличением порядка циклической группы или ее расширением до произведения двух или более групп: $C_m \times C_p \times \dots \times C_n$. В отличие от бинарных кватернионов, генераторы циклических групп – $q_a(C_m)$ и $q_b(C_p)$ (эти группы вообще могут быть различными $m \neq p$) могут иметь между собой более сложные коммутационные соотношения, например, для тернарного случая

$m=p=3$: $q_1 q_2 = j^k q_2 q_1$; $j = \exp\{2\pi i/3\}$,
где значение $k = 1$ или 2 .

Генераторы тернарной $tsu(3)$ -алгебры строятся также из 3×3 -матриц $Q_m = (m=1, \dots, 8)$ с $\text{Tr} Q_m = 0$, $\det Q_m = 1$, удовлетворяющих свойствам тернарной симметрии и необычным коммутационным соотношениям [4-6]:

$$Q_k = q^k \begin{pmatrix} 0 & a_k & 0 \\ 0 & 0 & b_k \\ c_k & 0 & 0 \end{pmatrix}, Q_{k+3} = q^{2k} \begin{pmatrix} 0 & 0 & u_k \\ s_k & 0 & 0 \\ 0 & t_k & 0 \end{pmatrix}, Q_{7,8} = q^k \begin{pmatrix} 1 & 0 & 0 \\ 0 & j(j^2) & 0 \\ 0 & 0 & j^2(j) \end{pmatrix} \quad (11)$$

где $k=1, 2, 3$, $q^3 = q_0$, $q^* = jq$, $\det Q_k = 1$.

Соответствующие этой группе ($q_1 \in C_3$, $q_2 \in C_3$) единичные тернарные комплексные числа определяют групповое многообразие, определяемое тернарной группой $TSU(3)$, которое, как и в случае кватернионов, можно определить через детерминант тернарно-унитарной матрицы [1,4]:

$$U = \begin{pmatrix} z_0 & q_2 z_1 & q_2^2 z_2 \\ q_2^2 \tilde{z}_2 & \tilde{z}_0 & q_2 \tilde{z}_1 \\ q_2 \tilde{z}_1 & q_2^2 \tilde{z}_2 & \tilde{z}_0 \end{pmatrix}, \det U = F(x_0, \dots, x_8) = 1 \quad (12)$$

где $z_0 = x_0 q_0 + x_7 q_1 + x_8 q_1^2$, $z_1 = x_1 q_0 + x_2 q_1 + x_3 q_1^2$, $z_2 = x_4 q_0 + x_5 q_1 + x_6 q_1^2$,
значок «тильда» означает тернарное сопряжение $\tilde{q} = j^k q$, $k=1, 2$. Соответствующая кубическая гиперповерхность в R^9 приобретает следующий вид [4-6] (см. (10)):

$$\det U = (x_0^2 + x_7^3 + x_8^3 - 3x_7 x_7 x_8) + (x_1^3 + x_2^3 + x_3^3 - 3x_1 x_2 x_3) + (x_4^3 + x_5^3 + x_6^3 - 3x_4 x_5 x_6) - 3x_0(x_1 x_4 + x_2 x_5 + x_3 x_6) - 3x_7(x_1 x_5 + x_2 x_6 + x_3 x_4) - 3x_8(x_1 x_6 + x_2 x_4 + x_3 x_5), \quad (13)$$

Важным отличием от эрмитового кватернионного варианта $su(3)$ -алгебры является то, что тернарная $tsu(3)$ -алгебра естественно вытекает из теории C_3 -неабелевых комплексных чисел, как это произошло с открытием $SU(2)$ -группы и ее $su(2)$ -алгебры за счет расширения бинарных комплексных чисел до кватернионов. Исключительным фактом в нашем случае является расширение понятия антикоммутативности [1,4-6]

$$q_1 q_2 = j^k q_2 q_1, \quad q_2 q_1 = j^{n-k} q_1 q_2, \quad (14)$$

введение которого в квантовую теорию поля приводит к возможному новому типу спиновой материи: $P(\psi_1 \psi_2) = j \psi_2 \psi_1$, $P(\psi_2 \psi_1) = j^2 \psi_1 \psi_2$, $P(P(\psi_1 \psi_2)) = \psi_1 \psi_2$ [1,4-6].

3. Унитарность в бинарных алгебрах с делением

Исторически открытие Киллинг-Картан-Ли алгебр и соответствующих симметрий было тесно связано с четырьмя алгебрами с делением R, C, H, O , т.е. действительные числа, комплексные числа, кватернионы и октонионы соответственно. Например, хорошо известно, что комплексные числа $z = x + iy$ единичной нормы $|z| = 1$ отвечают многообразию абелевой группы

$$U(1) = S^1 = \{|z|^2 = x^2 + y^2 = 1\}.$$

Три мнимые единицы кватернионов участвуют в образовании алгебры $su(2)$, а добавлением единичного вещественного кватерниона образуют группу $SU(2) \approx S^3$. Наконец, октонионы относятся к исключительной $G(2)$ -алгебре.

Конечномерные ассоциативные алгебры с делением над действительными числами встречаются очень редко, их ровно три. Согласно известной теореме нормированных алгебр с делением только четыре – R, C, H, O : вещественные числа R , C – комплексные числа, H – кватернионы, O – октонионы. В связи с этими теоремами наш путь был основан на обобщении самих чисел, норма которых определялась через квадратичную форму $|Z|^2$. Указанные алгебры с делением, являющиеся нормированными векторными пространствами и допускающими анти-инволюцию (сопряжение) $(z^*)^* = z$, для которых норма определяется через квадратичную форму $|z|^2 = zz^*$, будем называть бинарными алгебрами с делением. Для таких алгебр норма произведения двух чисел равна произведению норм каждого числа, то есть в виде равенства $|z_1 \cdot z_2|^2 = |z_1|^2 |z_2|^2$, которое, например, для комплексных чисел $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$; $z = z_1 z_2 = x_0 + iy_0$ принимает следующее равенство:

$$(x_0^2 + y_0^2) = (x_1^2 + y_1^2) (x_2^2 + y_2^2).$$

Итак, R, C – коммутативные ассоциативные нормальные алгебры, H – некоммутативная ассоциативная алгебра, O – неассоциативная альтернативная алгебра. Алгебра альтернативна, если $z(zw) = z^2 w$ и $(zw)w = zw^2$ ($z(wz) = (zw)z$), которые имеют обратный и единичный элементы. Единственные альтернативные бинарные алгебры с делением – это R, C, H, O . Комплексные числа, кватернионы и октонионы могут быть представлены в общем виде:

$$q = x_0 e_0 + x_1 e_1 + \dots + x_p e_p, \quad x_k \in R, \quad (15)$$

где $e_0^* = e_0$ реальный единичный элемент, p – число «мнимых» базисных векторов, меняющих знак при сопряжении $e_p^* = -e_p$. Так $p=1$ комплексные числа C образуют двумерную алгебру с базисом $\{e_0, e_1 = i\}$, $C = R \oplus iR$; где $e_1 = i$ – мнимая единица, $i^2 = -e_0$. Кватернионы, содержащие три мнимых единиц,

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

$q = x_0 e_0 + x_1 e_1 + x_2 e_2 + x_3 e_3; q \in \mathbb{H}$ (16)
образуют 4-х мерную алгебру, $\{e_1=i, e_2=j, e_3=i-j=k;\}$ с операцией анти-инволюции $e_p^* = -e_p$, $p=1,2,3$. Кватернионы можно рассматривать, как пару комплексных чисел $H = C \oplus jC$. Важнейшим следствием для создания квантовой физики стал тот факт, что умножение любой пары из 3-х мнимых базисных элементов $\{e_1=i, e_2=-j, e_3=ij=k; e_i^2=-1\}$ анти-коммукативно, то есть:

$$ij = -ji = k, jk = -kj = i, ki = -ik = j. \quad (17)$$

Так реализация единичных мнимых кватернионов в 2x2-матрицах Паули:

$$e_1 = i\sigma_1 = i \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, e_2 = i\sigma_2 = i \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, e_3 = i\sigma_3 = i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (18)$$

оказалась тесно связана с алгеброй $su(2)$:

$$[T_k, T_l] = i\epsilon_{klm} T_m \quad (19)$$

где $T_p = 1/2\sigma_p$, $p=1,2,3$ – генераторы алгебры и ϵ_{klm} – полностью антисимметричный тензор.

Если благодаря делительному свойству умножения $|z_1 z_2| = |z_1| |z_2|$ комплексные числа $z = x_0 e_0 + x_1 e_1 = x_0 e_0 + x_1 i \in \mathbb{C}$ единичной нормы $|z|^2 = z z^* = x_0^2 + x_1^2 = 1$ образуют абелеву унитарную группу $z = e^{i\theta} \in \mathbb{S}^1 \approx U(1)$, то единичные кватернионы $q \in \mathbb{H}_1$, $|q|^2 = q^+ q = 1$, образуют унитарную неабелеву группу $SU(2)$:

$$q^+ q = x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1; \{x_0, x_1, x_2, x_3\} \in \mathbb{S}^3 \approx SU(2). \quad (20)$$

Для произведения пары кватернионов имеется основное соотношение

$$e_m e_p = -\delta_{mp} + \epsilon_{mp\ell} e_\ell$$

где δ_{mp} – тензор Кронекера и $\epsilon_{mp\ell}$ – абсолютно антисимметричный тензор.

8-мерная неассоциативная алгебра O включает семь мнимых единиц $e_p^2 = -e_0$ с сопряжением $e_p^* = -e_p$, $p=1,2,\dots,7$. Для октонионов

$$o = x_0 e_0 + x_1 e_1 + \dots + x_7 e_7 \quad (21)$$

также имеется связь со сферой S^7 :

$$o^+ o = x_0^2 + x_1^2 + \dots + x_7^2 = 1; \{x_0, x_1, \dots, x_7\} \in \mathbb{S}^7, \quad (22)$$

которая не является группой Ли.

Алгебра $su(2)$ изоморфна алгебре Ли $so(3)$: $su(2) \approx so(3)$, в которой вместо антисимметричных образующих A_n ($n=1,2,3$) можно также использовать эрмитовы генераторы $L_n = iA_n$ ($n=1,2,3$):

$$L_1 = i \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, L_2 = i \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, L_3 = i \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad (23)$$

которые, как и в алгебре $su(2)$, образуют те же коммутационные соотношения:

$$[L_i, L_j] = i\epsilon_{ijm} L_m. \quad (24)$$

Алгебре $so(3)$ соответствует ортогональная группа $SO(3) \approx SU(2)/Z_2$, в которой преобразования вращения на угол θ вокруг оси направленной вдоль вектора \vec{n} приобретают следующий вид [8]:

$$R(\vec{n}, \theta) = \exp\{-i\theta \hat{n} \cdot \vec{L}\} = \hat{1} + \sin \theta (-i\hat{n} \cdot \vec{L}) + (1 - \cos \theta)(-i\hat{n} \cdot \vec{L})^2 \quad (25)$$

Между представлениями алгебры Ли и представлением группы Ли также существует экспоненциальная связь. Так трехмерное представление алгебры $so(3)$:

$$[d(L_k), d(L_l)] = i \epsilon_{klm} d(L_m), \quad (26)$$

отвечающее орбитальному моменту $L=1$, в котором собственные состояния оператора $d(L_3)$ определяются в следующем базисе

$$|1,1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |1,0\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |1,-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad (27)$$

Действия повышающего $d(L_+) = 1/\sqrt{2}(d(L_1) + id(L_2))$ и понижающего $d(L_-) = 1/\sqrt{2}(d(L_1) - id(L_2))$ операторов в приведенном базисе состояний:

$$d(L_+) |1,1\rangle = 0, d(L_+) |1,0\rangle = \sqrt{2} |1,1\rangle, d(L_+) |1,-1\rangle = \sqrt{2} |1,0\rangle \quad (28)$$

$$d(L_-) |1,1\rangle = \sqrt{2} |1,0\rangle, d(L_-) |1,0\rangle = \sqrt{2} |1,-1\rangle, d(L_-) |1,-1\rangle = 0$$

соответствуют следующему матричному $(2L+1)=3$ -х мерному представлению алгебры $so(3)$:

$$d(L_3) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}, d(L_+) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, d(L_-) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & -i & 0 \\ i & 0 & -i \\ 0 & i & 0 \end{pmatrix} \quad (29)$$

Теперь можно построить соответствующее неприводимое представление $D(1)$ группы $SO(3)$, заданное экспоненциальной формулой (см. (8)):

$$D(\vec{L}) = \exp\{-i\theta \hat{n} \cdot d(\vec{L})\} \quad (30)$$

Для геометрической характеристики этого представления приведем выражение для $O = x_k d(L_k)$:

$$\hat{O} = \begin{pmatrix} x_3 & 1/\sqrt{2}(x_1 - ix_2) & 0 \\ 1/\sqrt{2}(x_1 + ix_2) & 0 & 1/\sqrt{2}(x_1 - ix_2) \\ 0 & 1/\sqrt{2}(x_1 + ix_2) & -x_3 \end{pmatrix} \quad (31)$$

4. Расширение унитарности и симметрии многомерных циклических многообразий

Если вещественные числа находятся во взаимно однозначном соответствии с одномерной координатной осью R^1 , то комплексные числа основаны на комплексификации двумерной плоскости R^2 , а кватернионы с особой некоммутативной комплексификацией R^4 . Ожидаемые топологические и алгебраические структуры в многомерных пространствах R^n , $n=4,5,6,\dots$ также могут привести к ряду важнейших феноменологических приложений, если учесть возможности многомерных C_n -циклических комплексных чисел. Так сохраняется важнейшее бинарное соотношение для произведения двух C_n -циклических комплексных чисел. Например, для C_3 -тернарных комплексных чисел

$$z_1 = x_0 q_0 + x_1 q + x_2 q^2 \text{ и } z_2 = y_0 q_0 + y_1 q + y_2 q^2,$$

$$q^3 = q_0 = 1$$

$|z_k|^3 = z_k \tilde{z}_k \tilde{\tilde{z}}_k = 1, k=1,2$ групповое свойство $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ действительно выполняется:

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

$$\begin{aligned}
 |z_1 \cdot z_2|^2 &= (x_0 y_0 + x_1 y_2 + x_2 y_1) q_0 + (x_2 y_2 + x_0 y_1 + x_1 y_0) q + (x_1 y_1 + x_0 y_2 + x_2 y_0) q^2 + \\
 &= (x_0 y_0 + x_1 y_2 + x_2 y_1)^2 + (x_2 y_2 + x_0 y_1 + x_1 y_0)^2 + (x_1 y_1 + x_0 y_2 + x_2 y_0)^2 - \\
 &- 3(x_0 y_0 + x_1 y_2 + x_2 y_1)(x_2 y_2 + x_0 y_1 + x_1 y_0)(x_1 y_1 + x_0 y_2 + x_2 y_0) = \\
 &= (x_0^2 + x_1^2 + x_2^2 - 3x_0 x_1 x_2)(y_0^2 + y_1^2 + y_2^2 - 3y_0 y_1 y_2) = |z_1|^2 \cdot |z_2|^2
 \end{aligned} \quad (32)$$

В результате, единичные тернарные комплексные числа порождают двухпараметрическую абелеву тернарную группу. По тройному аналогу Эйлера можно построить следующую «унитарную» n -мерную циклическую C_n -группу $U(1)^{(n-1)} = \exp\{\alpha_1 q + \dots + \alpha_{n-1} q^{n-1}\}$ с соответствующей мнимой единицей вида $q^n = +1$, либо $q^n = -1$:

$$U \cdot U^{(1)} \dots U^{(n-1)} = \hat{1}, U^{(n)} = U \quad (33)$$

где $\alpha_1, \dots, \alpha_{n-1}$ – параметры групп, и введена операция n -мерного комплексного сопряжения

$$\begin{aligned}
 \tilde{q} &= q^{(1)} = j q, \dots, q^{(k)} = j^k q, \dots, q^{(n)} = \pm q_0 : \\
 U^{(k)} &= \exp(j^k \alpha_1 q + \dots + j^{n-k} \alpha_{n-1} q^{n-1}), k = 0, \dots, n \quad (34)
 \end{aligned}$$

Успех алгебр Ли низшего ранга $U(1)$ и $SU(2)$ в электрослабом секторе Стандартной Модели пришел в результате открытия массивных векторных бозонов W_μ^\pm, Z_μ^0 и Хиггсовского бозона H^0 , тем более, что с последним связывают существование нового вакуума природы, ответственного за образование масс кварков и лептонов, фактически всей видимой материи. Возможности использования групп Ли высших рангов сталкиваются со сложностью исследования соответствующих этим группам Ли многообразий, например, Ли группа $SU(3)$ является 8-мерным многообразием! Другой вопрос касается определения унитарности групп на основе инвариантности квадратичной нормы, которой может оказаться не достаточно для описания многочастичных процессов. Рассмотрение трех частичных и более взаимодействий может дополнить понятие унитарности, расширения скобки Ли. и соответственно, может значительно расширить границы групповых симметрий в природе. С такими возможностями мы столкнулись в теорий новых «комплексных» чисел, где мы использовали метод конечных абелевых групп, в котором были использованы C_n -циклические группы (см. таблицу 1).

Таблица 1

Ряд конечных групп до порядка 12

порядок	группы
1	C1
2	C2
3	C3
4	C4, D2=C2xC2
5	C5
6	C6=C2xC3, D3
7	C7
8	C8, C4xC2, C2xC2xC2, Q
9	C9, C3xC3
10	C10=C2xC5, D5
11	C11
12	C12 = C3xC4, C6xC2=C2xC2xC2, D6=C2xD3, A4, W

На этом пути мы уже частично исследовали [4-6], как теории многомерных «циклических» комплексных чисел в рамках n -арных алгебр ($n=3,4,\dots$) с делением, так и некоторые следствия, касающиеся новых многомерных многообразий (пространств), которые мы строим на базе норм $|z|^n$, инвариантных относительно соответствующих абелевых и не абелевых симметрий [4-6]. В соответствии с таблицей 1 мы продолжаем построение и анализ новых комплексных чисел, для которого мы используем n -одномерных неприводимых представлений C_n -циклических групп с учетом их разложения на подгруппы. Если бинарные альтернативные алгебры (комплексные числа, кватернионы, октонионы) над действительными числами имеют размерности 2^p , $p=1,2,3,4,\dots$, то $n=3$ -арные и $n=4$ -арные нормированные алгебры с делением имеют размерности n^p , $p=1,2,3$, соответственно.

Чтобы рассмотреть не абелевы циклические комплексные числа, вводятся две «мнимые» единицы, $q_1=q$ и $q_2=q_s$ со свойствами $q_1^n=q_0$ и $q_2^m=q_0$, $n,m>2$, являющиеся генераторами двух циклических групп C_n и C_m и в соответствии с одномерными представлениями характеров определены соответствующие операции автоморфизмов $q_1 \in C_n$ и $q_2 \in C_m q_2$ [4,5].

5. Геометрия C_4 -циклических алгебр с делением

Рассмотрим два случая квартетных комплексных чисел $q^4=q_0$ и $q^4=-q_0$:

$$z = x_0 q_0 + x_1 q_1 + x_2 q_2 + x_3 q_3, x_i \in \mathbb{R}. \quad (35)$$

Для первого случая: $q^4=q_0$ можно ввести базис, соответствующий выделению двух одномерных идеалов K и T , $K \cdot T = 0$:

$$K = 1/4(q_0 + q + q^2 + q^3), K^n = K,$$

$$T = 1/4(q_0 - q + q^2 - q^3), T^n = T,$$

и одному двумерному $G = \{S, I: I \cdot S = I\}$, $G \cdot K = G \cdot T = 0$:

$$S = 1/2(q_0 - q^2), I = 1/2 q(q_0 - q^2),$$

$$S^n = S, I^{2n} = (-1)^n S, I^{(2n+1)} = (-1)^n I.$$

Тогда можно переписать квартетные комплексные числа в новом базисе:

$$Z = (x_0 + x_1 + x_2 + x_3)K + (x_0 - x_1 + x_2 - x_3)T + (x_0 - x_2)S + (x_1 - x_3)I \quad (38)$$

и определить их единичную норму:

$$\begin{aligned}
 |z|^4 &= |F_K| |F_T| \{|F_S|^2 + |F_I|^2\} = \\
 &= (x_0 + x_1 + x_2 + x_3)(x_0 - x_1 + x_2 - x_3) \cdot \\
 &\quad \cdot [(x_0 - x_2)^2 + (x_1 - x_3)^2] = \\
 &= [(x_0 + x_2)^2 - (x_1 + x_3)^2] [(x_0 - x_2)^2 + (x_1 - x_3)^2] = \\
 &= [x_0^2 + x_2^2 - 2x_1 x_3]^2 - [x_1^2 + x_3^2 - 2x_0 x_2]^2 = 1.
 \end{aligned} \quad (39)$$

Гиперповерхность (39) инвариантна относительно 3-х параметрических абелевых преобразований, которые имеют следующий экспонен-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

циальный вид:

$$\begin{aligned} F(\alpha_1, \alpha_2, \alpha_3) &= \exp\{\alpha_1 q + \alpha_2 q^2 + \alpha_3 q^3\} = \\ &= \exp\{\alpha(K-T)\} \cdot \exp\{\beta(K+T-S)\} \cdot \exp\{\gamma I\} = \\ &= f_0 q_0 + f_1 \alpha_1 q + f_2 \alpha_2 q^2 + f_3 \alpha_3 q^3, \end{aligned} \quad (40)$$

где $\alpha = \alpha_1 + \alpha_2$, $\beta = \alpha_2$, $\gamma = \alpha_1 - \alpha_2$ и f_i ($i=0,1,2,3$) являются C_4 -тригонометрическими функциями, удовлетворяющих равенству аналогичному (39):

$$(f_0^2 + f_2^2 - 2f_1 f_3)^2 - (f_1^2 + f_3^2 - 2f_0 f_2)^2 = 1. \quad (41)$$

Для второго случая $q^4 = -q_0$ можно построить два двумерных идеала

$$G_+ = \{T_+, U_+\} \text{ и } G_- = \{T_-, U_-\}, \quad G_+ \cdot G_- = 0,$$

где

$$\begin{aligned} T_{\pm} &= 1/2\{q_0 \pm 1/\sqrt{2}(q - q^3)\}, \quad (T_{\pm})^n = T_{\pm}, \\ U_{\pm} &= 1/2\{q^2 \pm 1/\sqrt{2}(q + q^3)\}, \\ (U_{\pm})^{2n} &= (-1)^n T_{\pm}, \quad (U_{\pm})^{2n+1} = (-1)^n U_{\pm}, \end{aligned} \quad (42)$$

Выражая квартетное комплексное число в новом базисе

$$\begin{aligned} Z &= z\{F(G_+)\} + z\{F(G_-)\} = \\ &= \{T_+ [x_0 + 1/\sqrt{2}(x_1 - x_3)] + U_+ [x_0 + 1/\sqrt{2}(x_1 + x_3)] \\ &\quad + \{T_- [x_0 - 1/\sqrt{2}(x_1 - x_3)] + U_- [x_0 - 1/\sqrt{2}(x_1 + x_3)]\}, \end{aligned} \quad (43)$$

мы убеждаемся, что норма этого C_4 -числа определяет торическое многообразие $T^2 = S_1 \otimes S_1$:

$$\begin{aligned} |z|^4 &= \{[x_0 + 1/\sqrt{2}(x_1 - x_3)]^2 + [x_0 + 1/\sqrt{2}(x_1 + x_3)]^2\} \\ &\quad \{[x_0 + 1/\sqrt{2}(x_1 - x_3)]^2 + [x_0 + 1/\sqrt{2}(x_1 + x_3)]^2\} = \\ &= [x_0^2 - x_2^2 + 2x_1 x_3]^2 + [x_3^2 - x_1^2 + 2x_0 x_2]^2 = 1 \end{aligned} \quad (44)$$

6. Инвариантные гиперповерхности в C_6 -комплексифицированном 6-мерном пространстве

Рассмотрим C_6 -комплексификацию 6-мерного пространства:

$$z = x_0 q_0 + x_1 q + x_2 q^2 + x_3 q^3 + x_4 q^4 + x_5 q^5. \quad (45)$$

Для случая $q^6 = q_0 = 1$ это C_6 -комплексное число в соответствии с соотношением $C_6 = C_3 \otimes C_2$ можно разложить на пару C_{3A} и C_{3B} -циклических комплексных чисел:

$$z = (u_0 A_0 + u_1 A_1 + u_2 A_2) + (v_0 B_0 + v_1 B_1 + u_2 B_2), \quad (46)$$

где

$$\begin{aligned} u_0 &= 1/2(x_0 + x_3), \quad u_1 = 1/2(x_1 + x_4), \quad u_2 = 1/2(x_2 + x_5), \\ v_0 &= 1/2(x_0 - x_3), \quad v_1 = 1/2(x_1 - x_4), \quad v_2 = 1/2(x_2 - x_5), \end{aligned} \quad (47)$$

и

$$\begin{aligned} A_0 &= 1/2(q + q^3), \quad A_1 = qA_0 = 1/2(q + q^3)q, \quad A_2 = q^2 A_0 = \\ &= 1/2(q + q^3)q^2, \\ B_0 &= 1/2(q - q^3), \quad B_1 = qB_0 = 1/2(q - q^3)q, \\ B_2 &= q^2 B_0 = 1/2(q - q^3)q^2. \end{aligned} \quad (48)$$

Проверим свойства построенных генераторов двух семейств $\{A_i\}, \{B_i\}$ C_6 -комплексных чисел, соответствующих двум непересекающимся вариантам тернарных чисел с различными условиями:

$$\begin{aligned} C_{3A} &= \{A_0, A_1, A_2 \mid A_1^3 = A_0, A_0^n = A_0\} \\ C_{3B} &= \{B_0, B_1, B_2 \mid B_1^3 = -B_0, B_0^n = B_0\}. \end{aligned} \quad (49)$$

Два 3-х мерных идеала в C_6 определяются следующим выбором базисов

$$\begin{aligned} K_A &= 1/3(A_0 + A_1 + A_2), \quad K_B = 1/3(B_0 - B_1 + B_2), \\ E_A &= 1/3(2A_0 - A_1 - A_2), \quad E_B = 1/3(2B_0 + B_1 - 2B_2), \\ I_A &= 1/\sqrt{3}(A_1 - A_2), \quad I_B = -1/\sqrt{3}(B_1 + B_2), \end{aligned} \quad (50)$$

так что $\{K_A, E_A, I_A\} \cdot \{K_B, E_B, I_B\} = 0$ и еще дополнительными условиями для одномерного и двумерного идеалов в каждой C_{3A} и C_{3B} группах: $\{K_A\} \cdot \{E_A, I_A\} = 0$, $\{K_B\} \cdot \{E_B, I_B\} = 0$. Используя выражения для $\{A_0, A_1, A_2\}$ и $\{B_0, B_1, B_2\}$ в базисе идеалов:

$$\begin{aligned} A_0 &= K_A + E_A, \quad B_0 = K_B + E_B \\ A_1 &= K_A - 1/2 E_A - \sqrt{3}/2 I_A, \quad B_1 = -(K_B - 1/2 E_B - \sqrt{3}/2 I_B), \\ A_2 &= K_A - 1/2 E_A + \sqrt{3}/2 I_A, \quad B_2 = K_B - 1/2 E_B + \sqrt{3}/2 I_B \\ A_1^2 &= K_A - 1/2 E_A - \sqrt{3}/2 I_A, \quad B_1^2 = K_B - 1/2 E_B - \sqrt{3}/2 I_B \\ A_2^2 &= K_A - 1/2 E_A + \sqrt{3}/2 I_A, \quad B_2^2 = K_B - 1/2 E_B + \sqrt{3}/2 I_B \end{aligned} \quad (51)$$

можно получить окончательное выражение для C_6 -циклического комплексного числа

$$\begin{aligned} z &= (u_0 + u_1 + u_2)K_A + [u_0 - 1/2(u_1 + u_2)]E_A + \\ &\quad + \sqrt{3}/2(u_1 - u_2)I_A + (v_0 + v_1 + v_2)K_B + [v_0 + \\ &\quad + 1/2(v_1 - v_2)]E_B - \sqrt{3}/2(v_1 + v_2)I_B \end{aligned} \quad (52)$$

учитывая два 3-х мерных идеала (каждый из которых состоит из одномерного и двумерного идеалов) норму C_6 -циклического комплексного числа можно представить в виде произведения двух кубических полиномов в прямом соответствии композитной структуры циклической C_6 -группы, $C_6 = C_3 \times C_2$:

$$\begin{aligned} |z|^6 &= |F_A|^3 \cdot |F_B|^3 = (u_0 + u_1 + u_2)^3 \{ [u_0 - 1/2(u_1 + u_2)]^2 \\ &\quad + [\sqrt{3}/2(u_1 - u_2)]^2 \} \\ &\quad (v_0 + v_1 + v_2)^3 \{ [v_0 + 1/2(v_1 - v_2)]^2 + [\sqrt{3}/2(v_1 + v_2)]^2 \} = \\ &= \{ u_0^3 + u_1^3 + u_2^3 - 3u_1 u_2 u_3 \} \cdot \{ v_0^3 + v_1^3 + v_2^3 + 3v_1 v_2 v_3 \} = \\ &= \{ (x_0 + x_3)^3 + (x_1 + x_4)^3 + (x_2 + x_5)^3 - \\ &\quad - 3(x_0 + x_3)(x_1 + x_4)(x_2 + x_5) \} \\ &\quad \{ (x_0 - x_3)^3 - (x_1 - x_4)^3 + (x_2 - x_5)^3 + \\ &\quad + 3(x_0 - x_3)(x_1 - x_4)(x_2 - x_5) \} = 1 \end{aligned} \quad (53)$$

Эта гиперповерхность инвариантна относительно 5-ти параметрических преобразований, которые мы отнесли к расширенным унитарным преобразованиям $U(1)^5$:

$$(x'_0, \dots, x'_5)^T = U(x_0, \dots, x_5)^T, \quad (54)$$

для экспоненциальной формы, которых C_6 групповое обобщение формулы Эйлера имеет следующий вид:

$$U = \exp(\varphi_1 q + \dots + \varphi_5 q^5) = m_0(\varphi_1, \dots, \varphi_5) q_0 + \dots + m_5(\varphi_1, \dots, \varphi_5) q^5, \quad (55)$$

где функции $\{m_0, m_1, \dots, m_5\}$ удовлетворяют соотношению (53).

Рассмотрим случай $q^6 = -q_0 = -1$. Три двумерных идеала $\{T_+, V_+\}$, $\{T, V\}$, $\{E, J\}$ строятся следующим образом:

$$\begin{aligned} T_{\pm} &= 1/6(2q_0 + q^2 - q^4) \pm 1/(2\sqrt{3})(q - q^5) \\ V_{\pm} &= q^3 T_{\pm} = 1/6(q + 2q^3 + q^5) \pm 1/(2\sqrt{3})(q^2 + q^4) \\ P &= 1/3(q_0 - q^2 + q^4), \quad J = 1/3 q (q_0 - q^2 + q^4). \end{aligned} \quad (56)$$

Можно проверить, что эти три идеала между собой не пересекаются:

$$\{T_+, V_+\} \cdot \{T, V\} = \{T_+, V_+\} \cdot \{P, J\} = \{T, V\} \cdot \{P, J\} = 0. \quad (57)$$

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

В так построенном базисе C_6 -комплексное число приобретает следующее выражение:

$$\begin{aligned} Z &= x_0 q_0 + \dots + x_5 q^5 = \\ &= \{ T_+ [x_0 + 1/2(x_2 - x_4) + \sqrt{3}/2(x_1 - x_5)] + \\ &+ V_+ [x_3 + 1/2(x_1 + x_5) + \sqrt{3}/2(x_2 + x_4)] \} + \\ &+ \{ T_- [x_0 + 1/2(x_2 - x_4) - \sqrt{3}/2(x_1 - x_5)] + \\ &+ V_- [x_3 + 1/2(x_1 + x_5) - \sqrt{3}/2(x_2 + x_4)] \} + \\ &+ \{ P[x_0 - x_2 + x_4] + J[-x_3 + x_1 + x_5] \}. \end{aligned} \quad (58)$$

В результате 5-ти параметрическую инвариантную гиперповерхность 6-ой степени можно определить через единичную норму C_6 -комплексного числа:

$$\begin{aligned} |z|^6 &= |F(T_+, V_+)|^2 \cdot |F(T_-, V_-)|^2 \cdot |F(P, J)|^2 = \\ &= \{ [x_0 + 1/2(x_2 - x_4) + \sqrt{3}/2(x_1 - x_5)]^2 + \\ &+ [x_3 + 1/2(x_1 + x_5) + \sqrt{3}/2(x_2 + x_4)]^2 \} \cdot \\ &\cdot \{ [x_0 + 1/2(x_2 - x_4) - \sqrt{3}/2(x_1 - x_5)]^2 + \\ &+ [x_3 + 1/2(x_1 + x_5) - \sqrt{3}/2(x_2 + x_4)]^2 \} \cdot \\ &\cdot \{ [x_0 - x_2 + x_4]^2 + [-x_3 + x_1 + x_5]^2 \} = 1. \end{aligned} \quad (59)$$

Мы рассмотрели только несколько примеров *таблицы 1*. Наши интересы в данном пункте касаются возможности применения единой теории, объединяющей унитарные группы неабелевых симметрий, отвечающих циклическим группам различных порядков.

Литература

1. Смуров С.В., Волков Г.Г. Спин-партоновый путь к квантованию протона // Известия Института инженерной физики, 2024. №1(71). С.71-80.
2. Juan Rojo. The Partonic Content of Nucleons and Nuclei arXiv: 1910.03408v2 [hep-ph] 25 February, 2020.
3. A. Deur, S. J. Brodsky, G. F. de Teramond. The Spin Structure of the Nucleon arXiv: 1807.05250v3 [hep-ph] 24 Apr 2019.
4. Смуров С.В., Волков Г.Г. Обобщенные унитарные группы симметрий в многомерной телепортации // Известия Института инженерной физики, 2023. №3(69). С.73-82.
5. Смуров С.В., Волков Г.Г. Об исключительных особенностях мультинарных комплексных неабелевых алгебрах // Известия Института инженерной физики, 2021. №4(62). С.60-68.
6. G. Volkov. Ternary «Quaternions» and Ternary TU(3) algebra, arXiv: 1006.5627 (2010).
7. T'Hoof. Lie groups in physics. Institute for Theoretical Physics. Utrecht University Beta Faculty, 2007.
8. Eef van Beveren, Some notes on group theory. Departamento de Física Faculdade de Ciências e Tecnologia P-3000 COIMBRA (Portugal). February, 2012.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056

МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ НА ОСНОВЕ ОПТИМАЛЬНОЙ ДОСТОВЕРНОСТИ СТЕГАНОГРАФИЧЕСКОГО АНАЛИЗА ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ A METHODOLOGY FOR ENSURING INFORMATION SECURITY OF AUTOMATED MILITARY SYSTEMS BASED ON THE OPTIMAL RELIABILITY OF STEGANOGRAPHIC ANALYSIS OF TRANSMITTED INFORMATION

Олег Игоревич Атакищев

*почетный работник науки и высоких технологий РФ
доктор технических наук, профессор
заместитель генерального директора
по специальным проектам
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл., г. Серпухов,
Большой Ударный пер., д. 1а
Тел. +7(4967)35-31-93
E-mail: aoi007@mail.ru*

Вадим Геннадьевич Грибунин

*почетный работник науки и техники РФ
доктор технических наук, доцент
главный научный сотрудник
АНО «Институт инженерной физики»
E-mail: wavelet2@mail.ru*

Иван Демьянович Комаров

*кандидат технических наук, доцент
начальник отдела
АО «ЦНИИ машиностроения»
Адрес: 141070, Московская обл., г. Королев,
ул. Пионерская, д. 4
Тел.: +7 (495) 513-59-72
E-mail: info416@tsniimash.ru*

Александр Юрьевич Борисенко

*ведущий специалист
АО «МПОВТИ»
Адрес: 129515, Москва,
ул. Академика Королева, д. 13, стр. 1
Тел.: 8(925)090-42-69*

Юлия Сергеевна Ермакова

*младший научный сотрудник отдела
АО «ЦНИИ машиностроения»
Адрес: 141070, Московская обл., г. Королев,
ул. Пионерская, д. 4
Тел.: +7 (495) 513-47-07
E-mail: info416@tsniimash.ru*

Аннотация

В статье представлена методика обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стенографического анализа передаваемой информации.

Ключевые слова: стеганоанализ, надёжность, алгоритмы, каналы передачи, стеганографический анализ.

Summary

The article presents a methodology for ensuring information security of automated military systems based on the optimal reliability of shorthand analysis of transmitted information.

Keywords: steganalysis, reliability, algorithms, transmission channels, steganographic analysis.

Введение

Создание и совершенствование автоматизированных систем военного назначения (АС ВН), направленное на повышение эффективности управления войсками (силами), относится к разряду наиболее сложных проблем. Одним из основных путей ее решения является реализация и широкое внедрение в АС ВН информационных технологий (ИТ).

Как известно, АС ВН создаются в целях повы-

шения качества принимаемых решений и обеспечения устойчивости, непрерывности, оперативности и скрытности управления. В свою очередь, качество управленческих решений непосредственно зависит от информации, на основе которой они принимаются. Поэтому ИТ призваны обеспечить достоверность информации, циркулирующей в системе управления войсками (силами), с учетом уровня управления, полномочий лица, принимающего решение, и других факторов.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

С развитием ИТ и переводом основных потоков информации в цифровую форму приобрела актуальность проблема обеспечения информационной безопасности. При этом единственным выходом для сохранения конфиденциальности и целостности информации является создание комплексной системы защиты информации. Важную роль в обеспечении информационной безопасности играет подсистема контроля информации. Однако стандартные методы и средства контроля информации на настоящий момент ориентированы на проверку лишь ограниченного числа явных атрибутов и современные средства сокрытия информации – цифровой стеганографии – позволяют преодолевать существующие системы контроля доступа к сетевым ресурсам. Скрытые каналы передачи информации позволяют преодолеть ограничения стандартных средств контроля трафика. Информация может быть скрыта в любом формате данных, который разрешён к передаче данным пользователем во внешнюю сеть, в том числе в определённых полях сетевых пакетов, запрашиваемых ссылках и иных объектах. В качестве носителя скрытой информации в цифровой стеганографии могут быть использованы оцифрованные аналоговые сигналы, тексты документов, исполнимый код, пакеты сетевого трафика и т.д. с сохранением семантики. Таким образом, принципиально возможна организация скрытых каналов утечки при наличии любой избыточности в исходящем трафике. Применение стеганографических средств для сокрытия информации в файлах, передаваемых затем на сайты мультимедиа-контента и файлообменные серверы позволяет скрытно организовывать и координировать проведение различного рода противоправных действий. При получении доступа организованными преступными группировками к передающим средствам сотовой и стационарной телефонной связи, спутниковым каналам связи, телевидения и радиовещания возможна организация скрытых каналов передачи информации глобальных масштабов. В этих условиях особенно актуальной становится задача обнаружения скрытой информации, её извлечения и уничтожения, а также анализ стойкости существующих стеганографических алгоритмов, и разработка новых методов выявления скрытой информации – стеганоанализ.

В настоящее время при передаче мультимедийной информации по каналам автоматизированных систем военного назначения повышается число мест в цифровом контейнере, где могут быть стеговложения, что приводит к увеличению вероятности сокрытия сообщений и риска

нарушения информационной безопасности этих систем.

Поэтому для обеспечения информационной безопасности АС ВН, заключающегося в обнаружении с определённой вероятностью скрытого сообщения во мультимедийной передаваемой информации, проводится её стеганоанализ (т.е. контроль наличия стеговложений).

Несмотря на огромное разнообразие алгоритмов сокрытия факта передачи информации в графических файлах, почти все они сводятся к нескольким базовым методам стеганографии. К их числу относятся метод сокрытия в наименьших значащих битах пикселей с помощью анализа критерия Хи-квадрат, RS-метод, а также метод Коха-Жао, кодирующий информацию в представлении изображения в частотной области.

Большинство остальных стеганографических методов являются модификациями или вариациями данных методов.

Результаты анализа работ [1-12], показывают, что существующие модели, методики и методы планирования объёмов стеганоанализа требуют контролировать большое количество мест (более 10 мест) цифрового контейнера. Однако в силу ограничений на выделяемые временные ресурсы такой объём контроля обеспечить не представляется возможным, поэтому контроль наличия стеговложений в передаваемой мультимедийной информации проводится только по малой выборке мест (не более 5 мест) цифрового контейнера.

Опыт применения разработанных к настоящему времени базовых методов стеганографии показал, что **такие объёмы контроля** приводят к возникновению **рисков пропуска стеговложений и вызывают нарушения информационной безопасности** автоматизированных систем военного назначения [1,12,28-30].

Учитывая степень стохастического подобия стеганоанализа вероятностно-статистическим выборочным методам контроля надёжности изделий ракетно-космической техники (ИРКТ) [13-27] в условиях малой выборки (5 и менее изделий или испытаний) необходимо использовать их для того, чтобы дать стеганоаналитику методический аппарат, применение которого позволяло бы ему минимизировать риски пропуска сообщения в контейнере по малой выборке и тем самым обеспечивать информационную безопасность автоматизированных систем военного назначения.

Таким образом, в процессе стеганографического анализа мультимедийной информации, передаваемой в автоматизированных системах военного назначения, особую остроту приобре-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

тает **противоречие** между планируемыми объёмами контроля наличия стеговложений в рамках установленной продолжительности стеганоанализа и невозможностью выполнения заданных требований к обеспечению информационной безопасности этих систем при реализации таких объёмов контроля.

Однако, как считают авторы, указанное **противоречие может быть разрешено на основе минимизации рисков пропуска стеговложений** во мультимедийной информации в процессе многоуровневого стеганографического анализа по малым выборкам контроля мест стеговложений в цифровом контейнере за счёт учёта результатов всех предыдущих этапов контроля [13-27].

Именно необходимость разрешения данного противоречия определяют **важность и актуальность** решения **научной задачи, связанной с разработкой методики обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стеганографического анализа передаваемой информации.**

Постановка задачи

Объект исследования: система предотвращения утечек мультимедийной информации, передаваемой в АС ВН (стеганоанализ).

Предмет исследования: методики стеганографического анализа.

Целью исследования является минимизация рисков ошибок контроля мест стеговложений в цифровом контейнере мультимедийной информации в процессе стеганографического анализа по малым выборкам для обеспечения информационной безопасности автоматизированных систем военного назначения.

Для достижения цели исследования необходимо решить следующие основные вопросы.

1. Проведение анализа обеспечения информационной безопасности автоматизированных систем военного назначения (АС ВН) на основе стеганографического анализа передаваемой мультимедийной информации и его научно-методического обеспечения. Постановка задачи исследования.

2. Разработка математических моделей оптимального планирования контроля мест стеговложений в цифровом контейнере и оценки рисков пропуска стеговложений в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации

3. Разработка математической модели оптимизации достоверности стеганографического многоуровневого анализа передаваемой мультимедийной информации в автоматизированных системах военного назначения в условиях малых выборок мест контроля стеговложений в цифровом контейнере.

4. Разработка методики обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стеганографического анализа передаваемой информации.

5. Проведение экспериментальных исследований разработанных моделей и методики, сравнение с аналогами.

Основными научными результатами следует считать следующие.

1. Математические модели оптимального планирования контроля мест стеговложений в цифровом контейнере и оценки рисков пропуска стеговложений в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации.

2. Математическая модель оптимизации достоверности стеганографического многоуровневого анализа передаваемой мультимедийной информации в автоматизированных системах военного назначения в условиях малых выборок мест контроля стеговложений в цифровом контейнере.

3. Методика методики обеспечения информационной безопасности автоматизированных систем военного назначения на основе оптимальной достоверности стеганографического анализа передаваемой информации.

Научная новизна научных результатов должна содержать следующие особенности и отличия от моделей, методик и методов планирования объёмов стеганоанализа.

Первый научный результат основан на оптимальном планировании контроля мест стеговложений в цифровом контейнере и оценках рисков пропуска стеговложений по результатам контроля малых выборок в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации.

В качестве исходной общей математической модели контроля мест стеговложений в цифровом контейнере и оценки рисков пропуска стеговложений по результатам контроля малых выборок в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации наиболее естественно и целесообразно использовать функцию достоверности, которая имеет следующий вид [13-18,22,26,27]:

$$D=1-(\alpha+\beta), \quad (1)$$

где D – функция достоверности контроля мест стеговложений в цифровом контейнере; α, β – риски 1 и 2 рода.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

Модель построена на вновь установленных закономерностях точечного и интервального несмещённого медианного оценивания рисков пропуска стеговложений во мультимедийной информации в процессе стеганографического анализа по малым выборкам, использование которых обеспечит более высокую точность полученных оценок по сравнению с традиционными статистическими методами оценивания, что позволяет обнаружить встроенные в цифровой контейнер сообщения при объёмах порядка 1,5-2% от максимальной его ёмкости.

В качестве моделей рисков 1 и 2 рода приняты следующие закономерности [26,27]:

$$\alpha = \sum_{j=1}^n \left\{ \int_{x_{ij}}^{x_{ij}} f(x_j) \left[1 - \int_{x_{ij}}^{x_{ij}} f_1(t_j) dt_j \right] dx_j \right\}, \quad (2)$$

$$\beta = \prod_{j=1}^n \left\{ \left[1 - \int_{x_{ij}}^{x_{ij}} f(x_j) \right] \left[\int_{x_{ij}}^{x_{ij}} f_1(t_j) dt_j \right] dx_j \right\}, \quad (3)$$

где n – число контролируемых мест стеговложений в цифровом контейнере на одном уровне стегоанализа (объём контроля), в фигурных скобках представлены аналитические выражения рисков 1 и 2 рода – α_j, β_j , возникающих вследствие ошибок контроля одного места стеговложения в цифровом контейнере;

$\int_{x_{ij}}^{x_{ij}} f(x_j)$ – плотность распределения стеговложения в контролируемом месте;

$\int_{x_{ij}}^{x_{ij}} f_1(t_j)$ – плотность распределения риска контроля места стеговложения в цифровом контейнере. В работах [11-12] показано, что риски 1 и 2 рода в зависимости от величины n изменяются в противоположных направлениях, поэтому целевая функция (1) всегда имеет максимум, которому соответствует оптимальный план контроля.

Использование моделей в процессе планирования контроля мест стеговложений в цифровом контейнере даёт возможность:

- обеспечить минимальные риски контроля мест стеговложений на каждом уровне стегоанализа;

- сократить объёмы контроля мест стеговложений на более высоких уровнях стегоанализа за счёт учёта результатов контроля нижних уровней.

Второй научный результат построен на полумарковской модели минимизации рисков пропуска стеговложений во мультимедийной информации в процессе многоуровневого стеганографического анализа по малым выборкам, которая позволит обнаруживать стеганографические сообщения при объёмах заполнения 2-5% в полноцветных изображениях и до 0,2% от максимального, в контейнерах, полученных из формата JPEG.

Разработанные ранее (первый научный результат) математические модели позволяют построить оптимальные планы контроля. Вместе с тем эти модели не позволяют учесть следующие особенности: ограничения средств стоимостных ресурсов, которые выделяются на проведение контроля, а также ограничения по времени проведения контроля.

Кроме того, процесс контроля имеет определённые уровни выполнения, которые задают организацию процесса стегоанализа. При этом организация процесса происходит в течение определенного времени и сопровождается расходом выделяемых на контроль ресурсов.

Поэтому различные варианты организации процесса контроля имеют разную стоимость и разное время их проведения, то есть стоимость и время проведения контроля взаимосвязаны. Отсюда, очевидно, что обеспечение этой взаимосвязи при ограниченных стоимостных и временных ресурсах возможно лишь на основе оптимальной организации процесса контроля. Анализ показал, что наиболее приемлемым математическим подходом для моделирования организации указанного процесса является использование аппарата управляемых полумарковских процессов. Такой подход характеризуется следующими особенностями полумарковских моделей (ПММ) [22-26].

В ПММ процесс проведения контроля может находиться в различных состояниях, в соответствии с уровнями процесса стеганографического анализа мультимедийной информации. ПММ аккумулирует экономические и временные ресурсы по всем состояниям (уровням), что позволяет учесть экономические и временные ограничения.

Основу ПММ составляют:

- формализованная схема (граф состояний) организации процесса контроля мест стеговложений на каждом уровне стегоанализа (*рисунком 1*) [26];

- функционал стоимости контроля мест стеговложений на каждом уровне стегоанализа [26],

$$J = \frac{\left\{ C_2 \mu_2 P_{12} + C_1 \mu_1 + C_3 \mu_3 [P_{12} P_{23} + (\beta_{15} + P_{12} \beta_{25})(P_{33} + P_{36} P_{67})] + C_4 \mu_4 \alpha_{14} + (\beta_{15} + P_{12} \beta_{25}) \cdot (C_5 \mu_5 + C_6 \mu_6 P_{36} + C_7 \mu_7 P_{36} P_{67}) \right\}}{\left\{ \mu_1 + \mu_2 P_{12} + \mu_3 [P_{12} P_{23} + (\beta_{15} + P_{12} \beta_{25})(P_{33} + P_{36} P_{67})] + \mu_4 \alpha_{14} + (\beta_{15} + P_{12} \beta_{25}) (\mu_5 + \mu_6 P_{36} + \mu_7 P_{36} P_{67}) \right\}} \quad (4)$$

где J – удельные средние стоимостные затраты ресурсов на процесс контроля мест стеговложений;

α_{ij}, β_{ij} – риски 1 и 2 рода, обусловленные ошибками контроля мест стеговложений, определяемые с помощью зависимостей (1)-(2) и используемые в качестве вероятностей переходов про-

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

цесса из состояния i в состояние j ;

C_1, \dots, C_7 – средние стоимостные затраты ресурсов на пребывание процесса в соответствующем состоянии;

μ_1, \dots, μ_7 – средние времена пребывания процесса в соответствующем состоянии;

P_{ij} – вероятности безошибочных переходов процесса из состояния i в состояние j , определяемые с помощью следующей зависимости [26,27]:

$$P_{ij} = 1 - (\alpha_{ij} + \beta_{ij}); \quad (5)$$

• функционал продолжительности контроля мест стегановложений на каждом уровне стеганоанализа [26]:

$$\mu = \frac{\left\{ \mu_1 + \mu_2 P_{12} + \mu_3 [P_{12} P_{23} + (\beta_{15} + P_{12} \beta_{25})(P_{33} + P_{36} P_{63})] + \mu_4 \alpha_{14} + (\beta_{15} + P_{12} \beta_{25})(\mu_5 + \mu_6 P_{56} + \mu_7 P_{56} P_{67}) \right\}}{[1 + P_{12} + P_{12} P_{23} + \alpha_{14} + (\beta_{15} + P_{12} \beta_{25})(1 + P_{33} + P_{36} + P_{36} P_{63} + P_{56} P_{67})]} \quad (6)$$

где μ – средняя продолжительность контроля мест стегановложений;

• функционал стоимости экономии выделяемых и затраченных стоимостных ресурсов в процессе контроля мест стегановложений. Этот функционал имеет следующий вид [26]:

$$\Delta S = (S_{\text{выд}} - S_{\text{факт.затр}}) = [S_{\text{выд}} - (J\mu)], \quad (7)$$

где ΔS – функционал экономии выделяемых и затраченных стоимостных ресурсов в процессе контроля мест стегановложений за счёт минимизации рисков контроля и стоимостных потерь;

$S_{\text{выд}}$ – выделенные стоимостные ресурсы на процесс контроля мест стегановложений;

$S_{\text{факт.затр}}$ – средние фактические стоимостные затраты ресурсов на процесс контроля мест стегановложений [26];

новложений [26]:

$$S_{\text{факт.затр}} = J\mu. \quad (8)$$

В модели в качестве математических операторов переходов процесса из состояния в состояние впервые используются риски 1 и 2 рода (риск пропуска или ложного забракования мест стеговложений в цифровом контейнере), которые являются результатом решения вопроса по оптимизации планирования объёма контроля мест стеговложений в цифровом контейнере.

ПММ обеспечивает максимум экономии выделяемых и затраченных стоимостных ресурсов в процессе контроля мест стегановложений за счёт минимизации рисков контроля и стоимостных потерь, связанных с принятием ошибочных решений.

Третий научный результат построен на основе математических моделей математических моделей оптимального планирования контроля мест стеговложений в цифровом контейнере, оценки и минимизации рисков пропуска стеговложений по результатам контроля малых выборок в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации.

Методика, в отличие от традиционных статистических методов оценивания, позволяет проводить извлечение всей полезной информации, содержащейся в выборке, в виде законов распределения оценок рисков пропуска стеговложений по результатам контроля мест стеговложений в цифровом контейнере в процессе многоуровневого стеганографического анализа пере-

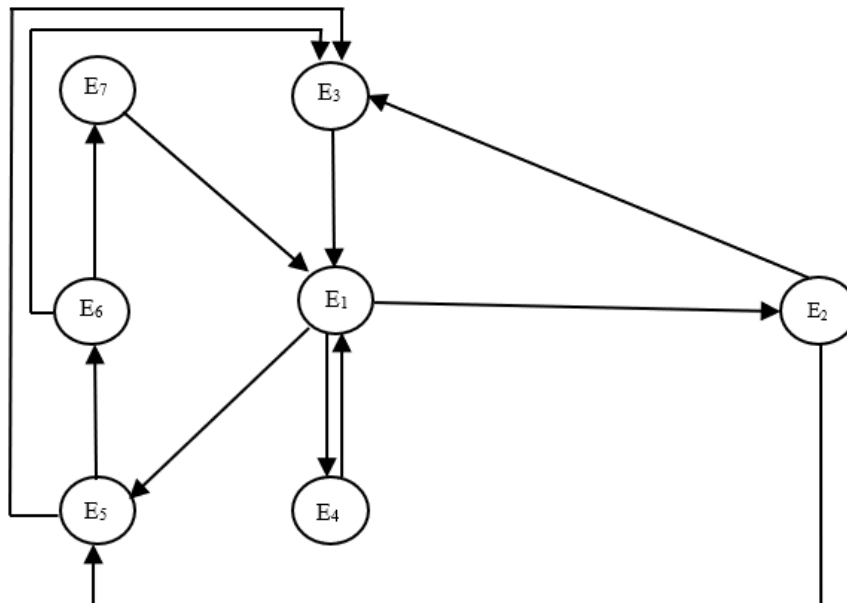


Рис. 1. E_1 – первый уровень стеганоанализа; E_2 – второй уровень стеганоанализа; E_3 – третий уровень стеганоанализа; E_4 – устранение стеговложения; E_5 – скрытое стегановложение; E_6 – нарушение информационной безопасности АС ВН; E_7 – ликвидация последствий нарушения информационной безопасности АС ВН

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

даваемой мультимедийной информации. При этом обеспечивается несмещенность и эффективность получаемых оценок рисков даже при ограниченном объеме данных наблюдений.

Методика позволяет обеспечить заданные требования к информационной безопасности автоматизированных систем военного назначения на основе минимизации рисков пропуска стеговложений во мультимедийной информации в процессе стеганографического анализа по малым выборкам.

Научная значимость научных результатов заключается в следующем:

- во впервые установленных вероятностно-статистических закономерностях несмещенного медианного оценивания рисков пропуска стеговложений во мультимедийной информации в процессе стеганографического анализа по малым выборкам, использование которых обеспечивает более высокую точность полученных оценок по сравнению с традиционными статистическими методами оценивания;

- в теоретическом обобщении и развитии математических методов в теории информационной безопасности автоматизированных систем военного назначения, позволяющим компенсировать неточности оценок рисков пропуска стеговложений во мультимедийной информации в процессе стеганографического анализа по малым выборкам и повысить достоверность её контроля на соответствие заданным требованиям при малом объеме испытаний;

- в совершенствовании методов планирования объемов контроля мест стеговложений в цифровом контейнере в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации, позволяющем при малой длине встроенного сообщения достичь высокой точности стеганоанализа.

Практическая значимость работы

Разработанные модели и методика обеспечивают возможность использования при создании многоуровневых автоматизированных систем универсального стеганоанализа.

Разработанные модели и методика позволяют создавать адаптируемые системы обнаружения сообщений, скрытых методами изменения НЗБ.

Выводы

В результате рассмотрения трафика мультимедийной информации по каналам автоматизированных систем военного назначения в условиях повышения числа мест стеговложений в цифровом контейнере, приводящих к увеличению

вероятности скрытия сообщений и риска нарушения информационной безопасности этих систем предложена методика обеспечения информационной безопасности этих систем на основе оптимальной достоверности стеганографического анализа передаваемой информации.

Методика базируется на математических моделях оптимального планирования контроля мест стеговложений в цифровом контейнере, оценки и минимизации рисков пропуска стеговложений по результатам контроля малых выборок в процессе многоуровневого стеганографического анализа передаваемой мультимедийной информации.

Использование моделей и методики позволяет минимизировать риски пропуска стеговложений по результатам контроля малых выборок в процессе многоуровневого стеганографического анализа передаваемой в АС ВН мультимедийной информации и тем самым обеспечить её информационную безопасность.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-Пресс, 2018. 262 с.
2. Аграновский А.В., Балакин А.В., Грибунин В.Г. и др. Стеганография, цифровые водяные знаки и стеганоанализ: Монография. М.: Вузовская книга, 2009. 217 с.
3. Грачев Я.А., Сидоренко В.Г. Стегоанализ методов скрытия информации в графических контейнерах // Надежность, 2021. №3. С. 39-46.
4. Варновский Н.П., Голубев Е.А., Логачев О.А. Современные направления стеганографии. Материалы конференции «Математика и безопасность информационных технологий». МГУ 28-29 октября 2004 г. М.:МЦНМО, 2005. С.32-64.
5. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев: «МК-Пресс», 2006. 286 с.
6. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. Dresden University of Technology, Department of Computer Science. Dresden, Germany, 1999.
7. Гонсалес Р.С., Вудс Р.Е. Цифровая обработка изображений. М.: Техносфера, 2005. 1105 с.
8. Fridrich J., Goljan M., Du R. Reliable Detection of LSB Steganography in Color and Grayscale Images. Binghamton University. New York, USA, 2001.
9. Syed Ali Khayam. The Discrete Cosine Transform (DCT): Theory and Application. Department of Electrical & Computer Engineering, Michigan State University. Michigan, USA, 2003.
10. Farid H. Digital Image Forensics. Scientific American, 2008. 199 с.

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

11. Белим С.В., Вильховский Д.Э. Стегоанализ алгоритма Коха-Жао // Математические структуры и моделирование, 2018. №4(48). С. 113-119.
12. Технические средства и методы защиты информации: учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. М.: ООО «Издательство Машиностроение», 2009 508 с.
13. Сухорученков Б.И. Анализ малой выборки. Прикладные статистические методы. М.: Вузовская книга, 2010. 384 с.
14. Кремер Н.Ш. Теория вероятностей и математическая статистика: учебник для вузов. 3-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА, 2012. 551 с.
15. Воинов В. Г., Никулин М. С. Несмещённые оценки и их применение. М.: Наука.1989. 440 с.
16. Беляев Ю.К. Вероятностные методы выборочного контроля. М.: Наука, 1975. 406 с.
17. Волков Л. И., Рудаков В. Б. Статистический контроль иерархических систем. М.: Высшая школа, 2002. 362 с.
18. Меньшиков В.А., Рудаков В.Б., Сычев В.Н. Контроль качества космических аппаратов при отработке и производстве. М.: Машиностроение, 2009. 400 с.
19. Надёжность и эффективность в технике: Справочник. Т. 2. Математические методы в теории надёжности. Под ред. А.Д. Соловьёва. М.: Машиностроение, 1988. 286 с.
20. Надёжность и эффективность в технике: Справочник. Т. 4. Методы подобия в надёжности. Под общ. ред. В.А. Мельникова, Н.А. Северцева. М.: Машиностроение, 1987. 280 с.
21. Надёжность и эффективность в технике: Справочник. Т. 6. Экспериментальная отработка и испытания. Под ред. Р.С. Судакова и О.И. Тескина. М.: Машиностроение, 1989. 326 с.
22. Надёжность и эффективность в технике: Справочник. Т. 8. Эксплуатация и ремонт. Под ред. В.И. Кузнецова и Е.Ю. Барзиловича. М.: Машиностроение, 1990. 320 с.
23. Беркетов Г.А., Блаженков В.В., Кравец Л.И., Оселедец В.И. Современные математические методы анализа и синтеза сложных систем. М.: ВА имени Ф.Э. Дзержинского, 1984. 399 с.
24. Барзилович Е.Ю., Беляев Ю.К., Каштанов В.А. и др. Вопросы математической теории надёжности. Под ред. Б.В. Гнеденко. М.: Радио и связь, 1983. 376 с.
25. Сильвестров Д.С. Полумарковские процессы с дискретным множеством состояний. М.: Сов. радио, 1980. 272 с.
26. Комаров И.Д., Ермакова Ю.С. Теоретические основы полумарковских математических моделей организации процессов обеспечения надёжности технических систем при экспериментальной отработке, производстве и эксплуатации. М.: Научно-технический сборник «Труды МИТ – наука, техника, производство», 2011. Вып. 11. Т. 1. Ч.2. С. 265-282.
27. Комаров И. Д., Ермакова Ю.С. Метод оценки достоверности контроля и прогнозирования параметрической безотказности опытных образцов изделий ракет-носителей в процессе испытаний на наземном комплексе и стартовом оборудовании. Сборник трудов ФГБУ «4 ЦНИИ» Минобороны России, 2022. Вып. 171. Т. 1. С.64-101.
28. Климов С.М., Астрахов А.В., Сычев М.П. Технологические основы противодействия компьютерным атакам. Электронное учебное издание. М.: МГТУ имени Н.Э. Баумана, 2013. 71 с.
29. Климов С.М., Астрахов А.В., Сычев М.П. Методические основы противодействия компьютерным атакам. Электронное учебное издание. М.: МГТУ имени Н.Э. Баумана, 2013. 110 с.
30. Климов С.М., Астрахов А.В., Сычев М.П. Экспериментальная оценка противодействия компьютерным атакам. Электронное учебное издание. М.: МГТУ имени Н.Э. Баумана, 2013. 116 с.



ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 681.5

МЕТОДИКА СИНТЕЗА СЛЕДЯЩЕЙ СИСТЕМЫ УПРАВЛЕНИЯ ДВИЖЕНИЕМ ПЕРСПЕКТИВНОГО РТК ВН В РЕЖИМЕ АВТОНОМНОГО НАВЕДЕНИЯ THE METHOD OF SYNTHESIS OF A TRACKING MOTION CONTROL SYSTEM OF A PROMISING RC MP IN THE AUTONOMOUS GUIDANCE MODE

Елена Юрьевна Пушкарёва

доктор технических наук, профессор
профессор кафедры
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл., г. Серпухов, ул.
Бригадная, д. 17
Тел.: 8 (915) 192-74-39.
E-mail: calgon100@yandex.ru

Игорь Викторович Пискулин

преподаватель
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл., г. Серпухов, ул.
Бригадная, д. 17
Тел.: 8 (925) 725-06-36.
E-mail: piksel.zte@gmail.com

Аннотация

Предложена структурная схема системы управления движением РТК ВН в режиме автономного наведения. Обоснован алгоритм определения структуры и параметров следящей системы автоматического управления движением РТК ВН по курсу, эквивалентной комбинированной системе. На основе проведенного моделирования представлены результаты анализа точности одноконтурных и двухконтурных систем автоматического управления, эквивалентных комбинированным системам, движением РТК ВН.

Ключевые слова

Робототехнический комплекс военного назначения, система автоматического управления движением, угол курса; устойчивость, точность.

Summary

A block diagram of the RC MP motion control system in the autonomous guidance mode is proposed. The algorithm for determining the structure and parameters of the tracking system of automatic motion control of the RC MP at a rate equivalent to the combined system is substantiated. Based on the conducted modeling, the results of an analysis of the accuracy of single-circuit and double-circuit automatic control systems equivalent to combined systems for the movement of RC MP are presented.

Keywords

Robotic complex for military purposes, automatic motion control system, course angle, stability, accuracy.

Введение

На протяжении последних двадцати лет мирового развития вооружения и военной техники (ВВТ) проблема их роботизации приобрела не только роль ключевого научно-технологического направления, но и стала одним из центральных звеньев в новых концептуальных подходах к формированию вооруженных сил, способам их боевого применения, развитию средств вооруженной борьбы и средств обеспечения. Как показывает отечественный и зарубежный опыт создания перспективных образцов ВВТ, непременным и обязательным условием успешного развития средств военной и специальной ро-

бототехники является своевременное создание научно-технического задела, являющегося базой для новых разработок и производства – как совокупность потенциальных инноваций, которые могут обеспечить создание перспективных робототехнических комплексов. Внедрение подобных инноваций позволяет обеспечить решение принципиально новых военно-технических и специальных задач и существенный прирост тактико-технических характеристик робототехнических комплексов [1,2].

В результате обобщения накопленного опыта при создании робототехнических комплексов, а также с учетом выбранного направления

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

роботизации существующих образцов военной техники, создана концепция создания унифицированной системы управления (СУ) робототехническими комплексами.

В состав данной системы управления предлагается включить следующие подсистемы:

- центральная вычислительная система;
- система связи и передачи данных;
- система электропитания;
- система управления движением;
- система технического зрения;
- система навигации;

● полезная нагрузка, в которую может войти боевой модуль, модуль разведки, модуль минирования/разминирования и др. [1].

В данной работе проводится исследование одной из указанных подсистем, а именно системы автоматического управления движением РТК ВН. Необходимость данного исследования вызвана возможным применением РТК в целях выполнения охранных функций для обеспечения безопасности объектов Ракетных войск стратегического назначения (РВСН) от воздействия диверсионно-разведывательных и террористических групп противника [3-6].

В условиях, позволяющих измерительным средствам, средствам распознавания, которые размещены на платформе РТК ВН, осуществлять функции по обнаружению нарушителей в охраняемой зоне, требуется иметь следящую автоматическую систему. Указанная система должна осуществлять функции сопровождения за перемещением объекта вторжения в охраняемую зону и автономного наведения РТК на цель (преследования цели) [3-5].

С учетом вышеуказанных обстоятельств предложен новый способ управления движением РТК ВН по курсу с использованием методов построения САУ движением РТК ВН с улучшенными показателями качества управления:

- автономное наведение может быть реализовано с помощью следящего управления, основанного на методе двухконтурных систем, эквивалентных комбинированным системам [7,8], с достижением инвариантности ошибки относительно задающего воздействия без влияния на устойчивость одноконтурной САУ.

Целью работы является повышение тактико-технических характеристик (точности) системы управления движением наземных робототехнических комплексов военного назначения (РТК ВН) гусеничного типа на основе применения метода построения двухконтурных систем автоматического управления, эквивалентных комбинированным системам.

1. Условия получения инвариантности в одноконтурных и двухконтурных системах автоматического управления, эквивалентных комбинированным системам

Задачей исследования является возможность достижения нулевой ошибки в одноконтурных и двухконтурных системах автоматического управления движением РТК. Для решения данной задачи необходимо определить структуру САУ и составить структурные схемы систем автоматического управления движением РТК ВН по углу курса. Данная задача может быть решена поэтапно. В ходе первого этапа рассматривается связь ошибок управления в одноконтурных системах автоматического управления с постоянным или линейным входными воздействиями. Следующим этапом является обоснование построения двухконтурных систем с учетом линейного входного воздействия. Далее необходимо определить параметры второго контура двухконтурной САУ движением РТК. В ходе решения задачи рассматривается связь динамической ошибки управления в двухконтурных САУ движением РТК по углу курса с линейным входным воздействием.

Робототехнический комплекс при выполнении охранных функций должен выполнять задачи обнаружения и распознавания целей в автоматическом режиме. Более простым способом управления движением РТК является случай, при котором скорость перемещения цели равна нулю, так как она неподвижна. В этом случае угол ψ_w курса должен являться величиной постоянной и равной углу цели $\psi_u = const$.

Структурная схема САУ движением РТК по углу курса в случае, при котором можно добиться нулевой ошибки, представлена в виде одноконтурной системы на *рисунке 1*.

Передаточные функции регулятора, привода и шасси определяются следующими выражениями [9]:

$$W_{pvc1}(P, \alpha) = K_{pvc} K(\alpha), \quad W_{np}(P, \alpha) = K_s K_\phi W(\alpha) / (1 + T_s P)(1 + T_\phi P), \quad (1)$$

$W_w(P) = K_w / (1 - T_w P)$, $K(\alpha) = 1/\alpha - 1$, $W(\alpha) = \alpha - 1$, $\alpha > 1$, где K_s , K_ϕ , K_w – коэффициенты усиления электромашиного усилителя, электродвигателя и шасси соответственно;

T_s , T_ϕ , T_w – их постоянные времени.

Следует отметить, что переменные коэффициенты $K(\alpha)$ и $W(\alpha)$ были получены на основе теории чувствительности при минимизации функций чувствительности САУ углом курса [9].

Передаточная функция разомкнутой системы управления углом курса с переменными параметрами будет определяться следующим выражением:

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

$$W_p(P, \alpha) = K_{ny} K_{pec} K_s K_d K_u K(\alpha) W(\alpha) / ((1 + T_s P)(1 + T_d P)(1 + T_u P)P) \quad (2)$$

где $K_v = K_{ny} K_{pec} K_s K_d K_u$ – коэффициент усиления САУ по скорости.

С учетом заданных входных полезных воздействий, выражение для установившихся ошибок ($t \rightarrow \infty, P \rightarrow \infty$) примет вид:

$$\varepsilon_\psi = D_0 \psi_u + D_1 d\psi_u/dt, \quad (3)$$

где $D_0 = W_\varepsilon(P)|_{P=0}$ – коэффициент ошибки по положению;

$D_1 = dW_\varepsilon(P)/dP|_{P=0}$ – коэффициент ошибки по скорости.

Исходя из того, что угол курса движения цели является величиной постоянной, т.е. $\psi_u = const$, то установившаяся ошибка будет равна только ошибке по положению ε_0 . Выражение для определения указанной ошибки примет вид:

$$\varepsilon_0 = D_0 \psi_u. \quad (6)$$

В соответствии со схемой рисунка 1 одноконтурная САУ имеет интегрирующее звено (порядок астатизма системы v равен единице). В САУ с астатизмом первого порядка коэффициент ошибки по положению равен нулю ($D_0 = 0$). Следовательно, в соответствии с выражением (6) ошибка по положению будет равна нулю, т.е.:

$$\varepsilon_0 = D_0 \psi_u = 0. \quad (7)$$

Исходя из вышесказанного и выражения (7) следует, что в одноконтурной САУ движением РТК ВН по курсу, структура которой представлена на рисунке 1, можно добиться нулевой ошибки воспроизведения угла курса только при постоянном входном воздействии.

Робототехнический комплекс в режиме слежения должен выполнять задачу по обнаружению двигающейся цели. При указанных выше условиях скорость передвижения цели не равна нулю (цель перемещается), соответственно угол курса изменяется с течением времени, т.е. $\psi_u(t) = \psi_0 + \psi'_u(t)$. Это, в свою очередь, затрудняет задачу управления движением РТК ВН в соответствии со структурной схемой, представленной на рисунке 1.

Добиться выполнения условия получения нулевой ошибки по скорости возможно повышением порядка астатизма представленной системы с первого порядка до второго порядка ($v=2$), если поставить еще один интегратор в разомкнутый канал схемы (рисунк 1). Однако в данном случае возникают проблемы с обеспечением устойчивости замкнутой системы, что следует из

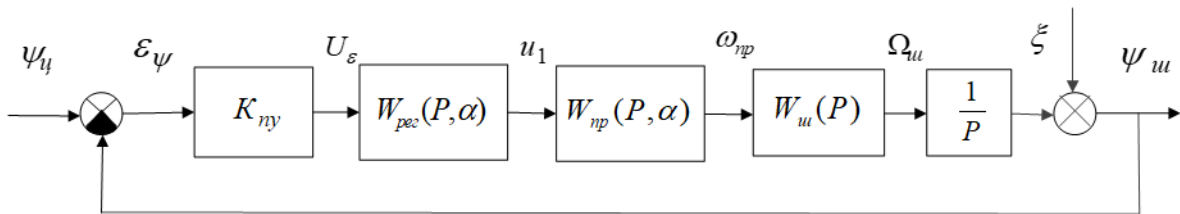


Рис. 1. Структурная схема одноконтурной САУ движением РТК по курсу. На схеме обозначены: ψ_u – угол курса цели; ε_ψ – ошибка воспроизведения угла курса; U_ε – сигнал от пеленгационного устройства; u_1 – управление по ошибке; ω_{np} – угловая скорость вала электродвигателя; Ω_w – угловая скорость поворота шасси; ξ – возмущающее воздействие; ψ_w – угол курса движения РТК; $W_{pec}(P, \alpha), W_{np}(P, \alpha), W_w(P)$ – передаточные функции регулятора, привода и шасси РТК соответственно, причем первые две из них – это параметрические передаточные функции. Пеленгационное устройство характеризуется усилительным звеном с коэффициентом усиления K_{ny} .

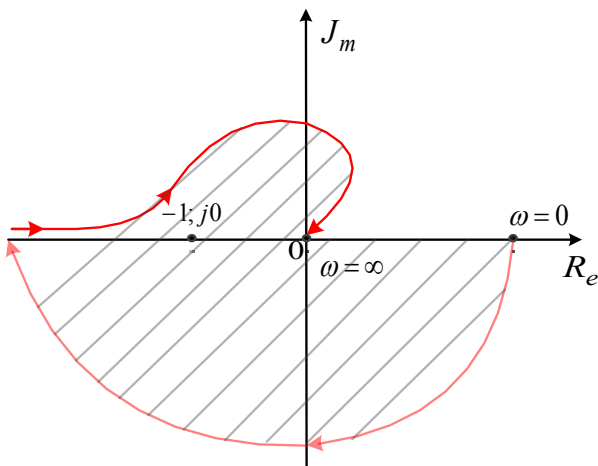


Рис. 2. К иллюстрации АФХ разомкнутой САУ второго порядка астатизма

построения амплитудно-фазовой характеристики (АФХ) разомкнутой системы (рисунк 2).

Как видно из рисунка 2, увеличение астатизма на единицу в схеме системы управления (т.е. включение в разомкнутый канал еще одного интегрирующего звена) приводит к ее неустойчивости, выйти из которой путем изменения параметров $K_{ny} K_{pec} K_s K_d K_u$ не представляется возможным.

Включение в разомкнутый канал управления форсирующих контуров не снимет проблему устойчивости в ситуациях, когда есть помехи и возмущения, которые приводят к увеличению случайных ошибок при введении указанных контуров (т.е. производных).

Повышение порядка астатизма, приводящее к выполнению требования нулевой скорости

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ной ошибки без нарушения устойчивости замкнутого контура, можно добиться в регуляторе второго контура двухконтурной системы, эквивалентной комбинированной автоматической системе.

Для получения комбинированного управления u_κ необходимо иметь две составляющие:

$$u_\kappa = u_1(\varepsilon) + u_2(\varepsilon), \quad (8)$$

где составляющая u_1 зависит от ошибки ε (первый контур), а u_2 от задающего воздействия ψ_u (второй контур).

На рисунке 3 представлена структурная схема двухконтурной системы автоматического управления, эквивалентная комбинированной системе.

В двухконтурной САУ, эквивалентной комбинированной системе, условие инвариантности ошибки относительно входного воздействия, имеет вид [7]:

$$A_1(P, \alpha)[C_{\text{пер}2}(P) - B_{\text{пер}2}(P)P^{-v}] = 0, \quad (9)$$

а характеристическое уравнение определяется следующим выражением

$$C_1(P, \alpha)C_{\text{пер}2}(P) = 0. \quad (10)$$

Здесь отношение полиномов $B_{\text{пер}2}(P)/C_{\text{пер}2}(P) = W_{\text{пер}2}(P)$, а полином $C_1(P, \alpha)$ является характеристическим полиномом первого контура; при этом полином $A_1(P, \alpha)$ – полином числителя ПФ по ошибке первого контура.

Отсюда видно, что указанная инвариантность может быть достигнута с помощью полинома $B_{\text{пер}2}(P)$, который не входит в характеристическое уравнение и, следовательно, не влияет на устойчивость.

Поэтому параметрическая ПФ двухконтурной системы по ошибке

$$W_{\varepsilon}^{(2)}(P, \alpha) = A_1(P, \alpha)[C_{\text{пер}2}(P) - B_{\text{пер}2}(P)P^{-v}] / C_1(P, \alpha)C_{\text{пер}2}(P). \quad (11)$$

Полученное выражение (11) для САУ рисун-

ка 3 позволяет выполнить критерий повышения точности управления движением РТК ВН по курсу без потери устойчивости первого контура.

2. Синтез структуры и параметров регуляторов следящей системы автоматического управления углом курса РТК ВН

Математическое условие достижения инвариантности ошибки следует из выражения (11) и с учетом входного воздействия примет вид:

$$[C_{\text{пер}2}(P) - B_{\text{пер}2}(P)P^{-v}]\psi_u(P) = 0. \quad (12)$$

В дальнейшем, для сокращения вычислительных процедур, примем регулятор второго контура первого порядка.

В связи с этим полиномы регулятора второго контура примут вид:

$$\begin{aligned} B_{\text{пер}2}(P) &= b_0 + b_1P, \\ C_{\text{пер}2}(P) &= c_0 + c_1P. \end{aligned} \quad (13)$$

Подставляя указанные полиномы в (12) и учитывая, что $v=1$, выражение в квадратных скобках примет вид:

$$c_0 + c_1P - b_0/P - b_1. \quad (14)$$

Учитывая, что в данной разности не должно быть членов с отрицательными степенями P , необходимо положить $b_0 = 0$.

Кроме того, исходя из требования повышения порядка астатизма на один порядок, необходимо положить $b_1 = c_0$, что превратит эту разность в одночлен c_1P .

В связи с этим, параметрическая ПФ (11) по ошибке двухконтурной системы примет вид:

$$W_{\varepsilon}^{(2)}(P, \alpha) = A_1(P, \alpha)c_1P / C_1(P, \alpha)(c_0 + c_1P). \quad (15)$$

С учетом наличия в полиноме $A_1(P, \alpha)$ свободного оператора P , а также аналогичного оператора при коэффициенте c_1 , получим в числителе ПФ по ошибке второго контура оператор P^2 . Следовательно двухконтурная САУ будет иметь

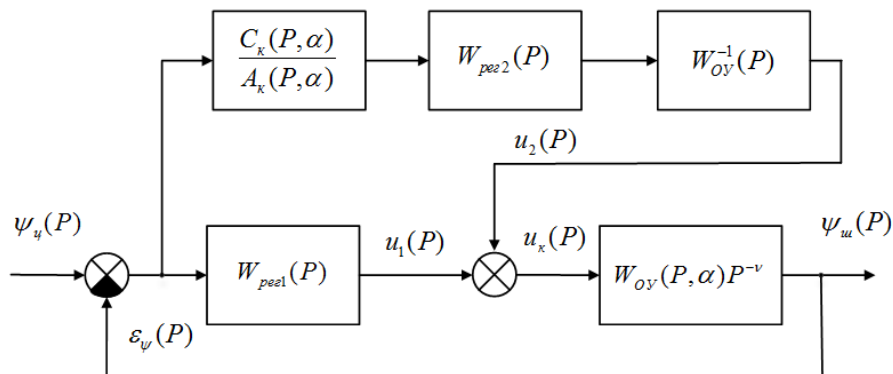


Рис. 3. Структурная схема двухконтурной системы автоматического управления углом курса РТК. На схеме обозначены: $C_\kappa(P, \alpha)/A_\kappa(P, \alpha)$ – ПФ идентификатора, равная обратной ПФ по ошибке комбинированной системы; $W_{ouy}^{-1}(P)$ – ПФ инвертора (обратная ПФ ОУ без учета интегрирующего звена); ψ_u – входное воздействие; u_1 – управляющее воздействие, формируемое первым контуром; u_2 – управляющее воздействие, формируемое вторым контуром; u_κ – комбинированное управляющее воздействие; ψ_u – выходное воздействие

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

второй порядок астатизма.

При этом ПФ самого регулятора второго контура определяется в соответствии с выражением:

$$W_{\text{рег2}}(P) = B_{\text{рег2}}(P) / C_{\text{рег2}}(P) = b_1 P / c_0 + c_1 P. \quad (16)$$

Полином знаменателя регулятора второго контура входит в характеристический полином всей двухконтурной САУ:

$$C_{\kappa}(P, \alpha) = C_1(P, \alpha)(c_0 + c_1 P). \quad (17)$$

Для устойчивости двухконтурной САУ (при условии, что полином $C_1(P, \alpha)$ также устойчив), необходимо иметь выражение для определения корня характеристического уравнения второго регулятора, т.е.

$$c_0 + c_1 P = 0 \Rightarrow P_1 = -c_0 / c_1 < 0. \quad (18)$$

Для того, чтобы корень P_1 находился на большем удалении от мнимой оси необходимо иметь условие $c_1 \ll c_0$.

С учетом вышеуказанных выражений, а также нормировки системы по коэффициенту α , можно записать более полное выражение для ПФ по ошибке двухконтурной САУ углом курса:

$$W_{\varepsilon}^{(2)}(P) = (1 + T_s P)(1 + T_0 P)(1 + T_w P) c_1 P^2 / [(1 + T_s P)(1 + T_0 P)(1 + T_w P) P + K J (c_0 + c_1 P)]. \quad (19)$$

Следовательно, система стала иметь второй порядок астатизма. Как показано в [5], для САУ с передаточной функцией (20) коэффициенты динамических ошибок имеют вид: $D_0 = 0$, $D_1 = 0$. Следовательно, ошибка по положению ε_0 будет равна нулю, и ошибка по скорости ε_v будет равна нулю.

Поэтому, в двухконтурных САУ углом курса РТК, эквивалентных комбинированным системам, при линейном законе входного воздействия возможно достижение инвариантности ошибки (сведение ее к нулю без влияния на устойчивость).

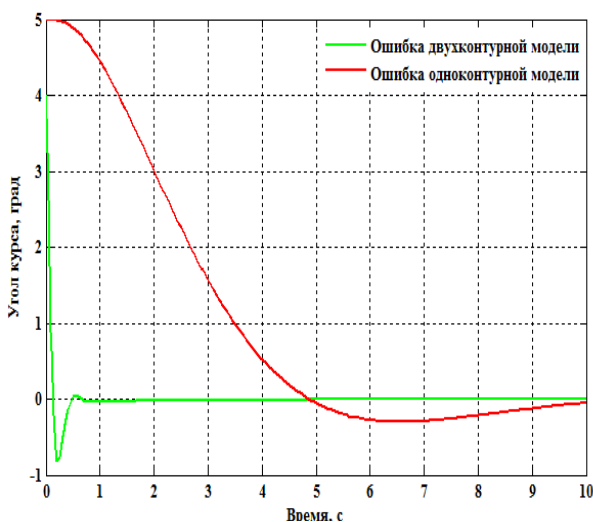


Рис. 4. К иллюстрации ошибки воспроизведения угла курса при постоянном входном воздействии

3. Исследование моделей одноконтурных и двухконтурных систем автоматического управления, эквивалентных комбинированным системам движением РТК ВН

В основу исследования точности моделей САУ движением РТК приняты структурные схемы одноконтурной САУ углом курса, изображенной на рисунке 1 и двухконтурной САУ, эквивалентной комбинированной системе, изображенной на рисунке 3. Параметры схем заданы исходными данными, определяемыми в [10,11].

Графики установившейся ошибки воспроизведения угла курса одноконтурной САУ и двухконтурной САУ движением РТК, эквивалентной комбинированной системе при различных входных воздействиях представлены на рисунке 4.

В соответствии с представленными графиками (рисунки 4 и 5) можно выявить следующее:

1) для модели двухконтурной САУ движением РТК по углу курса, эквивалентной комбинированной системе, в целях достижения установившегося значения нулевой ошибки требуется значительно меньше времени переходного процесса (примерно в 10 раз, что видно по рисунку 4), т.е. создается возможность повышения быстродействия отработки угла курса.

2) при исследовании модели двухконтурной САУ движением РТК по углу курса, эквивалентной комбинированной системе, значение установившейся ошибки воспроизведения угла курса в условиях различных значений линейного входного воздействия равно нулю.

Заключение

В связи с вышеописанными обстоятельствами использование модели САУ движением РТК

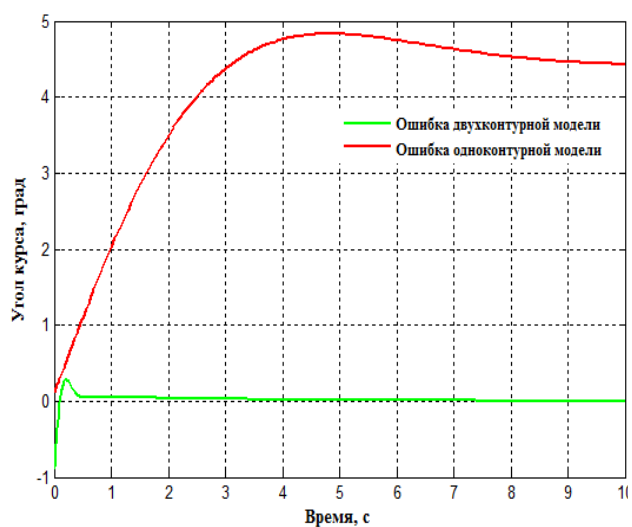


Рис. 5. К иллюстрации ошибки воспроизведения угла курса при линейном входном воздействии

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

ВН по курсу, для построения которой применяется метод двухконтурных систем автоматического управления, эквивалентных комбинированным системам, позволяет, кроме достижения инвариантности ошибки с соблюдением требования к устойчивости системы, повысить быстродействие. Таким образом, осуществляется выполнения критерия вида «точность плюс оперативность». Применение системы автоматического управления движением РТК на основе указанных моделей, как подсистемы, повышает точность и оперативность работы всей системы управления РТК ВН.

Литература

1. Лапшов В.С., Носков В.П., Рубцов И.В. Опыт создания автономных мобильных робототехнических комплексов специального назначения // Вестник МГТУ им. Н.Э. Баумана. «Специальная робототехника и мехатроника», 2011. С.7-24.
2. Рубцов И.В. Вопросы состояния и перспективы развития отечественной наземной робототехники военного и специального назначения // Избранные труды Всероссийской научно-практической конференции «Перспективные системы и задачи управления», 2015. Т. II. С.64-70.
3. Свиридов В.В., Пушкарёв Ю.А. Модель оценки качества характеристик робототехнического комплекса для обнаружения нарушителей в лесистой местности // МГТУ им. Н.Э.Баумана, 2021. №(29). С.77-90.
4. Пушкарёв Ю.А., Свиридов В.В. Метод распознавания объектов на основе их сигнально-геометрических признаков средствами робототехнического комплекса охраны // Математическое моделирование и численные методы, 2022. Т.34. №9. С.88-106.
5. Свиридов В.В. Применение робототехнических комплексов охраны и обороны критически важных объектов Ракетных войск стратегического назначения // Военная мысль, 2021. №6. С.57-64.
6. Фазлетдинов И.Р. Перспективы применения робототехнических комплексов военного назначения в интересах Ракетных войск стратегического назначения // Военная мысль, 2022. №5. С.105-111.
7. Пушкарёв Ю.А., Пушкарёва Е.Ю. Задачи и методы синтеза следящих и терминальных автоматических систем в ракетно-космической технике. М.: Машиностроение. Полет, 2022. 647 с.
8. Пушкарёв Ю.А., Пушкарёва Е.Ю. Системы автоматического управления в ракетно-космической технике. Задачи слежения и терминального управления. Монография. Серпухов: ФВА РВСН им. Петра Великого, 2020. 379 с.
9. Пушкарёв Ю.А., Пушкарёва Е.Ю., Пискулин И.В. Управление робототехническим комплексом по углу курса на основе метода разности скоростей // Известия Института инженерной физики, 2022, №4(66). С. 45-51.
10. Пушкарёва Е.Ю., Пискулин И.В. Методика определения параметров следящей системы управления движением РТК ВН в режиме автономного наведения // Известия ЮФУ. Технические науки, 2023. №1. С.88-100.
11. Пискулин И.В. Исследование точности моделей следящей системы управления движением РТК ВН в режиме автономного наведения // Известия ЮФУ. Технические науки, 2023. №2. С. 137-148.



УДК 004.89

ВЫБОР И ИНТЕГРАЦИЯ ПРИЗНАКОВ ДЛЯ НЕПРЕРЫВНОЙ АДАПТИВНОЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ СМАРТФОНА FEATURE SELECTION AND INTEGRATION FOR CONTINUOUS ADAPTIVE MULTI-FACTOR AUTHENTICATION OF A SMARTPHONE USER

Алексей Игоревич Бугаков

старший специалист
группы тестирования и отладки комплексов
АНО «Институт инженерной физики»
Адрес: 142210, Московская обл., г. Серпухов,
Большой Ударный пер., д. 1а
Тел.: +7(4967) 35-31-93
E-mail: aibugakov@iifmail.ru

Михаил Михайлович Шульга

аспирант
АНО «Институт инженерной физики»
Адрес: 142210 Московская обл., г. Серпухов,
Большой Ударный пер., д. 1а
Тел.: +7 (4967) 35-31-93
E-mail: mmshulga@yandex.ru

Аннотация

Рассматриваются особенности выбора и интеграции в фоновом режиме связанных с пользователем смартфона признаков для проведения его непрерывной адаптивной многофакторной аутентификации с целью исключения доступа к смартфону несанкционированных пользователей.

Ключевые слова: смартфон, пользователь, условия применения, признаки, интеграция, пороги, непрерывная фоновая аутентификация, допуск, адаптация, искусственный интеллект, вероятность, стандартизация, датчик, радиоканал, привязка, дообучение, оповещение.

Summary

The features of selecting and integrating features associated with the smartphone user in the background for continuous adaptive multifactor authentication in order to exclude unauthorized users from accessing the smartphone are considered.

Keywords: smartphone, user, conditions of use, signs, integration, thresholds, continuous background authentication, admission, adaptation, artificial intelligence, probability, standardization, sensor, radio channel, binding, additional training, notification.

В настоящее время аутентификация пользователя смартфона (СМ) осуществляется при его разблокировке с использованием первичного идентификатора, а также при вхождении в то или иное приложения (на тот или иной ресурс). При этом она может быть многофакторной, чаще всего – двухфакторной с обратной связью от приложения (ресурса). Однако этого явно недостаточно для гарантированного исключения несанкционированного доступа к хранимой в СМ информации и реализуемым им функциям, поскольку после получения доступа к информации (ресурсу) СМ, дальнейшие действия с ним может совершать любой человек. Очевидным решением данной проблемы является реализация непрерывной фоновой аутентификации пользователя.

На такой способ аутентификации пользо-

вателя электронного мобильного многофункционального устройства (смартфон – частный случай) была подана заявка на изобретение и к настоящему времени получено положительное решение на выдачу патента [1]. Этот способ описан в прошлом выпуске журнала [2].

В заявленном способе осуществляется непрерывная аутентификация пользователя, которая:

- не мешает использованию СМ по своему назначению;
- является многофакторной по возможностям регистрации связанных с пользователем признаков и адаптивной по их использованию, учитывающей параметры окружающей среды, текущие выполняемые задачи, технические возможности и техническое состояние СМ, включая оставшийся заряд аккумуляторной батареи;
- гарантирует исключение доступа к инфор-

мации и функциям СМ несанкционированных пользователей во всех возможных случаях, включая потерю СМ, его похищение (кражу или отъем) с информированием пользователя и (или) организации, выдавшей пользователю СМ, о наступлении таких случаев;

- носит вероятностно-пороговый характер для допуска к разным функциям (сервисам). Исходя из различного потенциального риска несанкционированного доступа с учетом условий применения СМ, задаются адаптивно изменяемые пороговые значения вероятностей аутентификации для допуска к различным функциям (сервисам);

- является максимально автономной (с минимальным обращением к хранимой вне СМ конфиденциальной информации);

- основывается на использовании датчиков (сенсоров) и вычислительных возможностей как СМ, так и находящихся при пользователе и связанных со СМ по радиоканалу дополнительных электронных устройств.

При необходимости, санкционированный пользователь (СП) может экстренно заблокировать доступ к разблокированному СМ (например, в случае принуждения к совершению недопустимых операций) посредством заранее определенного и отработанного при привязке СМ к СП действия (например, произнесения кодового слова или совершения особого жеста). Или даже стереть всю хранимую на нем информацию. А СМ в случае недостаточности для текущей аутентификации регистрируемой информации – «попросить» СП совершить то или иное, адаптированное к ситуации, действие.

Привязка СМ к пользователю заключается в предварительном обучении СМ адаптивному, удовлетворяющему вышеперечисленным свойствам, распознаванию пользователя в различных, соответствующих будущим реальным, условиях эксплуатации. А в процессе эксплуатации автоматически осуществляется дообучение СМ, улучшающее качество распознавания за счет накопления дополнительного опыта, учета возможных частичных изменений связанных с СП признаков.

Эффективность реализации способа во многом определяется способностью СМ и находящихся при пользователе дополнительных электронных устройств адаптивно (для тех или иных условий) выбирать наиболее информативные (из всех доступных для регистрации), связанные с пользователем признаки, минимизируя как их количество, так необходимые для их регистра-

ции и обработки вычислительные и энергетические затраты. В качестве классов таких признаков используется классическая триада: чем пользователь является, что он знает (умеет) и чем он владеет.

1. В качестве признаков пользователя, отражающих то, чем он является, могут использоваться статические и динамические физиологические и поведенческие биометрические признаки пользователя: тембр и спектр голоса, фото- и видеоизображения лица или его частей (уха, носа, губ), отпечаток пальца, рисунок радужной оболочки или (и) сетчатки глаза, рисунок сосудов лица (его частей) или сосудов руки (ладони), геометрия кисти руки, форма и геометрия ушной раковины, параметры пульса (частота, ритмичность, напряжение), размеры (форма) и динамика сердца, электрическая активность сердца (параметры электрокардиограммы), параметры электроэнцефалограммы или ее части, издаваемый пользователем запах, химический состав выдыхаемого пользователем воздуха, динамика движения тела при ходьбе (походка), динамика движения руки с СМ, подписи, набора букв на виртуальной клавиатуре СМ, микровибрации пальцев и др. – все те признаки, физическая реализация и эффективность применения которых в настоящее время экспериментально подтверждена¹.

2. Знания и умения пользователя выражаются в знании им заранее (при обучении СМ) установленных кодовых слов или фраз, мелодий, жестов, поз, мимических образов и пр. и умении их правильно воспроизвести в нужных ситуациях.

3. Владение отражает наличие у пользователя предметов, позволяющих формировать уникальные сенсорные образы (визуальные, звуковые, обонятельные, электромагнитные и др.).

Превышение расстояния между СП и СМ, регистрируемое посредством находящейся при СП RFID-метки, приводит к блокировке СМ с необходимым оповещением. Дополнительно может диагностироваться психофизиологическое состояние СП. Например, посредством регистрации сердечного ритма можно не только определять СП, но и в каком психофизиологическом состоянии он находится, что позволяет автоматически блокировать СМ в случае внезапного ухудшения состояния СП, в том числе в случае психического воздействия на него со стороны нарушителя. В качестве признака можно использовать местонахождение. Так, при нахождении СП в офисе организации, выдавшей ему СМ, или в своей квартире для допуска к СМ

¹ В [3] биометрические признаки, отсутствующие в общедоступных базах данных, именуются «тайными».

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И РОБОТОТЕХНИКА

может быть достаточным пройти первичную аутентификацию. А в других местах может, наоборот, включаться запрет на разблокировку СМ. Может учитываться текущее время суток.

Тогда задачу аутентификации пользователя в общем плане можно рассматривать и как задачу диагностики, используя два состояния: «норма» (СП+СМ), когда СМ находится у СП, и «не норма», когда пользователь СМ определен как несанкционированный (НСП) и (или) СМ находится от СП на недопустимом расстоянии (СП-СМ), см. *рисунок 1*.

Реализация вышерассмотренного невозможно без использования технологий искусственного интеллекта (ИИ), включающих в себя как технологию машинного обучения на основе искусственных нейронных сетей, так и основанную на тех или иных «моделях мира» и несущую «настоящее» понимание технологии классического, оперирующего знаниями, символического ИИ [4].

Каждый используемый для распознавания признак можно характеризовать рядом свойств, в частности: информативностью (уникальностью, значимостью), достоверностью (надежностью), стабильностью (инвариантностью), защищенностью от компрометации, «стоимостью» (аппаратной сложностью регистрации и обработки в различных условиях, потребляемой для регистрации и обработки энергией, временем распознавания при заданной производительности вычислений). Выбор признаков зависит

и от величин допускаемых при их регистрации и обработке ошибок первого (FRR) и второго (FAR) рода, которые, в свою очередь, зависят от величины задаваемых порогов и влияют на них. Например, как утверждается в [5], среди статических биометрических признаков в настоящее время наименьшими значениями ошибок FRR и FAR обладает способ аутентификации по радужной оболочке глаза (0,016% и 0,00001% соответственно²), в то время как значения этих параметров для распознавания по 2D лицу составляет недопустимые 2,5% и 0,1%. Однако и «стоимость» распознавания по «радужке» наиболее высокая. Очевидно, что, учитывая различные параметры и свойства признаков, в реальных условиях может быть целесообразным их адаптивное объединение, тем более, что наличие корреляционных связей между несколькими признаками³ позволяет формировать интегральный мета-признак, который, как утверждается в [6], в 2-3 раза информативнее случая их отдельного учета.

В [7] применительно к мультибиометрии выделяют пять категорий: мультимодальную, мультиалгоритмическую, мультиэкземплярную, мультидатчиковую и мультипредставление. Там же рассмотрены четыре уровня комбинирования (объединения) в мультибиометрических системах: уровень образцов, поступающих на вход; уровень признаков, извлекаемых из образцов; уровень степеней схожести, формируемых после сопоставления извлеченных признаков с



Рис. 1. Схема процесса аутентификации пользователя смартфона

² В соответствии с [3] аутентификацию с такими показателями можно отнести к высоконадежной биометрической аутентификации, под которой понимается «биометрическая аутентификация с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора».

³ В том числе физическими: например, между речью и движением губ или между размером ладони и лица.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И РОБОТОТЕХНИКА

заранее заданными шаблонами; уровень принятия решения, на котором объединяются ранее принятые решения по каждому рассмотренному образцу. Заметим, что использование уровневого подхода в таком же или даже расширенном виде⁴ целесообразно и при аутентификации пользователя СМ. Варианты объединения для нескольких признаков могут быть различными⁵. В общем случае при объединении учитываются достоверности частных результатов.

В зависимости от условий применения и возможностей СМ регистрация и обработка признаков может осуществляться как последовательно, так и параллельно. При последовательном представлении признаков решение о распознавании формируется в случае достижения вычисляемыми показателями (чаще всего – вероятностями) заданных пороговых значений, что может произойти и при представлении только одного признака. Если же пороговые значения не достигнуты, то рассматривается второй признак с последующим оцениванием преодоления заданных порогов или только с учетом этого второго признака, или его комбинации с первым признаком. При параллельном представлении вероятность распознавания каждого признака должна преодолеть заданное (для каждого признака свое) пороговое значение. Очевидно, что дальнейшим развитием может быть последовательно-параллельное представление. В целом, процесс принятия решения о порядке представления признаков целесообразно рассматривать как процесс оптимизации с учетом всех влияющих факторов.

Отметим, что вопросы использования биометрии для аутентификации пользователей мобильных устройств только в последние годы становятся объектом стандартизации в РФ. С июня 2020 года действует предварительный национальный стандарт [8]⁶, в котором изложены рассуждения о некоторых процессах применения биометрии в мобильных устройствах (в том числе – о возможности повышения общего уровня надежности посредством объединения модальностей) и формируемых показателей (уровни доверия и безопасности, показатели и пороги качества). Между тем вопросы исполь-

зования биометрии для аутентификации давно находятся в поле внимания Росстандарта (серии Р 58668, Р ИСО/МЭК 19794 и др.). Но в этих стандартах, на наш взгляд, присутствует излишнее терминологическое «разнообразие»⁷. Так, в [8] есть понятия: качество и точность источника образца, точность воспроизведения образцом источника, полезность образца, уровни (степени) и показатели полезности, качество алгоритма, показатели качества, схожесть показателей и др., наполнение которых общепринятыми смыслами проблематично. Требуется уточнение и минимизация понятийного аппарата.

При реализации непрерывной адаптивной многофакторной аутентификации целесообразно использовать все возможные группы признаков (детерминированные, вероятностные, логические, структурные, а также их комбинации), см. *таблицу 1*.

Совокупность всех признаков каждой группы («знаю», «являюсь», «имею») создает свое признаковое (статическое и (или) динамическое) пространство⁸, каждое из которых формируется на основе обработки соответствующего пространства наблюдений и после нормировки является основой для получения соответствующего пространства решений, совместная дальнейшая обработка которых позволяет сформировать итоговое решение.

Классический подход к процессу распознавания основывается на математической или физико-математической модели системы распознавания, построение которой требует решение следующих задач (приведено с учетом изложенного в [9]):

- определение полного перечня признаков пользователя;
- выбор принципа классификации;
- разработка априорного словаря признаков;
- описание пользователя СМ на языке признаков, включенных в априорный словарь (например, эталонов для детерминированных признаков);
- оптимальное разбиение априорного пространства признаков на классы «свой», «чужой»;
- разработка алгоритма распознавания с использованием той или иной меры близости (на-

⁴ Например, когда на уровне признаков и уровне схожести объединяется лишь часть информации с последующим итоговым объединением на уровне принятия решения.

⁵ Например, для уровня принятия решения наиболее простое объединение может быть реализовано с использованием схемы голосования на основе логических функций «И», «ИЛИ» [7].

⁶ Перевод ISO/IEC TR 30125:2016 «Information technology – Biometrics used with mobile devices»

⁷ Вероятнее всего, как следствие необходимости соответствия международному стандарту.

⁸ Очевидно, что первая группа признаков наиболее, а третья – наименее защищена от компрометации, причем в рамках каждой группы также можно выделить признаки разной защищенности.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И РОБОТОТЕХНИКА

Таблица 1
Признаки и способы их распознавания

Признаки	Способ распознавания
Детерминированные	Использование геометрических мер близости между распознаваемым признаками пользователя и их эталонами
Вероятностные	Использование вероятностных (на основе вероятностной меры близости) зависимостей между признаками и классом
Логические	Логический – на основе дискретного анализа и базирующегося на нем исчисления высказываний
Структурные	1. Учет взаимосвязи признаков, их весового влияния, формирование интегрального признака. 2. Обнаружение атомарных (непроизводных) элементов (признаков) и отношений между ними с последующим проведением синтаксического анализа (грамматического разбора) с целью установления грамматики, породившей такую структуру
Комбинированные	Специальные методы вычисления оценок с использованием таблицы с признаками (детерминированными, вероятностными, логическими, структурными) объекта «свой» (при необходимости – и «чужой»)

пример, среднеквадратичного расстояния для детерминированных признаков);

- определение рабочего словаря признаков как части априорного словаря, позволяющего с учетом ограничений (условия применения, возможности и состояние СМ и других находящихся при СП электронных средств), исключающих возможность использования части признаков, достичь максимального значения показателя эффективности (качества) распознавания;

- разработка алгоритма управления работой системы распознавания.

Для извлечения признаков в рамках нейросетевого подхода целесообразно использовать автокодировщик с различными (в зависимости от признаков) слоями (сверточными, рекуррентными и др.). Большими потенциальными возможностями обладает метаграмматический подход [10], объединение которого с методами нейросетевого машинного обучения является перспективным направлением разработки «настоящего» (понимающего) искусственного интеллекта.

Литература

1. Положительное решение Роспатента от 01.02.2024 на выдачу патента по заявке №2022126590/07 (058037) «Способ защиты электронного многофункционального мобильного устройства от несанкционированного доступа». Авторы: Бугаков А.И., Бугаков И.А., Царьков А.Н., Шульга М.М. Патентообладатель – АНО «Институт инженерной физики».
2. Бугаков А.И., Бугаков И.А., Царьков А.Н., Шульга М.М. Способ непрерывной адаптивной многофакторной аутентификации пользователя

смартфона // Известия Института инженерной физики, 2024. №1(71). С.94-101.

3. ГОСТ Р 52633.0 – 2006 «Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации». Утв. приказом ФСТЭК №372-ст от 27.12.2006.

4. Бугаков И.А. От глубокого обучения к глубокому пониманию (From Deep Learning to Deep understanding) // Известия Института инженерной физики, 2020. №3(57). С.95-102.

5. Биометрия от «А» до «Я». Полное руководство биометрической идентификации и аутентификации // <https://securityrussia.com/blog/biometriya.html>.

6. Сулавко А.Е. Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта. Дисс. на соиск. уч. степ. докт. тех. наук. Омск, 2023. 391 с.

7. ГОСТ Р 54411 – 2018. Информационные технологии. Биометрия. Мультибиометрические и другие мультибиометрические технологии. Утв. приказом Росстандарта №1045-ст от 30.11.2018.

8. ПНСТ 379 – 2019. Информационные технологии. Биометрия. Применение биометрии в мобильных устройствах. Утв. приказом Росстандарта №56-пнст от 19.12.2019.

9. Горелик А.А., Скрипкин В.А. Методы распознавания. М.: Высшая школа, 1984. 208 с.

10. Атакищев О.И., Аджемов С.С., Емельянов С.Г. и др. Формальные грамматики, метаграмматики и грамматические структуры. Их применение при принятии управленческих решений. М.: МТУСИ, 2010. 345 с.

УДК 539.143.34

ТВОРЧЕСКАЯ ИНТЕРПРЕТАЦИЯ НАУЧНЫХ ФАКТОВ КАК ЭЛЕМЕНТ ПОДГОТОВКИ ИНЖЕНЕРНЫХ И НАУЧНЫХ КАДРОВ (ОПЫТ СОЗДАНИЯ НАУЧНО- ИСТОРИЧЕСКОГО КВЕСТА) CREATIVE INTERPRETATION OF SCIENTIFIC FACTS AS AN ELEMENT OF TRAINING ENGINEERING AND SCIENTIFIC PERSONNEL (EXPERIENCE IN CREATING A SCIENTIFIC- HISTORICAL QUEST)

Виктор Васильевич Лесных

преподаватель кафедры физики
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17
Тел.: +7 (916) 664-64-12
E-mail: viktor-lesnykh@yandex.ru

Игорь Алексеевич Зверев

курсант 1-го курса
филиал ВА РВСН им. Петра Великого (г. Серпухов)
Адрес: 142210, Московская обл.,
г. Серпухов, ул. Бригадная, д. 17

Аннотация

В статье на историческом примере расчета энергии скрытой в атомном ядре, проведенного Лизой Мейтнер, предлагаются элементы методики подготовки обучаемых к освоению таких разделов физики как релятивистская механика, атомная и ядерная физика в виде научно-исторического квеста (приключения). Новый методический прием направлен на преодоление стереотипов мышления обучаемых, связанных с постулатами классической механики, формирование мотивации развития научного кругозора, уверенности в собственных силах при решении сложных исследовательских задач. Используя известный метод исторической ретроспективы авторы предлагают обучаемым пройти самостоятельно весь путь, приведший в конечном счете к созданию атомной энергетики. На конкретном примере показано применение в образовательном процессе нового методического приема, который учитывает психологические особенности молодежи, а именно стремление к приключениям и поиску сокровищ, в качестве которых в нашем случае выступают конкретные знания по физике.

Ключевые слова: деление урана, энергия связи, дефект массы, кулоновское взаимодействие, Отто Ган, Лиза Мейтнер, Нильс Бор, квест.

Summary

Using the historical example of Lise Meitner's calculation of the energy hidden in the atomic nucleus, the article proposes elements of a methodology for preparing students to master such branches of physics as relativistic mechanics, atomic and nuclear physics in the form of a scientific-historical quest (adventure). The new methodological technique is aimed at overcoming students' thinking stereotypes associated with the postulates of classical mechanics, creating motivation for the development of scientific horizons, and self-confidence in solving complex research problems. Using the well-known historical retrospective method, the authors invite students to go through on their own the entire path that ultimately led to the creation of nuclear energy. A specific example shows the use of a new methodological technique in the educational process, which takes into account the psychological characteristics of young people, namely the desire for adventure and treasure hunting, which in our case is specific knowledge in physics.

Keywords: uranium fission, binding energy, mass defect, Coulomb interaction, Otto Hahn, Lise Meitner, Niels Bohr, quest.

«Учить не мыслям, а мыслить!»

Иммануил Кант

**Формирование у обучаемых интереса к
исследуемой теме. Ретроспектива вопроса**

Наблюдение за обучаемыми при переходе от разделов классической механики к основам ре-

лятивистской показали наличие определенных стереотипов, сформированных предыдущим разделом, которые затруднили усвоение принципов релятивистской механики (РМ) и их применение для решения задач, связанных с расчетом параметров частиц микромира.

Основной стереотип, мешающий успешному освоению принципов и законов РМ – это понятие массы, как меры инертности тела или количества вещества в классической механике. По всей видимости, это свойственно не только современным обучаемым.

История открытия энергии атома показывает, что наличие стереотипов классической механики было присуще и ученым с мировыми именами. Это не позволило им увидеть в уже существующих научных открытиях и фактах своего времени совершенно новое качество массы, присущее релятивистскому миру. Несмотря на то, что все ученые, причастные к изучению явления радиоактивности, прекрасно знали теорию Эйнштейна о связи массы и энергии, но использовать эти знания для решения задачи расчета энергии выделяющейся при делении ядра атома они не смогли.

И сам Альберт Эйнштейн до конца не представлял, как его теория (специальная теория относительности – СТО) и фундаментальная связь энергия-масса, показанная им в уравнении его имени, позволит открыть тайны атома и получения атомной энергии.

Эрнест Резерфорд, открывший наличие в атоме ядра, не установил наличие связи между его зарядом и номером элемента в таблице Д. Менделеева. Эта связь была сформулирована позже, а Э. Резерфорд считал, что электрический заряд атомного ядра пропорционален массе элемента. Кроме того, стоит подчеркнуть, что он «негативно отзывался о перспективах ядерной энергетики» [1].

Выступая на съезде Британской ассоциации содействия развитию науки в 1933 году Э. Резерфорд заявил, что «всякий, кто ожидает получения энергии в результате трансформации атомов, говорит вздор» [2].

Отто Ган, получивший Нобелевскую премию за открытие деления ядер тяжелых металлов, не мог объяснить результаты своих экспериментов, в результате которых после обработки нейтронами ядра атома урана 235 в исследуемом веществе появились следы атомов бария и криптона. Для него это было такой неожиданностью, что он не мог поверить в истинность полученных результатов. До определенного времени в его лаборатории работала ассистентом ученый-физик Лиза Мейтнер, которая в силу своего происхождения была вынуждена покинуть Германию в конце 30-х годов прошлого века, и проживала на момент открытия Ганом расщепления атома урана в Стокгольме.

Именно к ней за помощью обратился будущий лауреат Нобелевской премии О. Ган с просьбой объяснить полученные им результаты.

В то время: «Лиза Мейтнер занималась определением энергии, выделяющейся при каждом распаде из-за дефекта массы. Она очень ясно представляла себе кривую дефекта масс. Оказалось, что за счет электростатического отталкивания элементы деления приобрели бы энергию около 200 МэВ, а это как раз соответствовало энергии, связанной с дефектом массы» [3].

Эти расчеты потрясли и саму Л. Мейтнер и ее племянника О. Фриша, который в это время гостил у нее. Величина энергии выделявшейся при делении одного ядра урана 235 была просто невероятной.

«Такую энергию еще не наблюдали ни в процессах ядерных превращений, ни тем более в химических реакциях: например, 1 моль углерода при сгорании дает лишь 2 эВ энергии, а 1 атом урана при своем делении – в сто миллионов раз больше!» [4].

В основе ее подхода к расчету энергии было твердое убеждение в том, что О. Ган не ошибся, и произошло разделение ядра урана на два ядра более легких элементов из таблицы Менделеева. При этом оба осколка имели положительные заряды, величины которых было нетрудно получить из периодической таблицы. Первоначальный расчет она произвела на основе закона Кулона, получив энергию примерно 200 МэВ. Повторно проверила полученные данные с учетом разности масс исходного ядра и суммы масс продуктов деления.

Результаты расчетов Л. Мейтнер через ее племянника Отто Фриша, с которым она обсуждала эту тему, стали быстро известны не только О. Гану, но и Нильсу Бору.

Вот как описывает О. Фриш реакцию Бора на его сообщение о расчетах тети: «Мы провели вместе два или три дня на рождество. Затем я вернулся в Копенгаген и едва успел сообщить Бору о нашей идее в тот самый момент, когда он уже садился на пароход, отправляющийся в США. Я помню, как он хлопнул себя по лбу, едва я начал говорить, и воскликнул: «О, какие мы были дураки! Мы должны были заметить это раньше». Но он не заметил, и никто не заметил» [3].

Что же заметила Л. Мейтнер и почему этого не видели другие ученые? Очень интересно пройти путем рассуждений ученого такого уровня, чтобы познакомиться с приемами интерпретации известных научных фактов для получения столь неожиданных результатов, которые потрясли все научное сообщество.

Понятие дефекта масс было на тот момент уже точно определено и можно было проводить расчеты энергии связи в ядре. Были известны основные силы, действующие в ядре атома. В

ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

первую очередь очевидны были силы кулоновского (электростатического) взаимодействия. Но при этом только одному человеку удалось применить эти знания для решения конкретной задачи по расчету энергии, которая выделится при делении исходного ядра.

Пройти путем рассуждений Лизы Мейтнер это очень интересное приключение, которое можно предложить обучаемым для формирования навыков самостоятельного мышления и приемов интерпретации полученных в ходе обучения знаний.

Для подготовки к такому научно-историческому квесту проведем с обучаемыми небольшой экскурс в историю физики, вспомним основные события, которые предшествовали открытию Л. Мейтнер.

Хронология событий, связанных с исследованием атомов и строения атомного ядра¹:

- 1749 г. Б. Франклин ввел термин заряд.
- 1785 г. Шарль Кулон. Закон взаимодействия электрических зарядов.
- 1833 г. М. Фарадей ввел термин «ион».
- 1838 г. М. Фарадей «закон сохранения электрического заряда».
- 1869 г. Д.И. Менделеев «Периодический закон. Периодическая таблица».
- 1896 г. А. Беккерель «Явление радиоактивности».
- 1897 г. Д. Д. Томсон открыл «электрон, как частицу».
- 1901 г. М. Планк ввел понятие «квант света».
- 1901 г. М. Кюри ввела понятие «радиоактивность».
- 1902 г. В. Рамзай представил радиоактивный процесс как «мономолекулярную реакцию распада вещества».
- 1902 г. Э. Резерфорд, Ф. Содди «первое объяснение механизма радиоактивного процесса, сопровождающегося испусканием α - или β -частиц и образованием атома нового элемента».
- 1903 г. Э. Резерфорд, Ф. Содди открыли «закон радиоактивных превращений и дали его математическое выражение, каноническая форма которого $N_t = N_0 \cdot e^{-\lambda t}$ общепринята в настоящее время».
- 1905 г. А. Эйнштейн в рамках своей теории показал, что кванты имеют не только энергию, но и импульс, и таким образом проявляют себя как частицы.
- 1910 г. Э. Резерфорд «Теория взаимодействия α -частиц с ядрами атомов». Сделано пред-

положение о действии закона Кулона между осколками деления ядер на расстояниях соизмеримых с диаметром атома.

- 1911 г. Э. Резерфорд «Открытие атомного ядра. Предложена планетарная модель строения атома».
- 1912 г. Р. Милликен измерил электрический заряд электрона.
- 1912-1913 гг. Н. Бор, А. Ван ден Брук, И. Ридберг опубликовали гипотезу о численном соответствии заряда ядра химического элемента его порядковому номеру в периодической системе.
- 1913-1914 г. Г. Мозли. Экспериментальное подтверждение гипотезы Н. Бора, А. Ван ден Брука, И. Ридберга.
- 1913 г. Э. Резерфорд. Гипотеза о том, что ядро атома водорода содержится в ядрах атомов всех химических элементов периодической системы.
- 1914 г. Э. Резерфорд. Высказал предположение о содержании в атомном ядре положительно заряженных частиц.
- 1919 г. Э. Резерфордом было сделано «открытие второй элементарной частицы – протона».
- В 1920 г. Э. Резерфорд. Предположение о существовании в ядре атома «частицы с массой, равной массе протона, но не имеющая электрического заряда».
- 1932 г. Джеймс Чедвик. Открытие нейтрона.
- 1932 г. Н. Фезер, Л. Мейтнер, У. Харкинс. Первые ядерные превращения химических элементов под действием нейтронов.
- 1934 г. И. и Ф. Жолио-Кюри. Открытие искусственной радиоактивности.
- 1934 г. Э. Ферми. Теория β -распада. Предположил, что «электрон и нейтрино возникают в момент распада нуклона в ядре, и постулировал новое взаимодействие как слабое».
- О. Ган, Л. Мейтнер и Ф. Штрассман, «проведя аналогичные эксперименты, подтвердили эту гипотезу и предложили несколько цепочек распада, заканчивающихся эказолотом».
- 1936 Н. Бор предложил капельную модель строения ядра.
- 1936 г. Юджин (Евгений) Пол Вигнер. Теория поглощения нейтронов ядрами атомов.
- 1938 г. О. Ган, Ф. Штрассман. «Процесс деления урана под действием нейтронов». Фактическое завершение исследований начатых в 1934 г. Э. Ферми по облучению урана медленными нейтронами.
- 1939 г. Л. Мейтнер и О. Фриш. Физическая интерпретация результатов химических опытов

¹ При составлении хронологии событий, связанных с исследованием атомов и строения атомного ядра, использовались материалы лекций доктора химических наук, профессора кафедры радиохимии химического факультета МГУ И.Н. Бекмана, взятые из открытых источников [8].

О. Гана и Ф. Штрассмана. Расчет кинетической энергии осколков от деления ядра атома урана 235. Сопоставление полученных результатов с энергией связи атомного ядра. Введение Лизой Мейтнер в терминологию ядерной физики понятия «деление ядра». **С этого момента практически началась эпоха атомной энергетики.**

- 1939 г. Л. Сцилард, Э. Ферми, Ф. Жолио-Кюри, Я.Б. Зельдович, Ю.Б. Харитон. Обоснование возможности протекания в уране цепной ядерной реакции деления.

- 1942 г. Э. Ферми. Осуществление управляемой цепной реакции деления в первом атомном реакторе.

- 1945 г. Нью-Мексико. Первое в мире испытание атомной бомбы.

- 1954 г. город Обнинск Калужской области. Пуск первой в мире атомной электростанция.

Приглашение на маршрут исследования. В поисках сокровищ!

Проведя с обучаемыми такой экскурс в историю и дав краткие комментарии этих событий, напомнив основные законы и уравнения, которые нам могут понадобиться для решения такой необычной учебной задачи, построим наши рассуждения, исходя из замечательной фразы философа XVIII века Клода Адриана Гельвеция «Знание некоторых принципов легко возмещает незнание некоторых фактов».

Давайте попробуем восстановить ход мыслей Л. Мейтнер, исходя из тех «принципов», которые ей были известны на момент получения письма от О. Гана.

Итак, Л. Мейтнер несколько не сомневалась в чистоте опытов О. Гана и Ф. Штрассмана, что исключало наличие экспериментальной ошибки. Поэтому она охотно взялась за эту задачу и решила повести анализ ситуации на основе капельной модели строения атомного ядра, чтобы рассчитать величину энергии кулоновского отталкивания, которое по ее мнению и разорвало исходное ядро на две части, имеющие отличные от исходного химического элемента свойства.

Процесс деления на основе капельной модели ядра был достаточно понятен. Поглотив дополнительный нейтрон, ядро урана 235 становилось «тяжелее» на один нуклон. Таким образом мы уже имели дело с ураном 236. Но это ядро было уже не таким устойчивым и силы поверхностного натяжения оболочки ядра, как тогда представляли ученые, уменьшались. Ядро становилось более «рыхлым». В результате этого в ядре начинали доминировать кулоновские силы отталкивания, поскольку оно состояло из заряженных частиц одного знака. Это было уже

установлено ранее Э. Резерфордом.

В силу этого, ядро, как капля жидкости начало вытягиваться до образования тонкой перемычки между двумя частями. [5]

В какой то момент ядерные силы, удерживающие нуклоны в ядре, становились меньше кулоновских сил и ядро делилось на два осколка. Которые как поняла Л. Мейтнер и были обнаружены О. Ганом. Это были ядра изотопов бария и криптона.

Какие же силы разорвали ядро? И какая энергия могла выделиться в результате этой реакции? Для человека, знакомого с законом Кулона, нет ничего проще, что бы ответить на этот вопрос, если... Да. Если кроме величин зарядов, которые без труда можно было найти в периодической системе, нам известно расстояние между зарядами r_{12} . При этом, энергию можно вычислить по формуле (1)

$$E = (q_1 \cdot q_2) / 4\pi \cdot \epsilon_0 \cdot r_{12} \quad (1)$$

И здесь, в нашем расследование начинается очень интересный эпизод. Если предположить, что за расстояние был принят порядок диаметра ядра урана, который по оценкам Э. Резерфорда составлял 10^{-14} метра, то мы выходим в расчетах на уровень энергии 290 МэВ.

Это не соответствует тому, что вычислила Л. Мейтнер, т.е. величину энергии около 200 МэВ.

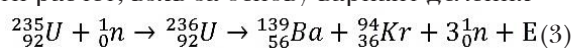
Значит, она знала то, что мы не увидели в хронологии. Вернемся в прошлое и еще раз проверим факты на предмет их использования для решения нашей задачи.

Повторный просмотр событий тех лет показал, что в результате опытов Э. Резерфорда по исследованию отклонений альфа частиц ядрами разных химических элементов, была выведена эмпирическая формула (2), которая связывала радиус ядра элемента и его атомный номер. Точнее, количество нуклонов, которые могли находится в объеме сферы такого радиуса

$$R = r_0 \cdot A^{1/3} \quad (2)$$

Интересная находка на нашем пути! Позднее мы убедимся, что она и является ключом к получению результата (200 МэВ) на основе анализа кулоновских взаимодействий.

Теперь надо определиться с числом A из уравнения (2). Для этого необходимо выбрать схему деления из нескольких наиболее вероятных вариантов. В процессе деления урана образуется достаточно много различных изотопов. Нам точно неизвестно какой вариант деления рассматривала Л. Мейтнер, но попытаемся провести расчет, взяв за основу вариант деления



Итак, берем изотоп бария с атомным числом 139 и изотоп криптона с атомным числом 94.

Рассчитаем радиусы ядер этих изотопов по формулам:

$$R_{Ba} = r_0 \cdot A_{Ba}^{1/3} \quad (4)$$

$$R_{Kr} = r_0 \cdot A_{Kr}^{1/3} \quad (5)$$

А вот и следующее препятствие и нашем пути! Что такое r_0 ?

Это эмпирический коэффициент пропорциональности, опять же полученный в результате опытов по рассеянию альфа частиц. Уже в конце 30-х годов прошлого века это было известно, что диапазон значений $r_0 = (1,2-1,7) \cdot 10^{-15}$ м.

Осталось для точности расчетов определить, какое значение выбрала Л. Мейтнер. Скорее всего, выбор пал на значения $(1,4-1,5) \cdot 10^{-15}$ м.

Эти коэффициенты наиболее точно отражали процессы взаимодействия ядер с альфа частицами. Такие значения соответствуют радиусу действия ядерных сил и характеризуют расстояние от центра ядра, на котором внешний нейтральный нуклон начинает впервые «ощущать» их действие. Значит, взяв для расчета, например коэффициент $r_0 = 1,4 \cdot 10^{-15}$ м можно достаточно точно рассчитать энергию кулоновского взаимодействия.

Проведем расчеты, подставив этот коэффициент в формулы (4) и (5). Для бария радиус составит

$$R_{Ba} = 7,25214 \cdot 10^{-15} \text{ м} \quad (6)$$

Для криптона:

$$R_{Kr} = 6,36557 \cdot 10^{-15} \text{ м} \quad (7)$$

Искомое расстояние, которое нам потребуется для формулы (1), будет представлять сумму этих радиусов:

$$r_{12} = R_{Ba} + R_{Kr} = 13,6 \cdot 10^{-15} \text{ м} \quad (8)$$

Заряды изотопов бария q_{Ba} и криптона q_{Kr} возьмем из периодической таблицы:

$$q_{Ba} = 56 \text{ Кл} \text{ и } q_{Kr} = 36 \text{ Кл} \quad (9)$$

Подставив значения r_{12} , q_{Ba} , q_{Kr} в формулу (1), получим значение энергии кулоновского взаимодействия:

$$E_k = (56 \cdot 36 \cdot e^2) / (4\pi \cdot \epsilon_0 \cdot 13,6 \cdot 10^{-15}) = 3,415 \cdot 10^{-11} \text{ Дж} = 213 \text{ МэВ} \quad (10)$$

Судя по полученной цифре, мы смогли в хорошем приближении восстановить ход мыслей Л. Мейтнер. Но это только первая часть ее расчетов. Из статьи ее племянника О. Фриша [3] мы знаем, что она проверила этот расчет, опираясь на уравнение А. Эйнштейна и понятие дефекта массы. При этом было получено практически такое же значение энергии, выделяющейся при делении ядра урана, как и в первом случае (200 МэВ).

На этом этапе сравним массы исходных элементов до начала процесса деления и сумму масс продуктов деления:

$$m_U + m_n + \Delta m = m_{Ba} + m_{Kr} + 3 \cdot m_n \quad (11)$$

В левой части этого уравнения появляется величина Δm , поскольку сумма масс продуктов распада оказывается больше, чем масса ядра и нейтрона до начала деления.

Рассчитаем точное значение Δm . От точности расчета будет зависеть и величина энергии, которую мы должны вычислить. Поэтому учитываем максимальное количество знаков после запятой. Берем справочные значения атомных масс соответствующих изотопов в атомных единицах массы (а.е.м.):

$$m_{Ba} = 139,331 \text{ а.е.м.}$$

$$m_{Kr} = 93,93436 \text{ а.е.м.}$$

$$m_U = 235,0439299 \text{ а.е.м.}$$

$$m_n = 1,00866 \text{ а.е.м.}$$

Преобразуем уравнение (11) относительно Δm :

$$\Delta m = m_{Ba} + m_{Kr} + 3 \cdot m_n - m_U - m_n \quad (12)$$

Подставив в выражение (12) соответствующие значения атомных масс, получим следующее значение Δm :

$$\Delta m = 0,23842 \text{ а.е.м.}$$

или в системных единицах измерения

$$\Delta m = 0,39577 \cdot 10^{-27} \text{ кг.}$$

Здесь надо сделать небольшое отступление и напомнить нашим путешественникам по извилистым дорогам научных открытий в физике, что основной стереотип, который мешал сделать последний шаг, и который преодолела Л. Мейтнер, это содержание понятия «масса» в РМ. В уравнении (12) Δm это не та масса, к которой мы привыкли, изучая классическую механику. Это не мера вещества [6]. Это эквивалент энергии.

Далее, для того, чтобы эквиваленты энергии привести к самой энергии, применим уравнение Эйнштейна:

$$E = m \cdot c^2 \quad (13)$$

В контексте наших рассуждений разница масс Δm будет эквивалентна энергии ΔE , которая нам закроет энергетический баланс, для выполнения закона ее сохранения:

$$\begin{aligned} (m_U \cdot c^2) + (m_n \cdot c^2) + \Delta E = \\ = (m_{Ba} \cdot c^2) + (m_{Kr} \cdot c^2) + (3 \cdot m_n \cdot c^2) \end{aligned} \quad (14)$$

И здесь Л. Мейтнер делает шаг, который открыл новый мир для человечества. Мир атомной энергии. Подставив в уравнение Эйнштейна значение Δm , она получает величину энергии ΔE , которая почти полностью совпало с величиной, рассчитанной на основе закона Кулона:

$$\Delta E = c^2 \cdot \Delta m \quad (15)$$

$$\Delta E = 3,56193 \cdot 10^{-11} \text{ Дж} \text{ или } \Delta E = 214 \text{ МэВ}$$

Решение задачи двумя способами и полученные практически идентичных результатов

$$E_k = 213 \text{ МэВ} \text{ и } \Delta E = 214 \text{ МэВ}$$

убедили Л. Мейтнер в правильности проведенных расчетов, а нас в том, что мы сумели само-

ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

стоятельно пройти весь путь ее рассуждений и получили навыки интерпретации известных фактов для решения новых задач.

Количественная оценка величины энергии выделяющейся при делении ядра урана, это то сокровище физических знаний, которые и привели к созданию атомного оружия и началу века атомной энергетики. Эти расчеты однозначно подтвердили, что обнаруженные О. Ганом изотопы бария и криптона есть продукты деления ядра урана.

А значит, деление ядра возможно и при этом

выделяется колоссальная энергия!

Следует обратить внимание обучаемых на то, что Л. Мейтнер на основании уравнения Эйнштейна пришла к однозначному выводу, что часть массы, которую мы обозначили, как Δm выделяется в виде энергии. Причем большая ее часть превращается в кинетическую энергию осколков деления. Это примерно 170 МэВ. Поскольку это происходит в короткое время, осколки, получившие очень большую скорость за этот короткий временной интервал, взаимодействуют с веществом внешней среды, что со-

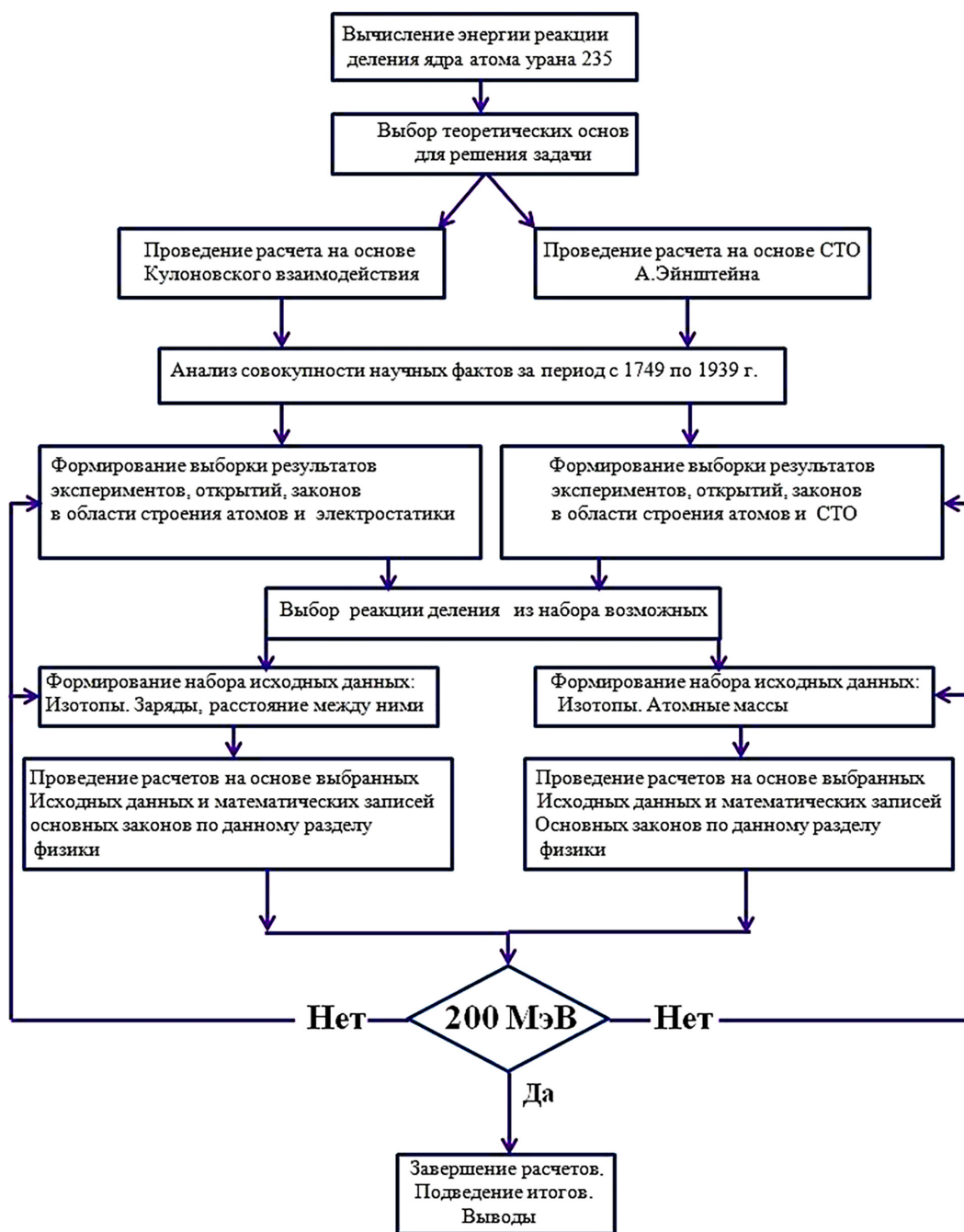


Рис. 1. «Дерево поиска решений» или алгоритм организации действия обучаемых на каждом этапе работы

проводятся выделением и тепловой энергии примерно такой же величины.

Эффект, который произвело сообщение Н. Бора о результатах расчетов Л. Мейтнер, подтверждающих факт деления атомного ядра медленными нейтронами, был феерический: «26 января 1939 года в Вашингтоне состоялась конференция по теоретической физике, на которую был приглашен и Бор. Он доложил собранию о делении атома урана. Не успел он договорить до конца, как несколько американских физиков вскочили, как ужаленные, со своих мест. В смокингах ворвались они в свои лаборатории, чтобы собственноручно проверить открытие, которое они прозевали» [3].

На этом выступлении Н. Бора мы завершим поиски сокровищ физики, которые вместе с вами были проведены в рамках этой статьи в виде научно-исторического квеста!

Графическое изображение наших действий по решению поставленной задачи и описанных в статье, представлены в общем виде на *рисунке 1* в виде «Дерева поиска решения» или алгоритма организации действия обучаемых на каждом этапе работы.

Заключение

«Теория и методика приключения сегодня недостаточно представлены в отечественной педагогической науке, хотя в зарубежных исследованиях этим вопросам уделяется немало внимания» [7]. Инновация предложенного в данной статье методического приема заключается в том, что под приключением при изучении физики мы предложили понимать не участие в археологических раскопках, совершение рискованных туристических походов и т.п., а научно-историческое расследование, т.е. квест (приключение) в широком понимании этого термина, как сложную и запутанную ситуацию, содержащую определенную интригу.

Надо отметить, что эффективность предложенного подхода к формированию у обучаемых интереса к решению аналогичных задач, сформулированных в виде научно-исторического квеста, подтверждается тем, что в ее решении участвовал курсант первого курса, успешно завершивший изучение раздела «Механика» (первый семестр) и только приступивший к освоению раздела физики «Электричество и магнетизм».

Дополнительные занятия проводились с ним факультативно в рамках работы Военного научного общества обучаемых. Проведенный эксперимент показал, что и на этом этапе можно формировать устойчивые навыки решения задач по разделам атомная и ядерная физика, которые

будут изучаться только во втором семестре. И судя по интересу, вызванному у обучаемого к такой форме постановки учебной задачи, появляется хорошая мотивация для изучения этих разделов, непосредственно связанных с его основной специальностью, которую он должен получить по окончании вуза.

Важно понимать, что развитие в нашей стране сырьевой экономики, достижение научного и технологического суверенитета возможно при наличии специалистов и ученых с нестандартным мышлением. Весь опыт развития науки показывает, что наличие стереотипов мышления, отсутствие навыков интерпретации известных фактов не позволяет делать научные открытия даже при наличии перспективных экспериментальных данных и основ новых научных теорий. Существует необходимость перестройки системы образования. Перейти от подготовки квалифицированных пользователей к подготовке создателей. Приведенный в статье пример открытия Лизы Мейтнер наглядно показывает, как стереотипы мышления мешали даже великим ученым разглядеть в существующих научных фактах совершенно новые явления. Учитывая этот опыт, необходимо внедрять в образовательный процесс новые методические приемы, повышающие эффективность решения стратегических задач по подготовке специалистов для российских предприятий и научных учреждений.

Литература

1. Плотников П.Г., Плотникова Л.В. Некоторые аспекты ядерной физики: Уч. пособ. СПб: НИУ ИТМО, 2016. 58 с.
2. Гинзбург В.Л. О физике и астрофизике: Статьи и выступления. 2-е изд., перераб. и доп. М.: Наука. Гл. ред. физ.-мат. лит., 1992. 528 с.
3. Фриш О., Уилер Дж. Из истории физики. Открытие деления ядер // Успехи физических наук, 1968. Вып.4. Т.96. 450 с.
4. Гофман К. Можно ли сделать золото? 2-е изд. Л.: Химия, 1984. 320 с.
5. Варламов А.А. Капельная модель ядра // Квант, 1986. №5. С. 23-24.
6. Окунь Л.Б. Масса. Энергия. Относительность // Успехи физических наук, 1989. Т.158. Вып.3. С. 511-530.
7. Миновская О.В. Приключение как инновация в воспитании учащейся молодежи // Современные наукоемкие технологии, 2011. №1. С. 123-124.
8. Бекман И.Н. Атомная и ядерная физика. Радиоактивность и ионизирующее излучение. Учебник для СПО. 2-е изд., испр. и доп. М.: Юрайт, 2020. 492 с.

УДК 519.21



ТЕНДЕНЦИИ РАЗВИТИЯ НАУКОГРАДОВ КАК ТЕРРИТОРИЙ С ВЫСОКИМ НАУЧНО-ТЕХНОЛОГИЧЕСКИМ ПОТЕНЦИАЛОМ TRENDS IN THE DEVELOPMENT OF SCIENCE CITIES AS TERRITORIES WITH HIGH SCIENTIFIC AND TECHNOLOGICAL POTENTIAL

Николай Михайлович Емелин
заслуженный деятель науки и техники РФСР
доктор технических наук, профессор
главный научный сотрудник
ФГБУ «Научно-технический институт
межотраслевой информации» «НТИМИ»
Адрес: 125252, Москва, ул. Зорге, д. 22, к. 1
Тел.: +7 (499) 943-11-17

Аннотация

В статье рассматриваются тенденции научно-технологического развития наукоградов как территорий с высоким научно-технологическим потенциалом, их пространственного развития. Показана динамика изменения показателей наукоградов.

Ключевые слова: наукограды, научно-технологическое развитие, показатели, тенденции развития.

Summary

The article examines the trends of scientific and technological development of science cities as territories with high scientific and technological potential, their spatial development. The dynamics of changes in the indicators of science cities is shown.

Keywords: science cities, scientific and technological development, indicators, development trends.

Поддержка отдельных территорий с высоким научно-технологическим потенциалом в целях его сохранения, укрепления и эффективного использования – один из путей создания инфраструктуры и условий, отвечающих современным принципам организации научной, научно-технической и инновационной деятельности, закрепленных в Стратегии научно-технологического развития Российской Федерации (утверждена Указом Президента Российской Федерации от 28 февраля 2024 г. №145).

Оставив вне рассмотрения правовые аспекты (к примеру, законодательно не определены понятия «научный потенциал», «научно-технологический потенциал», «территория с высоким научно-технологическим потенциалом»), отметим, что к территориям с высоким научно-технологическим потенциалом могут быть отнесены наукограды, закрытые административно-территориальные образования, особые экономические зоны, технопарки, технополисы [1-2], среди которых только для наукоградов за-

конодательно (Федеральный закон от 7 апреля 1999 г. №70-ФЗ «О статусе наукограда Российской Федерации») закреплены критерии присвоения муниципальному образованию статуса наукограда и сохранения такого статуса.

В настоящее время наукограды, являясь опорными точками научно-технологического развития регионов [3-5], получают государственную поддержку на дальнейшее развитие их научно-производственных комплексов (НПК). По результатам деятельности наукоградов в 2022 году тенденции изменения показателей НПК представлены в *таблице 1*.

Нетрудно видеть, что, с одной стороны, значения большинства показателей растут или стабильны, с другой – в критической зоне (определим её как двух процентная от пороговых значений) по показателю И1 находится наукоград Бийск, по показателю И2 – наукограды Бийск, Дубна, Фрязино, по показателю И3 – наукоград Бийск. Обращает на себя внимание тот факт, что наукоград Бийск по всем трем показателям на-

НАУЧНЫЕ ОБЗОРЫ • НАУЧНЫЕ РЕЦЕНЗИИ • ОТЗЫВЫ

Таблица 1
Динамика показателей НПК

Наукоград	(И1) Доля численности работников НПК в составе наукограда (не менее 20%)	(И2) Доля численности исследователей НПК (не менее 20%)	(И3) Доля отгруженных товаров НПК в общем объеме отгруженных товаров наукограда (не менее 50%)
Бийск	21	22	51
Дубна	46	20	96
Жуковский	40	38	57
Кольцово	70	34	81
Королев	47	34	70
Мичуринск	30	29	91
Обнинск	29	26	55
Протвино	29	40	64
Пущино	26	58	102
Реутов	24	43	85
Троицк	28	55	70
Фрязино	72	22	107
Черноголовка	36	37	106

-	Показатель убывает
0	Показатель стабилен
+	Показатель возрастает

ходится в критической зоне.

Тенденции развития наукоградов достаточно подробно изложены в материалах интернет-конференции [6], но на одной из них хотелось бы заострить внимание. При реализации мероприятий по обеспечению устойчивого и сбалансированного пространственного развития территорий Российской Федерации выявился дефицит

возможностей для пространственного развития наукоградов, подталкивающий к необходимости их территориальных укрупнений для создания прорывных производств и новых рабочих мест [1]. Так в Московской области в 2022 году был образован городской округ (г.о.) Серпухов, включающий целый ряд населенных пунктов (в том числе два наукограда: Пущино и Протвино)

Таблица 2
Показатели НПК городского округа Серпухов

Населенный пункт	Средне-численность работников организаций (чел.)	Численность научных работников (исследователей) организаций (чел.)	Численность профессорско-преподавательского состава (включая лиц, работающих по совместительству) организаций (чел.)	Общий объем произведенных товаров (выполненных работ, оказанных услуг) (тыс. руб.)	Затраты на инвестиции в основной капитал и основные средства, необходимые для производства высокотехнологичной промышленной продукции и (или) инновационных товаров (выполнения инновационных работ, оказания инновационных услуг) (тыс.руб.)	И1(%)	И2(%)	И3(%)
г. Протвино	2 248	851	66	6 277 894	221 141	10,5	9,2	5,5
г. Пущино	2 942	1 134	112	4 853 841	497 755	13,8	12,5	4,5
г. Серпухов	1 983	387	51	9 346 671	1 168 032	9,3	4,4	8,9
пос. Большевик	59	17	0	58199	346	0,3	0,2	0,1
пос. Оболенск	2 747	194	26	34 685 193	3 488 399	12,9	2,2	32,3
г.о. Серпухов	9979	2583	255	55 221 708	5 375 673	46,8	28,5	51,3

и обладающий рядом уникальных возможностей и преимуществ развития, что было закреплено в Стратегии социально-экономического развития г.о. Серпухов Московской области как наукограда Российской Федерации на период до 2032 года (далее – Стратегия), утвержденной решением Совета депутатов г.о. Серпухов Московской области от 20.10.2023 г. №613/68 в редакции решения Совета депутатов г.о. Серпухов Московской области от 27.12.2023 г. №20/3с изменениями, внесенными решением Совета депутатов г.о. Серпухов Московской области от 16.02.2024 г. №7/75.

На что хотелось бы обратить внимание – так это на обеспечение устойчивого, неснижаемого уровня функционирования населенных пунктов НПК, заявленных в Стратегии, а именно показателей НПК (таблица 2).

Анализ таблицы 2 указывает на несбалансированность НПК г.о. Серпухов по показателю ИЗ: так вклад пос. Оболенск значительно превышает значения показателя НПК других населенных пунктов и составляет 32,3% при примерно равной среднесписочной численности работников организаций (за исключением пос. Большевик). Значение заявленного показателя ИЗ=51,3% (объективности ради отметим, что не учтены данные ряда организаций оборонно-промышленного комплекса, которые носят закрытый характер) находится на грани требуемого значения (не менее 50%). Более того, в Государственной программе научно-технологического развития Российской Федерации среднее по наукоградам значение этого показателя на 2022-2024 годы установлено 54%. Представляется целесообразным подумать о возможностях выведения г.о. Серпухов по показателю ИЗ выше среднего и при положительном решении внести соответствующие изменения в Стратегию и план мероприятий по её реализации на период до 2032 года.

Литература

1. Кабышев С.В.. Наукограды Российской Федерации в механизме реализации государственной научно-технической политики: конституционно-правовые аспекты // Журнал российского права, 2023. Т.27. №9. С.15-27.
2. Лапшинова К.В. Российские наукограды в эпоху глобализации: социологический подход к типологии территорий с высоким научно-производственным потенциалом // По материалам III Всероссийской научно-практической конференции «Русский космизм: история и современность». Под редакцией Т.Ю.Кириловой, 2018. Ч.2. С.133-141.
3. Справка о результатах анализа соответствия показателей научно-производственных комплексов наукоградов Российской Федерации требованиям, установленным пунктом 8 статьи 2.1 Федерального закона №70-ФЗ «О статусе наукограда Российской Федерации», и достижения результатов, предусмотренных планами мероприятий по реализации стратегий социально-экономического развития наукоградов Российской Федерации в 2022 году <https://minobrнауки.gov.ru/upload/iblock/77c/cemgzf9g61hhktvme7dfmm9feddbfzv.pdf>
4. Емелин Н.М, Рябов П.А., Смирнова К.А. Оценка вклада наукоградов в научно-технологическое развитие Российской Федерации // Двойные технологии, 2020. №1(90). С.60-65.
5. Емелин Н.М., Мелихов В.О. Инновационная деятельность наукоградов как фактор обеспечения стабильности экономики муниципального образования // Стратегическая стабильность, 2016. №1(74). С.42-49.
6. Материалы интернет-конференции «Актуальные вопросы развития наукоградов Российской Федерации – муниципальных образований с особым статусом». <https://council.gov.ru/media/files/n2r3g1gmn3SOV6fa5iVVJjfvAyl9bV7/pdf>.

УДК 623.62

120 ЛЕТ РАДИОЭЛЕКТРОННОЙ БОРЬБЫ: ИСТОРИЯ, СОВРЕМЕННОСТЬ, ПЕРСПЕКТИВЫ 120 YEARS OF ELECTRONIC WARFARE: HISTORY, MODERNITY, PROSPECTS

Александр Ильич Куприянов
доктор технических наук, профессор
Московский авиационный институт
(национальный исследовательский университет)
Адрес: 125871, Москва, Волоколамское ш., д. 4
E-mail: aik@mai.ru



Аннотация

Рассматриваются история зарождения, цели, задачи, состав методов и средств радиоэлектронной борьбы (РЭБ). Роль и место РЭБ в вооруженной борьбе, актуальность методов и средств РЭБ в конфликте информационно-телекоммуникационных систем авиационных и ракетно-космических комплексов.

Ключевые слова: радиоэлектронная борьба, радиоэлектронная разведка, радиоэлектронная защита, информационный конфликт, авиационные и ракетно-космические комплексы.

Summary

The 120-year retrospective examines the scientific, technical and military aspects of the manifestation of the conflict of radio-electronic systems in the information space. The experience of using electronic warfare means is analyzed: radio and electronic reconnaissance, radio jamming, noise protection and electronic camouflage in world and local wars, during the Cold War. Based on an analysis of history, the paths of development and achievement of electronic warfare means and methods are predicted.

Keywords: electronic warfare, electronic intelligence, electronic protection, information conflict, history of electronic warfare.

1. РЭБ в прошлом

Изобретение ученым России А.С. Поповым в 1895 году радио для беспроводной передачи информационных сообщений посредством электромагнитных волн получило так много практических применений, что даже простое перечисление их похоже на попытку объять необъятное. Но одно из самых первых достижений – освоение принципиально нового средства связи и боевого управления силами морского флота.

Как и любое явление, радиосвязь вызвала к жизни и угрозу самой себе. Низкая скрытность и подверженность внешним помехам сделали радиосвязь уязвимым элементом системы управления, что обнаружилось на самых ранних этапах развития радиотехники, определив пути деструктивного воздействия на эти новые информационные каналы. Так, в докладе Морского технического комитета, составленном еще в январе 1902 года, прямо указывалось: «Телеграфирование без проводов обладает тем недостатком, что телеграмма может быть уловле-

на на всякую постороннюю станцию и, следовательно, прочтена и, кроме того, передаваемая телеграмма может быть перебита и перепутана посторонними источниками электричества. Это несовершенство приборов приобретает особую важность во время войны, когда телеграмма может быть перехвачена неприятелем или спутана и искажена им во время получения на нашем корабле» [1]. Таким образом, именно флот, открывши неосценимую пользу радиосвязи для удовлетворения информационных потребностей человечества, указал и на ее потенциальную опасность. Это диалектическое противоречие проявляется как информационный конфликт и в современной науке, и технике именуется радиоэлектронной борьбой (РЭБ).

Решающий шаг, позволивший перевести идеи радиоэлектронной борьбы в практическую область, был сделан в первые дни войны с Японией выдающимся русским флотоводцем и ученым вице-адмиралом С.О. Макаровым (рисунки 1).

Еще будучи Главным командиром Крон-

штадтской базы флота он активно содействовал работам профессора А.С. Попова в области создания беспроводного телеграфа и всесторонне оценил сильные и слабые стороны радиосвязи как нового средства боевого управления.

7 марта 1904 г., едва вступив в командование Тихоокеанской эскадрой, адмирал издал исторический приказ № 27 – первый официальный флотский документ в области радиоэлектронной борьбы. Приказ предписывал принять к руководству следующее [1]:

«1. Беспроводный телеграф обнаруживает присутствие, а потому теперь же поставить телеграфирование это под контроль и не допускать никаких отправительных депеш или отдельных знаков без разрешения командира, а в эскадре – флагмана.

Допускается на рейдах, в спокойное время, проверка с 8 до 8.30 часов утра.

2. Приемная часть телеграфа должна быть все время замкнута так, чтобы можно было следить за депешами и, если будет чувствоваться неприятельская депеша, то тогда же доложить командиру и определить, по возможности, заслоняя приемный провод, приблизительное направление на неприятеля, и доложить об этом.

3. При определении направления можно пользоваться маневром, поворачивая свое судно и заслоняя своим рангоутом приемный провод, причем по отчетливости можно судить иногда о направлении на неприятеля.

Минным офицерам предлагается произвести в этом направлении всякие опыты.

4. Неприятельские телеграммы следует все записывать и затем командир должен принять все меры, чтобы распознать вызов старшего, ответный знак, а если можно, то и смысл депеш.

Для способных молодых офицеров – тут целая интересная область.



Рис. 1. Профессор А.С. Попов демонстрирует адмиралу С.О. Макарову работу радиотелеграфа. С картины художника И.С.Соркина

Для руководства прилагается японская телеграфная азбука».

В этом коротком и емком тексте воинского приказа перечисляются все основные задачи и приемы радиоэлектронной борьбы. И указание на организацию радиоперехвата. И требование применить радиопеленгацию источников радиоизлучения, включая технические подробности того, как это следует сделать. И побуждение к научному поиску в новом для того времени и важном деле РЭБ. Есть и указания, выходящие за рамки технических инструкций и обращенные к пытливым молодежи, волею судеб оказавшейся у истоков новой предметной области знания – радиоэлектронной борьбы. Требования и указания приказа №27 не утратили актуальность и в наши дни, через 120 лет. Изменилась только терминология при полном сохранении сути, а также добавились новые направления.

Значение цитированного выше документа для практической постановки радиоэлектронной борьбы и радиоразведки в России не переоценимо. В короткий срок практически на всех кораблях и судах флота было организовано несение вахт радиоразведки. Кроме того, под Порт-Артуром к решению этой задачи привлекалась береговая радиостанция, расположенная в районе Золотой горы.

Приказ возымел скорое действие. Уже 11 апреля 1904 года была проведена первая операция радиоразведки. В этот день была перехвачена и расшифрована японская радиограмма. Операцию осуществили радиотелеграфисты крейсера «Громобой». Тогда Владивостокский отряд крейсеров под командованием вице-адмирала К.П. Иессена благодаря полученной информации не только сумел избежать боевого столкновения с эскадрой японского вице-адмирала Камимурэ, но и уничтожил три японских судна, в том числе и войсковой транспорт «Кинсю Мару».

2 (15) апреля 1904 года впервые в мировой истории был сделан практический шаг от организации радиоразведки к ведению радиоэлектронной борьбы в боевых действиях. В этот день японцы предприняли очередной обстрел Порт-Артура корабельной артиллерией, вошедший в историческую хронику обороны крепости под названием «третьей перекидной стрельбы» (рисунок 2).

Официальный рапорт временно исполняющего должность командующего флотом Тихого океана контр-адмирала П.П. Ухтомского на имя наместника императора содержит следующее сообщение: «В 9 час. 11 мин. утра неприятельские броненосные крейсера «Ниссин» и «Касуга», маневрируя на зюйд-зюйт-вест от мая-

ка Ляотешань, начали перекидную стрельбу по фортам и внутреннему рейду. С самого начала стрельбы два неприятельских крейсера, выбрав позиции против прохода Ляотешанского мыса, вне выстрелов крепости, начали телеграфировать, почему немедленно же броненосец «Победа» и станции Золотой горы начали перебивать большой искрой неприятельские телеграммы, полагая, что эти крейсера сообщают стреляющим броненосцам о попадании их снарядов. Неприателем выпущено более 60 снарядов большого калибра. Попаданий в суда не было».

Русско-японская война 1904-1905 годов дала и другие, противоположные примеры важности использования РЭБ.

В ходе морского сражения в Цусимском проливе командиры крейсера «Изумруд» и миноносца «Громкий» использовали корабельные радиостанции для создания помех радиосвязи между японскими кораблями слежения за действиями русской эскадры (кстати, по собственной инициативе, вопреки запрету адмирала З.П. Рожественского).

Сразу после окончания русско-японской войны причины и обстоятельства Цусимской трагедии стали предметом особого рассмотрения специальной комиссии под председательством адмирала А.В. Колчака, созданной при Главном морском штабе. Комиссией самым внимательным образом анализировались и вопросы применения радиопомех. Выводы комиссии в этой

части были совершенно конкретны: «Адмиралу Рожественскому надлежало, как только он был открыт японцами, сделать все возможное, чтобы нарушить радиотелеграфную связь между отрядами противника. Японцы, дабы не упустить нашей эскадры, были принуждены рассеять свои силы по большому пространству, и радиотелеграфная связь являлась существеннейшим элементом их сил. Нарушение этой связи радиостанциями нашей эскадры, шедшей соединенно и поэтому не столь нуждавшейся в радиотелеграфе, было тем преимуществом нашей эскадры, которым грех было не воспользоваться. Это было бы ударом по слабому месту противника. Несколько мощных, умело примененных радиотелеграфных станций на русской эскадре, нарушив связь между отрядами, сделали бы большее дело, чем десятки пушек» [1].

Эти выводы, и особенно последний из них, сопоставляющий эффективность РЭБ и боевых средств, заслуживают высокой оценки даже с позиций нынешнего времени.

1907-1914 годы характеризуются как период общего подъема радиотехники в Российском флоте. В полной мере этот подъем коснулся и вопросов РЭБ.

В начале 1911 года статским советником А.А. Петровским, преподавателем Николаевской Морской академии и Минного офицерского класса, были выполнены первые теоретические исследования в области РЭБ, результаты которых

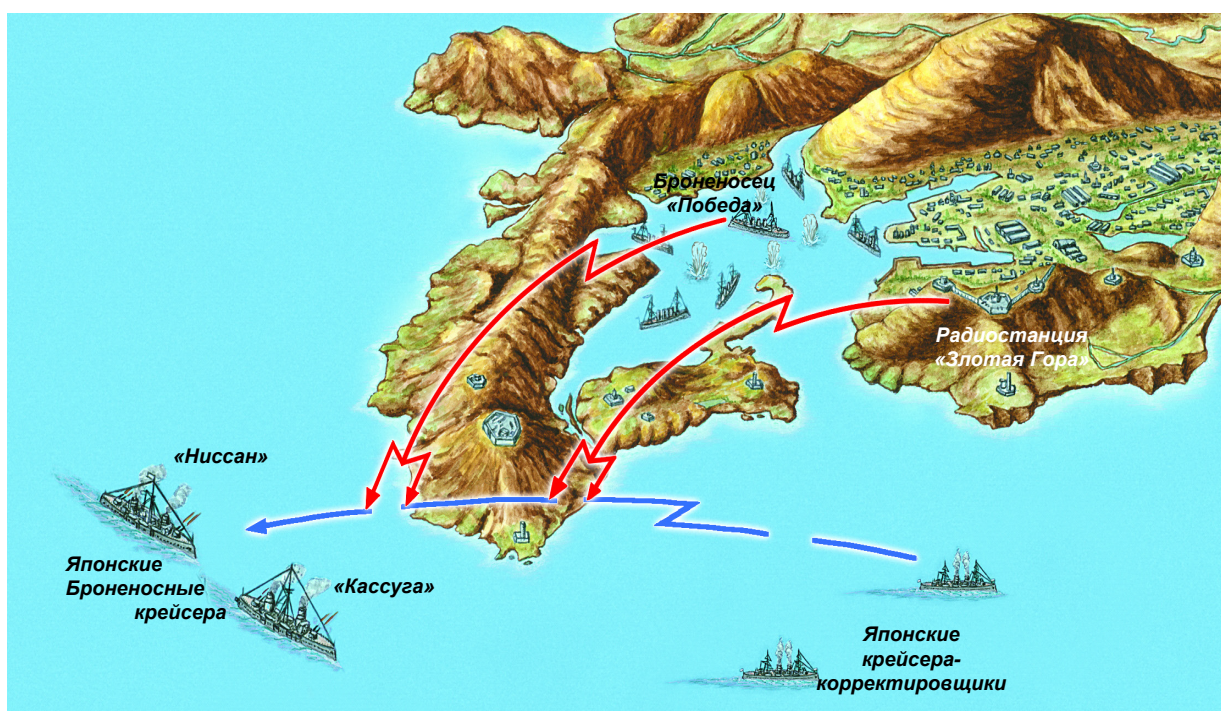


Рис. 2. Схема организации радиоэлектронного противодействия третьей перекидной стрельбе в Порт-Артуре в апреле 1904 года

он изложил в своей статье под названием «При каких условиях возможно помешать противнику пользоваться радиотелеграфом». Статья, представленная 29 марта 1911 года к опубликованию в «Известиях Николаевской Морской академии», была направлена начальником академии в адрес председателя Морского технического комитета и дала основание для проведения на Российском флоте первых экспериментов в области РЭБ.

Эксперименты под руководством А.А. Петровского состоялись летом 1911 года на Черноморском флоте. В результате их проведения были впервые получены количественные оценки допустимой расстройки помехи и сигнала при подавлении «слуховой» телеграфии.

В ходе этих экспериментов А.А. Петровский также использовал помехи в виде сплошного тира, ряда точек и беспорядочно передаваемых знаков (по современной терминологии это прицельные сигналоподобные помехи). Было установлено, что, при прочих равных условиях, использование помехи в виде беспорядочных сигналов обеспечивает заданную эффективность подавления при наименьшем соотношении интенсивности помехи и подавляемого сигнала. Таким образом, А.А. Петровский в результате своих экспериментов 1911 года вплотную подошел к одному из важных вопросов теории радиоэлектронного подавления – вопросу «оптимальной помехи».

В октябре 1911 года соответствующим циркуляром основные результаты экспериментов были доведены до специалистов на флотах и в последующем использовались при разработке способов радиоподавления, а также защиты от радиопомех противника.

Методы радиоразведки и радиоподавления применялись воюющими армиями в ходе Первой мировой войны. Основательный анализ применения РЭБ в этот период нашел отражения в литературе [1,2]. Применение РЭБ в этот период были эпизодическими, но и они оказали влияние на ход и исход боевых операций.

Вторая мировая война окончательно оформила практику применения методов и средств РЭБ как одного из важных видов обеспечения боевых действий на суше, на море и в воздухе. Появление и развитие в этот период радиолокации вызвало к жизни новые направления РЭБ. Это радиотехническая разведка, действия которой направлены на добывание сведений о типе, назначении и пространственных координатах радиолокационных и радионавигационных средств. О параметрах сигналов, используемых этими средствами.

В период после окончания Второй миро-

вой войны, в многочисленных локальных войнах и вооруженных конфликтах методы и средства РЭБ не только обогащали опыт тактических приемов вооруженной борьбы, но открыли новое направление. Так в ходе войны во Вьетнаме впервые были применены противорадиолокационные ракеты (ПРР) класса воздух-поверхность, специально предназначенных для поражения радиолокаторов в комплексах ПВО. Этот пример создания и применения оружия радиоэлектронной борьбы, но не для информационного поражения помехами, а для силового поражения. В дальнейшем ракеты с пассивными радиоголовками самонаведения нашли применение и для борьбы не только с РЛС, но и с другими информационными системами, демаскирующими свою работу электромагнитным радиоизлучением.

2. РЭБ в настоящем

По современным воззрениям РЭБ – это совокупность взаимосвязанных по цели, задачам, месту и времени мероприятий, действий, направленных на выявление радиоэлектронных средств и систем противника (радиоэлектронная разведка РЭР), их подавлению (РЭП), а также по радиоэлектронной защите (РЭЗ) своих радиоэлектронных систем и средств от средств РЭБ противника в информационном конфликте. Емкое синтетическое понятие РЭБ также и радиоэлектронную маскировку (РЭМ), противостоящую радиоэлектронной разведке противника.

Диалектическое единство и конфликтное взаимодействие таких противоположностей, как РЭР и РЭМ, РЭП и РЭЗ в основном определяет динамику бурного развития средств и методов РЭБ (рисунок 3).

Не будет большим преувеличением и утверждение о том, что единство и борьба этих противоположностей во многом определяет характер современного этапа развития радиоэлектроники.

Проблема РЭБ характеризуется широтой, глубиной и многообразием проявлений. В конфликтное взаимодействие вовлечены информационные системы всех известных классов: передачи и извлечения информации, радиоуправления и разрушения информации.

Проблема РЭБ очень четко стратифицирована. Она предусматривает разделение на уровни и объединение множества уровней описания методов, средств конфликтного взаимодействия. На этих уровнях располагаются описания физических и технических принципов построения и функционирования средств, участвующих в информационном конфликте; описания и модели системных принципов их проектирования и организации взаимодействия; принципы тактики

и оперативного искусства применения средств и методов РЭБ в мирное время и на разных этапах развития вооруженных конфликтов.

История показала, что РЭБ оказалась у истоков очень важного процесса бурного, опережающего развития теории и техники информационных систем. Основной движущей силой этого развития было и остается конфликтное взаимодействие радиоэлектронных систем и средств, являющихся технологической основой функционирования информационной среды нынешнего столетия, с противодействующими факторами и явлениями.

Наиболее очевидны проявления конфликта информационных систем с природой. Именно природа ограничивает скорость и помехоустойчивость передачи информации по каналам связи, производительность источников информации, емкость хранилищ информационного ресурса. Но природа, как афористично утверждал А. Эйнштейн, изощрена, но не злонамеренна. В соревновании коллективного инженерного интеллекта создателей информационных систем с природой в наше время чаще всего побеждают инженеры. Другое дело – конфликт информационных систем с противодействующими системами антропогенной природы, когда сталкиваются интересы и коллективный интеллект разных людей (групп, коалиций). Исход этого конфликта совсем не так однозначен, как в конфликтном взаимодействии с природой. Формы проявления информационного конфликта развиваются и изменяются. Но самое устойчивое и адекватное название для его современного этапа «радиоэлектронная борьба».

3. РЭБ в будущем

За последние 20 лет активной жизни на втором веке своего существования предметная область РЭБ показала, что она отнюдь не снижает темпов своего развития и продолжает впитывать и активно осваивать научные и технологические достижения.

Во-первых, наметившиеся технологические достижения в области создания мощных источников электромагнитных полей открывают возможности для создания средств функционально-

го поражения – нелетального оружия, селективно направленного на подавления электронных подсистем и компонентов информационных систем противника. Но подавления не помехами, как при РЭП, а физического – сильными электромагнитными полями, оказывающими деструктивное воздействие на компонентную базу электронных устройств информационно-телекоммуникационных систем [3]. Известная тенденция к увеличению степени интеграции элементной базы микроэлектроники за счет уменьшения технологического зазора не только увеличивает возможности радиоэлектронных приборов и систем, но и повышает их уязвимость средствами функционального поражения.

Во-вторых, уже сейчас наблюдается увеличение степени интеграция средств РЭБ с иными информационными системами в единые сетевые комплексы средств вооружения, военной и специальной техники. Следует ожидать расширение и углубление этой тенденции в будущем.

В-третьих, развитие методов и средств создания дезинформирующих помеховых воздействий как дальнейшее развитие имитирующих помех для адаптации информационного противодействия к используемым и совершенствуемым приемам помехозащиты. По-видимому, на этом пути РЭБ будет впитывать и использовать методы, развиваемые в системах искусственного интеллекта.

Следует также ожидать, что РЭБ не останется в стороне от создания и внедрения деструктивных программных воздействий в информационно-телекоммуникационные системы и сети противника. То есть, замет подобающее место в среде оружия кибервойн.

Прогнозирование будущего предметной области РЭБ, и даже прогнозирование ее развития задача не очень благодарная. Но, наблюдая тенденции и темпы развития РЭБ за прошедшие 120 лет, можно с уверенностью утверждать, что в этой области возможны большие достижения и неожиданные открытия.

Литература

1. Палий А.И., Куприянов А.И. Очерки истории радиоэлектронной борьбы. М.: Вузовская книга, 2006. 384 с.
2. Радиоэлектронная борьба. От экспериментов прошлого до решающего фронта будущего. Под ред. Н.А. Колесова и М.Г. Насенкова. М.: Центр анализа стратегий и технологий, 2015. 248 с.
3. Радиоэлектронная борьба: функциональное поражение радиоэлектронных средств. М., Воюлда: Инфра-Инженерия, 2021. 268 с.

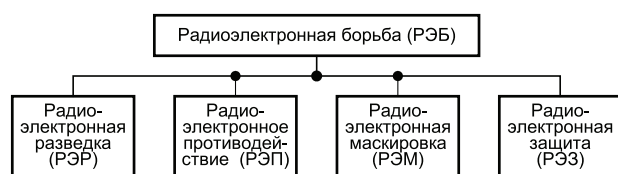


Рис. 3. Современная структура проблемы РЭБ

СОБЫТИЯ

В ИНСТИТУТЕ ИНЖЕНЕРНОЙ ФИЗИКИ СОСТОЯЛОСЬ ВЫЕЗДНОЕ ЗАСЕДАНИЕ КОМИТЕТА ГОСУДАРСТВЕННОЙ ДУМЫ ПО ОБОРОНЕ



Заседание межведомственной рабочей группы по топогеодезическому и навигационному обеспечению было посвящено подведению итогов и докладу об основных результатах работы в 2023 году, постановке основных задач на 2024 год и обсуждению необходимых мер по совершенствованию законодательства Российской Федерации в сфере геодезии, картографии и инфраструктуры пространственных данных в интересах обороны и безопасности государства.

С приветственным словом к собравшимся обратился Президент Института Алексей Николаевич Царьков. Он подчеркнул, что выездные заседания Комитета Государственной Думы по обороне проходят в Институте уже не в первый раз, но впервые это происходит на территории вновь созданного самого большого наукограда страны – Большого



Серпухова. Это очень важный шаг в развитии региона, и есть уверенность, что это позволит в еще большей мере реализовать научно-технический потенциал ученых Большого Серпухова.

Открыл заседание Первый заместитель Председателя Комитета по обороне Андрей Леонидович Красов, который поставил основные цели и задачи совещания. Порядок работы заседания, доклад о результатах работы в 2023 году представил Советник начальника Генерального штаба ВС РФ, руководитель межведомственной рабочей группы по топогеодезическому и навигационно-



му обеспечению Сергей Викторович Козлов. Затем участники совещания представили свои доклады, которые вызвали активное обсуждение. В завершение заседания были подведены итоги и поставлены задачи на подготовку и согласование проекта протокола заседания межведомственной рабочей группы по топогеодезическому и навигационному обеспечению Комитета Государственной Думы по обороне.

После заседания члены межведомственной рабочей группы посетили лабораторию испытаний навигационно-геодезических комплексов и лабораторию квантовых информационных технологий и лазерной физики.



Abood Basel. Graduate student. Moscow technical university of communications and informatics. Moscow, st. Aviamotornaya, 8a.

Alatortsev Alexey I. Doctor of Technical Sciences. Head of the department. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny l., 1a.

Atakischev Oleg I. Honorary Worker of Science and High Technologies of the Russian Federation. Doctor of Technical Sciences, Professor. Deputy General Director for Special Projects. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoi Udarny l., 1a.

Bakmaev Sabir M.-K. Candidate of Physic and Mathematic Sciences. Head Researcher. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoi Udarny l., 1a.

Bessonov Maxim A. Candidate of Technical Sciences. MTUCI. Moscow, st. Aviamotornaya, 8a.

Borisenko Alexander Y. Leading Specialist JSC «MPOVTI». Moscow, st. Academician Koroleva, 13, building 1.

Bugakov Alexey I. Senior Specialist complex testing and debugging groups. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny l., 1a.

Buzakin Ivan S. Cadet. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Daragan Alexey D. Doctor of Technical Sciences. Professor of the department. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Demin Ivan V. Head of the Operations Department of the Energy Supply Department of the educational process support base. Military space Academy named after A.F. Mozhaisky. St. Petersburg, ul. Zhdanovskaya, 13.

Durnov Artyom S. Candidate for the degree of Candidate of Technical Sciences. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny l., 1a.

Efremov Anton A. Candidate of Technical Sciences. Deputy head of the department. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Elistratov Alexander V. Leading engineer. The Institute of Theoretical and Experimental Biophysics. Moscow reg., Pushchino, Institutskaya st., 3.

Emelin Nikolay M. Honored Scientist of the RSFSR, Doctor of Technical Sciences, Professor, Chief Researcher of the Federal State Budgetary Institution «STII». Moscow, Zorge street, 22.

Ermakova Yulia S. Junior researcher of the department JSC Central Research Institute of Mechanical Engineering. Moscow reg., Korolev, st. Pionerskaya, 4.

Frankov Sergey V. Department head. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny l., 1a.

Goncharov Vladimir V. Doctor of Technical Sciences, Professor. Professor at Moscow technical university of communications and informatics. Moscow, st. Aviamotornaya, 8a.

Gribunin Vadim G. Honored Worker of Science and Technology of the Russian Federation. Doctor of Technical Science. Associate Professor. Chief Researcher. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny l., 1a.

Karpov Konstantin V. Post-graduate. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Kazakov Rafael' R. Candidate of Technical Sciences. Deputy Head of the Department of «Tactics of units and subdivisions of rocket and space defense». Military space Academy named after A.F. Mozhaisky. St. Petersburg, ul. Zhdanovskaya, 13.

Klementyev Egor G. Post-graduate. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Kolombet Valeriy A. Candidate of Physical and Mathematical Sciences. Head of the laboratory. The Institute of Theoretical and Experimental Biophysics. Moscow reg., Pushchino, Institutskaya st., 3.

Komarov Ivan D. Candidate of Technical Sciences. Associate Professor. JSC Central Research Institute of Mechanical Engineering. Moscow reg., Korolev, st. Pionerskaya, 4.

Krikunov Alexey A. Candidate of Technical Sciences. Doctoral student. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Kuchmenko Tat'yana A. Doctor of Chemical Sciences. Professor. Head physical and analytical chemistry department. Voronezh state university of engineering technologies. Voronezh, Revolution Av., 19.

Kupriyanov Alexander I. Doctor of Technical Sciences. Professor. Moscow Aviation Institute (NRU) Moscow, Volokolamskoe highway, 4.



AUTHORS

Lesnykh Vadim N. Junior scientist. The Institute of Theoretical and Experimental Biophysics. Moscow reg., Pushchino, Institutskaya st., 3.

Lesnykh Viktor V. Teacher of the Department of Physics. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya st., 17.

Lychagov Alexander S. Candidate of Technical Sciences. Doctoral student. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya st., 17.

Nakonechny Andrey B. Researcher. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Piskulin Igor V. Lecturer. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya st., 17.

Podvigin Sergey V. Candidate of technical Sciences. Head of laboratory quantum informatics technology. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Popov Alexandr V. Adjunct of the Department. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya st., 17.

Poryadina Dar'ya A. Candidate of Chemical Sciences. Lecturer. Branch of the Military Academy of the Strategic Missile Force. Moscow reg., Serpukhov, Brigadnaya st., 17.

Pushkareva Elena Y. Doctor of Technical Sciences. Professor. Professor of the Department. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya st., 17.

Rudenko Edvard M. Candidate of Technical Sciences. Associate Professor of the Department of Mathematics. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Semikina Elena V. Lecturer. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Shakhov Denis S. Student. MAI branch «Strela». Moscow reg., Zhukovsky, st. Zhukovskogo, 8.

Shimanov Sergey N. Honorary Worker of Higher Professional Education of the Russian Federation, Honorary Radio Operator of the Russian Federation. Doctor of Technical Sciences, Professor. Leading Researcher. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Sholokhov Aleksei V. Doctor of Technical Sciences, Professor. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.

Shulga Mikhail M. Graduate student. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Smirnov Dmitriy V. Honored Worker of Science and Technology of the Russian Federation, Doctor of Technical Sciences, associate professor. Full member of the Academy of Engineering Sciences. Professor of the Department FSBEI of HE MAI (NRU). First Vice President of the Institute – Deputy Chairman of the Board of the Institute of Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Smurov Sergey V. Honored Worker of Science and Technology of the Russian Federation, Doctor of Technical Sciences, professor. First Vice President of the Institute – Chief Designer. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Taganov Nikita S. Graduate. Moscow technical university of communications and informatics. Moscow, st. Aviamotornaya, 8a.

Vasilyev Valentin V. Candidate of Technical Sciences, Associate Professor. Moscow Aviation Institute (National Research University). Moscow, Volokolamsk Highway, 4.

Volkov Gennadiy G. Doctor of Physical and Mathematical Sciences. Professor. Senior Researcher. Institute of Engineering Physics. Moscow reg., Serpukhov, Bolshoy Udarny I., 1a.

Zakharov Vladimir L. Doctor of Military Sciences, professor. Full member of the Academy of Military Sciences. Professor. FSBEI of HE MAI (NRU). Moscow, Volokolamsk Highway, 4.

Zelenevsky Vladimir V. Honored Worker of Science and Technology of the Russian Federation Doctor of Technical Sciences, Professor, professor of the department. Branch of the Military Academy of the Strategic Missile Force. Moscow reg., Serpukhov, Brigadnaya st., 17.

Zelenevsky Yury V. Doctor of Technical Sciences, associate professor. Researcher. Military Academy of the Strategic Missile Force. Moscow Reg., Balashikha, Karbysheva st., 8.

Zverev Igor A. Cadet. Branch of the Military Academy of the Strategic Missile Forces. Moscow reg., Serpukhov, Brigadnaya St., 17.



ЭТИКА НАУЧНЫХ ПУБЛИКАЦИЙ

Редакционный совет и редакционная коллегия научно-технического журнала «Известия Института инженерной физики» придерживаются принятых международным сообществом принципов публикационной этики, отраженных, в частности, в рекомендациях Комитета по этике научных публикаций (Committee on Publication Ethics).

Все статьи, предоставленные для публикации в журнале «Известия Института инженерной физики», проходят рецензирование на оригинальность, этичность и значимость. Соблюдение стандартов этического поведения важно для всех сторон, принимающих участие в публикации: авторов, редакторов журнала, рецензентов, издателя.

ОБЯЗАННОСТИ РЕДАКТОРА

Редактор в своей деятельности обязуется:

- постоянно совершенствовать журнал;
- следовать принципу свободы мнений;
- стремиться к удовлетворению потребностей читателей и авторов журнала;
- исключать влияние интересов бизнеса или политики на принятие решений об опубликовании материалов;
- принимать решения на основании принципа справедливости и беспристрастности, обеспечивать прозрачность редакционной деятельности на всех ее этапах;
- не раскрывать информацию о предоставленных материалах никому, кроме соответствующих авторов, рецензентов, других редакционных консультантов;
- оценивать рукописи исключительно по их научному содержанию;
- принимать решение о публикации материалов, руководствуясь следующими главными критериями: соответствие рукописи тематике журнала; актуальность, новизна и научная значимость представленной статьи; ясность изложения; достоверность результатов и законченность выводов. Качество исследования и его актуальность являются основой для решения о публикации;
- принимать меры для обеспечения высокого качества публикуемых материалов и защиты конфиденциальности персональной информации. При обнаружении содержательных, грамматических, стилистических и иных ошибок редакция обязуется предпринимать все меры для их устранения;
- обосновать свое решение в случае принятия или отклонения статьи;
- предоставить автору рецензируемого материала возможность для обоснования своей исследовательской позиции;
- поощрять дискуссии и предоставлять возможность для изложения точки зрения оппонентов;
- не использовать в собственных исследованиях информацию из неопубликованных материалов.

ОБЯЗАННОСТИ ЧЛЕНОВ РЕДСОВЕТА (РЕДКОЛЛЕГИИ)

Решение о публикации.

Редсовет (редколлегия) журнала «Известия Института инженерной физики» являются ответственными за принятие решения о том, какие статьи будут опубликованы в журнале. Решение принимается на основании представляемых на статью рецензий

Редсовет (редколлегия) придерживаются политики журнала и действуют в рамках законных требований, поскольку несут ответственность за нарушение авторских прав.

Конфиденциальность.

Рецензенты или кто-либо из сотрудников редакции не должны разглашать никакую информацию о предоставленной рукописи кому-либо, кроме самого автора, рецензентов, потенциальных рецензентов, членов редакционного совета (коллегии) и издателя, поскольку она является конфиденциальной.

Раскрытие информации и конфликт интересов.

Неопубликованные материалы, находящиеся в предоставленной статье, не должны быть использованы в собственном исследовании научного редактора и рецензентов без специального письменного разрешения автора.

ОБЯЗАННОСТИ РЕЦЕНЗЕНТОВ

Рецензенты оказывают помощь членам редакционного совета (редколлегии) при принятии редакционного решения, а также помогают автору усовершенствовать работу.

Конфиденциальность.

Любые рукописи, полученные для рецензирования, должны восприниматься как конфиденциальные документы. Они не могут быть показаны либо обговорены с другими лицами, кроме тех, которые уполномочены редакцией.

Подтверждение источников.

Рецензенты должны идентифицировать опубликованную работу, которая не была процитирована автором. Любое утверждение, что наблюдение, происхождение либо аргумент ранее были сообщены, необходимо сопровождать соответствующей ссылкой. Рецензент должен также донести до сведения редакции о любой существенной схожести или частичном совпадении между рукописью, которая рецензируется, и другой уже опубликованной работой, которая ему знакома.

Раскрытие информации и конфликт интересов.

Приватная информация или идеи, возникшие в процессе рецензирования, должны остаться конфиденциальными и не могут быть использованы в личных интересах. Рецензент не должен рассматривать рукопись, если имеет место конфликт интересов в результате его конкурентных, партнерских либо других отношений или связей с кем-либо из авторов, компаний или организаций, связанных с материалом публикации.

ОБЯЗАННОСТИ АВТОРОВ

Оригинальность и плагиат.

Авторы должны гарантировать, что они написали полностью оригинальную работу. Если авторы использовали работу и/или слова других авторов, это должно быть соответственно указано и процитировано.

Доступ к данным и сохранность.

Автор должен быть готов обеспечить доступ к данным, связанными с материалом публикации, если таковой возможен. Во всяком случае, автор должен быть готов сохранять такие данные на протяжении разумного периода времени после опубликования.

Многоразовая, избыточная или конкурирующая публикация.

Автор не должен публиковать работы, которые описывают по сути одно и то же исследование, более чем один раз или более чем в одном журнале.

Предоставление рукописи более чем в один журнал одновременно означает неэтичное издательское поведение и является недопустимым.

Подтверждение источников.

Необходимо предоставлять должное подтверждение работ других авторов. Авторы должны процитировать публикации, которые имели значение при создании заявленной работы.

Авторство материала.

Авторство необходимо ограничить теми лицами, которые внесли ощутимый вклад в концепцию, проект, исполнение или интерпретацию заявленной работы. Всех, кто внес ощутимый вклад, следует внести в список соавторов.

Автор должен гарантировать, что список авторов содержит только действительных авторов и в него не внесены те, кто не имеет отношения к данной работе, а также то, что все соавторы ознакомились и одобрили окончательную версию статьи и дали согласие на ее публикацию.

Раскрытие информации и конфликт интересов.

Все авторы должны сообщать, если в их работе имеется финансовый либо другой конфликт интересов, который может повлиять на результаты или интерпретацию их рукописи.

Ошибки в опубликованных работах.

Если автор обнаружит существенную ошибку или неточность в своей опубликованной работе, его обязанность – незамедлительно сообщить об этом в редакцию журнала или издателя и сотрудничать с редакцией при исправлении ошибок.

НАРУШЕНИЯ

При возникновении ситуации, связанной с нарушением публикационной этики со стороны редактора, автора или рецензента, требуется ее обязательное рассмотрение. Редакционный совет (редколлегия) обязана потребовать разъяснения, без привлечения лиц, которые могут иметь конфликт интересов с одной из сторон.

Если материал, содержащий значительные неточности, был опубликован, он должен быть незамедлительно исправлен в форме, доступной для читателей и систем индексирования.

ТРЕБОВАНИЯ К АВТОРАМ СТАТЕЙ

Для публикации принимаются статьи на русском языке. Объем статьи – 0,2–0,4 п.л. (8000–16000 знаков).

Тексты должны быть представлены:

- в электронном виде (Word 2003). Иллюстративный материал (сложные формулы, рисунки, фотографии и т.д.) кроме размещения в тексте обязательно должны предоставляться отдельными файлами!

- на бумажном носителе формата А4.

Текст статьи должен быть набран через 1,5 интервала (гарнитура «Times New Roman»), кегль 14.

Простые символы и формулы не набирать в математическом редакторе!

Напечатанный текст должен иметь поля: верхнее и левое – 2,5 см, правое и нижнее – 2 см.

Вверху первой страницы статьи размещаются:

- рубрика журнала (см. Приложение 1);
- УДК;
- название статьи с переводом на английский язык;
- имя, отчество, фамилия автора (авторов), ученая степень, ученое звание, должность и место работы.

Список литературы (Литература) размещается в конце статьи.

После литературы помещаются:

- список ключевых слов, краткая аннотация (на русском и английском языках).

Завершает рукопись полная информация об авторе (авторах):

- ФИО;
- ученая степень, ученое звание, должность и место работы с переводом на английский язык;
- адрес места работы, контактные телефоны, электронный адрес.

Обращаем особое внимание на:

- точность и правильность библиографического оформления списка литературы (в соответствии с ГОСТ Р 7.0.5-2008);
- выверенность статьи в компьютерном наборе;
- полное соответствие файла на электронном носителе и бумажного варианта.

Редакционная коллегия оставляет за собой право на редактирование статей, при этом с точки зрения научного содержания авторский вариант сохраняется.

Статьи, не принятые к публикации, не возвращаются. Плата с аспирантов за публикацию рукописей не взимается!

Приложение 1

РУБРИКАЦИЯ ЖУРНАЛА «Известия Института инженерной физики»

Постоянные рубрики

- **Приборостроение, метрология и информационно-измерительные приборы и системы.**
- **Радиотехника и связь.**
- **Информатика, вычислительная техника и управление.**

Разовые рубрики

- **Техника специального назначения.**
- **Инновационные проекты.**
- **Техническое регулирование.**
- **Профессиональное образование.**
- **Искусственный интеллект и робототехника.**
- **Современная медицина и фармацевтика.**
- **Наукометрия.**
- **Диагностические системы.**
- **Научные обзоры. Научные рецензии. Отзывы.**

В соответствии с Решением Межведомственной комиссии РФ по защите государственной тайны №69 от 26 февраля 2001 г., требованиями законов №5485-1 «О государственной тайне» от 21 июля 1993 г., №149-ФЗ «Об информации, информационных технологиях и защите информации» от 27 июля 2006 г. статьи для публикации принимаются только при наличии экспертного заключения с разрешением на открытое опубликование.



CONTENTS

INSTRUMENT MAKING, METROLOGY AND INFORMATION-MEASURING DEVICES AND SYSTEMS

Vasiliev V.V., Shakhov D.S.

The design concept of an all-in-one center wingbox made of made of polymer composite materials 2

Poryadina D.A., Kuchmenko T.A., Buzakin I.S.

Auto-identification of automotive fuels based on the results of the full analysis using the principal component method 7

Zakharov V.L., Smirnov D.V., Demin I.V., Kazakov R.R.

Analysis of the features of safe operation of power equipment in space force units 10

RADIO ENGINEERING AND COMMUNICATION

Shimanov S.N., Krikunov A.A., Frankov S.V.

The influence of the diffuseness of router metrics on the optimal solution of the routing problem in a packet-switched communication network 15

Alatortsev A.I., Podvigin S.V., Bakmaev S.M-K.

Model of a quantum repeater based on a nitrogen vacancy in a diamond single crystal as a promising direction for the implementation of secure quantum networks 22

Zelenevsky V.V., Zelenevsky Y.V., Popov A.V., Durnov A.S., Nakonechny A.B.

Statistical analysis of ways to increase the noise immunity of data transmission systems 26

INFORMATION SCIENCE, COMPUTING AND MANAGEMENT

Taganov N.S., Bessonov M.A.,

Building a DLP system mail analyzer based on keywords..... 31

Rudenko E.M., Semikina E.V.

The method of calculating eulerian and hamiltonian routes for UAVS using reduction 39

Sholokhov A.V., Lychagov A.S., Karpov K.V.

Determining whether a moving object is located on a section of a digital road map 45

Kolombet V.A., Lesnykh V.N., Elistratov A.V.

The perspective of the study of psychoactive substances in biophysical psychoanalysis 49

Daragan A.D., Efremov A.A., Klementyev E.G., Rudenko E.M., Semikina E.V.

Objective functions of routes on eulerian and hamiltonian graphs 57

Abod B., Goncharov V.V.

Efficiency of image encryption using AES and elliptic curves: experimental evaluation 62

Smurov S.V., Volkov G.G.

Unitary symmetries in parton dynamics of the proton 71

Atakishev O.I., Gribunin V.G., Komarov I.D., Borisenko A.Y., Ermakova Y.S.

A methodology for ensuring information security of automated military systems based on the optimal reliability of steganographic analysis of transmitted information 79

Pushkareva E.Y., Piskulin I.V.

The method of synthesis of a tracking motion control system of a promising RC MP in the autonomous guidance mode 86

ARTIFICIAL INTELLIGENCE AND ROBOTICS

Bugakov A.I., Shulga M.M.

Feature selection and integration for continuous adaptive multi-factor authentication of a smartphone user 92

PROFESSIONAL EDUCATION

Lesnykh V.V., Zverev I.A.

Creative interpretation of scientific facts as an element of training engineering and scientific personnel (experience in creating a scientific-historical quest) 97

SCIENTIFIC REVIEWS. SCIENTIFIC CRITIQUES. COMMENTS

Emelin N.M.

Trends in the development of science cities as territories with high scientific and technological potential 104

Kupriyanov A.I.

120 years of electronic warfare: history, modernity, prospects107

EVENTS

..... 112

AUTHORS

..... 113

THE ETHICS OF SCIENTIFIC PUBLICATIONS

..... 115

REQUIREMENTS TO AUTHORS

..... 116

Учредитель и издатель – АНО «Институт инженерной физики».

Адрес: 142210,
Московская обл., г.о. Серпухов, г. Серпухов, Большой Ударный пер., д. 1а, стр. 1.

Подписной индекс: 59190
по каталогу «Урал-Пресс»

Адрес редакции: 142210, Московская обл.,
г.о. Серпухов, г. Серпухов, Большой Ударный пер., д. 1а, стр.1.

Тел: +7 (4967) 35-31-93, 35-13-71
Факс: +7 (4967) 35-44-20 <http://www.iifrf.ru>
E-mail: info@iifmail.ru

Издание зарегистрировано в Федеральной службе по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия.

Свидетельство о регистрации СМИ ПИ №ФС 77-84007 от 30.09.2022
Отпечатано на полиграфической базе АНО «Институт инженерной физики».

Адрес: 142210, Московская обл., г.о. Серпухов, г. Серпухов,
Большой Ударный пер., д. 1а, стр. 1.

Подписано в печать 19.04.2024.

Дата выхода в свет 27.04.2024. Тираж 2000 экз. Цена свободная.

© Автономная некоммерческая организация
«Институт инженерной физики», 2024.



Автономная некоммерческая организация
“Институт инженерной физики”

142210, Московская обл., г. о. Серпухов, г. Серпухов, Большой Ударный переулок, д. 1а, стр. 1
<http://www.iifrf.ru> e-mail: info@iifmail.ru
Тел.: +7(4967) 35-31-93, 35-13-71, +7 (499) 400-05-75, факс: +7(4967) 35-44-20