

Министерство науки и высшего образования
Российской Федерации

КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет математики и компьютерных наук

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И МОДЕЛИ В РЕШЕНИИ ПРИКЛАДНЫХ ЗАДАЧ

Материалы
Всероссийской научно-практической конференции

г. Краснодар, 30–31 октября 2023 г.

Краснодар
2023

УДК 57-1

ББК 22.1

М 34

Редакционная коллегия:

*В. В. Василенко, В. Ю. Барсукова, А. С. Сергиенко,
А. В. Рожков, С. П. Грушевский*

Рецензент: доктор технических наук, профессор, заслуженный
работник высшей школы Российской Федерации

О. А. Финько

М 34 Математические методы и модели в решении прикладных задач: материалы Всероссийской научно-практической конференции / под редакцией В. В. Василенко; Министерство науки и высшего образования Российской Федерации, Кубанский государственный университет. – Краснодар: Кубанский гос. ун-т, 2023. – 108 с. – 500 экз.
ISBN 978-5-8209-2346-3

Представлены научные труды участников Всероссийской научно-практической конференции «Математические методы и модели в решении прикладных задач», организованной 30 — 31 октября 2023 г. кафедрой функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета.

Адресуется студентам, магистрантам, преподавателям вузов и специалистам в области математического моделирования.

УДК 57-1

ББК 22.1

ISBN 978-5-8209-2346-3

© Кубанский государственный университет, 2023

СОДЕРЖАНИЕ

СЕКЦИЯ 1. ИНЖЕНЕРНОЕ ДЕЛО, РОБОТОТЕХНИКА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Андикаев С.П., Кошелев Д.А., Ромашов А.А. ПРИМЕНЕНИЕ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ В КАНАЛЕ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ	7
Емельянов В.А., Козлов Б.С., Кошелев Д.А., Шульгин М.Г. СХЕМА ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ	11
Канищев К.К., Ханазарян А.Д., Мороз И.А., Голуб М.В., Еремин А.А. ПЛАНИРОВАНИЕ И ПРОВЕДЕНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ ПО ИЗУЧЕНИЮ СВОЙСТВ АКУСТИЧЕСКИХ МЕТАМАТЕРИАЛОВ И ПЛАСТИКОВ, ПОЛУЧАЕМЫХ С ПОМОЩЬЮ 3D ПЕЧАТИ.....	16
Романюта Д.Ю. МОБИЛЬНЫЕ НЕЙРОСЕТЕВЫЕ МОДЕЛИ ДЛЯ РАСПОЗНАВАНИЯ ЛИЦ.....	20
Стасюк К.В. ИСПОЛЬЗОВАНИЕ УСЛОВНЫХ СЛУЧАЙНЫХ ПОЛЕЙ (CRF) ДЛЯ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЯ.....	23
Черная Ю.О. РАЗРАБОТКА ОНТОЛОГИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ГРАФА ЗНАНИЙ МЕДИЦИНСКИХ КАРТ.....	29

СЕКЦИЯ 2. ЭКОНОМИКА И СОЦИАЛЬНАЯ СФЕРА. ЗАДАЧИ ЦИФРОВИЗАЦИИ В СОВРЕМЕННОМ ОБЩЕСТВЕ

Баранцев Д.Д. РАСПОЗНАВАНИЕ ТЕКСТА, ПРЕДВАРИТЕЛЬНАЯ БИНАРИЗАЦИЯ.....	33
Васкевич Т.В. РЕГРЕССИОННЫЙ АНАЛИЗ ИНВЕСТИЦИОННОЙ ПРИВЛЕКАТЕЛЬНОСТИ РЕГИОНОВ РФ.....	38
Белоусов Н.А., Захаров М.Ю., Овсиенко Н.И., Касперович Ю.И. ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ДОСТОВЕРНОСТИ ДОПУСКОВОГО КОНТРОЛЯ, ДИАГНОСТИКИ И БИНАРНОЙ КЛАССИФИКАЦИИ.....	44
Овчинникова А.А. УСИЛЕНИЕ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА НА ОСНОВЕ АЛГОРИТМА RSA	49

СЕКЦИЯ 3. ЕСТЕСТВЕННОНАУЧНЫЕ ЗАДАЧИ И АЛЬТЕРНАТИВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

Афанасьева Т.Н., Ойнас И.Л., Гумбатова С.Ф. МОДЕЛИ РАСПРОСТРАНЕНИЯ НЕРВНОГО ИМПУЛЬСА	53
--	----

Беженар М.В., Малышко В.В. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ВОЗНИКНОВЕНИЯ ПУЗЫРЬКОВ ДЕНАТУРАЦИИ В МОЛЕКУЛЕ ДНК	59
Василенко В.В., Сергиенко А.С. О НЕКОТОРЫХ СВОЙСТВАХ ПОДКАСАТЕЛЬНЫХ	63
Лясота О.М., Джимаков С.С., Дроботенко М.И. МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ВОЗНИКНОВЕНИЯ ОТКРЫТЫХ СОСТОЯНИЙ В ОБЛАСТИ САГ-ПОВТОРОВ ГЕНА АТХN2	65
Сверкунова Д.А., Дорошенко О.В., Голуб М.В., Ханазарян А.Д., Шпак А.Н. АЛГОРИТМ ПОСТРОЕНИЯ МЕТАМОДЕЛИ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ПРЕДСКАЗАНИЯ ЭКСПЕРИМЕНТАЛЬНО ИЗМЕРЯЕМОГО ОТКЛИКА СЕНСОРА НА ПЛАСТИНЕ С ВЫЕМКОЙ	69
Титов Г.Н., Зинченко Т.В., Скибицкий Д.Р. ОБ ОДНОМ АЛГОРИТМЕ НАХОЖДЕНИЯ ЧИСЛА ФРОБЕНИУСА ТРОЙКИ НАТУРАЛЬНЫХ ЧИСЕЛ	74
Толкачева Е.Г., Пуляев В.Ф. О СПЕКТРЕ ЛИНЕЙНЫХ НЕПРЕРЫВНЫХ ОПЕРАТОРОВ	82
Христюк Е.А., Савин В.Н. ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СЛУЧАЙНЫХ ЧИСЕЛ	86
Шашков Д.И., Дроботенко М.И. ФИЗИКО-МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА СИНТЕЗА НАНОЧАСТИЦ СЕРЕБРА	91

СЕКЦИЯ 4. МЕЖДИСЦИПЛИНАРНЫЕ ПРОБЛЕМЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ

Барсукова В.Ю., Бочаров А.В., Цалюк М.В. О ПРОБЛЕМАХ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ» НА ФАКУЛЬТЕТЕ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК КУБГУ	97
---	----

***Приветственный адрес почётного гостя
Всероссийской научно-практической конференции
«Математические методы и модели в решении
прикладных задач»***

***заместителя председателя Краснодарского краевого суда
Борисовой Ольги Васильевны***

***Об актуальности задач математического
моделирования в вопросах цифровизации судебной власти РФ***

Уважаемые участники конференции! Уважаемые коллеги!

С развитием высоких цифровых технологий всё больше ощущается потребность в специалистах смежных классов профессий. Сегодня, после технологического прорыва прошлых десятилетий, уже никого не удивляют не только применение искусственного интеллекта, но и разработки ИТ-технологий, внедряемые повсеместно в быт и деятельность современного человека. Медицина, средства связи и передачи информации, общественный транспорт, образование, а также государственная форма правового регулирования взаимоотношений в современном обществе уже невообразимы без «цифры».

К одной из перспективных развивающихся отраслей относится цифровизация судебной власти в Российской Федерации — это достаточно новое направление в научном мире, которое может становиться и воплощаться лишь в интегрированном научном развитии, на первый взгляд, абсолютно несмежных отраслей. Основная сложность в данном направлении заключается в слиянии цифровых технологий, норм права и этики в единое целое.

Одно из важнейших качеств, необходимых для планирования и решения задач цифровизации — это согласованность между специалистами различных профессиональных сообществ, таких как: математики, юристы, судьи, программисты... Этот подход комплексного разрешения «внедрения цифры» ставит серьёзные задачи как перед профессиональными сообществами по отдельности, так и по интеграции научных знаний в целом. А потому подготовка специалистов высокого уровня образованности по праву может считаться приоритетной задачей нашей страны, что подтверждает высокий интерес и актуальность конференции, как текущая — «Математические методы и модели в решении прикладных задач».

Именно такие становления научных трендов формируют много глобальных задач, успешное решение которых заложит основу всего конструкта целых экосистем цифровых технологий. Это позволит в будущем решать поставленные государством задачи и развиваться в траекториях оптимизации инфотрафика, обозначенных руководством страны.

Я благодарю оргкомитет за предоставленную возможность быть причастной к миру современных технологий и математики, необходимых для решения задач цифровизации, и смею надеяться на взаимное, плодотворное сотрудничество в решении задач внедрения IT-технологий для ветви судебной власти РФ.

Позвольте пожелать всем участникам конференции успехов и прекрасных результатов в научной деятельности!

С уважением, О.В. Борисова

СЕКЦИЯ 1. Инженерное дело, робототехника и искусственный интеллект

С.П. Андикаев, Д.А. Кошелев, А.А. Ромашов

ПРИМЕНЕНИЕ МЕТОДОВ ЦИФРОВОЙ СТЕГАНОГРАФИИ ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ В КАНАЛЕ УПРАВЛЕНИЯ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

В статье рассматривается возможность применения методов цифровой стеганографии для скрытия информации, передаваемой по каналам робототехнических комплексов и обосновывается эффективность применения рассмотренных алгоритмов.

Ключевые слова: стеганография, сообщение, контейнер, стегоключ, алгоритмы сжатия, пиксели.

The article considers the possibility of using digital steganography methods to hide information transmitted through the channels of military (special) purpose robotic complexes and substantiates the effectiveness of the algorithms considered.

Key words: Steganography, message, container, stegoclick, compression algorithms, pixels.

Концепция развития беспилотных летательных аппаратов до 2030 года ставит задачу по достижению качественно нового уровня развития передовых информационных технологий и способов их применения.

По этой причине высокую актуальность обретает разработка и совершенствование систем связи и передачи данных.

Еще с древнейших времен человечество использовало различные методы криптографической защиты для сокрытия значимой информации. Однако их применение скрывает только содержимое тайного сообщения, при этом оставляя явным сам факт наличия информации. Потенциально эффективным решением данной проблемы является применение методов стеганографии.

Стеганография – способ передачи или хранения информации, обеспечивающий сохранение в тайне самого факта передачи (хранения) [1].

Преимущество стеганографии над чистой криптографией состоит в том, что сообщения, передаваемые ее методами, не выдают своего наличия и поэтому не привлекают к себе внимания.

В настоящее время под стеганографией чаще всего понимают скрытие информации в текстовых, графических либо аудиофайлах путём использования специального программного обеспечения. При этом независимо от применяемых методов используется единый понятийный аппарат.

Сообщение — передаваемая скрытая информация.

Контейнер — любая информация, используемая для сокрытия тайного сообщения.

Пустой контейнер — контейнер, не содержащий секретного послания.

Заполненный контейнер (стегоконтейнер) — контейнер, содержащий секретное послание.

Ключ (стегоключ) — секретный ключ, нужный для сокрытия стегоконтейнера. Ключи в стегосистемах бывают двух типов: закрытые (секретные) и открытые. Если стегосистема использует закрытый ключ, то он или должен быть создан до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно из него восстановить закрытый ключ. В этом случае открытый ключ можно передавать по незащищённому каналу.

Наиболее современным и актуальным направлением классической стеганографии является цифровая стеганография, основанная на сокрытии информации в цифровых объектах путем вызывания в них некоторых искажений. Интерес представляет тот факт, что в роли контейнеров выступают мультимедиа-объекты, и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.

В качестве стегоконтейнеров чаще всего используются изображения, что обусловлено несколькими значимыми причинами:

цифровые изображения обладают большим информационным объёмом, что позволяет скрывать значительное количество информации, либо обеспечивать большую устойчивость внедрения;

многие изображения имеют области, которые имеют шумовую структуру и хорошо подходят для встраивания информации.

Криптоанализ таких систем начинается, обычно, с визуальной оценки, однако глаз не способен различить незначительные изменения оттенка, вызванные записью сообщения в битовое представление цветов, благодаря чему такой канал передачи данных остается нераскрытым.

Для решения задачи сокрытия информации в телеметрической составляющей канала управления БЛА могут быть применены различные методы стеганографии.

Метод наименьшего значащего бита (Least Significant Bit, далее - LSB), который заключается в замене последних значащих битов в контейнере на биты скрываемого сообщения. При этом разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

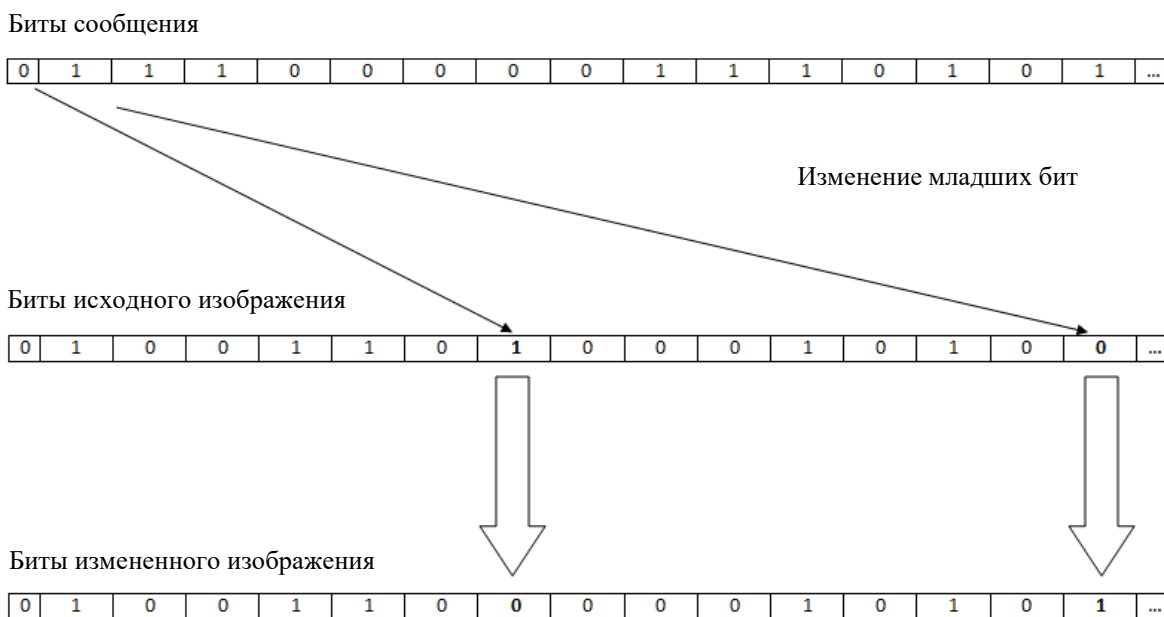


Рис. 1. Метод наименьшего значащего бита (LSB)

Данный метод имеет следующий алгоритм работы:

1. Имеется 8-битное изображение в градациях серого, 00h(00000000b) — черный цвет, FFh (11111111b) — белый цвет, всего 256 градаций (2^8).

2. Допустим, скрываемое сообщение состоит из 1 байта. Например: 01101011b.

3. Если использовать 2 младших бита, то потребуется 4 пикселя. Предположим, что они черного цвета, тогда пиксели, которые будут содержать скрытое сообщение, принимают следующий вид: 00000001, 00000010, 00000010 и 00000011.

4. Цвет этих пикселей изменится следующим образом: первого — $1/255$, второго — $2/255$ и т.д., такие градации не только не заметны для человека, но и не отображаются на низкокачественных устройствах вывода, что делает вероятность обнаружения скрытой информации достаточно низкой.

Поскольку метод LSB является аддитивным, то он характеризуется крайней неустойчивостью ко всем видам атак. Более того, при работе с различными форматами сжатия (JPEG) или при потере данных данный метод является неэффективным, из-за неустойчивости к геометрическим преобразованиям, возникающим при изменении количественной и качественной структур контейнеров [2].

Еще одним из стеганографических алгоритмов, используемых для скрытия информации в изображении, является алгоритм Куттера-Джордана-Боссена. Он основан на использовании слабой восприимчивости зрительной системы человека к изменению яркости синего цвета.

Исходя из этого, для размещения дополнительной информации в 1 пиксель контейнера встраивается 1 бит сообщения, а секретный ключ содержит координаты пикселей, в которые будет встроено сообщение. При встраивании битов скрываемой информации показатели яркости зеленого и красного цветов остаются без изменения, что значительно уменьшает вероятность обнаружения изменений изображения. Дополнительную скрытность передаваемого сообщения обеспечивает отсутствие необходимости в наличии у принимающей стороны оригинального изображения, так как значение яркости синего цвета прогнозируется.

Также к достоинствам данного метода относятся высокая пропускная способность, высокая устойчивость к частотному детектированию, устойчивость к разрушению младших бит контейнера, устойчивость к атаке сжатия [3].

Однако вероятностный характер извлечения яркости цвета также является недостатком, поэтому для уменьшения вероятности ошибки и повышения надежности системы рекомендуется использовать методы помехоустойчивого кодирования.

В отличие от алгоритма Куттера-Джордана-Боссена, алгоритм Брайндокса использует фиксированную область пикселей (8*8).



Рис. 2. Примеры блоков с нечетким и резко выраженным контрастом

Он содержит следующие этапы:

1. Классификация, или разделение пикселей внутри блока на две группы с примерно однородными яркостями [4];
2. Разбиение каждой группы на категории, определяемые данной сеткой;
3. Модификация яркости пикселей в каждой категории каждой группы с целью внедрения информационного сообщения.

При сравнении данного алгоритма с ранее рассмотренным было выявлено, что алгоритм Брайндокса превосходит алгоритм Куттера по таким ключевым параметрам, как временная сложность (как внедрения, так и извлечения), устойчивость, скрытность, а также надежность в области больших значений параметров внедрения сообщения.

Все вышеперечисленные методы стеганографии, используя избыточность визуальной информации, обеспечивают достаточный уровень скрытности передаваемых сообщений и, несмотря на наличие недостатков, обладают целым рядом описанных ранее достоинств.

Однако это не исключает возможности обнаружения стегаканала злоумышленником, поэтому при передаче сообщения, скрываемого в файле изображения, необходимо дополнительно применять методы шифрования исходного сообщения, чтобы даже при обнаружении факта передачи злоумышленник не имел возможности сразу получить исходное сообщение.

Таким образом, применение методов цифровой стеганографии обеспечивает возможность скрытной передачи информации в телеметрическом информационном потоке, без нанесения ущерба оперативности ее доведения.

Библиографический список

1. Стеганография / [Электронный ресурс] // Википедия : [сайт]. — URL: [#https://ru.wikipedia.org/wiki/Стеганография#](https://ru.wikipedia.org/wiki/Стеганография).D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB (дата обращения: 23.10.2023).
2. Губенко, Н. Е., Сипаков, Д. С. Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам [Текст] / Н. Е. Губенко, Д. С. Сипаков // ИНФОРМАТИКА И КИБЕРНЕТИКА. — 2015. — № 2. — С. 28-38.
3. Стеганографический метод Куттера-Джордана-Боссена / [Электронный ресурс] // Хабр : [сайт]. — URL: <http://habrahabr.ru/post/115287/> (дата обращения: 23.10.2023).
4. Васильева, Е. В. Цифровая стеганография [Текст] / Е. В. Васильева // Дискретная математика: алгоритмы. — 2006. — № 1. — С. 1-20.

В.А. Емельянов, Б.С. Козлов, Д.А. Кошелев, М.Г. Шульгин СХЕМА ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье проведен анализ угроз, нарушителей, демаскирующих признаков и каналов утечки информации в автоматизированных информационных системах. По результатам анализа построена диаграмма Исикавы.

Ключевые слова: защита информации, угроза информационной безопасности, комплексная защита, автоматизированная система, информационная система, канал утечки информации.

The article analyzes threats, intruders, unmasking signs and methods of information leakage in the context of military use of a military unit. Based on the results of the analysis, an Isshikawa diagram was constructed.

Key words: Key words: information protection, threat to information security, comprehensive protection, automatic system, military countermeasures information system, information leakage channel.

Автоматизированные информационные системы (далее АИС) в настоящее время играют важную роль в системе управления гражданских летательных процессов. Они позволяют увеличить скорость принятия решений, упростить процесс обмена информацией, а также содержат в себе огромное количество данных, большинство из которых являются информацией ограниченного распространения. В связи с этим автоматизированные информационные системы вызывают огромный интерес со стороны потенциальных злоумышленников.

Под информационной безопасностью (далее ИБ) понимают защищенность информации от преднамеренных или случайных действий, приводящих к нанесению какого-либо ущерба. Поэтому решается обширный комплекс задач для обеспечения ИБ и защиты информации в АИС. Одной из основных задач в создании комплексной системы защиты информации является определение вероятных угроз, нарушителей, каналов утечки информации (далее КУИ), а также демаскирующих признаков (далее ДМП) информационных систем. При этом также требуется выполнить анализ деятельности центров управления полетами, исследовать информационные каналы, проходящие через подразделения, составить перечень информации ограниченного распространения, выделить круг лиц, имеющих доступ к данной информации.

Анализ информационных ресурсов центра управления полетами – это этап выделения информации, которая представляет ценность, является одним из важных этапов. Распространение такой информации третьим лицам может повлечь значительные материальные потери и может проявляться как дестабилизирующий фактор для деятельности и функционирования как информационных систем, так и центров управления полетами целиком. Обрабатываемую в подобных организациях информацию необходимо разделить на общедоступную информацию, информацию ограниченного распространения, доступ к которой ограничен федеральными законами и другими нормативно-правовыми актами Российской Федерации. Для более четкого понимания законодательством РФ определен перечень сведений, подлежащих отнесению к служебной тайне в области управления полетами. В него входит научно-техническая информация, оперативная информация, распорядительные, информационно-справочные и организационные документы, а также управленческая информация, информация по безопасности персональных данных, планы и объемы проводимых мероприятий, сведения о кадровом составе и правилах его формирования.

Построение схемы причинно-следственных связей.

Построение системы защиты информации в организации является ответственным этапом, на котором определяются вероятные угрозы, нарушители, КУИ, а также ДМП информационных систем. Далее рассмотрим каждый из составляющих компонентов подробнее. В АИС можно выделить следующие вероятные угрозы безопасности информации:

- утечка информации;
- несанкционированный доступ;
- несанкционированная модификация (искажение);
- несанкционированная подмена;
- удаление информационных ресурсов;
- отказ в обслуживании;
- ненадлежащее использование;
- нарушение функционирования.

Под нарушителем ИБ понимается физическое лицо, которое случайно или намеренно совершило действие, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационной системе. Рассматривая АИС, можно выделить следующие типы нарушителей:

- нарушитель, обладающий базовыми возможностями – хакеры, бывшие работники, авторизованные пользователи систем и сетей;
- нарушитель, обладающий базовыми повышенными возможностями – преступные группы, системные администраторы и администраторы безопасности, поставщики вычислительных услуг;
- нарушитель, обладающий средними возможностями – террористические, экстремистские группировки, разработчики программных средств;
- нарушитель, обладающий высокими возможностями – специальные службы иностранных государств.

Под КУИ понимаются методы и пути утечки информации из информационной системы. Рассматривая АИС, можно выделить следующие КУИ:

- физические;
- технические;
- инсайдерские;
- каналы утечки, создаваемые атаками внутри информационных систем и извне.

Под ДМП системы понимается характеристика физического поля, которая создается объектом защиты, если эта характеристика раскрывает наличие объекта (отличие его от других). Рассматривая АИС, можно выделить следующие ДМП:

- технические – характерные признаки самих средств связи и информатизации;
- оперативные – характерные признаки, связанные с порядком применения информационной системы в процессе управления;

прямые – признаки, проявляющиеся через физическое поле объекта защиты и отличающиеся по уровню на фоне помех;

косвенные – признаки, проявляющиеся в результате функционирования объекта защиты через изменения окружающей среды;

групповые – признаки, позволяющие установить принадлежность информационной системы к определенному типу;

индивидуальные – признаки, содержащие информацию о конкретной информационной системе из совокупности систем одного типа.

Расчет реализации угрозы ИБ с учетом возможностей нарушителя, КУИ и вероятных угроз безопасности информации может быть выполнен с использованием методологий, таких как модель DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability), который является методом оценки риска информационной безопасности, который помогает определить уровень угрозы для конкретной уязвимости или события безопасности.

Вероятность реализации угрозы:

$$P = (D + R + E + AU + Ds) / 50$$

где:

D - Damage (Ущерб) - Этот критерий оценивает максимальный потенциальный ущерб, который может быть нанесен организации, если угроза реализуется. Важные вопросы, которые могут помочь в оценке Damage, включают в себя степень потери конфиденциальной информации, целостности данных и доступности ресурсов.

R - Reproducibility (Воспроизводимость) - Этот критерий оценивает насколько легко нарушитель может воспроизвести атаку, используя данную уязвимость. Если уязвимость легко воспроизводима, то она может представлять большую угрозу.

E - Exploitability (Эксплуатируемость) - Этот критерий оценивает насколько уязвимость уязвима для эксплуатации. Это включает в себя оценку сложности эксплуатации и необходимых привилегий для успешной атаки.

AU - Affected Users (Затронутые пользователи) - Этот критерий определяет количество пользователей или систем, которых затронет угроза. Чем больше пользователей или систем подвергнуты риску, тем выше угроза.

Ds - Discoverability (Обнаруживаемость) - Этот критерий оценивает насколько легко угрозу можно обнаружить до того, как она будет реализована. Если угроза трудно обнаруживается, она может представлять большую угрозу, так как могут отсутствовать предупреждающие меры.

Оценка каждого критерия может быть субъективной и зависит от экспертных мнений и опыта тех, кто проводит оценку.

По итогу анализа вероятных угроз информационной безопасности в АИС, КУИ, ДМП информационной системы и возможных нарушителей

формируется схема причинно-следственных связей, так называемая диаграмма Исикавы, которая отражает воздействие различных факторов на АИС.

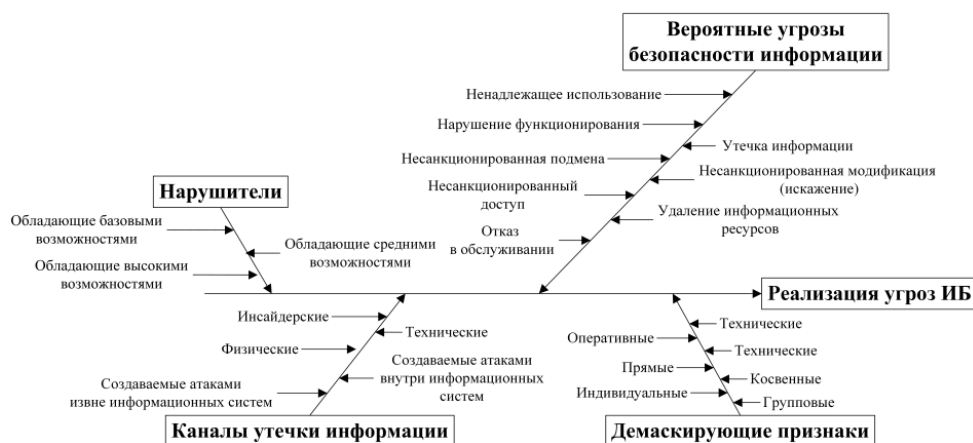


Рис. 1. Схема причинно-следственных связей реализации угроз информационной безопасности

Вывод.

Данная схема позволяет увидеть и определить основные факторы, приводящие к реализации угроз информационной безопасности АИС.

С помощью данной схемы причинно-следственных связей можно выполнить операции по предупреждению или установлению влияния угроз информационной безопасности, путем внедрения необходимых технических, программно-аппаратных защитных мер и проведения организационных мероприятий. Таким образом, в ходе работы был проведен анализ угроз, нарушителей, ДМП и КУИ в АИС центров управления полетами. По результатам анализа построена диаграмма Исикавы, отражающая факторы, приводящие к реализации угроз информационной безопасности АИС.

Библиографический список

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М., 2006.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИНФРА-М, 2011. 416 с.
3. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

4. Федеральная служба по техническому и экспортному контролю приказ от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

**К.К. Канищев, А.Д. Ханазарян, И.А. Мороз,
М.В. Голуб, А.А. Еремин**

ПЛАНИРОВАНИЕ И ПРОВЕДЕНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ ПО ИЗУЧЕНИЮ СВОЙСТВ АКУСТИЧЕСКИХ МЕТАМАТЕРИАЛОВ И ПЛАСТИКОВ, ПОЛУЧАЕМЫХ С ПОМОЩЬЮ 3D ПЕЧАТИ

В работе рассматриваются вопросы планирования и проведения экспериментальных исследований по изучению свойств акустических метаматериалов и пластиков, получаемых с помощью 3D печати. В работе описывается процесс разработки и реализации базы данных для управления информацией о свойствах и характеристиках акустических метаматериалов и пластиков, полученных с помощью аддитивных технологий. Также обсуждается важность эффективного управления данными для оптимизации процессов производства и последующего анализа экспериментальных данных.

Ключевые слова: база данных, управление данными, аддитивные технологии, упругие метаматериалы.

The planning and the implementation of experimental studies on the properties of elastic metamaterials and plastics produced by 3D printing is studied in this paper. The process of designing and implementing a database for managing information on the properties and characteristics of acoustic metamaterials and plastics produced by additive technologies is described. The importance of efficient data management for optimizing manufacturing processes and subsequent analysis of experimental data is also discussed.

Key words: Database, data management, additive manufacturing, elastic metamaterials.

Современные технологии позволяют совершенствовать материалы, улучшать характеристики и способствуют их практическому применению. Отдельное внимание в научных и инженерных сообществах уделяется акустическим метаматериалам и смарт-структурам, которые открывают новые возможности для управления распространением волн [1]. Благодаря своим уникальным свойствам эти материалы могут обеспечить ряд уникальных волновых свойств, таких как отрицательная рефракция и формирование запрещенных зон. Применение периодических композитных структур находит применение в различных областях, таких как разработка датчиков, систем активного шумоподавления, фокусировки и т.п. Благодаря прогрессу в

разработке акустическим метаматериалам, структуры на их основе находят применение в ультразвуковой технике, акустоэлектронике, гидроакустике, архитектурной акустике и звукопоглощении. Продолжается изучение и проектирование новых типов акустическим или упругих метаматериалов, так как они имеют большой потенциал для создания и внедрения новых усовершенствованных устройств.

В недавней работе авторов [2] было исследовано распространение упругих волн в многослойных метаматериалах с пустотами. Хотя экспериментальные и теоретические данные коррелируют (изучались запрещенные зоны), имеет место заметное отклонение в расположении запрещенных зон, что можно связать с неточными значениями в упругих модулях пластиков, используемых при расчетах. Численные эксперименты показывают, что даже небольшие изменения в коэффициенте Пуассона и модуле Юнга ведут к значительным изменениям в характеристиках волноводных или смарт-структур, изготовленных из пластиковых материалов. Кроме того, свойства пластиковых образцов, полученных из разных марок пластика и от различных производителей, могут значительно варьироваться, а процесс 3D печати при определенных условиях может приводить к анизотропии свойств слоев ламинатов.

Для восстановления свойств материалов были изготовлены образцы с помощью аддитивных технологий. Исследование этих образцов позволяет восстановить необходимые свойства. На данный момент коллекция насчитывает более 50 образцов из более чем 10 различных материалов. Одни образцы исследовались для восстановления коэффициентов Пуассона и модуля упругости, другие на наличие анизотропных свойств у материала (Рисунок 1).

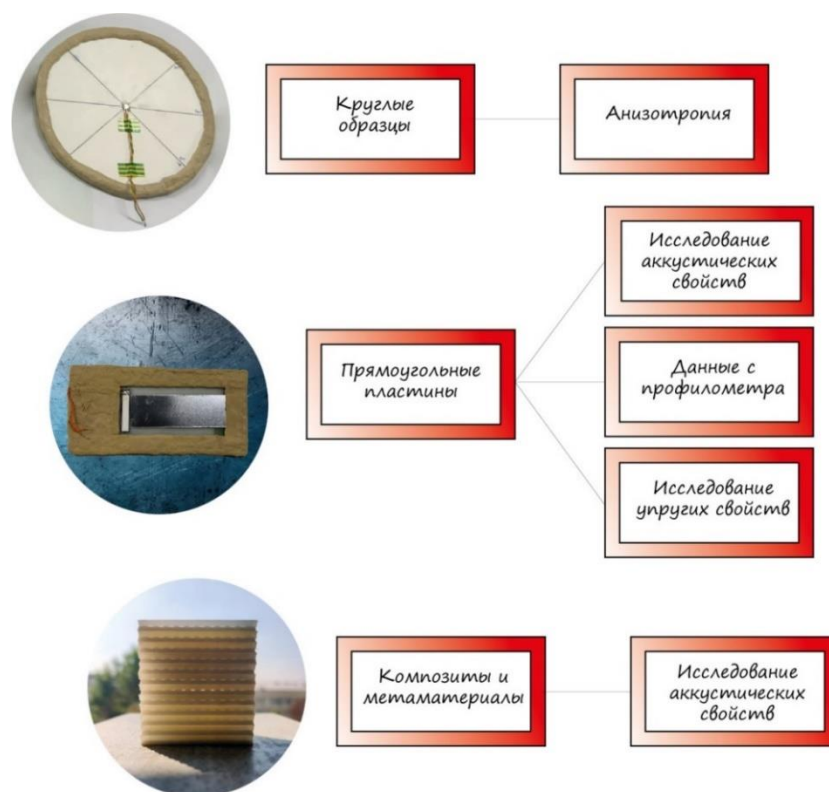


Рис. 1. Классификация образцов

В совокупности уже имеется большой массив данных, который будет в дальнейшем быстро разрастаться, поэтому требуется систематизации и хранение этих данных. Решить эту задачу можно созданием базы данных образцов и материалов, что позволяет обеспечить удобный доступ к данным для последующего анализа или выбора параметров для изготовления новых материалов, также база данных способствует сохранению целостности данных, их долгосрочному хранению и защите от потери или повреждения. Кроме того, для такой базы данных нужен интерфейс, который позволит максимально быстро и удобно ориентироваться в большом массиве данных. Общая структура разработанной базы данных приведена на Рисунке 2.



Рис. 2. Структура базы данных

База данных с четкой структурой обладает оптимальной организацией для хранения и управления большим объемом экспериментальных данных. Ее основные таблицы, такие как "material", "sample", "sample's kind" и "measurements", содержат минимальный набор ключевых данных, который позволяющих легко отслеживать, анализировать и обрабатывать информацию о материалах и образцах.

В таблице "material" хранятся основные характеристики материалов, такие как название, описание, модуль упругости, коэффициент Пуассона, плотность, заявленная производителем, фактическая плотность, наличие анизотропных свойств, а также ссылка на соответствующую папку, где сохранены связанные файлы. Таблица "sample" содержит информацию о конкретных образцах, включая материалы, из которых они состоят, тип образца, его размер, описание, количество слоев, количество ячеек и ссылку на папку с фотографиями образцов для визуальной идентификации. "Sample's kind" предоставляет информацию о типах образцов, описание и данные об их производстве, что способствует более углубленному пониманию процессов изготовления. Таблица "measurements" содержит информацию о замерах и измерениях, проведенных на образцах. Она включает уникальный идентификатор измерения, связанный с идентификатором образца, название файла, а также дополнительную информацию о характере проводимых измерений, такие как тип сигнала, центральная частота и вольтаж.

Благодаря своей структуре и организации, эта база данных подходит для хранения, обработки и извлечения разнообразной информации о материалах, образцах и проводимых измерениях, обеспечивая удобное и систематизированное управление экспериментами и данными (Рисунок 2). Для создания описанной базы данных был выбран язык программирования Python, фреймворк Flask и модуль SQLite3. Данный набор совместно с языком гипертекстовой разметки HTML позволил создать полноценное веб-приложение.

Были написаны скрипты на языке программирования Python с использованием библиотеки SQLite3 для создания и управления базой данных. Фреймворк Flask был использован для создания веб-приложения, обеспечивая интеграцию базы данных с веб-интерфейсом. Flask был выбран из-за своей гибкости. Он предоставляет удобный набор инструментов, позволяющих создавать веб-приложения. С его помощью была реализована логика маршрутизации, отображения данных из базы данных и обработки запросов от пользователей. Flask также обеспечивает простое подключение к базе данных и удобное взаимодействие с ней, что значительно упрощает разработку и сопровождение приложения.

Использование SQLite3 обеспечило простоту и портативность. Этот интегрированный в Python модуль позволяет эффективно управлять базой данных, что идеально подходит для данного проекта. Созданное в результате веб-приложение позволяет пользователям не только удобно восприни-

мать информацию, но и осуществлять редактирование, добавление и удаление записей в базе данных. Сочетание Flask и SQLite3 создало эффективное окружение для разработки и внедрения базы данных, обеспечивая удобное управление данными, легкость разработки и поддержки, а также надежность и гибкость всей системы.

Таким образом, созданная база данных и веб-приложение являются полезным инструментом, который позволяет эффективно управлять и анализировать данные, оптимизировать процессы производства и разрабатывать новые материалы с улучшенными характеристиками.

Работа выполнена при поддержке гранта РФФИ № 22-11-00261.

Библиографический список

1. G. Liao, C. Luan, Z. Wang, J. Liu, X. Yao, J.; Fu, J. // Acoustic metamaterials: A review of theories, structures, fabrication approaches, and applications, *Advanced Materials Technologies*. 6 2021. 2000787.
2. M.V. Golub, I.A. Moroz, Y. Wang, A.D. Khanazaryan, K.K. Kanishchev, E.A. Okoneshnikova, A.N. Shpak, S.A. Mareev, C. Zhang // Design, manufacturing, experimental and theoretical study of elastic wave propagation in multilayered acoustic metamaterial with interfacial crack-like voids, *Acoustics*, 5:1 2023, 122-135.
3. M. Askari, D.A. Hutchins, P.J. Thomas, L. Astolfi, R.L. Watson, M. Abdi, M. Ricci, S. Laureti, L. Nie, S. Freear, R. Wildman, C. Tuck, M. Clarke, E. Woods, A.T. Clare // Additive manufacturing of metamaterials: A review, *Additive Manufacturing*, 36 2020, 101562.
4. M.V. Golub, O.V. Doroshenko, M.A. Arsenov, A.A. Eremin, Y. Gu, I.A. Bareiko // Improved Unsupervised Learning Method for Material-Properties Identification Based on Mode Separation of Ultrasonic Guided Waves, *Computation*, 10:6, 2022, 93.

Д.Ю. Романюта

МОБИЛЬНЫЕ НЕЙРОСЕТЕВЫЕ МОДЕЛИ ДЛЯ РАСПОЗНАВАНИЯ ЛИЦ

В статье рассматриваются нейросетевые модели для распознавания объектов на изображении, их архитектура, принципы работы и основные методы обучения. Также будет рассмотрена система распознавания лиц с помощью нейросетевых моделей и проведено сравнение эффективности различных нейросетевых моделей для распознавания лиц.

Ключевые слова: сверточные нейронные сети, модели глубокого обучения, распознавания лиц, Tensorflow.

The article discusses neural network models for recognizing objects in an image, their architecture, principles of operation and basic teaching methods. The

facial recognition system using neural network models will also be considered and the effectiveness of various neural network models for facial recognition will be compared.

Keywords: Convolutional neural networks, deep learning models, face recognition, Tensorflow.

В последние годы нейросетевые модели стали основным инструментом для решения задач в области компьютерного зрения и обработки изображений, включая распознавание лиц. Методы машинного обучения – это современный подход к распознаванию лица, который использует алгоритмы машинного обучения для обучения системы распознавать лица на основе большого количества данных. Он используется в системах, требующих высокой точности идентификации, например, в системах безопасности и онлайн-аутентификации.

Распознавание лиц — это процесс идентификации или проверки внешности одного или нескольких человек в кадре изображения. Этот процесс полного распознавания, разделенный на две части, во-первых, должен обнаружить лицо человека в кадре изображения, а во-вторых, распознать личность человека. Для идентификации личности ищется похожее лицо в коллекции лиц и соответствующий ярлык.

Предлагаемая структура системы распознавания лиц с помощью искусственного интеллекта показана на рисунке 1. Весь процесс разделен на три части. Сначала на вход поступает изображение человека и на нем определяют область лица, а затем определяют различные части лица, глаза, нос или рот, чтобы проверить лицо. На втором этапе анализируются основные признаки, полученные с изображения и, наконец, последним этапом является идентификация человека на изображении на основе выбранных признаков.

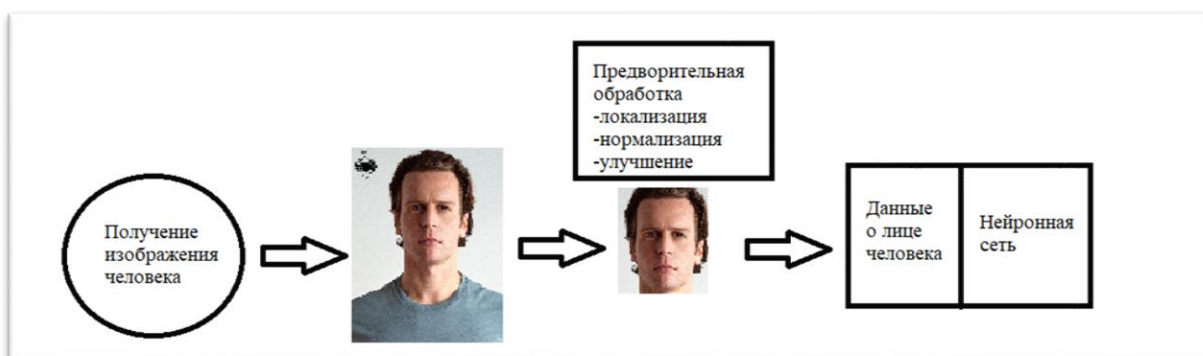


Рис. 1. Процесс распознавания лиц

С развитием сверточных нейронных сетей в предыдущем десятилетии появились модели глубокого обучения для нахождения объектов на изображении за минимальное возможное время. Например, модели MobileNet,

ShuffleNet, SqueezeNet и EfficientNet. Эти модели имеют меньшее количество параметров и используют более эффективные сверточные операции, что позволяет снизить требования к вычислительным ресурсам.

Mobilenet V2 была выпущена в 2018 году и является улучшенной версией оригинальной модели Mobilenet. Она была создана с целью улучшения эффективности и точности модели на мобильных устройствах. Данная модель основана на инвертированной остаточной структуре, в которой остаточные соединения находятся между узкими слоями. [1].

SqueezeNet - это сверточная нейронная сеть, разработанная в 2016 году, которая обладает высокой эффективностью и точностью. Она имеет меньшее количество параметров по сравнению с другими сверточными сетями, что делает ее более быстрой и эффективной. SqueezeNet использует специальные блоки, называемые "fire modules", которые состоят из двух слоев свертки и слоя сжатия. Эти блоки позволяют извлекать более сложные функции из входных данных, сохраняя при этом эффективность сети [2].

AlexNet - это первая сверточная нейронная сеть, которая достигла высокой точности в задаче классификации изображений. Она была представлена в 2012 году и использовала три сверточных слоя и два полносвязных слоя. AlexNet обучалась на наборе данных ImageNet и достигла точности 84.7%.

Для создания мобильной нейросетевой системы для идентификации личности данные модели будут дообучены на наборе данных DigFace 1M. Датасет содержащий 72 тысяч изображений для 10 тысяч сгенерированных человек. Дообучение каждой модели будет длиться 3 часа, оно будет проводиться с помощью библиотеки Tensorflow.

Необходимо, чтобы изображения были не слишком большие. Каждое из них должно быть менее 200 КБ, а их разрешение не должно превышать 720x1280. При использовании этих данных в детекторе обнаружения их предварительно следует также пометить на предмет того, что следует находить. Для маркировки изображений используется инструмент LabelImg, который сохраняет данные в виде файлов XML в формате PASCAL VOC. Эти XML-файлы будут использоваться для создания TFRecords, которые являются одним из входных данных для модели обучения TensorFlow.

При настройке модели задается количество различаемых объектов, директории нахождения модели, файлов TFRecords, а также карты меток. Карта меток сообщает обучающей модели, что представляет собой каждый объект, определяя сопоставление имен классов с номерами идентификаторов классов.

Следующим этапом является обучение построенной модели. На каждом шаге обучения сообщается значение функции потерь. Так первоначальное значение модели SqueezeNet была равна 88,1216 и по прошествии 300 итераций стала равна 1,89, что является хорошим результатом. Переобученная модель сохраняется в файле вывода (типа pb).

Для выбора наиболее эффективной модели, которая будет использоваться в мобильной системе для идентификации личности будут обучены следующие модели: SqueezeNet, MobileNetV1, MobileNetV2, AlexNet.

При тестировании модели были получены следующие результаты, и были проведены тесты на каждой итерации, чтобы убедиться в отсутствии переобучения или недостаточного подбора. В таблице 1 представлены точности для всех моделей, после прохождения 300 итераций.

Модель	Точность
SqueezeNet	98,11
MobileNetV1	97,85
MobileNetV2	98,4
AlexNet	97,84

Таблица 1. Результаты дообученных моделей

Библиографический список

1. MobileNetV2 // Papers with code: [сайт]. – 2019. – URL: <https://paperswithcode.com/method/mobilenetv2>.
2. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <0.5MB model size // Arxiv: [сайт]. – 2016. – URL: <https://arxiv.org/abs/1602.07360>.

К.В. Стасюк

ИСПОЛЬЗОВАНИЕ УСЛОВНЫХ СЛУЧАЙНЫХ ПОЛЕЙ (CRF) ДЛЯ СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЯ

В статье исследуются вопросы применения семантической сегментации в компьютерном зрении. Рассмотрены ключевые аспекты этой задачи, включая методы классификации и выделения объектов на изображениях. Особое внимание уделено гибридным подходам, объединяющим глубокое обучение и классические методы обработки изображений, а также модели CRF-RNN (Conditional Random Field Recurrent Neural Network), предназначенной для улучшения точности сегментации. Статья представляет полный обзор современных методов семантической сегментации в контексте их практических применений.

Ключевые слова: семантическая сегментация, классификация изображений, гибридные методы, CRF-RNN, компьютерное зрение, понимание сцены, искусственный интеллект.

This article explores the importance and application of semantic segmentation in computer vision. The key aspects of this task are considered, including

methods of classification and selection of objects in images. Special attention is paid to a hybrid approach combining deep learning and classical image processing methods, as well as a CRF-RNN model designed to improve segmentation accuracy. The article presents a complete overview of modern methods of semantic segmentation in the context of their practical applications.

Key words: Semantic segmentation, image classification, hybrid methods, CRF-RNN, computer vision, scene understanding, artificial intelligence.

Семантическая сегментация в компьютерном зрении - это процесс разделения изображения на сегменты, представляющие объекты разных классов, с учётом их контекста и структуры. Это объединяет классификацию, обнаружение объектов и сегментацию для точной интерпретации изображений.

Семантическая сегментация - мощный инструмент в различных областях. В медицинской диагностике семантическая сегментация выделяет структуры и органы на изображениях, улучшая точность диагнозов [2]. В автономных транспортных средствах она определяет свободное пространство на дороге и обнаруживает дорожные знаки, повышая безопасность и навигацию [2]. В геологических исследованиях сегментация выделяет геологические образования на спутниковых снимках, помогая в анализе ландшафтов и картографии [2]. В биометрии она играет ключевую роль в распознавании отпечатков пальцев, увеличивая точность идентификации личности.

Таким образом, семантическая сегментация играет важную роль в различных областях, обеспечивая более глубокое и точное понимание содержания изображений.

Для сегментации применяются самые разнообразные техники обработки изображений в зависимости от области интересов. Наиболее популярные: сегментация на основе градации серого, условные случайные поля, методы глубокого обучения и гибридные методы [2].

Рассмотрим применение гибридных методов в задаче семантической сегментации изображений, которые комбинируют в себе глубокое обучение и традиционные подходы. Глубокое обучение автоматически извлекает признаки и строит сложные модели для классификации пикселей, но имеет ограничения в учете контекстной информации и обработке граничных областей объектов. Классические методы учитывают контекст и зависимости между пикселями, особенно на границах объектов, улучшая качество сегментации. Например, CRFS (Conditional Random Field System) можно использовать для преодоления недостатков использования CNN(Convolutional Neural Network) для задач маркировки на уровне пикселей [1, с.2]. Гибридные методы устраняют шум, обеспечивают точность классификации и более плавные результаты сегментации. Они также могут быть временно и вычислительно эффективными, но требуют настройки и сочетания компонентов,

включая выбор моделей глубокого обучения и классических методов, а также оптимизацию системы.

CRF-RNN (Conditional Random Field Recurrent Neural Network) - это глубокая модель, объединяющая свойства условных случайных полей (CRF) и рекуррентных нейронных сетей (RNN). Она применяется в задачах сегментации изображений, разделяя изображение на семантические области, классифицируя каждый пиксель. CRF-RNN учитывает контекст и зависимости между пикселями, повышая точность сегментации. Её архитектура включает RNN и CRF.

Рекуррентная нейронная сеть (RNN):

RNN — это тип нейронной сети, который имеет внутреннюю память и может обрабатывать последовательности данных различной длины. В случае CRF-RNN, RNN используется для изучения зависимостей между пикселями в изображении. Каждый пиксель рассматривается как входное значение на определенном временном шаге. RNN принимает входные данные пошагово и сохраняет информацию о предыдущих шагах, чтобы учесть контекст в последовательности пикселей.

Условные случайные поля (CRF).

CRF — это статистическая модель, которая моделирует зависимости между метками или классами в последовательности данных. В случае CRF-RNN, CRF используется для учета контекстной информации и глобальных зависимостей между пикселями. CRF позволяет модели учитывать соседние пиксели и их классы при принятии решений о классификации пикселей в задаче сегментации. Обычно условные случайные поля используются для сглаживания зашумленных карт сегментации [4, с.6]. Основная функция этих короткодействующих CRFs предназначена для устранения ложных прогнозов слабых классификаторов, построенных на основе локальных функций, созданных вручную [4, с.6].

Обучение CRF-RNN происходит путем комбинирования обучения RNN и обучения CRF. Сначала RNN обучается находить зависимости между пикселями в изображении. Затем CRF используется для учета глобальной информации и для регуляризации сегментации, чтобы получить более согласованные и качественные результаты.

Для исследования сегментации изображений было разработано программное приложение, которое принимает изображение, обрабатывает его с помощью нейронной сети и затем отображает на экране два изображения: исходное и результат сегментации.

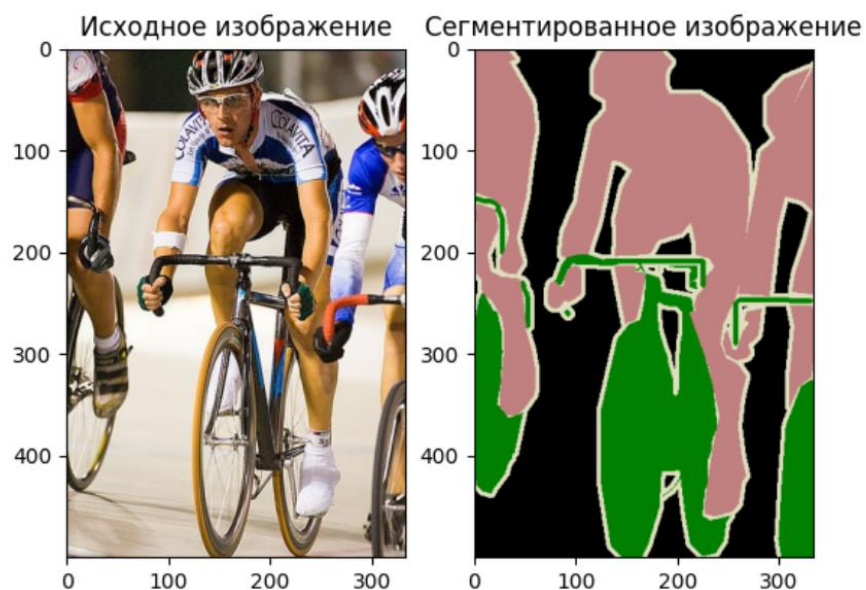


Рис. 1. Результат работы программы

В программе используется набор данных VOCSegmentation для обучения и тестирования модели сегментации изображений. В данном наборе отдельным классам объектов сопоставляется конкретный цвет. Датасет состоит из 20 классов объектов переднего плана и одного фоновых класса. Исходный набор данных содержит 1 464, 1 449 и 1 456 изображений для обучения, валидации и тестирования соответственно [3, с.7].

B-ground	Aero plane	Bicycle	Bird	Boat	Bottle	Bus
Car	Cat	Chair	Cow	Dining-Table	Dog	Horse
Motorbike	Person	Potted-Plant	Sheep	Sofa	Train	TV/Monitor

Рис. 2. Цвета для датасета PASCALVOC

Так же был проведен сравнительный анализ работы нейронной сети CRF-RNN с методами пороговой сегментации и k-средних.

На рисунке 3 приведен результат работы пороговой сегментации изображения со сложным фоном:

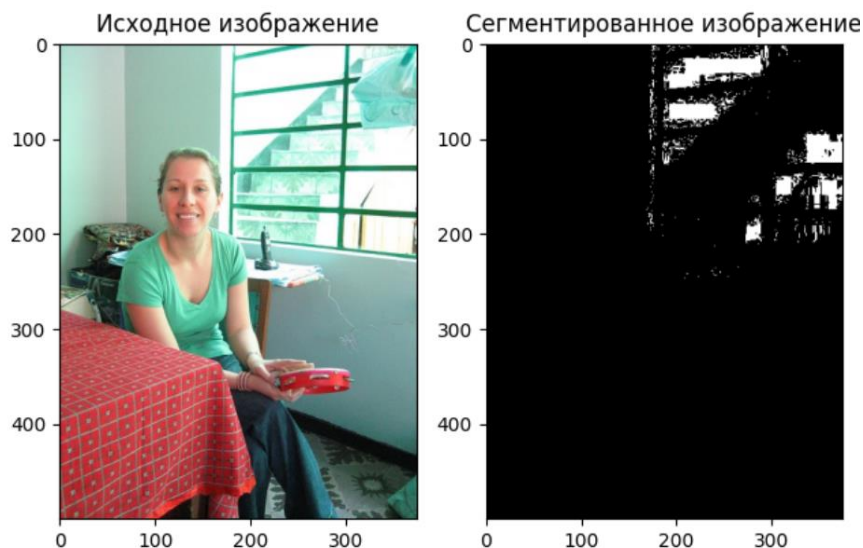


Рис. 3. Результат сегментации с помощью метода пороговой сегментации

На изображении 4 представлено, как метод *k*-средних справился с рассматриваемым изображением.



Рис. 4. Результат сегментации с помощью метода *k*-средних

На 5 рисунке можно увидеть, как модель CRF-RNN обработала изображение с запутанным задним планом.

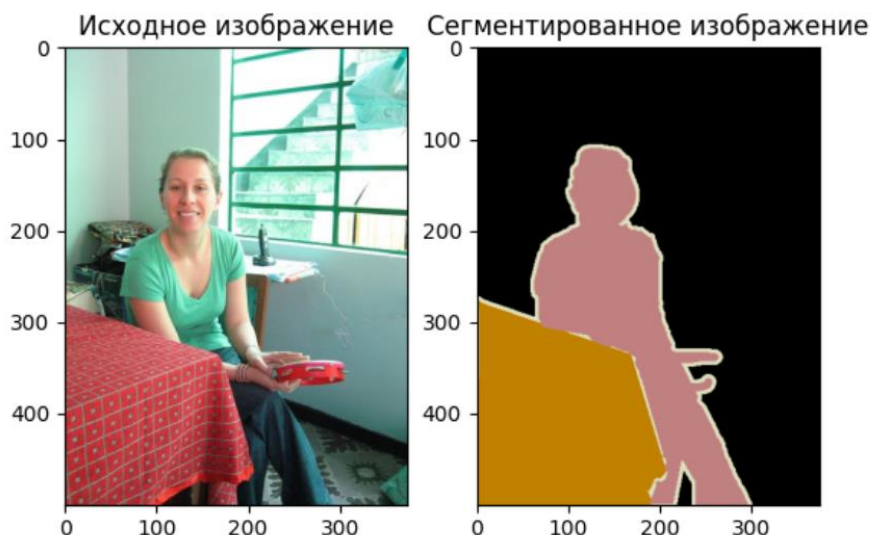


Рис. 5 Результат сегментации с помощью модели crf-rnn.

Результаты работы трех методов сегментации показывают, что пороговая сегментация - простой и быстрый метод, но подходит для изображений с явно различимыми объектами и фоном. Метод определяет порог, максимизируя дисперсию между различными сегментами изображений [5, с.3]. Сегментация с использованием k-средних более гибка, но требует выбора кластеров и может быть чувствительна к начальной инициализации так как алгоритм формирует кластеры, каждый из которых представляется центроидом и выбирается на основе признаков входных данных [5, с.10]. CRF-RNN учитывает контекст и зависимости между пикселями, подходит для сложных изображений, но требует больших ресурсов для обучения и применения.

можно сделать вывод, что семантическая сегментация играет важную роль в компьютерном зрении, обеспечивая понимание сцены и находя применение в различных сферах, от медицинской диагностики до автономных транспортных средств. Гибридные методы, такие как CRF-RNN, представляют собой многообещающие подходы для улучшения точности сегментации. Дальнейшие исследования и инновации в этой области будут способствовать развитию машинного зрения и его практическому применению.

Библиографический список

1. Conditional Random Fields as Recurrent Neural Networks — Текст: электронный// Shuai Zheng , Sadeep Jayasumana, Bernardino Romera-Paredes, Chang Huang, and Philip H. S. Torr — 2012. — URL: <https://www.robots.ox.ac.uk/~szheng/papers/CRFasRNN.pdf>.
2. A Simple Guide to Semantic Segmentation — Текст: электронный// Bharath Raj — 2019. — URL: <https://medium.com/beyondminds/a-simple-guide-to-semantic-segmentation-effcf83e7e54>.

3. SEMANTIC IMAGE SEGMENTATION WITH DEEP CONVOLUTIONAL NETS AND FULLY CONNECTED CRFS — Текст: электронный// Liang-Chieh Chen, George Papandreou, Iasonas Kokkinos, Kevin Murphy and Alan L. Yuille — 2015. — URL: <https://arxiv.org/pdf/1412.7062.pdf>.

4. DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs — Текст: электронный// Liang-Chieh Chen, George Papandreou, Senior Member, IEEE, Iasonas Kokkinos, Member, IEEE, Kevin Murphy, and Alan L. Yuille, Fellow, IEEE — 2017. — URL: <https://arxiv.org/pdf/1606.00915.pdf>.

5. Усовершенствованные варианты архитектуры нейронных сетей — Текст: электронный — URL: <https://www.williamsublishing.com/PDF/978-5-907144-25-5/part.pdf>.

Ю.О. Черная

РАЗРАБОТКА ОНТОЛОГИЧЕСКОГО ПРЕДСТАВЛЕНИЯ ГРАФА ЗНАНИЙ МЕДИЦИНСКИХ КАРТ

В статье рассматривается алгоритм разработки онтологии, выбор предметной области, описание необходимых для работы понятий и технологий, реализация онтологического представления графа знаний в заданной предметной области.

Ключевые слова: граф знаний, онтология, онтологическое представление графа знаний, дескрипционная логика, формальная логика и семантика, OWL.

The article discusses the algorithm of ontology development, the choice of the subject area, the description of the concepts and technologies necessary for the work, the implementation of the ontological representation of the knowledge graph in a given subject area.

Keywords: knowledge graph, ontology, ontological representation of the knowledge graph, descriptive logic, formal logic and semantics, OWL.

Граф знаний – это относительно новый способ хранения данных. Название уже подразумевает структуру сети – графа, где знания находятся и взаимодействуют в схеме: узел – ребро.

Чтобы более детально ознакомиться с данным понятием, разработаем онтологическое представление графа знаний в заданной предметной области.

Для начала определим, что такое онтология. Генезис этого термина берет свое начало в философии, и лишь в 1970-х годах термин вводится в компьютерную сферу. Наиболее точное определение ввел Том Грубер – он

рассматривает онтологию как «формализованное описание понятий и отношений», имея в виду иерархию классов и иерархию отношений сущностей соответственно [1].

Онтология — это аналогия русского языка и его правил: данные представлены по определенным и прописанным законам, которые обязательно подчиняются логике. Онтология может описать каждый объект, также используя дескрипционную логику, которая позволяет избежать двусмысленности.

Для создания онтологии предметной областью была выбрана карта вызова скорой медицинской помощи. Выбранная тематика совмещает в себе свойства пациента (характеристики человека) и медицинскую сферу (виды травм, анамнез и т. д.).

Экспертами в данной онтологии выступила бригада №3 подстанции скорой помощи №2 города Краснодара. Учетная форма N 110/у "Карта вызова скорой медицинской помощи" (далее - Карта) заполняется на станциях (подстанциях, отделениях) скорой медицинской помощи выездными врачебными и фельдшерскими бригадами. Учетная форма N 110/у утверждена приказом Минздравсоцразвития РФ от 02.12.2009 N 942.

Карта содержит 38 пунктов данных. Фрагменты карты вызова скорой медицинской помощи учетной формы N 110/у можно увидеть на рисунке 1.

Приложение № 3
к Приказу Министерства
здравоохранения и социального
развития Российской Федерации
от 02.12.2009 № 942

Медицинская документация
Учетная форма № 110/у
Утверждена Приказом
Министерства здравоохранения
и социального развития
Российской Федерации
от 02.12.2009 № 942

(наименование медицинской организации)

(адрес, телефон) _____

КАРТА
вызова скорой медицинской помощи № _____
" ____ " ____ 20__ г.

1. Номер фельдшера по приему вызова _____
2. Номер станции (подстанции), отделения _____
3. Номер бригады скорой медицинской помощи _____

4. Время (часы, минуты):

принят вызов	передана выезда бригаде скорой медицинской помощи	выезд на вызов	прибытие на место вызова	начало транспортировки больного	прибытие в медицинскую организацию	оценка выезда	возвращение на станцию (подстанцию, отделение)	затраченное на выполнение вызова
_____	_____	_____	_____	_____	_____	_____	_____	_____

5. Адрес вызова: район _____ город/село _____ населенный пункт _____ улица _____ дом _____ корп. _____ кв. _____ комн. _____ подъезд _____ код подъезда _____ этаж _____
7. Кто вызвал _____ № телефона вызывающего _____
8. Фельдшер, принявший вызов _____
9. Фельдшер, передавший вызов _____

6. Сведения о больном: фамилия _____ имя _____ отчество _____ возраст _____ лет/месяцев/дней Пол м ж Место работы _____ Серия и номер документа, удостоверяющего личность (при наличии) _____

19. Наличие клиники опьянения: да; нет
20. Жалобы: _____

21. Анамнез _____

22. Объективные данные.
Общее состояние: удовлетворительное; средней степени тяжести; тяжелое;
 агональное; смерть
Поведение: спокойное; возбужденное; агрессивное; депрессивное
Сознание: ясное; спутанное; заторможенное; отсутствует (коматозное).
Менингеальные знаки: есть; нет
Зрачки: нормальные; широкие; узкие. Анизокория: есть; нет
Нистагм: есть; нет
Реакция на свет: есть; нет
Кожные покровы: обычные (нормальные); бледные; гиперемированные;
 желтушные; сухие
Акроцианоз: есть; нет
Мраморность: есть; нет

Рис. 1. Карта вызова скорой медицинской помощи

Основой для составления классификации жалоб и анамнеза помимо экспертов взято учебно-методическое пособие «Учебная история болезни: правила обследования пациента и оформление результатов» Каулиной Е. М. и Лобановой Н. А. Для классификации анамнеза используется Международ-

ная классификация болезней 10-го пересмотра (МКБ-10). Основными тематиками разрабатываемой онтологии будут являться характеристики пациента, врача, а также медицинские сведения о потерпевшем.

Графы знаний могут быть построены либо нисходящим способом (topdown), либо восходящим (bottom-up). В данной работе для создания графа знаний был выбран нисходящий способ - сначала будет строиться структура базы знаний, а именно – онтология.

Разработка онтологии проходила в WebOWL. WebOWL состоит из сообщества интеллектуальных агентов, действующих в качестве поисковых роботов, способных обнаруживать и узнавать расположение окрестностей семантической паутины в сети, семантической базы данных для хранения данных из различных онтологий, механизма запросов, который поддерживает семантические запросы в OWL (язык описаний онтологий), и алгоритм ранжирования, который определяет порядок возвращаемых результатов на основе семантических отношений классов и отдельных лиц.

Руководство по языку веб-онтологий OWL демонстрирует использование языка OWL для следующих задач:

- формализовать домен, определив классы и свойства этих классов;
- определять индивидуумов и утверждать о них свойства;
- рассуждать об этих классах и индивидуумах в той степени, в которой это допускается формальной семантикой языка OWL.

Разделы организованы так, чтобы представить поэтапное определение набора классов, свойств и отдельных лиц, начиная с основ и переходя к более сложным языковым компонентам [2].

Перед началом разработки онтологии надо заполнить параметры редактирования: ввести название онтологии, IRI (идентификатор ресурса концентрации данных), версию и указать авторство. Также добавляется описание для создаваемой онтологии.

В OWL существует два вида предикатов: объектные и литеральные. Первые, Object property, имеют своим значением экземпляры классов, вторые, Data property, - XML типы данных (строки, числа, тип boolean, даты, и т. д.).

Далее распределим имеющиеся данные на классы и иерархии классов. В разрабатываемой онтологии на данный момент составлено 57 классов и 34 предиката. Опишем некоторые из них.

Класс CallPlace – обозначает место вызова. Классы Flat, Workplace, PublicPlace, School, MedOrganization, Preschool, Street, FederalHighway являются подклассами класса CallPlace согласно пункту 17 карты. Класс Complaint – обозначает жалобы пациентов, имеет два подкласса MainComplaint и OtherComplaint [3].

Онтологическое представление графа знаний можно увидеть на рисунке 2.

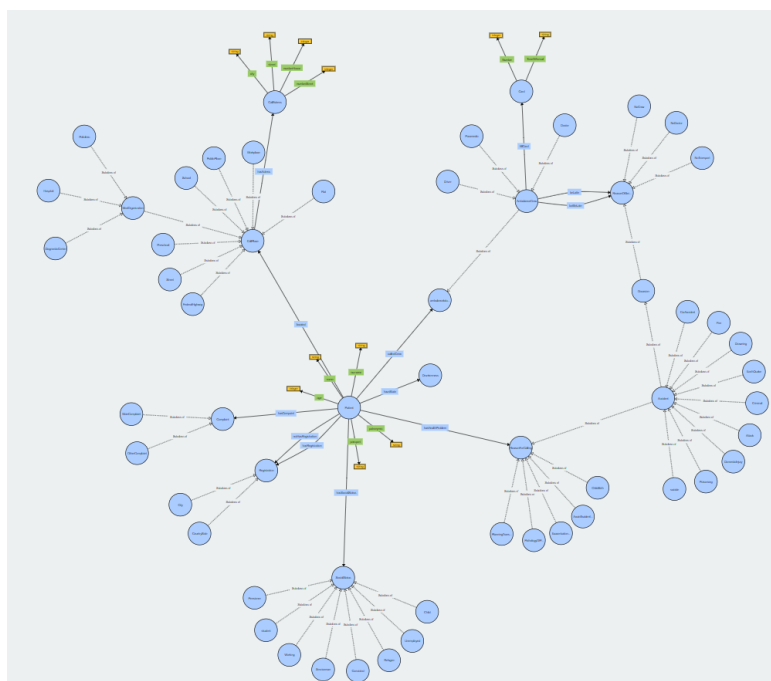


Рис. 2. Онтологическое представление графа знаний

Предикат `haveState` определен для класса `Patient` и имеет своим значением инстанс класса `Drunkness`.

Предикат `passport` определен для класса `Patient` и имеет своим значением XML типы данных.

Фрагмент онтологического представления графа знаний можно увидеть на рисунке 3.

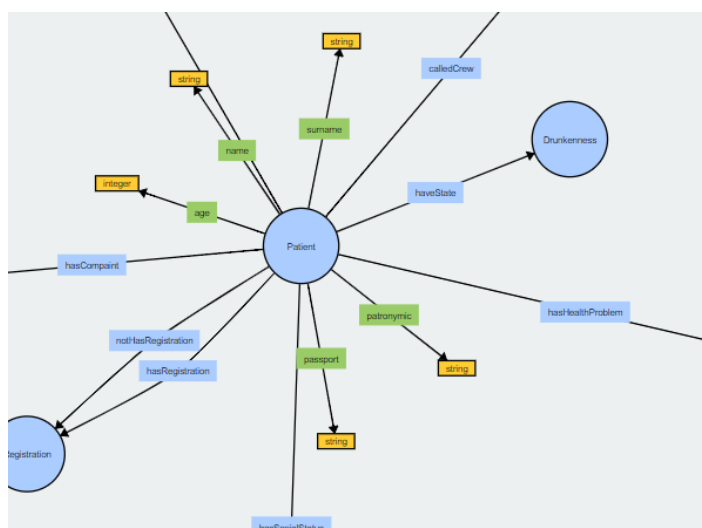


Рис. 3. Фрагмент онтологического представления графа знаний

В данной работе был изучен алгоритм построения графа знаний и необходимый для этого стек технологий; выбрана и подробно разобрана предметная область; разработано и реализовано в WebOwl онтологическое пред-

ставление графа знаний медицинских карт. В дальнейшем планируется увеличение классов и предикатов, заполнение графа знаний данными, а также создание приложения на его основе.

Библиографический список

1 Волкова И. А, Шамаева Е. Д., Экскурс в графы знаний // Научная электронная библиотека Киберленинка – Научные статьи — 2022. URL: <https://cyberleninka.ru/article/n/ekskurs-v-grafy-znaniy/viewer>.

2 Метод коллективной визуальной разработки онтологического графа знаний // Санкт-Петербургский институт информатики и автоматизации РАН, г. Санкт-Петербург, Россия // ООО "Информационные крылья" — 2019. URL: <http://www.isa.ru/aidt/images/documents/2019-01/27-38.pdf>.

3 Каулина Е. М. и Лобанова Н. А., «Учебная история болезни: правила обследования пациента и оформление результатов» // Учебно-методическое пособие — 2019. URL: <http://old.lib.unn.ru/students/src/anamnesis.pdf>.

СЕКЦИЯ 2. Экономика и социальная сфера. Задачи цифровизации в современном обществе

Д.Д. Баранцев

РАСПОЗНАВАНИЕ ТЕКСТА, ПРЕДВАРИТЕЛЬНАЯ БИНАРИЗАЦИЯ

В данной статье рассматриваются разработки по автоматизации распознавания последовательности символов из визуальных образов, для оцифровки текста, написанного человеком. У данной системы есть потенциал использования в сферах, где задействован документооборот и архивация записей. Основная задача разрабатываемого ПО – определить наличие текста, распознать его отдельные токены, и привести его к читаемому виду.

Ключевые слова: бинаризация, распознавание текста, метод Оцу, обработка данных, алгоритм Оцу.

This article discusses developments to automate the recognition of sequences of characters from visual images for the digitization of text written by a person. This system has potential for use in areas where document management and record archiving are involved. The main task of the software being developed is to determine the presence of text, recognize its individual tokens, and bring it into a readable form.

Key words: binarization, text recognition, Otsu method, data processing, Otsu algorithm.

Распознавание текста является одной из задач обработки естественного языка (Natural Language Processing). Существует большое множество программных решений для задач NLP под разные операционные системы; каждое такое ПО использует в своей реализации одну, а может и несколько разных моделей ИНС. В основном это свёрточные нейронные сети (CNN), рекуррентные сети (RNN) и сети долгой краткосрочной памяти (LSTM).

Бинаризация изображений рукописного текста.

Предварительно обработку данных необходимо разбить на несколько этапов, таких как бинаризация, сегментация, обнаружение текста, реализация бинаризации, в данной статье подробно будет рассматриваться полный процесс бинаризации с её реализацией.

Любое изображение, можно разбить на две части: передний план – основная информация фотографии её содержание, и дополняющий его фон. В рамках данной работы, текст рассматривается как содержимое растрового изображения графического формата JPG. Основным и важным этапом является процесс бинаризации, который разделяет передний план от фона путём повышения и понижения интенсивности пикселей относительно некоторого граничного значения. Данное действие еще называют «пороговой бинаризацией» - процедура преобразования 8-битного изображения в бинарное, содержащее только оттенки черного и белого, вычисляется яркость каждого пикселя по следующей формуле (1):

$$Y = 0.3R + 0.59G + 0.11B \quad (1)$$

где R,G,B – составляют октет из значений интенсивности цветовой модели RGB. Затем по определенному из возможных алгоритмов находится некоторое значение Y с которым будет происходить сравнение яркости текущего пикселя и применяться соответствующее преобразование. На рисунках 1-2 продемонстрированы примеры бинаризации.

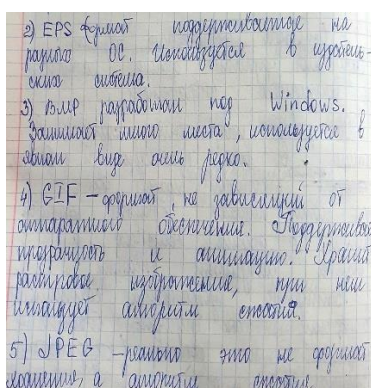


Рис. 1. Изображение текста до бинаризации

2) EPS формат используется на радио от используется в уровне-сина экрана.

3) BMP работает под Windows. Формат имеет цвета, используется в основном виде очень редко.

4) GIF – формат, не зависящий от аппаратного обеспечения. Поддерживает прозрачность и анимацию. Формат работает медленно, при нем используется анимация.

5) JPEG – формат это не формат хранения, а алгоритм сжатия.

Рис. 2. Изображение текста после бинаризации

Как было сказано ранее, качество результата выполнения данного действия напрямую зависит от порогового значения и методов поиска. В данной работе был выбран и реализован метод Оцу [1], для расчета глобального порогового уровня интенсивности монохромного изображения за счёт максимизации дисперсии между классами, что позволяет разделить множество пикселей на два класса: фоновые и целевые. Время работы алгоритма напрямую зависит от размера исходного изображения, т.к. в ходе поиска необходимо построить гистограмму для каждого уровня интенсивности. Далее на рисунке 3 представлена гистограмма изображения 1.

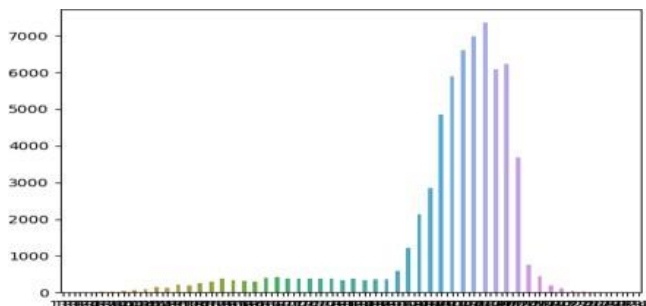


Рис. 3. Гистограмма изображения рисунка 1, ось X – все уровни интенсивности серого цвета, ось Y – количество пикселей

Гистограмма построена для входного изображения (рис. 1) размером 640 на 640, формата JPG и глубиной цвета в 24 бита. Была получена с использованием библиотеки matplotlib.

```
{250: 5225, 252: 1, 251: 3381, 249: 2580, 248: 2, 246: 1, 247: 690, 244: 1, 240: 1, 238: 1, 242: 1, 254: 1, 236: 1,
239: 197, 245: 322, 241: 238, 243: 273, 253: 1388, 255: 1801, 235: 63, 237: 81, 234: 1, 215: 43, 194: 1, 180: 3,
171: 70, 167: 299, 166: 1, 174: 2, 179: 36, 188: 2, 200: 3, 216: 3, 233: 58, 230: 1, 204: 1, 208: 1, 160: 3, 152:
1, 150: 1, 153: 295, 156: 1, 158: 1, 154: 1, 229: 43, 202: 1, 163: 1054, 151: 305, 148: 2, 176: 1, 226: 3, 159:
404, 172: 1, 210: 4, 198: 1, 192: 1, 232: 3, 184: 1, 149: 177, 157: 334, 162: 3, 164: 1, 161: 618, 147: 103, 169:
110, 207: 31, 185: 40, 228: 1, 182: 1, 146: 1, 222: 4, 165: 822, 155: 319, 168: 1, 221: 37, 217: 36, 191: 37, 170:
1, 220: 2, 142: 1, 175: 50, 199: 37, 187: 40, 173: 47, 186: 3, 218: 1, 214: 1, 227: 45, 178: 2, 231: 34, 195: 36,
193: 35, 190: 2, 212: 1, 224: 1, 197: 34, 138: 1, 144: 3, 213: 43, 183: 33, 196: 1, 181: 34, 177: 38, 189: 36,
219: 37, 223: 35, 206: 2, 201: 37, 143: 26, 209: 36, 205: 30, 145: 44, 211: 32, 225: 36, 140: 1, 134: 1, 203: 34,
139: 9, 136: 1, 141: 14, 135: 4, 137: 5, 133: 1}
```

Рис. 4. Словарь с вариациями серого цвета и количеством пикселей

На рисунке 4, расположен словарь, содержащий пары «ключ: значение», где ключом выступает уровень интенсивности, а значением - количество пикселей. Анализируя полученную структуру и гистограмму, можем вывести вероятность для каждого порога серого, учитывая, что суммарное количество пикселей $N = 409600$, а длина словаря равна $L = 123$:

$$p_i = \frac{n_i}{N} \quad (2)$$

где n_i – количество пикселей с прозрачностью серого с индексом $i = 1 \dots L$.

Метод Оцу, как было упомянуто выше, максимизирует дисперсию δ^2 между двумя классами C_1 (меньше порога) и C_2 (больше) выражается следующей формулой:

$$\delta^2 = p_1(m_1 - m_G)^2 + p_2(m_2 - m_G)^2 \quad (3)$$

где p_1, p_2 – вероятности определения пикселей в категории C_1 и C_2 соответственно, m_1, m_2 – средние значения соответствующих категорий, а m_G – глобальное значение. Упростив (3), мы получим следующее выражение:

$$\delta^2 = p_1 p_2 (m_1 - m_2)^2 \quad (4)$$

значение которого нам нужно максимизировать, для этого необходимо пройти по всем уровням серого k от $0 \dots 255$ которое используется в выражениях (5), (6) и (7) и приведёт к максимальной межклассовой дисперсии, тем самым укажет на пороговое значение k .

$$p_1 = \sum_{i=0}^k p_i \quad (5)$$

$$m_1 = \frac{1}{p_1} \sum_{i=0}^k i p_i \quad (6)$$

$$m_2 = \frac{1}{p_2} \sum_{i=k+1}^{L-1} i p_i \quad (7)$$

Рассуждение выше уместно в случае неизвестного порога k , приведём некоторые выражения. Среднее арифметическое уровня k определяется как кумулятивным средним значением уровня k , если $T = k$, тогда (8):

$$m_k = \sum_{i=0}^k i p_i \quad (8)$$

$$m_G = \sum_{i=0}^{L-1} i p_i \quad (9)$$

Тогда m_1 и m_2 можно выразить через (8) и (9) следующим образом:

$$m_1 = \frac{m_k}{p_1} \quad (10)$$

$$m_2 = \frac{m_G - m_k}{p_2} \quad (11)$$

Подставляя m_1 (10) и m_2 (11) в (4), мы получим конечную форму (12) межклассовой дисперсии:

$$\delta^2 = \frac{(m_G p_1 - m_k)^2}{p_1(1 - p_1)} \quad (12)$$

где уровень k является порогом бинаризации по Оцу при максимальном значении дисперсии.

Для реализации алгоритма с целью проверки качества работы метода поиска пороговой бинаризации Оцу [2], так как он используется в библиотеке `keras_ocr`, а также во множестве современных фреймворках работающих с изображениями, например, `orencv` и `Pillow` для Python..

Далее будет приведена реализация алгоритма Оцу [3] для поиска порога бинаризации, как было сказано выше, данный способ нахождения порогового значения, на вход получает изображение серых оттенков, пример, рисунок 5.

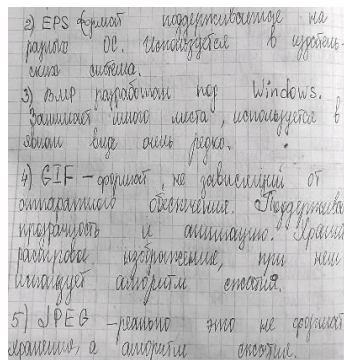


Рис. 5. Изображение 1 в серых тонах

В реализации алгоритма используется только функции `convert()`, с аргументом `LA` для изменения цветовой палитры фотографии, а именно в оттенки серого, чтобы в дальнейшем построить гистограмму градации серого цвета необходимой для работы метода Оцу.

В результате этих манипуляций с изображением, получаем общее количество пикселей, сумму интенсивностей всех пикселей и словарь (`dictionary`), содержит пару «ключ-значение», в роли ключа выступает степень интенсивности серого цвета, а значения – число пикселей с такой степенью. Полученные данные передаются в функции `otsu_threshold`.

Результат работы метода – переменная `best_thresh`, является тем самым порогом для бинаризации. Сам же алгоритм бинаризации состоит обычного прохода по всем пикселям и сравнения их степени с найденным порогом. В

итоге, мы получаем изображение (рисунок 6) в черно-белом цвете, где темным выделены нужные нам целевые объекты, а белым фоновые.

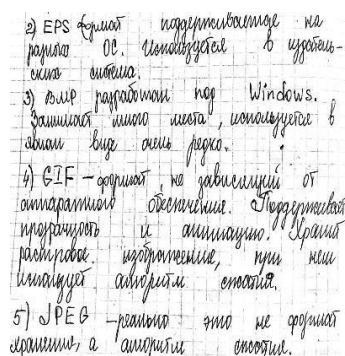


Рис. 6. Изображение после бинаризации с использованием метода Оцу

В данной работе был рассмотрен пример использования алгоритма Оцу для бинаризации изображения в качестве этапа предварительной обработки, выделения необходимой информации на изображении и последующего распознавания рукописного текста.

Библиографический список

1. Ana Sofia Nicholls, Gene Tanaka, A Neural Model for Text Segmentation (Stanford CS224N Custom Project) – URL: https://web.stanford.edu/class/archive/cs/cs224n/cs224n.1214/reports/final_reports/report001.pdf.
2. Wysterlanya K. P. Barros, Leonardo A. Dias, Marcelo A. C. Fernandes, Fully Parallel Implementation of Otsu Automatic Image Thresholding Algorithm on FPGA – URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8234950/>
3. Otsu N. A Threshold Selection Method from Gray-Level Histograms. IEEE Trans. Syst. Man Cybern. 1979 – URL: https://cw.fel.cvut.cz/b201/_media/courses/a6m33bio/otsu.pdf.

Т.В. Васкевич

РЕГРЕССИОННЫЙ АНАЛИЗ ИНВЕСТИЦИОННОЙ ПРИВЛЕКАТЕЛЬНОСТИ РЕГИОНОВ РФ

В статье рассматривается алгоритм анализа инвестиционной привлекательности регионов России сквозь призму регрессионного анализа. Исследование базируется на построении, оптимизации и интерпретации регрессионных моделей инвестиционной привлекательности регионов РФ за 2017-2022 гг.

Ключевые слова: регрессионный анализ, моделирование, корреляционный анализ, инвестиционная привлекательность.

The article considers an algorithm for analyzing the investment attractiveness of Russian regions through the prism of regression analysis. The study is based on the construction, optimization and interpretation of regression models of investment attractiveness of the regions of the Russian Federation for 2017-2022.

Keywords: regression analysis, modeling, correlation analysis, investment attractiveness.

Моделирование инвестиционной привлекательности регионов России выступает важным инструментом для прогноза инвестиционного потенциала. Работа по моделированию инвестиционной привлекательности состояла из следующих этапов: изучение теоретических и методических основ моделирования инвестиционного потенциала; проведение анализа основных индикаторов инвестиционного потенциала регионов России; разработка модели инвестиционного потенциала регионов России; анализ и интерпретация результатов моделирования; рекомендации по улучшению инвестиционного потенциала регионов России.

Гипотеза исследования заключается в том, что инвестиционная привлекательность регионов России зависит от совокупности множества детерминантов, таких как: экономический рост, качество жизни населения, инфраструктура, наличие инновационного потенциала и других факторов.

Объектом исследования послужили статистические данные субъектов Российской Федерации в период за 2017–2022 годы.

Новизна данного исследования заключается в создании авторской модели инвестиционной привлекательности регионов России, учитывающей как классические, так и новые факторы, а также в проведении анализа результатов моделирования, сделанных на основе современных методов статистического анализа.

Информационной базой научной работы послужили материалы, опубликованные в научной литературе, разработки в исследуемой области российских и зарубежных ученых-аналитиков. Для выполнения аналитической части работы были использованы статистические данные субъектов Российской Федерации [1].

Для условий оптимального использования инвестиций в экономической науке и практике используется категория инвестиционной привлекательности. В связи с этим вполне логичным представляется увеличивающийся интерес субъектов инвестиционной деятельности, прежде всего инвесторов, к существующим методам оценки инвестиционного климата страны. Следует отметить, что для российских регионов сегодня характерна значительная региональная дифференциация социально-экономических условий. Поэтому правильнее будет говорить об оценке инвестиционной привлекательности регионов РФ, а не инвестиционного климата страны в целом.

Между эффективностью инвестиций, инвестиционной привлекательностью и инвестиционной деятельностью существует тесная взаимосвязь.

Эффективность инвестиций определяет инвестиционную привлекательность, а инвестиционная привлекательность – инвестиционную деятельность. Чем выше эффективность инвестиций, тем выше уровень инвестиционной привлекательности и масштабнее инвестиционная деятельность, и наоборот.

Под инвестиционной привлекательностью на макроуровне понимаются условия (экономические, правовые, политические, социальные и другие), созданные государством всем субъектам хозяйствования, а также иностранным инвесторам для выгодного вложения инвестиций с целью развития национальной экономики

Инвестиционная привлекательность регионов – интегральная характеристика отдельных регионов страны с позиции инвестиционного климата, уровня развития инвестиционной инфраструктуры, возможности привлечения инвестиционных ресурсов и других факторов, существенно влияющих на формирование доходности инвестиций и инвестиционных рисков.

Определение инвестиционной привлекательности региона позволяет выявить две ее составляющие: инвестиционный потенциал и инвестиционный риск. Соответственно следует выделить две основные группы факторов: оказывающие влияние на инвестиционный потенциал региона; определяющие инвестиционный риск региона.

Среди факторов, оказывающих влияние на инвестиционный потенциал региона, можно выделить следующие группы факторов: относящиеся к труду (трудовые ресурсы и их образовательный уровень); потребительские (совокупная покупательная способность населения); инфраструктурные (экономико-географическое положение региона и его инфраструктурная обеспеченность); производственные (совокупный результат хозяйственной деятельности предпринимательских структур и населения региона); инновационные (уровень развития науки и внедрения достижений научно-технического прогресса); финансовые (прибыльность предприятий региона и доходы населения); природно-ресурсные (средневзвешенная обеспеченность экономической деятельности в регионе балансовыми запасами основных видов природных ресурсов).

Современный экономический рынок России представляет собой множество возможностей для инвесторов, открывающих широкие горизонты для развития как на федеральном, так и на региональном уровне. Однако, при выборе региона для инвестирования необходимо учитывать множество социально-экономических показателей, которые могут влиять на успех инвестиционного проекта. Необходимость анализа инвестиционной привлекательности регионов России в свете социально-экономических показателей становится очевидной. Выбор и использование математических моделей

может помочь в определении наиболее привлекательных регионов для инвестирования, а также в оценке потенциального риска и доходности инвестиционных проектов.

Сценарий, разработанный для исследования инвестиционного потенциала регионов России на основе социально-экономических показателей, представлен ниже на рисунке 1 на примере 2022 года. Для 2017 и 2020 годов сценарий выглядит аналогично. Разработка сценария выполнялась в low-code платформе Loginom (рис.1) [2].

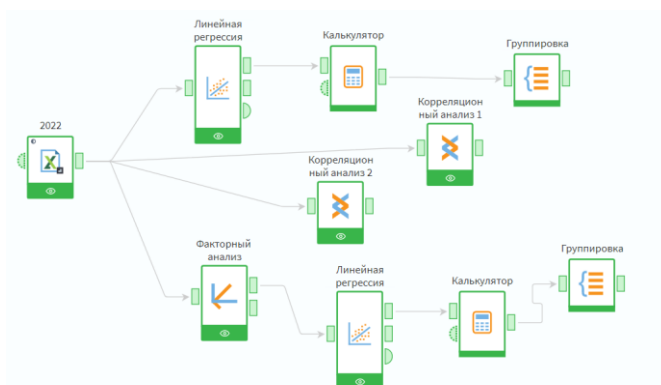


Рис. 1. Сценарий для исследования инвестиционного потенциала регионов России на основе социально-экономических показателей за 2022 год

Анализ регионов был произведен на основе следующих факторов: площадь территории; численность населения; среднегодовая численность занятых; среднедушевые денежные доходы; потребительские расходы в среднем на душу населения; валовой региональный продукт; основные фонды в экономике; ввод в действие жилых домов; оборот розничной торговли; среднемесячная номинальная начисленная заработная плата; сальдированный финансовый результат. Откликом послужили инвестиции в основной капитал.

Чтобы определить силу взаимосвязи между откликом и анализируемыми факторами, был проведен корреляционный анализ по коэффициенту корреляции Пирсона с помощью одноименного компонента. Почти все факторы, кроме площади территории, больше критического значения коэффициента Пирсона. Это справедливо для всего исследуемого периода. Далее будем анализировать факторы, исключив только данные о площади территории, которые, как показал анализ, оказывают наименьшее влияние на отклик. Чтобы исключить взаимную зависимость факторов проведем корреляционный анализ на выявление мультиколлинеарности. Это необходимо для выявления линейной зависимости между объясняющими переменными. После исключения мультиколлинеарных факторов, коэффициент корреляции которых превышает значение 0.8, набор факторов выглядит следующим

образом: ввод в действие жилых домов, оборот розничной торговли, среднедушевые денежные доходы, потребительские расходы в среднем на душу населения, основные фонды в экономике.

Далее был проведен регрессионный анализ. В качестве зависимой переменной была установлена переменная «Инвестиции в основной капитал» (рис.2). Отбор факторов производился по методу Enter - Принудительное включение, уровень доверия был установлен 95%, критерий отбора факторов – F-тест (порог значимости при исключении факторов – 0,05).

Модель		...				
Финальная модель		Атрибут	Коэффициент	Стандартная ош...	T-статистика	P-значение
Показатель	Значение					
Константа	Включена	-98 Константа	-221 007,401700	112 142,852319	-1,970767	0,052947
Логарифм функции правдоподобия	-1 043,312229	-98 Ввод в действие жилых домов...	-1 127,620189	96,337466	-11,704898	9,335473e-18
Коэффициент детерминации	0,980630	-98 Оборот розничной торговли, ...	5,278402	0,255676	20,644882	1,677857e-30
Коэффициент детерминации (скорр.)	0,979749	-98 Основные фонды в экономик...	9,998182	0,342233	29,214567	1,795103e-39
Стандартное отклонение	740 397,241297					
Число степеней свободы ошибки	66,00					
Число степеней свободы модели	3,000000					
F-статистика	1 113,755188					
P-значение модели	5,551115e-16					
Критерий Акаике	29,923207					
Критерий Акаике (скорр.)	29,931998					
Критерий Байеса	30,051692					
Критерий Ханнана-Куинна	29,974243					

Рис. 2. Отчет по регрессии 2022 год

Величина коэффициента детерминации модели линейной регрессии в 2022 году, равна 0,98, что заметно выше, чем в 2017 и 2020 годах, которые равны 0,79 и 0,92 соответственно. Поэтому модель, построенная на основе данных за 2022 год, наиболее точно описывает зависимость отклика от отобранных факторов. В связи с этим, более подробно рассмотрим результаты, полученные за 2022 год.

В отчете по регрессии величина коэффициента детерминации равна 98,08%, это означает, что качество модели очень высокое – модель объясняет 98% дисперсии результативной переменной. Выше в отчете по регрессии на рисунке 3 были приведены регрессионные коэффициенты и уровень их значимости (P-значение). Таким образом, регрессионная модель имеет следующий вид (1):

$$Y = -221\,007,40 - 1\,127,62 * X1 + 5,28 * X2 + 10,00 * X3 \quad (1)$$

где

$X1$ – ввод в действие жилых домов (тыс. кв. метров),

$X2$ – оборот розничной торговли (млн. руб.),

$X3$ – основные фонды в экономике (млн. руб.).

Параметры уравнения значимы при заданном уровне значимости 0,05.

Интерпретируем уравнение регрессии: на объем инвестиций, вложенных в основной капитал региона, существенное влияние оказывают следующие показатели: ввод в действие жилых домов, оборот розничной торговли, основные фонды в экономике.

Стоит заметить, что оборот розничной торговли для каждого исследуемого года оказывает существенное влияние на инвестиции. В 2022 году это влияние наибольшее и положительное.

Таким образом, добиться увеличения притока инвестиций в регион можно с помощью повышения оборота розничной торговли и увеличения основных фондов в экономике. Для этого необходимо улучшить использование материально-технической базы предприятий: с этой целью установить оптимальный режим работы предприятий, вести внедрение прогрессивных форм торговли, а также провести обновление основных фондов.

Далее был проведен анализ инвестиционного потенциала регионов России на основе социально-экономических показателей. Получили следующий список регионов с высокой инвестиционной привлекательностью: г. Москва, Краснодарский край, Московская область, Тюменская область, Ростовская область, г. Санкт-Петербург, Республика Татарстан, Белгородская область, Воронежская область, Свердловская область.

В отчете по регрессии величина коэффициента детерминации равна 97,05%, это означает, что качество модели очень высокое – модель объясняет 97% дисперсии резульативной переменной. В отчете по регрессии (приложение С) были приведены регрессионные коэффициенты и уровень их значимости (Р-значение). Таким образом, регрессионная модель имеет следующий вид (3):

$$Y = 2,84 + 0,000096X_1 + 0,0049X_2 + 0,003X_3 + 0,097X_4 + 0,00056X_5 \quad (3)$$

где

X_1 – среднедушевые денежные доходы (руб.),

X_2 – инвестиции в основной капитал (млрд. руб.),

X_3 – ввод в действие жилых домов (тыс. кв. метров),

X_4 – перевозки грузов (млн т),

X_5 – грузооборот (млн т-км).

Параметры уравнения значимы при заданном уровне значимости 0,05.

Таким образом, для увеличения инвестиционного потенциала региона следует принять меры по снижению цен на продукты питания и повышению прожиточного минимума. Также необходимо разработать стратегию по застройке и введению в действие жилых домов.

Библиографический список

1. Федеральная служба государственной статистика. Режим доступа: <https://rosstat.gov.ru/> (дата обращения: 10.08.2023 г.)
2. Официальный интернет-ресурс Low-code платформы для реализации аналитических процессов Loginom. Режим доступа: <https://loginom.ru/>

**Н.А. Белоусов, М.Ю. Захаров,
Н.И. Овсиенко, Ю.И. Касперович**
**ВЕРОЯТНОСТНО-СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ
ДОСТОВЕРНОСТИ ДОПУСКОВОГО КОНТРОЛЯ,
ДИАГНОСТИКИ И БИНАРНОЙ КЛАССИФИКАЦИИ**

В статье предложена методика вероятностно-статистического исследования достоверности процессов допускового контроля, диагностики и бинарной классификации более точно и корректно по сравнению с существующими ГОСТами учитывающая исходные условия для расчета вероятности общей ошибки, а, следовательно, и общей достоверности.

Ключевые слова: случайные события, статистические гипотезы, ошибки 1-го и 2-го рода, вероятность события, условная вероятность, относительная частота, доверительный интервал, доверительная вероятность, статистические оценки, планирование объемов эксперимента, обработка экспериментальных данных, допусковой контроль, диагностика, бинарная классификация.

The article proposes a method of probabilistic-statistical study of the reliability of the processes of tolerance control, diagnostics and binary classification more accurately and correctly in comparison with existing GOSTs, taking into account the initial conditions for calculating the probability of a total error, and, consequently, the overall reliability.

Key words: random events, statistical hypotheses, errors of the 1st and Type 2, probability of an event, conditional probability, relative frequency, confidence interval, confidence probability, statistical estimates, planning of experimental volumes, processing of experimental data, tolerance control, diagnostics, binary classification.

Для вероятностно-статистического исследования достоверности «процессов решения» (которыми могут быть, в частности, допусковой контроль, диагностика и бинарная классификации) введем гипотезы (названия – условные):

основную $H_0 = \{\text{"изделие годное"}\}$,
альтернативную $H_1 = \{\text{"изделие бракованное"}\}$.

Рассмотрим также события (названия – условные):

$O = \{\text{"ошибка диагностики"}\}$,
 $D = \{\text{"достоверная диагностика"}\}$.

Потребуется для исследования также события (названия – условные):

$H_{0\text{диаг}} = \{\text{"изделие признано годным при диагностике"}\}$,
 $H_{1\text{диаг}} = \{\text{"изделие признано бракованным при диагностике"}\}$.

Очевидно, что пары событий H_0 и H_1 , O и D , $H_{0\text{диаг}}$ и $H_{1\text{диаг}}$ являются противоположными событиями, поэтому справедливы соотношения:

$$P(H_0) + P(H_1) = 1, \quad (1)$$

$$P(O) + P(D) = 1, \quad (2)$$

$$P(H_{0\text{диаг}}) + P(H_{1\text{диаг}}) = 1. \quad (3)$$

При проверке гипотез H_0 и H_1 могут возникнуть ошибки вида: отвергнуть правильную гипотезу H_0 – ошибка 1-го рода, принять неправильную гипотезу H_0 – ошибка 2-го рода.

Вероятности ошибок 1-го и 2-го рода обозначают обычно с использованием α и β соответственно.

Пусть доступные фактические значения α и β равны: $\alpha_{\text{факт}} = 1\%$, $\beta_{\text{факт}} = 0,2\%$. Приведённые фактические значения вероятностей ошибок 1-го и 2-го рода получают обычно от соответствующих предприятий-изготовителей и представляют собой экспертно-эмпирические точечные оценки указанных вероятностей.

Допустим, что при рассматриваемом «производстве» допустимым является 3% брака. Поэтому можно положить:

$$P(H_1) = 3\% = 0,03. \quad (4)$$

Из формулы (1) следует, что

$$P(H_0) = 1 - 0,03 = 0,97. \quad (5)$$

Обозначим вероятности ошибок 1-го и 2-го рода, оцениваемые в ходе исследований, через P_α и P_β соответственно. Эти вероятности можно представить в виде условных вероятностей:

$$P_\alpha = P(H_{1\text{диаг}} | H_0), \quad (6)$$

$$P_\beta = P(H_{0\text{диаг}} | H_1). \quad (7)$$

Для оценки P_α и P_β в (6), (7) будем использовать их выборочные аналоги $P_\alpha^{\text{выб}}$ и $P_\beta^{\text{выб}}$, полученные на основании экспериментальных данных. Также зададимся полудлинами ΔP_α , ΔP_β доверительных интервалов и доверительной вероятностью $1 - \gamma$ (где γ – уровень значимости). Указанные доверительные интервалы имеют вид:

$$P_\alpha \in (P_\alpha^{\text{выб}} - \Delta P_\alpha; P_\alpha^{\text{выб}} + \Delta P_\alpha), \quad (8)$$

$$P_\beta \in (P_\beta^{\text{выб}} - \Delta P_\beta; P_\beta^{\text{выб}} + \Delta P_\beta). \quad (9)$$

Соотношения (8) и (9) выполняются с доверительной вероятностью $1 - \gamma$.

Используя методику оценки постоянной вероятности события при независимых испытаниях по относительной частоте его появления, можно оценить приведенные в (8) и (9) полудлины доверительных интервалов следующим образом [1]:

$$\Delta P_\alpha \geq \frac{t \sqrt{P_\alpha^{\text{выб}}(1 - P_\alpha^{\text{выб}})}}{\sqrt{n_\alpha}}, \quad (10)$$

$$\Delta P_{\beta} \geq \frac{t \sqrt{P_{\beta}^{\text{выб}}(1-P_{\beta}^{\text{выб}})}}{\sqrt{n_{\beta}}}, \quad (11)$$

где t – аргумент функции Лапласа, соответствующий доверительной вероятности $1 - \gamma$: $\Phi(t) = (1 - \gamma)/2$, n_{α} , n_{β} – количества опытов для оценки вероятностей ошибок 1-го и 2-го рода соответственно, общее количество опытов $n = n_{\alpha} + n_{\beta}$.

Выражения (10) и (11) для оценок полудлин доверительных интервалов справедливы, поскольку количества опытов n_{α} , n_{β} имеют порядок сотен.

Для получения дальнейших оценок рассмотрим в общем виде и проанализируем на возрастание/убывание подкоренные выражения в числителях формул (10), (11):

$$f(p) = p(1 - p) = p - p^2. \quad (12)$$

Производная функции $f(p)$ в (12) равна:

$$f'(p) = 1 - 2p. \quad (13)$$

Поскольку аргумент p в (12), (13) имеет смысл вероятности, то $p \in [0; 1]$.

$$f'(p) > 0, p \in [0; 0,5), \quad (14)$$

$$f'(p) < 0, p \in (0,5; 1]. \quad (15)$$

Из соотношений (14) и (15) следует, что $f(p)$ в (12) возрастает при $p \in [0; 0,5)$ и убывает при $p \in (0,5; 1]$.

В силу значений $\alpha_{\text{факт}} = 1\% = 0,01$, $\beta_{\text{факт}} = 0,2\% = 0,002$ можно считать вполне адекватными следующие априорные оценки сверху (с некоторым «запасом») для выборочных значений $P_{\alpha}^{\text{выб}}$ и $P_{\beta}^{\text{выб}}$:

$$P_{\alpha}^{\text{выб}} \leq 2\% = 0,02 (= 2\alpha_{\text{факт}}), \quad (16)$$

$$P_{\beta}^{\text{выб}} \leq 0,5\% = 0,005 (= 2,5\beta_{\text{факт}}). \quad (17)$$

На основании оценок (16), (17) и результатов по возрастанию/убыванию выражений вида (12) получим для формул (10) и (11):

$$P_{\alpha}^{\text{выб}}(1 - P_{\alpha}^{\text{выб}}) \leq 0,02 \cdot (1 - 0,02) = 0,0196, \text{ а следовательно,}$$

$$\sqrt{P_{\alpha}^{\text{выб}}(1 - P_{\alpha}^{\text{выб}})} \leq \sqrt{0,0196} = 0,14, \quad (18)$$

$$P_{\beta}^{\text{выб}}(1 - P_{\beta}^{\text{выб}}) \leq 0,005 \cdot (1 - 0,005) = 0,004975, \text{ а следовательно,}$$

$$\sqrt{P_{\beta}^{\text{выб}}(1 - P_{\beta}^{\text{выб}})} \leq \sqrt{0,004975} = 0,07. \quad (19)$$

Планирование эксперимента по оценке достоверности допускового контроля, диагностики и бинарной классификации

На основании оценок (18), (19), используя соотношения (10) и (11), получим оценки количества опытов для построения доверительных интервалов (8), (9):

$$n_{\alpha} \geq \left(\frac{0,14t}{\Delta P_{\alpha}} \right)^2, \quad (20)$$

$$n_{\beta} \geq \left(\frac{0,07t}{\Delta P_{\beta}} \right)^2. \quad (21)$$

Положим в соотношениях (20) и (21) $\Delta P_{\alpha} = 0,01$; $\Delta P_{\beta} = 0,005$ (что вполне соответствует значениям $\alpha_{\text{факт}} = 0,01$, $\beta_{\text{факт}} = 0,002$ и оценкам (16), (17)), а также $t = 1,96$, что соответствует доверительной вероятности для интервалов (8), (9) $1 - \gamma = 0,95$ (уровень значимости $\gamma = 0,05$). Получим количества опытов:

$$n_{\alpha} \geq 750, \quad (22)$$

$$n_{\beta} \geq 750, \quad (23)$$

где n_{α} и n_{β} – количества опытов, необходимых для оценок вероятностей ошибок 1-го и 2-го рода соответственно, с указанными вероятностными характеристиками. Положим, исходя из (22), (23):

$$n_{\alpha} = n_{\beta} = 750. \quad (24)$$

Количество опытов n_{α} должно проводиться с "изделием годным", а n_{β} – с "изделием бракованным". Размер выборки: $n = n_{\alpha} + n_{\beta} = 1500$.

Поскольку для исследуемых вероятностей P_{α} и P_{β} ошибок 1-го и 2-го рода важны только оценки сверху, из доверительных интервалов (8) и (9) получим:

$$P_{\alpha} \leq P_{\alpha}^{\text{выб}} + \Delta P_{\alpha}, \quad (25)$$

$$P_{\beta} \leq P_{\beta}^{\text{выб}} + \Delta P_{\beta}. \quad (26)$$

Неравенства (оценки) (25), (26) выполняются с вероятностью $1 - \gamma/2 = 0,975$. Количества опытов (24) будут представляться в виде сумм:

$$n_{\alpha} = n_1 + n_2, \quad (27)$$

$$n_{\beta} = n_3 + n_4, \quad (28)$$

где n_1 – количество наступлений события $H_{0\text{диаг}}$ при верности гипотезы H_0 – обозначим ($H_{0\text{диаг}}|H_0$), n_2 – количество наступлений ($H_{1\text{диаг}}|H_0$); n_3 – количество наступлений ($H_{1\text{диаг}}|H_1$), n_4 – количество наступлений ($H_{0\text{диаг}}|H_1$).

Выборочные значения $P_{\alpha}^{\text{выб}}$ и $P_{\beta}^{\text{выб}}$ – другими словами, относительные частоты наступлений ошибок 1-го и 2-го рода соответственно – будут определяться следующим образом:

$$P_{\alpha}^{\text{выб}} = \frac{n_2}{n_1 + n_2}, \quad (29)$$

$$P_{\beta}^{\text{выб}} = \frac{n_4}{n_3 + n_4}. \quad (30)$$

Обработка экспериментальных данных по оценке достоверности допускового контроля, диагностики и бинарной классификации

Фактическое состояние	Результаты «процесса решения»	
	«Изделие <u>признано</u> годным» ($H_{0\text{диаг}}$)	«Изделие <u>признано</u> бракованным» ($H_{1\text{диаг}}$)
«Изделие – годное» (H_0)	n_1	n_2
«Изделие – бракованное» (H_1)	n_4	n_3

Таблица 1. Результаты экспериментов

На основании данных таблицы 1 по формулам (29), (30) рассчитываем $P_\alpha^{\text{выб}}$ и $P_\beta^{\text{выб}}$ (проверяем справедливость оценок (16), (17)).

Конкретные значения n_i , $i = \overline{1,4}$, полученные в ходе опытов и расчетные значения $P_\alpha^{\text{выб}}$ и $P_\beta^{\text{выб}}$:

$$\begin{aligned} n_1 &= 739, n_2 = 11, \\ P_\alpha^{\text{выб}} &\approx 0,015 = 1,5 \%, \\ n_3 &= 748, n_4 = 2, \\ P_\beta^{\text{выб}} &\approx 0,003 = 0,3 \%. \end{aligned}$$

Исходя из того, ошибка 1-го рода может наступать только при условии справедливости гипотезы H_0 , а ошибка 2-го рода может наступать только при условии справедливости гипотезы H_1 , получим, что вероятность общей «ошибки диагностики» (события O) будет определяться по формуле полной вероятности:

$$\begin{aligned} P(O) &= P(H_0) * P(H_{1\text{диаг}}|H_0) + P(H_1) * P(H_{0\text{диаг}}|H_1) = \\ &= P(H_0) * P_\alpha + P(H_1) * P_\beta. \end{aligned} \quad (31)$$

Заметим, что предлагаемая методика вероятностно-статистического исследования достоверности допускового контроля, диагностики и бинарной классификации более точно и корректно по сравнению с ГОСТ Р 8.731-2010 ([2]) учитывает исходные условия для расчета вероятности общей «ошибки диагностики» (см. формулу (31)). Поскольку в [2] используются только условные вероятности ошибок 1-го и 2-го рода (6), (7), а также условные вероятности правильной диагностики: $P_1 = P(H_{1\text{диаг}}|H_1)$ и $P_0 = P(H_{0\text{диаг}}|H_0)$, но не используются вероятности соответствующих гипотез (условий) $P(H_0)$ и $P(H_1)$. Это приводит к некорректной расчетной формуле: $P_\alpha + P_\beta + P_1 + P_0 = 1$ (см. формулу (1) [2]), корректно будет $P_\alpha + P_\beta + P_1 + P_0 = 2$.

На основании оценок (25), (26) вероятность ошибки в (31) можно оценить так:

$$P(O) \leq P(H_0) * [(P)_{\alpha}^{\text{выб}} + \Delta P_{\alpha}] + P(H_1) * [(P)_{\beta}^{\text{выб}} + \Delta P_{\beta}].$$

Подставляя в выражение (32) конкретные числовые значения, получим:

$$P(O) \leq 0,97 * (0,015 + 0,01) + 0,03 * (0,003 + 0,005) = 0,0245 = 2,45 \%. \quad (33)$$

Неравенство (оценка) (33) выполняется с доверительной вероятностью

$$1 - \gamma/2 = 0,975 \text{ при уровне значимости } \gamma/2 = 0,025.$$

Представляется целесообразным продолжить исследование предложенной методики с целью, в частности, более полного и обоснованного использования эмпирических данных.

Библиографический список

1. Гмурман, В. Е. Теория вероятностей и математическая статистика : учебник для вузов / В. Е. Гмурман. — 12-е изд. — Москва : Издательство Юрайт, 2023. — 479 с. — (Высшее образование). — ISBN 978-5-534-00211-9. — Текст : непосредственный.
2. ГОСТ Р 8.731-2010. СИСТЕМЫ ДОПУСКОВОГО КОНТРОЛЯ. Основные положения (2010) // Государственная система обеспечения единства измерений. Москва: Стандартинформ.

А.А. Овчинникова

УСИЛЕНИЕ БЕЗОПАСНОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА НА ОСНОВЕ АЛГОРИТМА RSA

В статье рассматривается разработка метода усиления криптографического алгоритма RSA. Введение дополнительной засекреченной операции, такой как разбиение на блоки позволит обеспечить безопасность сохранности данных.

Ключевые слова: криптографическая система RSA, асимметричные алгоритмы, протоколы RSA, кодирование информации, декодирование информации, усиление безопасности RSA.

The article discusses the development of a method for strengthening the RSA cryptographic algorithm. The introduction of an additional secret operation, such as partitioning into blocks, will ensure the security of data safety.

Keywords: RSA cryptographic system, asymmetric algorithms, RSA protocols, information encoding, information decoding, RSA security enhancement.

Криптографическая схема RSA, иногда называемая алгоритмом Ривеста-Шамира-Адлемана, в настоящее время является наиболее широко используемой асимметричной криптографической схемой, но на практике чаще всего используется для: шифрование небольших фрагментов данных, особенно для передачи ключей и цифровых подписей.

Однако следует отметить, что шифрование RSA не предназначено для замены симметричных шифров, поскольку оно в несколько раз медленнее. Это происходит из-за большого количества вычислений

В основе односторонней функции RSA лежит проблема целочисленной факторизации: умножить два больших простых числа с вычислительной точки зрения несложно, но разложить полученное произведение на множители очень сложно.

Алгоритм RSA

1. Выбор p, q : Чтобы произвести шифрование и дешифрование данных необходима пара ключей (открытый и личный). Их получим путем случайного выбора простых чисел

2. Найдем так называемый модуль сравнения при шифровании и дешифровании $n = p \cdot q$

3. Вычислим функцию Эйлера $f(x) = (p - 1)(q - 1)$, которая показывает сколько натуральных чисел в промежутке от 1 до $n-1$ имеют с n только 1 общий делитель равный 1, данное число не будет простым.

4. Выберем число e по критериям 1) $e < n$, 2) $GCD(f(x), e) = 1$

5. Вычислим $d: f(x)ed \equiv 1 \pmod{f(x)}$

Теперь имеем открытый ключ (n, e) и личный ключ (n, d)

Кодирование информации:

1. Получаем сообщение m

2. Шифруем полученной сообщение методом: $c = m^e \pmod{n}$, где m - сообщение, (n, e) – открытый ключ, c - зашифрованное сообщение.

Декодирование информации:

1. $m = c^d \pmod{n}$, где m -сообщение, c - зашифрованное сообщение, (n, d) – личный ключ.

Протокол RSA

Предположим, Боб хочет передать Алисе какое-то сообщение, но лично он это сделать не может, поэтому ему необходимо использовать посредника, например Стива. Однако Боб передаёт Алисе информацию, которую Стив знать не должен. И тут ему пригодится протокол RSA.

1. Перед обменом сообщением, Боб просит у Алисы её открытый ключ

2. После получения ключа, переданного через Стива, Боб шифрует своё сообщение ключом Алисы

3. Далее Боб, через Стива, передаёт Алисе зашифрованное сообщение

4. Алиса расшифровывает сообщение своим закрытым ключом

Таким образом, Стив видел открытый ключ Алисы и зашифрованное сообщение от Боба, но без закрытого ключа Алисы это сообщение не расшифровать. То есть, пусть Стив и держал в руках все передаваемые данные, но он не может узнать, что Боб передал Алисе.

Способ усиления защиты алгоритма

Подготовка к кодированию:

1. Получаем сообщение для передачи

```
in[46]:= m = "Ту-160-бомбардировщик ";
```

2. Переводим полученное сообщение в цифры и сливаем в одно число

```
Out[49]= {1, 0, 5, 8, 1, 0, 9, 1, 2, 0, 4, 5, 2, 0, 4, 9, 2, 0, 5, 4, 2, 0,
          4, 8, 8, 2, 1, 2, 1, 0, 7, 3, 1, 0, 8, 6, 1, 0, 8, 4, 1, 0, 7, 3,
          1, 0, 7, 2, 1, 0, 8, 8, 1, 0, 7, 6, 1, 0, 8, 0, 1, 0, 8, 8, 1, 0,
          8, 6, 1, 0, 7, 4, 1, 0, 9, 7, 1, 0, 8, 0, 1, 0, 8, 2, 2, 0, 3, 2}
```

3. Для большой надежности выбираем шаг разбиение на блоки (секретная информация)

```
Out[52]= {{1, 0, 5, 8}, {1, 0, 9, 1}, {2, 0, 4, 5}, {2, 0, 4, 9},
          {2, 0, 5, 4}, {2, 0, 4, 8}, {8, 2, 1, 2}, {1, 0, 7, 3},
          {1, 0, 8, 6}, {1, 0, 8, 4}, {1, 0, 7, 3}, {1, 0, 7, 2},
          {1, 0, 8, 8}, {1, 0, 7, 6}, {1, 0, 8, 0}, {1, 0, 8, 8}, {1, 0, 8, 6},
          {1, 0, 7, 4}, {1, 0, 9, 7}, {1, 0, 8, 0}, {1, 0, 8, 2}, {2, 0, 3, 2}}
```

Кодировка:

1. Шифруем каждый полученный блок

```

Out[54]= { 129 131 575 866 273 730 951 343 736 002 149 068 688 278 866 576 664 402 534 739 705 660 528 428,
688 351 803 758 280 851 012 579 603 649 636 104 231 550 204 534 714 688 610 982 614 426 171 331,
733 252 168 173 605 284 633 309 303 515 163 753 554 439 903 994 460 967 238 470 322 756 875 775,
50 599 762 435 958 378 589 692 180 452 499 423 725 204 758 922 944 823 589 924 939 904 221 371,
221 913 914 155 739 313 881 344 582 916 387 097 703 973 895 021 802 342 641 479 593 003 436 410,
748 128 994 780 434 914 102 988 709 995 083 825 835 772 127 670 064 599 164 290 032 749 395 773,
603 764 446 039 761 070 739 778 894 305 800 261 464 103 859 296 684 553 559 456 726 079 020 742,
96 435 321 605 669 545 697 646 534 959 559 271 674 469 573 823 262 939 387 234 262 625 170 217,
613 560 712 386 809 879 181 535 620 885 393 515 799 499 726 557 691 528 960 680 }

```

2. В отдельный вектор соберем длины полученных блоков (т. к. при шифровке длины блоков будут меняться)

```

Out[80]= {72, 72, 72, 71, 72, 72, 72, 71, 72, 72,
71, 72, 71, 72, 73, 71, 72, 72, 72, 73, 71, 72}

```

3. Сливаем блоки в одно число

```

Out[18]= 67 686 771 037 494 488 098 974 807 042 783 408 628 558 631 746 277 402 637 147 972 936 617 247 179 799 641 449 207 184 915 770 326 973 309 499 638 798 215 130 191 958 193 405 784 867 152 317 683 216 580 618 498 960 324 525 785 001 210 314 652 863 174 134 610 107 876 282 647 163 936 461 143 365 331 001 503 303 032 372 148 942 813 980 767 628 825 501 524 843 393 826 930 698 927 054 234 699 102 825 050 712 550 871 486 760 793 143 318 414 611 523 250 724 971 809 174 901 106 926 430 045 046 233 183 490 912 769 709 263 114 967 147 689 052 064 553 350 810 708 192 018 462 326 411 552 951 531 532 355 536 667 229 725 546 377 483 217 950 897 309 864 579 236 140 387 986 883 396 595 023 106 837 661 931 190 527 096 666 659 004 699 920 232 738 532 253 767 119 166 472 821 155 295 153 153 235 553 666 722 972 554 637 748 321 795 089 730 986 457 923 614 038 798 688 392 435 163 027 882 629 903 622 898 801 424 391 637 151 516 901 196 051 689 542 974 782 377 672 783 573 591 879 238 784 246 714 915 344 135 993 827 114 981 429 616 049 192 691 763 983 179 729 945 848 986 741 836 635 446 338 946 618 043 593 039 931 472 095 483 313 185 199 519 900 199 569 458 489 867 418 366 354 463 389 466 180 435 930 399 314 720 954 833 131 851 995 199 001 995 683 327 756 563 241 156 545 113 747 079 700 236 319 960 299 799 493 798 474 266 924 934 466 946 380 367 244 355 083 214 }

```

4. Можем высылать полученное число (открытый доступ).

5. Полученным вектором так же обмениваемся (используя систему обмена ключами).

Декодирование:

1. В соответствии с вектором длин разбиваем полученный в 4 пункте число на блоки нужной длины
2. Декодируем каждый блок
3. Сливаем число и разбиваем на блоки обговоренной длины
4. Переводим численные значения в буквы и получаем расшифрованное сообщение

[Out\[39\]](#) Ту-160 – российский бомбардировщик-ракетоносец

Таким образом, введя дополнительные действия в алгоритм RSA, такие как разбиение на блоки, мы усилили безопасность.

Библиографический список

1. Christof Paar, Jan Pelzl Понимание криптографии. - Heidelberg: Springer-verlag GmbH, 2010. - 372 с.
2. <https://www.wolfram.com/resources/index.php.ru?source=footer>.
3. <https://habr.com/ru/articles/745820>.

СЕКЦИЯ 3. Естественнонаучные задачи и альтернативные направления исследований

Т.Н. Афанасьева, И.Л. Ойнас, С.Ф. Гумбатова МОДЕЛИ РАСПРОСТРАНЕНИЯ НЕРВНОГО ИМПУЛЬСА

В статье рассматриваются модели распространения нервного импульса в живой среде, а именно система Ходжкина-Хаксли и более простая исследуемая система ФитцХью-Нагумо. При определенных значениях параметров определен характер состояний равновесия системы ФитцХью-Нагумо в ограниченной фазовой плоскости.

Ключевые слова: система ФитцХью-Нагумо, характеристическое уравнение, особая точка, узел, фокус, фазовая плоскость.

The article discusses models of nerve impulse propagation in a living environment, in particular, the Hodgkin-Huxley system and the FitzHugh system, which is easier to study. At certain values of the parameters, the character of equilibrium states of the FitzHugh-Nagumo system in a limited phase plane is determined.

Key words: FitzHugh-Nagumo system, characteristic equation, singularity, knot, focus, phase plane.

Распространение нервного импульса – пример автоволнового процесса в живых системах. Известно, что возбуждённый участок нервного волокна становится генератором электрического тока. При этом механизмы генерации нервного импульса долгое время были неясны и стали доступны, в основном, благодаря работам Алана Ходжкина и Эндрю Хаксли.

Работа выполнялась на аксоне гигантского кальмара, представляющем длинную цилиндрическую трубку, отходящую от нейрона. Тогда электрический сигнал распространяется вдоль внешней поверхности мембраны этой трубки, а толщина нервного волокна в сотни раз превышает толщину нервных волокон млекопитающих. Ходжкиным и Хаксли была предложена модель процессов ионного транспорта через мембрану и прохождения импульса потенциала вдоль мембраны.

Механизм работы мембранного генератора основан на разности потенциалов между положительно заряженной наружной поверхностью мембранного волокна и внутренней отрицательно заряженной протоплазмой, что объясняется различием ионного состава протоплазмы и окружающей внеклеточной жидкости, в частности, большим отличием концентраций ионов калия и натрия снаружи и внутри (в десятки раз).

На основе экспериментальных данных Ходжкиным и Хаксли была получена модель, описываемая следующей системой нелинейных дифференциальных уравнений [1]

$$\begin{cases} C \frac{\partial V}{\partial t} = \bar{g}_K n^4 (V_K - V) + \bar{g}_{Na} m^3 h (V_{Na} - V) + \bar{g}_l (V_l - V) + a \frac{\partial^2 V}{\partial x^2}, \\ \frac{dm}{dt} = \alpha_m(V)(1 - m) - \beta_m(V)m, \\ \frac{dh}{dt} = \alpha_h(V)(1 - h) - \beta_h(V)h, \\ \frac{dn}{dt} = \alpha_n(V)(1 - n) - \beta_n(V)n, \end{cases} \quad (1)$$

где n, m и h – функции потенциала и времени, определяющие поведение натриевого и калиевого тока, a – радиус волокна, R – удельное сопротивление протоплазмы, C – удельная ёмкость мембраны, $V_K, V_{Na}, V_l, \bar{g}_K, \bar{g}_{Na}, \bar{g}_l$ – постоянные параметры, а $\alpha_n(V), \alpha_m(V), \alpha_h(V)$ и $\beta_n(V), \beta_m(V), \beta_h(V)$ – полученные эмпирически функции потенциала вида

$$\alpha_m = \frac{0,1(V + 25)}{\exp \frac{V + 25}{10} - 1}, \quad \beta_m = 4 \exp \left(\frac{V}{18} \right),$$

$$\alpha_n = \frac{0,01(V + 10)}{\exp \frac{V + 10}{10} - 1}, \quad \beta_n = 0,125 \exp \left(\frac{V}{80} \right),$$

$$\alpha_h = 0,07 \exp \left(\frac{V}{20} \right), \quad \beta_h = \frac{1}{\exp \frac{V + 30}{10} + 1}.$$

Однако система (1) оказалась слишком сложной для аналитического исследования. Были построены упрощённые модели, а самой популярной оказалась предложенная независимо ФитцХью и Нагумо.

В этой модели система локальных процессов сводится к системе двух уравнений вида

$$\begin{cases} \frac{du}{dt} = u(a - u)(u - 1) + J_a - v \\ \frac{dv}{dt} = bu - \gamma v \end{cases}, \quad (2)$$

где функции u и v зависят от времени t , $0 < a < 1$, $\gamma > 0$, $b > 0$, $J_a \geq 0$. Здесь u заменяет мембранный потенциал V , а v выполняет роль переменных n , m и h в системе (1).

Интерес представляет строгое обоснование поведения решений системы (2) на фазовой плоскости. Параметр J_a отвечает за внешнее воздействие на систему. Если оно не оказывается (на мембрану не поступает электрический ток), то $J_a = 0$. Случай $J_a > 0$ рассматривался, например, в работе [4].

Рассмотрим случай $J_a = 0$. Приведем систему (2) к виду

$$\begin{cases} \frac{du}{dt} = u(a - u)(u - 1) - v, \\ \frac{dv}{dt} = bu - \gamma v \end{cases} \quad (3)$$

и найдём ее особые точки

$$\begin{cases} -u^3 + (a + 1)u^2 - au - v = 0 \\ bu - \gamma v = 0. \end{cases} \quad (4)$$

Из второго уравнения системы найдем $v = \frac{bu}{\gamma}$. Решая первое уравнение, получим

$$u_1 = 0, \quad u_2 = \frac{a + 1 + \sqrt{(a - 1)^2 - \frac{4b}{\gamma}}}{2},$$

$$u_3 = \frac{a + 1 - \sqrt{(a - 1)^2 - \frac{4b}{\gamma}}}{2}.$$

Все корни являются простыми состояниями равновесия системы (3).

При условии $(a - 1)^2 - \frac{4b}{\gamma} > 0$, имеем три особые точки системы

$$S_0(0; 0), \quad S_1\left(u_2; \frac{bu_2}{\gamma}\right), \quad S_2\left(u_3; \frac{bu_3}{\gamma}\right) \text{ (рис.1).}$$

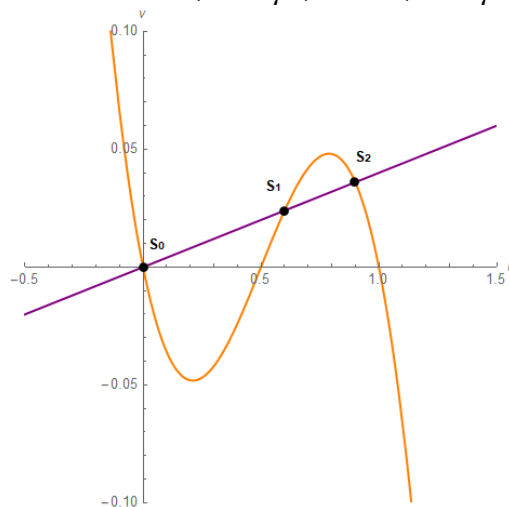


Рис. 1. Главные изоклины системы
 Параметры: $a = 0.5, b = 0.096, \gamma = 2$

Классифицируем сначала точку $S_0(0; 0)$.

Представляя (3) в виде

$$\begin{pmatrix} u \\ v \end{pmatrix}' = A \begin{pmatrix} u \\ v \end{pmatrix} + g(t, u, v),$$

где $A = \begin{pmatrix} -a & -1 \\ b & -\gamma \end{pmatrix}$, $g(t, u, v) = \begin{pmatrix} -u^3 + (a + 1)u^2 \\ 0 \end{pmatrix}$, применим теорему об устойчивости по первому приближению [3]. Заметим, что

$$\sup_{t \geq 0} \|g(t, u, v)\| = o(|u| + |v|) = o(\|(u, v)\|), \quad (5)$$

где $(u, v) \rightarrow 0$, а $\det(A - \lambda E) = \lambda^2 + (a + \gamma)\lambda + (\gamma a + b)$, т.е. уравнение $\det(A - \lambda E) = 0$ равносильно уравнению $\lambda^2 - \sigma\lambda + \Delta = 0$, где $\sigma = -a - \gamma = \text{Sp } A$ – след матрицы A , а $\Delta = \gamma a + b = \det A$. При $0 < a < 1$ и $\gamma > 0$, $b > 0$ имеем $\sigma = -a - \gamma < 0$, $\Delta = \gamma a + b > 0$, т.е коэффициенты характеристического уравнения $-\sigma$ и Δ положительны. Значит точка $S_0(0; 0)$ – устойчивый узел (когда дискриминант уравнения $D = \sigma^2 - 4\Delta > 0$) либо устойчивый фокус (когда $D < 0$) [3, с.98] (на рис. 2 и рис. 3 соответственно).

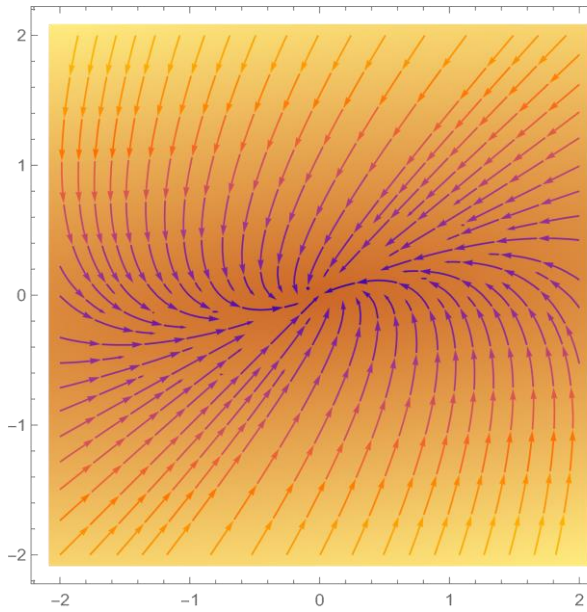


Рис. 2. Устойчивый узел

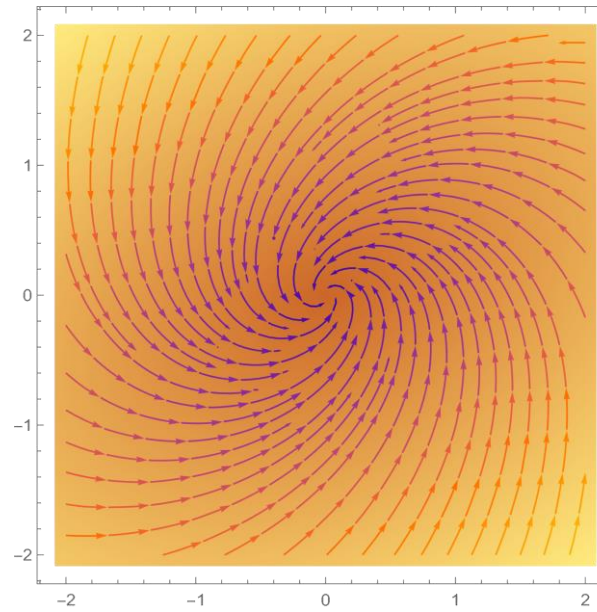


Рис. 3. Устойчивый фокус

Классифицируем точки S_1 и S_2 .

Рассмотрим точку $S_1 \left(u_2; \frac{bu_2}{\gamma} \right)$. Сделаем замену

$$\begin{cases} u = \xi + u_2 \\ v = \eta + \frac{bu_2}{\gamma} \end{cases}$$

Тогда

$$\begin{cases} \frac{d\xi}{dt} = (2u_2(a+1) - 3u_2^2 - a)\xi - \eta + (a+1 - 3u_2)\xi^2 - \xi^3 \\ \frac{d\eta}{dt} = b\xi - \gamma\eta \end{cases}$$

Здесь $A = \begin{pmatrix} 2u_2(a+1) - 3u_2^2 - a & -1 \\ b & -\gamma \end{pmatrix}$, а $g(t, u, v) = \begin{pmatrix} (a+1 - 3u_2)\xi^2 - \xi^3 \\ 0 \end{pmatrix}$.

Условие (5) выполнено, а $\det(A - \lambda E) = \lambda^2 - \sigma\lambda + \Delta$, где

$$\sigma = (2u_2(a+1) - 3u_2^2 - a) - \gamma = \text{Sp } A,$$

$$\Delta = -\gamma(2u_2(a+1) - 3u_2^2 - a) + b = \det A.$$

Тогда дискриминант характеристического уравнения

$$D = \sigma^2 - 4\Delta.$$

Далее, так как u_2 – решение системы (4), то

$$\gamma(u_2^2 - (a+1)u_2 + \left(a + \frac{b}{\gamma}\right)) = 0, \text{ поэтому}$$

$$\Delta = b + a\gamma + \gamma(3u_2^2 - 2u_2(a+1)) = 2u_2^2\gamma - (a+1)u_2\gamma =$$

$$= u_2\gamma(2u_2 - a - 1) = u_2\gamma\sqrt{(a-1)^2 - \frac{4b}{\gamma}} > 0 \text{ при } 0 < a < 1, \gamma > 0 \text{ и}$$

$$SpA = -\sigma = -(2u_2(a+1) - 3u_2^2 - a) + \gamma = \frac{\Delta-b}{\gamma} + \gamma = \frac{\Delta}{\gamma} + \left(\gamma - \frac{b}{\gamma}\right) > 0$$

при $b < \gamma^2$.

Таким образом, при этих условиях коэффициенты характеристического уравнения снова положительны. Значит при $D > 0$ S_1 – устойчивый узел, а при $D < 0$ S_1 – устойчивый фокус [3].

Для точки $S_2\left(u_3; \frac{bu_3}{\gamma}\right)$ рассматриваем аналогичную с S_1 замену

$$\begin{cases} u = \xi + u_3 \\ v = \eta + \frac{bu_3}{\gamma} \end{cases}$$

и для характеристического уравнения $\lambda^2 - \sigma\lambda + \Delta = 0$ подобным образом получаем $\sigma = (2u_3(a+1) - 3u_3^2 - a) - \gamma = SpA$,

$$\Delta = -\gamma(2u_3(a+1) - 3u_3^2 - a) + b = det A.$$

В силу тех же соображений,

$$\Delta = u_3\gamma(2u_3 - a - 1) = -u_3\gamma\sqrt{(a-1)^2 - \frac{4b}{\gamma}}.$$

Следовательно, при $\gamma > 0$, $0 < a < 1$ и $(a-1)^2 - \frac{4b}{\gamma} > 0$ имеем $\Delta < 0$.

В силу последнего неравенства, дискриминант $D = \sigma^2 - 4\Delta > 0$.

Таким образом, по классификации $S_2\left(u_3; \frac{bu_3}{\gamma}\right)$ – седло [3, с.98]

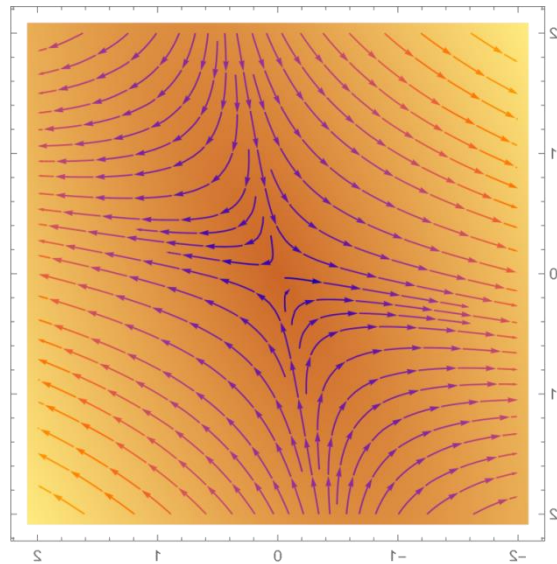


Рис. 4. Седло

Проверим для данной точки условие теоремы Пуанкаре [2]. Для этого обозначим

$$\begin{cases} P(u, v) = -u^3 + (a + 1)u^2 - au - v \\ Q(u, v) = bu - \gamma v \end{cases}$$

и найдём частные производные

$$\begin{cases} \frac{\partial P}{\partial u} = -3u^2 + 2(a + 1)u - a, \\ \frac{\partial Q}{\partial v} = -\gamma. \end{cases}$$

Выясним существование особых точек на изоклине $v = \frac{bu}{\gamma}$, т.е. решим систему

$$\begin{cases} -3u^2 + 2(a + 1)u - a = 0 \\ -\gamma = 0 \end{cases}.$$

Так как $\gamma > 0$, то второе уравнение системы неверно, т.е. система не имеет решений. Поэтому на исследуемой изоклине нет особых точек. Значит, в силу теоремы Пуанкаре, точка S_2 является простым седлом.

Таким образом, доказана

Теорема. Пусть в системе (2) при $J_a = 0$, $\gamma > 0$, $0 < a < 1$, $0 < b < \gamma^2$ и $(a - 1)^2 - \frac{4b}{\gamma} > 0$, тогда система (1) имеет в ограниченной части фазовой плоскости три простых состояния равновесия: точки $S_0(0; 0)$, $S_1(u_2; \frac{bu_2}{\gamma})$ – устойчивые узлы или фокусы, $S_2(u_3; \frac{bu_3}{\gamma})$ – седло.

Библиографический список

1. Hodgkin A.L. and Huxley A.F. A quantitative description of membrane current and its application to conduction and excitation in nerve. J.Physiol.117(4): 500-544, 1952.
2. Андронов А.А. Теория бифуркаций динамических систем на плоскости – М.: Наука, 1967. 488 с.
3. Петровский И.Г. Лекции по теории обыкновенных дифференциальных уравнений – М.: Изд-во МГУ, 1984. – 296 с.
4. Ушхо А. Д., Феклистов Г.С. Исследование дифференциальной модели ФитцХью-Нагумо // Вестник Адыгейского госуниверситета. Сер. Естественно-математические и технические науки. 2016. Вып. 4 (191). С. 60-67.

М.В. Беженар, В.В. Малышко **МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ** **ВОЗНИКНОВЕНИЯ ПУЗЫРЬКОВ ДЕНАТУРАЦИИ** **В МОЛЕКУЛЕ ДНК**

В статье рассматривается механическая модель, на основании которой

была исследована динамика молекулы ДНК. Данная модель учитывает такие эффекты как вязкость среды, внешнее периодическое воздействие и связывания ионов.

Ключевые слова: математическая модель, молекула ДНК, открытые состояния, пузырьки денатурации.

The article considers a mechanical model based on which the dynamics of the DNA molecule was investigated. This model considers such effects as the viscosity of the medium, external periodic exposure and ion binding.

Keywords: mathematical model, DNA molecule, open states, denaturation bubbles.

Молекула ДНК является основной структурой, передающей наследственную информацию во всех живых организмах, и понимание ее строения и функции имеет фундаментальное значение для биологии и медицины. Изучение трехмерных структур и динамики ДНК является ключом для понимания их биологических функций. Однако изучение ДНК на экспериментальном уровне является сложной задачей, поскольку на данный момент не существует инструментов, позволяющих достоверно изучить динамику молекулы [1]. В связи с этим, оправдано применение математических моделей и компьютерных методов [1, 2]. Различные модели ДНК могут учитывать вязкость среды, внешнее воздействие, гибкости и связывания ионов [3-6]. Благодаря чему исследователи могут изучать различные аспекты динамики ДНК, такие как ее суперскручивание, репликация, транскрипция и мутации, а также изучать влияние различных факторов на эти процессы.

В данной работе на основе механической модели ДНК [7], без упрощений и усреднения [3, 4] исследована динамика открытых состояний. В рамках модели молекула ДНК, представляет собой две цепочки дисков, которые связаны между собой поперечными пружинами. Данная система описывается следующими уравнениями Ньютона:

$$I_1^i \frac{d^2 \varphi_1^i(t)}{dt^2} = K_1^i [\varphi_1^{i-1}(t) - 2\varphi_1^i(t) + \varphi_1^{i+1}(t)] - \delta^i (k_{12}^i R_1^i (R_1^i + R_2^i) \sin \varphi_1^i + k_{12}^i R_1^i R_2^i \sin(\varphi_1^i - \varphi_2^i)) + F_1^i(t), \quad i = \overline{2, n-1}, \quad (1)$$

$$I_1^1 \frac{d^2 \varphi_1^1(t)}{dt^2} = K_1^1 [\varphi_1^2(t) - \varphi_1^1(t)] - \delta^1 (k_{12}^1 R_1^1 (R_1^1 + R_2^1) \sin \varphi_1^1 + k_{12}^1 R_1^1 R_2^1 \sin(\varphi_1^1 - \varphi_2^1)) + F_1^1(t), \quad (2)$$

$$I_1^n \frac{d^2 \varphi_1^n(t)}{dt^2} = K_1^n [\varphi_1^{n-1}(t) - \varphi_1^n(t)] - \delta^n (k_{12}^n R_1^n (R_1^n + R_2^n) \sin \varphi_1^n + k_{12}^n R_1^n R_2^n \sin(\varphi_1^n - \varphi_2^n)) + F_1^n(t), \quad (3)$$

$$I_2^i \frac{d^2 \varphi_2^i(t)}{dt^2} = K_2^i [\varphi_2^{i-1}(t) - 2\varphi_2^i(t) + \varphi_2^{i+1}(t)] +$$

$$+\delta^i(k_{12}^i R_2^i (R_1^i + R_2^i) \sin \varphi_2^i - k_{12}^i R_1^i R_2^i \sin(\varphi_2^i - \varphi_1^i)) + F_2^i(t), \quad i = \overline{2, n-1}, \quad (4)$$

$$I_2^1 \frac{d^2 \varphi_2^1(t)}{dt^2} = K_2^1 [\varphi_2^2(t) - \varphi_2^1(t)] + \quad (5)$$

$$+\delta^i(k_{12}^1 R_2^1 (R_1^1 + R_2^1) \sin \varphi_2^1 - k_{12}^1 R_1^1 R_2^1 \sin(\varphi_2^1 - \varphi_1^1)) + F_2^1(t),$$

$$I_2^n \frac{d^2 \varphi_2^n(t)}{dt^2} = K_2^n [\varphi_2^{n-1}(t) - \varphi_2^n(t)] + \quad (6)$$

$$+\delta^i(k_{12}^n R_2^n (R_1^n + R_2^n) \sin \varphi_2^n - k_{12}^n R_1^n R_2^n \sin(\varphi_2^n - \varphi_1^n)) + F_2^n(t).$$

где $\varphi_j^i(t)$ – угловое отклонение i -го азотистого основания j -й цепи, отсчитываемое против часовой стрелки в момент времени t ;

I_j^i – инерция вращения i -го азотистого основания j -й цепи;

R_j^i – расстояние от центра инерции i -го азотистого основания j -й цепи до сахарофосфатной цепи;

K_j^i – константа, характеризующая крутящий момент i -го сегмента j -й сахарофосфатной цепи;

k_{12}^i – константа, характеризующая упругие свойства связи i -й пары азотистых оснований оснований;

$F_j^i(t)$ – внешнее воздействие на i -е азотистое основание j -й цепи одновременно;

n – количество пар оснований азота в системе.

Предполагается, что величина внешнего воздействия равна $F_j^i(t) = -\beta_j^i \frac{d\varphi_j^i}{dt}(t) + F_0 \cos \omega t$, где член $-\beta_j^i \frac{d\varphi_j^i}{dt}(t)$ имитирует эффекты диссипации, вызванные взаимодействием со средой, окружающей молекулу ДНК, а член $F_0 \cos \omega t$ представляет собой внешний периодический эффект.

Ген IFNA17 был разделен на области, которые были почти равны друг другу (ген I, II, III части) по количеству нуклеотидов, после чего, с помощью выбранной модели, была показана возможность регуляторной роли некодирующей области IFNA17 в образовании пузырьков ДНК даже после однократной ^2H -замены в III части гена [8, 9].

Установлено, что одиночные замены $^2\text{H}/^1\text{H}$ в определенных азотистых основаниях могут быть механизмом поддержания жизнедеятельности гена интерферона альфа-17 человека (IFNA17) в критических условиях. В целом, разработанный метод математического моделирования обеспечивает глубокое понимание поведения ДНК в самом высоком диапазоне критических энергий водородных связей, что значительно расширяет научное понимание взаимодействия нуклеиновых оснований.

Кроме того, было обнаружено, что положительные значения частот появления пузырьков в IFNA17, во всех случаях и при условии, что все водородные связи в парах оснований равны ^1H , имеют обратную зависимость

от размера пузырьков ДНК во всем диапазоне энергий от $0,250 \times 10^{-22}$ Н·м до $0,500 \times 10^{-22}$ Н·м. Такой результат подтверждает критическую роль маленьких и метастабильных пузырьков денатурации в поддержании функциональных возможностей ДНК (во всем диапазоне энергий) инициировать экспрессию генов, во время которой требуется образование пузырьков большего размера.

Библиографический список

1. Pyne, A. L. B., Noy, A. Main Base-pair resolution analysis of the effect of supercoiling on DNA flexibility and major groove recognition by triplex-forming oligonucleotides // *Nature Communications*. – 2021. – Vol. 12, №1053. – URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7887228/> – Дата публикации 06.02.2021.

2. Mu, Z.C., Tan, Y.L., Liu, J. Computational Modeling of DNA 3D Structures: From Dynamics and Mechanics to Folding // *Molecules*. – 2023. – Vol. 28, №12. – URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10303651/> – Дата публикации 17.06.2023.

3. Обзор математических моделей, описывающих механические движения в молекуле ДНК / М.В. Беженар, А.А. Елкина, Х.Л. Эрнандес Касерес [и др.]. // *Биофизика*. – 2022. – Т. 67. – № 6. – С. 1068–1078. – DOI: 10.31857/S0006302922060035.

4. Svidlov, A.A., Drobotenko, M.I., Basov, A.A. Influence of Environmental Parameters on the Stability of the DNA Molecule // *Entropy*. – 2021. – Vol. 23, №11. – URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8622188/> – Дата публикации 31.10.2021.

5. Dzhimak, S.S., Svidlov, A.A., Elkina, A.A. Genesis of Open States Zones in a DNA Molecule Depends on the Localization and Value of the Torque // *Int. J. Mol. Sci.* – 2022. – Vol. 23, №8. – URL: <https://www.mdpi.com/1422-0067/23/8/4428> – Дата публикации 17.04.2022.

6. Svidlov, A.A., Drobotenko, M.I., Basov, A.A. DNA Dynamics under Periodic Force Effects // *Int. J. Mol. Sci.* – 2021. – Vol. 22, №15. – URL: <https://www.mdpi.com/1422-0067/22/15/7873> – Дата публикации 23.07.2021.

7. Yakushevich, L.V. *Nonlinear Physics of DNA* / L.V. Yakushevich. – Weinheim : Wiley-VCH Verlag GmbH & Co, 2004. – 220 p. – ISBN 9783527603701.

8. Basov, A.A., Drobotenko, M.I., Svidlov, A.A. Influence of Single Deuterium Replacement on Frequency of Hydrogen Bond Dissociation in IFNA17 under the Highest Critical Energy Range // *Int. J. Mol. Sci.* – 2022. – Vol. 23, №24. – URL: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9778762/> – Дата публикации 07.12.2022.

9. Basov, A.A., Dorohova, A.A., Malyshko, V.V. Influence of a Single Deuterium Substitution for Protium on the Frequency Generation of Different-

В.В. Василенко, А.С. Сергиенко

О НЕКОТОРЫХ СВОЙСТВАХ ПОДКАСАТЕЛЬНЫХ

В статье рассматривается ряд свойств подкасательной при локальном исследовании функции. Обозначенные особенности подкасательных могут быть полезны при исследовании свойств функций, а так же в реализации численных методов решения задач дифференциального исчисления.

Ключевые слова: дифференциал, производная, касательная, подкасательная, функция, нормаль.

The article discusses a number of properties of a subtangent in the lo-cal study of a function. The indicated features of subtangents can be useful in studying the properties of functions, as well as in implementing numerical methods for solving problems of differential calculus.

Keywords: differential, derivative, tangent, subtangent, function, normal

Дифференциальное и интегральное исчисления имеют давнюю историю становления – считается что они были созданы в 70-80-х годах XVII в. Хотя основные идеи анализа к тому времени уже были известны и разработаны, но до определенного момента они не были обличены в отвлеченную форму. По сути, они рассматривались в неразрывной связи с геометрическими и механическими задачами, хотя общность операций отчётливо осознавалась.

Так, задачи спрямления кривой, нахождения центра тяжести тела, восстановления пути, фактически сводились к задачам квадратур (например – определением площади, порожденной движением ординаты кривой), а для квадратур были рекомендованы методы, схожие с методами интегрального исчисления. Исторически такие методы развивались в достаточно узком классе задач, что с работами Ньютона и Лейбница было дополнено рядом вычислительных приемов, покрывших недостатки техники решения проблем.

Понятие производной функции также выступало в геометрической и механической формах: отыскивали скорости по заданному закону движения, находили подкасательную кривой, заданной в декартовой системе координат. Именно подкасательные рассматривались во многих задачах как инструмент дифференциального исчисления, позволяющий исследовать решения задач без явного применения производной, что в некоторых случаях «выручало» упрощением ряда вычислительных процедур.

Рассмотрим классическое определение подкасательной.

Для однозначной, дифференцируемой в области функции

$$y = f(x), \quad x \in [a, b] = D, \quad x_0 \in D$$

определим подкасательную P_{x_0} к графику функции в точке $x_0 \in D$ как проекцию касательной на ось абсцисс, что аналитически может быть представлено формулой:

$$P_{x_0} = -\frac{f(x_0)}{f'(x_0)}.$$

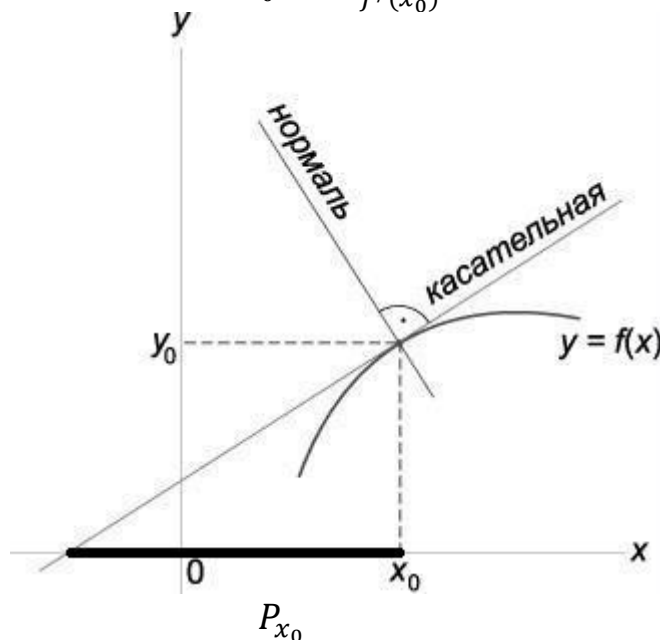


Рис. 1. Локальная подкасательная P_{x_0}

Отметим некоторые очевидные свойства подкасательной:

1. Зная длину подкасательной, можно построить касательную.
2. Отношение ординаты к подкасательной – есть производная ординаты относительно абсциссы. Заметим, что такое свойство подкасательной в данном случае рассматривается исключительно в геометрическом смысле. Действительно, в таком случае не принципиально – рассматривается ли функция $\frac{dy}{dx}$ или функция $y \frac{dx}{dy}$, дающая длину касательной.
3. Если $|P_{x_0}| \rightarrow 0$ – функция $y = f(x_0) \rightarrow \infty$, а значит подкасательная в пределе является в таком случае особой точкой при интегрировании.
4. Если $\sum_{i=1}^{\infty} |P_{x_i}| \rightarrow 0$, то функция $y = f(x)$, $x \in D, \forall x_i \in D, (i = 1, 2, \dots)$ монотонна и неограниченно растет по абсолютной величине.
5. Множество всех подкасательных на интервале монотонности функции $y = f(x)$, $x \in D$ – есть линейное подпространство, содержащееся в D .

Доказательства приведенных свойств очевидны, потому авторы их оставят без особого внимания. В основном свойства 1-4 вытекают из самого определения подкасательной и геометрического смысла производной функции в точке и на интервале.

Как отражено выше, подкасательная может быть полезна в случае невырожденной гладкой кривой, отражая природу самой гладкой линии через проекцию касательной к графику.

Учитывая свойство 5, можно утверждать, что такой подход к исследованию локально (на интервале) гладких кривых может быть полезен как альтернатива для определения, к примеру, особенностей фазовых портретов динамических систем, исследования фазовых траекторий на наличие поворотных точек (как, к примеру в [1]).

Можно справедливо заметить, что аналогичными свойствами так же обладают и поднормали [2], с поправкой лишь, на наличие противоположного направления, если в постановке задачи важен фактор порядка следования.

Библиографический список

1. Неймарк Ю.И. Математические модели в естествознании и технике: Учебник. Н.Новгород: Изд. Нижегородского госуниверситета им Н.И. Лобачевского, 2004. 401 с.

2. Пискунов Н. С. Дифференциальное и интегральное исчисления для втузов, т.1: Учебное пособие для втузов.— 13-е изд.— М.: Наука. Главная редакция физико-математической литературы, 1985. — 432 с.

О.М. Лясота, С.С. Джимак, М.И. Дроботенко МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДИНАМИКИ ВОЗНИКНОВЕНИЯ ОТКРЫТЫХ СОСТОЯНИЙ В ОБЛАСТИ CAG-ПОВТОРОВ ГЕНА ATXN2

В данной работе исследована динамика возникновения открытых состояний в области CAG-повторов гена ATXN2 под влиянием торсионного момента с различной пространственной и временной локализацией. Изучение механических свойств ДНК является важной областью исследований, так как они играют существенную роль в различных процессах, связанных с физическим взаимодействием и функционированием ДНК. Это позволяет исследовать и предсказывать механические свойства ДНК в различных условиях и принимать во внимание их влияние на биологические процессы.

Ключевые слова: динамика ДНК, ген ATXN2, математическая модель, открытые состояния.

In this work, we investigated the dynamics of the emergence of open states in the region of CAG repeats of the ATXN2 gene under the influence of a torsion moment with different spatial and temporal localization. The study of the mechanical properties of DNA is an important area of research, as they play an essential

role in various processes associated with the physical interaction and functioning of DNA. This makes it possible to study and predict the mechanical properties of DNA under various conditions and take into account their influence on biological processes.

Key words: DNA dynamics, ATXN2 gene, mathematical model, open states.

Наследственные атаксии обусловлены мутациями в генах, которые управляют функцией нервной системы. Группа заболеваний, известных как наследственные атаксии, возникает из-за патологического расширения три-нуклеотидного CAG-повтора в кодирующей области гена ATXN2. Последовательность три-нуклеотидного повтора CAG в кодирующей области гена ATXN2 обычно повторяется у нормальных людей от 14 до 31 раз, тогда как патологические аллели содержат более 35 CAG-повторов [1]. Увеличение длины повторов CAG-мутаций может вызывать различные патологии [2; 3]. Например, спиноцеребеллярная атаксия 2 типа (SCA2) - прогрессирующее нейродегенеративное заболевание с аутосомно-доминантным наследованием. Клинически прогрессирующая мозжечковая атаксия является основным симптомом. Кроме того, она часто сопровождается синдромом Паркинсона, дистонией и т. д., что серьезно влияет на нормальную сенсорную и двигательную активность.

Нами было проведено исследование возникновения аномальных зон открытых состояний (ОС) в области CAG-повторов гена ATXN2 с помощью математического моделирования ДНК.

Математическая модель угловых движений азотистых оснований опирается на аналогию между молекулой ДНК и механической системой, состоящей из двух цепочек взаимосвязанных маятников. При этом вращающимся маятникам соответствуют азотистые основания, а упругой нити, к которой прикреплены эти маятники, -- сахаро-фосфатные цепочки молекулы ДНК; водородной связи пары комплементарных азотистых оснований соответствует упругая связь соответствующей пары маятников [4; 5].

Таким образом, математическая модель угловых движений включает следующие уравнения Ньютона:

$$I_1^i \frac{d^2 \varphi_1^i(t)}{dt^2} = K_1^i [\varphi_1^{i-1}(t) - 2\varphi_1^i(t) + \varphi_1^{i+1}(t)] - \delta^i (k_{12}^i R_1^i (R_1^i + R_2^i) \sin \varphi_1^i + k_{12}^i R_1^i R_2^i \sin(\varphi_1^i - \varphi_2^i)) + F_1^i(t), i = \overline{2, n-1}, \quad (1)$$

$$I_1^1 \frac{d^2 \varphi_1^1(t)}{dt^2} = K_1^1 [\varphi_1^2(t) - \varphi_1^1(t)] - \delta^1 (k_{12}^1 R_1^1 (R_1^1 + R_2^1) \sin \varphi_1^1 + k_{12}^1 R_1^1 R_2^1 \sin(\varphi_1^1 - \varphi_2^1)) + F_1^1(t), \quad (2)$$

$$I_1^n \frac{d^2 \varphi_1^n(t)}{dt^2} = K_1^n [\varphi_1^{n-1}(t) - \varphi_1^n(t)] - \delta^i (k_{12}^n R_1^n (R_1^n + R_2^n) \sin \varphi_1^n + k_{12}^n R_1^n R_2^n \sin(\varphi_1^n - \varphi_2^n)) + F_1^n(t), \quad (3)$$

$$I_2^i \frac{d^2 \varphi_2^i(t)}{dt^2} = K_2^i [\varphi_2^{i-1}(t) - 2\varphi_2^i(t) + \varphi_2^{i+1}(t)] + \delta^i (k_{12}^i R_2^i (R_1^i + R_2^i) \sin \varphi_2^i - k_{12}^i R_1^i R_2^i \sin(\varphi_2^i - \varphi_1^i)) + F_2^i(t), \quad (4)$$

$i = \overline{2, n-1}$,

$$I_2^1 \frac{d^2 \varphi_2^1(t)}{dt^2} = K_2^1 [\varphi_2^2(t) - \varphi_2^1(t)] + \delta^i (k_{12}^1 R_2^1 (R_1^1 + R_2^1) \sin \varphi_2^1 - k_{12}^1 R_1^1 R_2^1 \sin(\varphi_2^1 - \varphi_1^1)) + F_2^1(t), \quad (5)$$

$$I_2^n \frac{d^2 \varphi_2^n(t)}{dt^2} = K_2^n [\varphi_2^{n-1}(t) - \varphi_2^n(t)] + \delta^i (k_{12}^n R_2^n (R_1^n + R_2^n) \sin \varphi_2^n - k_{12}^n R_1^n R_2^n \sin(\varphi_2^n - \varphi_1^n)) + F_2^n(t). \quad (6)$$

Здесь:

$\varphi_j^i(t)$ – угловое отклонение i -го маятника j -й цепочки, отсчитываемое против часовой стрелки, в момент времени t ;

I_j^i – момент инерции i -го маятника j -й цепочки;

R_j^i – расстояние от центра масс i -го маятника j -й цепочки до нити;

K_j^i – константа, характеризующая крутящий момент i -го участка j -й нити;

k_{12}^i – константа, характеризующая упругие свойства связи i -й пары маятников;

$F_j^i(t)$ – внешнее силовое воздействие на i -й маятник j -й цепочки в момент времени t ,

n – количество пар маятников в рассматриваемой системе.

В уравнениях (1)-(2) первое слагаемое справа от знака равенства описывает силовое воздействие на i -й маятник со стороны упругой нити, второе слагаемое – со стороны парного маятника, третье слагаемое – внешнее силовое воздействие. Величина внешнего воздействия принимается равной $F_j^i(t) = -\beta_j^i \frac{d\varphi_j^i}{dt}(t) + M^i(t)$, где слагаемое $-\beta_j^i \frac{d\varphi_j^i}{dt}(t)$ моделирует эффекты диссипации, обусловленные взаимодействием с окружающей молекулу ДНК жидкостью, слагаемое $M^i(t)$ – торсионный момент [6].

Уравнения (1)-(6) позволяют моделировать водородную связь в i -й паре ($\delta^i = 1$) и разрыв этой связи ($\delta^i = 0$). Будем считать, что в i -й паре оснований возникает разрыв, если потенциальная энергия связи в этой паре превышает некоторое критическое значение E_{AT} для пары AT и E_{GC} для пары GC; связь восстанавливается, если ее потенциальная энергия становится меньше критического значения.

К уравнениям (1)-(6) добавим начальные условия:

$$\varphi_1^i(0) = \varphi_{1,0}^i, \frac{d\varphi_1^i}{dt}(0) = \varphi_{1,1}^i, \quad (7)$$

$$\varphi_2^i(0) = \varphi_{2,0}^i, \frac{d\varphi_2^i}{dt}(0) = \varphi_{2,1}^i, i = \overline{1, n}. \quad (8)$$

Начальные условия (7)-(8) задавали невозмущенное состояние, т.е.

$$\varphi_{1,0}^i = \varphi_{1,1}^i = \varphi_{2,1}^i = 0, \varphi_{2,0}^i = \pi, i = \overline{1, n},$$

Торсионное воздействие $M^i(t)$ выбиралось постоянным во времени и пространственно локализованным на отрезке $[i_1, i_2]$, т.е.

$$M^i(t) = M_0^i, i = \overline{1, n},$$

причем, $M_0^i = M_0$ при $1 \leq i_1 \leq i \leq i_2 \leq n$ и $M_0^i = 0$ для остальных значений i .

На основе численного решения задачи (1)-(8) с помощью оригинальной программы, написанной авторами статьи [7] был исследован процесс образования и динамика зон ОС в молекуле ДНК. Расчеты показывают, что значимые ОС образуются при $t \leq 10^{-10}$ с, поэтому численное моделирование проводилось на временном отрезке $[0, 10^{-10}$ с]. Установлено, что возникновение зон ОС в промоторной области происходит при значении торсионного момента $M_0 = 8.28$ пН · нм. При $M_0 > 8.28$ пН · нм в области CAG-повторов могут возникать дополнительные зоны ОС.

Согласно полученным результатам, вероятность образования зон ОС зависит от содержания пар А - Т на участке локализации торсионного момента, от размера этого участка и от величины промежутка временной локализации. Важно отметить, что при пространственной локализации торсионного момента вблизи концов молекулы возрастает вероятность возникновения зон ОС. Кроме того, зоны ОС могут снова закрываться при прекращении торсионного воздействия.

Нами показано, что торсионное воздействие на участок гена ATXN2, кроме образования ОС в промоторной области может приводить к образованию дополнительных зон ОС различного размера в области CAG-повторов. Установлено, что частота возникновения дополнительных зон большого размера увеличивается с увеличением количества CAG-повторов.

Работа выполнена при финансовой поддержке государственного задания ЮНЦ РАН № 122020100351-9.

Библиографический список

1. Mutesa L., Pierquin G., Segers K., et al. Spinocerebellar ataxia type 2 (SCA2): Clinical features and genetic analysis // Journal of Tropical Pediatrics. 2008. V. 54. № 5. P. 350–352. <https://doi.org/10.1093/tropej/fmn034>.

2. Hu T., Morten M.J., Magennis S.W. Conformational and migrational dynamics of slipped-strand DNA three-way junctions containing trinucleotide repeats // Nature Communications. 2021. V. 12. P. 204. <https://doi.org/10.1038/s41467-020-20426-3>.

3. Pan F., Zhang Y., Xu P., et al. Molecular conformations and dynamics of nucleotide repeats associated with neurodegenerative diseases: double helices and CAG hairpin loops // Computational and Structural Biotechnology Journal. 2021. V. 19. P. 2819-2832. <https://doi.org/10.1016/j.csbj.2021.04.037>.

4. Svidlov A., Drobotenko M., Basov A., et al. DNA dynamics under periodic force effects // International Journal of Molecular Sciences. 2021. V. 22. № 15. P. 7873. <https://doi.org/10.3390/ijms22157873>.

5. Svidlov A., Drobotenko M., Basov A., et al. Influence of environmental parameters on the stability of the DNA molecule // Entropy. 2021. V. 23. № 11. P. 1446. <https://doi.org/10.3390/e23111446>.

6. Dzhimak S., Svidlov A., Elkina A., et al. Genesis of Open States Zones in a DNA Molecule Depends on the Localization and Value of the Torque // International Journal of Molecular Sciences. 2022. V. 23. № 8. P. 4428. <https://doi.org/10.3390/ijms23084428>.

7. Дроботенко М.И., Свидлов А.А., Барышев М.Г., Джимаков С.С. Расчет вращательных движений в двухцепочечной молекуле ДНК // Свидетельство о регистрации программы для ЭВМ RU 2017660682, 22.09.2017. Заявка № 2017617542, 31.07.2017.

**Д.А. Сверкунова, О.В. Дорошенко, М.В. Голуб,
А.Д. Ханазарян, А. Н. Шпак**

АЛГОРИТМ ПОСТРОЕНИЯ МЕТАМОДЕЛИ ДЛЯ ПОВЫШЕНИЯ ТОЧНОСТИ ПРЕДСКАЗАНИЯ ЭКСПЕРИМЕНТАЛЬНО ИЗМЕРЯЕМОГО ОТКЛИКА СЕНСОРА НА ПЛАСТИНЕ С ВЫЕМКОЙ

В работе представляется алгоритм построения метамодели для повышения точности предсказания экспериментально измеряемого отклика сенсора на пластине с выемкой. Для этого были произведены измерения экспериментально полученных сигналов и использовалась двумерная конечно-элементная математическая модель для пластины с выемкой для центральных частот в диапазоне от 20 до 220 кГц. Метамоделю строят путем аппроксимации разности между спектрами сигналов с помощью сплайнов и добавления к рассчитанному сигналу.

Ключевые слова: эксперимент, математическое моделирование, метамоделю, бегущие волны.

Thy paper presents an algorithm of metamodel construction to improve the prediction accuracy of the experimentally measured sensor response in an elastic plate with a notch. For this purpose, signals experimentally acquired and calculated using the two-dimensional finite element mathematical model have been used for central frequencies in the range from 20 to 220 kHz. The metamodel is constructed by approximating the difference between the signal spectra, after which the error function is interpolated using splines added to the calculated spectrum.

Key words: Experiment, mathematical modeling, meta-model, guided waves.

Несмотря на значительные успехи последних десятилетий в самых разных областях, своевременное обнаружение и локализация повреждений внутри объектов до их выхода из строя остается все столь же актуальным. Существует множество методов, основанных на различных физических принципах, среди которых использование бегущих волн, модальных свойств, применение акустической эмиссии и т.д. Целью научного исследования является обнаружение и локализация повреждений с помощью бегущих волн [1].

В рамках онлайн-опроса [2], проведённого среди более чем 450 немецких и европейских ученых, инженеров и специалистов, работающих в области неразрушающего контроля (НК), был задан вопрос о том, какие типы конструкций и виды повреждений наиболее интересны и важны для промышленного применения SHM-систем. Результаты показывают, что развитие методов мониторинга изотропных металлических компонент, таких как металлические пластины или оболочки, а также трубопроводы, по-прежнему, представляет наибольший интерес, см. рисунок 1. Наиболее опасными дефектами, требующими наискорейшего обнаружения, как видно из рисунка 2, специалистам видятся трещины разных типов, дефекты в сварных соединениях и коррозия металлических конструкций.

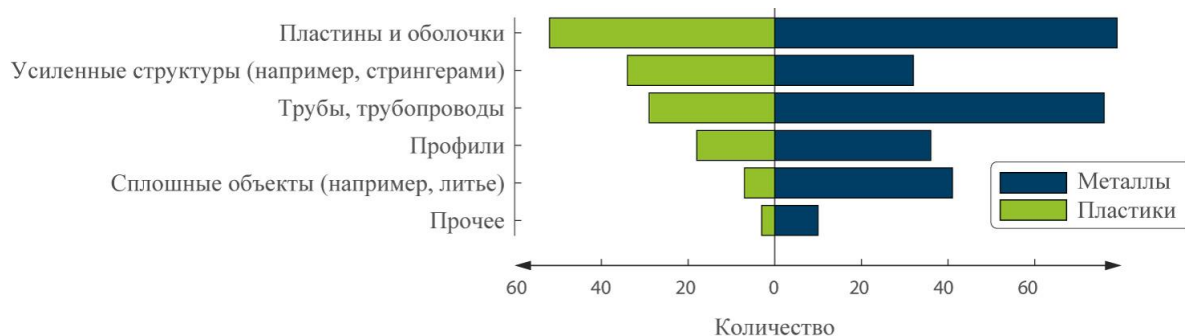


Рис. 1. Типы конструкций

В работе предполагается использовать метамоделю для настройки математической и компьютерной модели с целью наилучшего совпадения с

экспериментальными данными. Поскольку используется двухмерная модель и могут существовать объективные физические различия в изготовленных образцах, то ожидаются некоторые различия во временных рядах экспериментальных и численных данных.

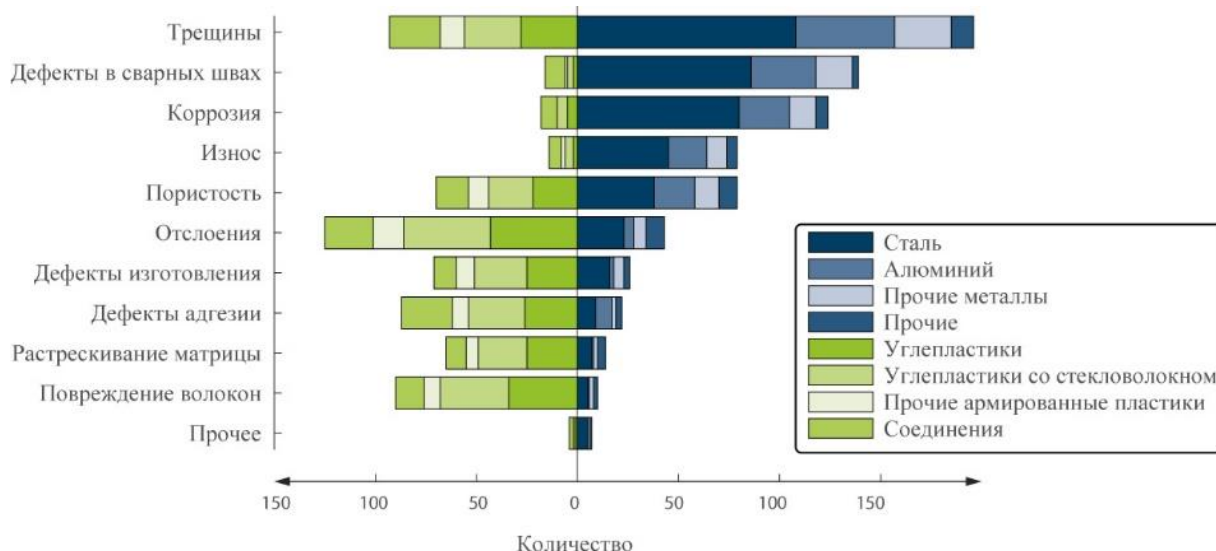


Рис. 2. Виды повреждений

Соответственно, необходимо разработать алгоритм, корректирующий выходные данные физической модели на основе ограниченного числа данных, предоставленных как физической моделью, так и экспериментальными измерениями. При этом предполагается использовать экспериментальные данные только для неповрежденной / поврежденной пластины и применять построенную метамодель для корректировки данных, сгенерированных физической моделью для неповрежденной / поврежденного состояния. Общая схема работы метамодели изображена на рисунке 3.



Рис. 3. Алгоритм построения метамодели

Имеются экспериментальные данные: $u_{exp}^{und}(f_c, t)$ и $u_{exp}^{dam}(f_c, t)$ – рисунок 4 в) - г) соответственно, измеренные на заданных центральных частотах в диапазоне $f_c = [20:2.5:220]$ кГц для неповрежденной и поврежденной пластин соответственно. Моделируемые сигналы обозначаются соответственно, $u_{sim}^{und}(f_c, t)$ и $u_{sim}^{dam}(f_c, t)$ – рисунок 4 а) - в) соответственно.

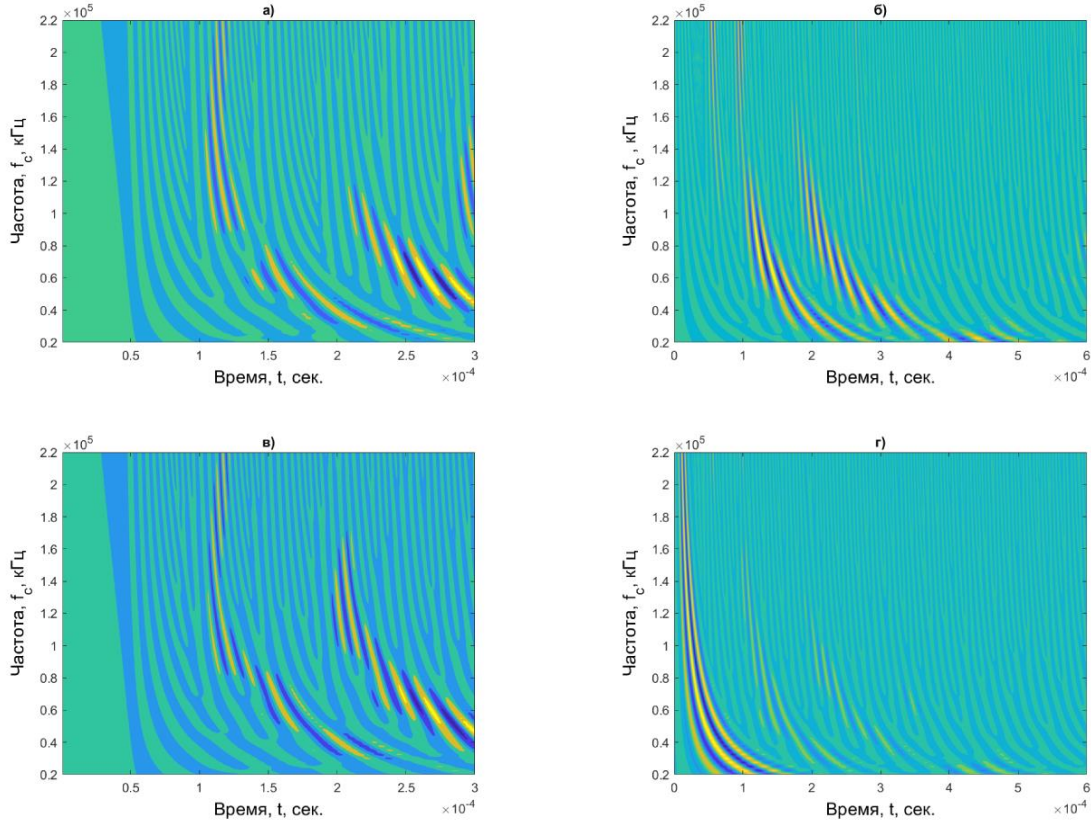


Рис. 4. Экспериментальные и моделируемые данные

Реализация алгоритма построения метамоделли:

1) Применяем преобразование Фурье \mathcal{F} к экспериментальным и моделируемым данным ($i = und, dam, m = exp, sim$):

$$U_m^i(f_c, \omega) = \mathcal{F}[u_m^i(f_c, t)],$$

2) Применяем преобразование Фурье к импульсу $p(f_c, t)$:

$$P(f_c, \omega) = \mathcal{F}[p(f_c, t)].$$

3) Определяем матрицу ошибок ($j = 1, 2$):

$$\varepsilon_j(f_c, \omega) = \frac{U_{exp}^i(f_c, \omega) - U_{sim}^i(f_c, \omega)}{P(f_c, \omega)}.$$

4) Применяем преобразования Ψ для получения $\hat{U}_{sim}^{und}(f_0, \omega)$ и $\hat{U}_{sim}^{dam}(f_0, \omega)$ соответственно:

$$\Psi_j(f_0, U_{sim}^i(f_0, \omega)) = U_{sim}^i(f_0, \omega) + \sigma_1(f_0, \omega) \cdot P(f_0, \omega),$$

$$\sigma_j(f_0, \omega) = Interpolation[\varepsilon_j(f_0, \omega)],$$

$$\hat{U}_{sim}^i(f_0, \omega) = \Psi_1[U_{sim}^i(f_0, \omega)].$$

5) Применяем обратное преобразование Фурье, чтобы получить $\hat{u}_{sim}^{und}(f_0, t)$ и $\hat{u}_{sim}^{dam}(f_0, t)$ соответственно:

$$\hat{u}_{sim}^i(f_0, t) = \mathcal{F}^{-1}[\hat{U}_{sim}^i(f_0, \omega)].$$

Для тестирования алгоритма было построено решение $\hat{u}_{sim}^{und}(f_c, t)$ на основе неповрежденных данных $u_{exp}^{und}(f_c, t)$ и $u_{sim}^{und}(f_c, t)$. Результаты применения метамоделей для корректировки математической модели для адекватного описания экспериментальных сигналов представлены на рисунке 5.

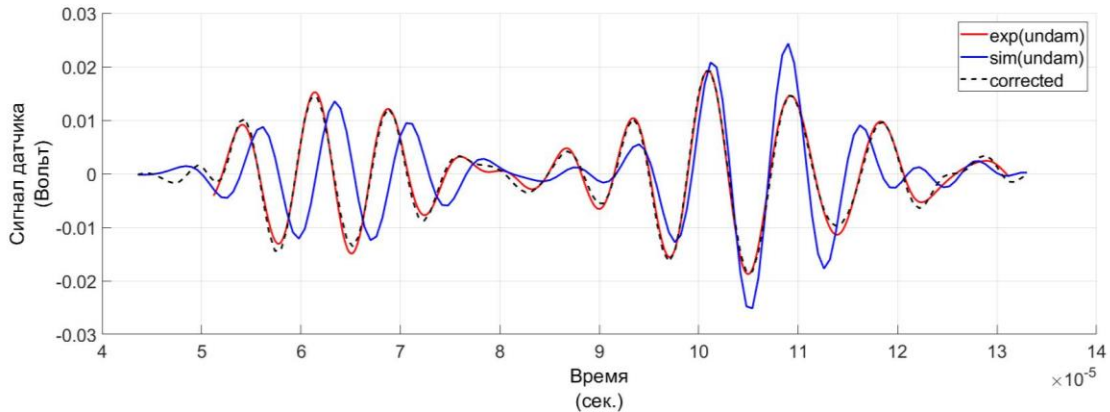


Рис. 5. Скорректированный сигнал $\hat{u}_{sim}^{und}(f_0, t)$ для центральной частоты $f_c = 130$ кГц

Кроме того, было построено решение $\hat{u}_{sim}^{dam}(f_0, t)$ на основе данных для поврежденных пластик $u_{exp}^{dam}(f_c, t)$ и $u_{sim}^{dam}(f_c, t)$. Соответствующие графики для сигналов представлены на рисунке 6. Можно видеть, что метамоделей справляется с задачей коррекции модели и позволяет получать качественную аппроксимацию экспериментальных данных в двумерном случае.

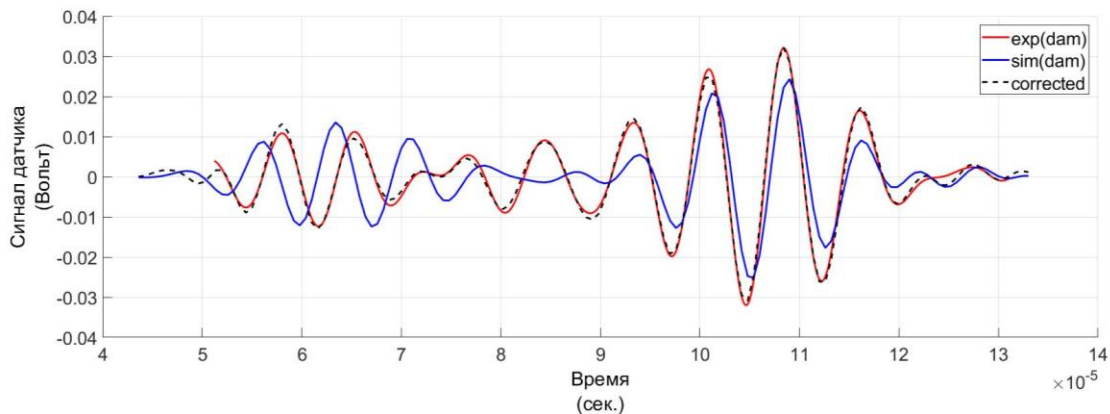


Рис. 6. Скорректированный сигнал $\hat{u}_{sim}^{dam}(f_0, t)$ для центральной частоты $f_c = 130$ кГц

Для уменьшения вычислительных затрат при моделировании ламинатов с дефектами типа трещин, отслоений, сварных швов и можно также использовать полуаналитические гибридные подходы, позволяющие моделировать протяженные слоистые волноводы [3-5].

Работа выполнена при поддержке гранта РФФИ № 22-11-00261.

Библиографический список

1. SHM using Guided Waves-Recent Activities and Advances in Germany / I. Mueller, J. Moll, K. Tschöke [et al.] // Structural health monitoring-an International journal. – 2019.
2. Feasibility of model-assisted probability of detection principles for structural health monitoring systems based on guided waves for fibre-reinforced Composites / K. Tschöke, I. Mueller, V. Memmolo [et al.] // IEEE Transactions on ultrasonics, ferroelectrics, and frequency control. – 2021. – Vol. 68. – P. 3156-3173.
3. Semi-analytical hybrid approach for modelling smart structures and guided wave-based SHM systems for a laminate with multiple delaminations and surface-mounted inhomogeneities / M.V. Golub, S.I. Fomenko, A.N. Shpak [et al.] // Applied mathematical modelling. – 2023. – Vol. 120. – P. 812-832.
4. Multi-layered and homogenized models for in-plane guided wave excitation, sensing, and scattering in anisotropic laminated composites / A.A. Eremin, M.V. Golub, S.I. Fomenko [et al.] // Applied Sciences. – 2023. – Vol. 13, № 3. – 1698 p.
5. Глушков, Е.В. Гибридная численно-аналитическая схема для расчета дифракции упругих волн в локально неоднородных волноводах / Е.В. Глушков, Н.В. Глушкова, А.А. Евдокимов // Акустический журнал. – 2018. – Т. 64, №1. – С. 3-12.

Г.Н. Титов, Т.В. Зинченко, Д.Р. Скибицкий ОБ ОДНОМ АЛГОРИТМЕ НАХОЖДЕНИЯ ЧИСЛА ФРОБЕНИУСА ТРОЙКИ НАТУРАЛЬНЫХ ЧИСЕЛ

Вопрос нахождения чисел Фробениуса тесно связан с известными вопросами дискретной математики. В настоящее время формула числа Фробениуса известна лишь для двух взаимно простых натуральных чисел. В работе приводится с компьютерной реализацией алгоритмическая формула для вычисления числа Фробениуса тройки взаимно простых натуральных чисел. Эта формула иллюстрирует алгоритм, основанный на полученном в

работе критерии неразрешимости линейных диофантовых уравнений с тремя неизвестными во множестве целых неотрицательных чисел.

Ключевые слова: взаимно простые натуральные числа, линейное диофантово уравнение, число Фробениуса, алгоритм, алгоритмическая формула.

The problem of finding the Frobenius numbers is closely related to well-known problems of discrete mathematics. At the present time the formula for calculating Frobenius number is known only for two positive coprime integers. The paper proves the algorithmic formula for calculating Frobenius number for three positive relatively prime integers using a computer implementation. This formula illustrates the algorithm, which based on the criterion for the unsolvability of linear Diophantine equations with three arguments in a set non-negative integers obtained in this article.

Keywords: positive relatively prime integers, linear Diophantine equation, Frobenius number, algorithm, algorithmic formula.

Вопросам нахождения чисел Фробениуса наборов взаимно простых натуральных чисел посвящено много научных работ. Актуальность этой тематики обусловлена тем, что она связана с некоторыми вопросами теории графов, а также с хорошо известными задачами о рюкзаке и о размене. Пусть a_1, \dots, a_n – взаимно простые натуральные числа ($n \in \mathbb{N}$) и f – наибольшее возможное целое число, для которого уравнение $a_1x_1 + \dots + a_nx_n = f$ не имеет решений во множестве целых неотрицательных чисел. Такое число f существует для любого указанного набора натуральных чисел a_1, \dots, a_n , его называют числом Фробениуса этого набора и обозначают в соответствии с [1] $frob(a_1, \dots, a_n)$. При $n = 2$ известна формула Сильвестра Д. Д. (1884 г.) $frob(a_1, a_2) = a_1 a_2 - a_1 - a_2$. Другие неалгоритмические формулы для вычисления чисел Фробениуса при $n \geq 3$ в настоящее время не известны. Поэтому рассмотрение даже случая при $n = 3$ до сих пор представляет определённый научный интерес (см., например, [1] (2022 г.) или [2] (2014 г.)). Алгоритмические решения проблемы Фробениуса в случае $n = 3$ получены и в более ранние годы. Известны классические алгоритмы Селмера-Бейера, Редсета и Дэвидсона, с которыми можно ознакомиться, например, в [3] (2005 г.). В этой работе строится новый алгоритм для случая $n = 3$, основанный на ниже доказанной теореме 1, а также получена соответствующая алгоритмическая формула, приведённая в теореме 2. Компьютерная иллюстрация полученной алгоритмической формулы реализована на языке Pascal ABC.NET.

Переходим к изложению результатов работы. Отметим, что в статье используются стандартные понятия и обозначения, которые могут быть найдены, например, в источниках [1 – 4]. Для ясности изложения материала, обсудим некоторые обозначения.

Множества целых чисел, натуральных чисел, неотрицательных целых чисел и натуральных больших единицы чисел обозначаем соответственно \mathbb{Z} , \mathbb{N} , $\mathbb{N} - 1$ и $\mathbb{N} + 1$. Если при $z, q, r \in \mathbb{Z}$ и $m \in \mathbb{N}$ имеем $z = mq + r$ и $0 \leq r < m$, то есть r и q – остаток и частное при делении z на m , то обозначают $r = z \bmod m$ и $q = \left[\frac{z}{m} \right]$ (обозначение $\left[\frac{z}{m} \right]$ соответствует общепринятому обозначению целой части числа $\frac{z}{m}$). Если $u, v \in \mathbb{Z}$ и $u \bmod m = v \bmod m$, то пишут $u \equiv v \pmod{m}$. Наибольший общий делитель чисел $a_1, \dots, a_n \in \mathbb{N}$ обозначают (a_1, \dots, a_n) , а при $(a_1, \dots, a_n) = 1$ эти числа называют взаимно простыми. Введём ещё удобные обозначения: если $u, v \in \mathbb{N}$ и $(u, v) = 1$, то через $\frac{1}{u} \bmod v$ обозначаем число из множества $\{0; \dots; v - 1\}$, для которого $u \cdot \left(\frac{1}{u} \bmod v\right) \equiv 1 \pmod{v}$, а также при $z \in \mathbb{Z}$ договариваемся вместо $\left(z \cdot \left(\frac{1}{u} \bmod v\right)\right) \bmod v$ писать $\frac{z}{u} \bmod v$.

Теперь может быть сформулирована

Теорема 1. Линейное диофантово уравнение вида $px + qy + rz = f$, где $p, q, r \in \mathbb{N}$ и $f \in \mathbb{N} - 1$, не имеет решения во множестве $\mathbb{N} - 1$ (то есть любая тройка чисел $x, y, z \in \mathbb{N} - 1$ не обращает его в истинное равенство) тогда и только тогда, когда для всех чисел $j \in \{0; \dots; \left[\frac{f}{r} \right]\}$ выполняется неравенство

$$\left[\frac{f-jr}{q} \right] < \frac{f-jr}{q} \bmod p. \quad (*)$$

Для доказательства теоремы нам понадобятся леммы 1 и 2.

Лемма 1. Пусть $p, q \in \mathbb{N} + 1$; $(p, q) = 1$ и $h \in \mathbb{N}$. Во множестве $\mathbb{N} - 1$ найдутся числа x и y , удовлетворяющие равенству $px + qy = h$, тогда и только тогда, когда выполняется неравенство $\frac{h}{q} \bmod p \leq \left[\frac{h}{q} \right]$.

Доказательство. Так как $(p, q) = 1$, то существуют $u, v \in \mathbb{Z}$ такие, что $pu + qv = 1$. Положим $v_0 = v \bmod p$ и $u_0 = \frac{1-qv_0}{p}$. Ясно, что $v_0, u_0 \in \mathbb{Z}$ и выполняется равенство $pu_0 + qv_0 = 1$. Более того, можно заметить, что $u_0 < 0$, а также $v_0 \in \{0; \dots; p - 1\}$ и $qv_0 \equiv 1 \bmod p$, то есть согласно принятому обозначению имеем $v_0 = \frac{1}{q} \bmod p$. Далее, общее решение диофантова уравнения $px + qy = h$ в целых числах будет иметь вид: $x = u_0h + qt$ и $y = v_0h - pt$, где $t \in \mathbb{Z}$. Из условий $x, y \geq 0$ получаем $u_0h + qt \geq 0$ и $v_0h - pt \geq 0$, то есть $-u_0h/q \leq t \leq v_0h/p$. Таким образом, разрешимость нашего диофантова уравнения в $\mathbb{N} - 1$ равносильна существованию целого числа t , принадлежащего отрезку $\left[-\frac{u_0h}{q}; \frac{v_0h}{p} \right]$. Последнее условие равносильно каждому из неравенств: $-\frac{u_0h}{q} \leq \left[\frac{v_0h}{p} \right], \quad -\frac{u_0h}{q} \leq \frac{v_0h - ((v_0h) \bmod p)}{p},$

$q((v_0h) \bmod p) \leq (pu_0 + qv_0)h$, а значит, $(v_0h) \bmod p \leq \frac{h}{q}$. Так как $(v_0h) \bmod p = \left(h \cdot \left(\frac{1}{q} \bmod p\right)\right) \bmod p = \frac{h}{q} \bmod p$, то приходим к условию $\frac{h}{q} \bmod p \leq \frac{h}{q}$, которое в силу $\frac{h}{q} \bmod p \in \mathbb{Z}$ равносильно условию $\frac{h}{q} \bmod p \leq \left\lfloor \frac{h}{q} \right\rfloor$. Лемма 1 доказана.

Лемма 2. Пусть $p, q, r \in \mathbb{N} + 1$; $(p, q) = 1$ и $f \in \mathbb{N}$. Во множестве $\mathbb{N} - 1$ найдутся числа x, y и z , удовлетворяющие равенству $px + qy + rz = f$, тогда и только тогда, когда для некоторого $j \in \{0; \dots; \left\lfloor \frac{f}{r} \right\rfloor\}$ выполняется неравенство $\frac{f-jr}{q} \bmod p \leq \left\lfloor \frac{f-jr}{q} \right\rfloor$.

Доказательство. Заметим, что в силу $p, q, r \in \mathbb{N} + 1$ и $x, y, z \in \mathbb{N} - 1$ при $z > \left\lfloor \frac{f}{r} \right\rfloor$ получаем, что $px + qy + rz \geq r \left(\left\lfloor \frac{f}{r} \right\rfloor + 1\right) > f$, то есть данное равенство $px + qy + rz = f$ не выполняется. Поэтому получаем ограничение на неизвестную z вида $0 \leq z \leq \left\lfloor \frac{f}{r} \right\rfloor$. Полагая $z = j$, приходим к выводу, что исходное уравнение $px + qy + rz = f$ разрешимо в $\mathbb{N} - 1$ тогда и только тогда, когда найдётся такое число $j \in \{0; \dots; \left\lfloor \frac{f}{r} \right\rfloor\}$, что в $\mathbb{N} - 1$ разрешимо уравнение вида $px + qy = f - jr$ с двумя неизвестными x и y . По лемме 1 при $h = f - jr$ последнее уравнение разрешимо в $\mathbb{N} - 1$ тогда и только тогда выполняется неравенство $\frac{f-jr}{q} \bmod p \leq \left\lfloor \frac{f-jr}{q} \right\rfloor$. Лемма 2 доказана.

Доказательство теоремы 1. Если $p, q, r \in \mathbb{N} + 1$ и $f \in \mathbb{N}$, то теорема 1 непосредственно следует из леммы 2.

Рассмотрим случай, когда $f \in \mathbb{N}$ и хотя бы одно из чисел p, q или r равно единице. В этом случае очевидно, что уравнение $px + qy + rz = f$ разрешимо в $\mathbb{N} - 1$ (для всех $f \in \mathbb{N}$). Докажем, что в этом случае утверждение теоремы 1 верно, то есть покажем, что для некоторого среди указанных значений j неравенство (*) не выполняется. При $p = 1$ положим $j = 0$, тогда правая часть неравенства (*) равна нулю, а левая больше или равна нулю, то есть неравенство не выполняется. При $q = 1$ тоже положим $j = 0$, тогда правая часть неравенства (*) равна $f \bmod p$, а левая равна f . Но при $f \in \mathbb{N}$ имеем $f \bmod p \leq f$, а значит неравенство ложно. При $r = 1$ положим $j = \left\lfloor \frac{f}{r} \right\rfloor = f$, тогда обе части неравенства (*) равны нулю и поэтому оно не выполняется.

Рассмотрим оставшийся случай, когда $f = 0$ и $p, q, r \in \mathbb{N}$. Очевидно, что в этом случае уравнение $px + qy + rz = 0$ разрешимо в $\mathbb{N} - 1$, так как превращается в истинное равенство при $x = y = z = 0$. Покажем, что в этом случае теорема 1 тоже работает. Так как множество $\{0; \dots; \left\lfloor \frac{f}{r} \right\rfloor\}$ при $f = 0$

имеет вид $\{0\}$, то существует $j = 0$, при котором очевидно обе части неравенства (*) равны нулю и поэтому оно является ложным. Теорема 1 доказана.

Теперь мы можем перейти к описанию алгоритма. Пусть $a, b, c \in \mathbb{N}$ и $(a; b; c) = 1$. Положим $p = a/(a, b)$, $q = b/(a, b)$ и $r = c$. Для нахождения числа Фробениуса тройки a, b, c используется известная формула Джонсона [4]: $frob(a, b, c) = (a, b) \cdot frob(p, q, r) + ((a, b) - 1)c$. Поэтому вопрос вычисления $frob(a, b, c)$ сводится к нахождению числа $frob(p, q, r)$, где $p, q, r \in \mathbb{N}$ и $(p, q) = 1$. Условия, накладываемые на числа p, q, r , соответствуют теореме 1.

Далее, замечаем, что при $g = frob(p, q) = pq - p - q$ выполняется неравенство $frob(p, q, r) \leq g$. Поэтому для нахождения числа Фробениуса тройки p, q, r мы можем последовательно снижать на единицу целые значения f , начиная от числа g (возможно до нуля) до тех пор, пока не возникнет первое значение f , для которого по теореме 1 уравнение $px + qy + rz = f$ окажется неразрешимым и тогда $frob(p, q, r)$ будет равно f . Если же такого значения f не найдётся (в этой ситуации f доберётся до значения нуля), то полагаем $frob(p, q, r) = -1$.

На этом завершается общее описание алгоритма вычисления $frob(a, b, c)$.

Теперь мы можем сформулировать в соответствии с приведённым алгоритмом теорему 2, в которой приводится описание алгоритмической формулы нахождения числа Фробениуса любой тройки взаимно простых натуральных чисел.

Теорема 2. Пусть $a, b, c \in \mathbb{N}$ и $(a; b; c) = 1$.

Полагаем: 1) $d = (a; b)$;

2) $p = a/d$;

3) $q = b/d$;

4) $g = pq - p - q$;

5) $H_{i,j} = \left[\frac{g-i-jc}{q} \right] - ((q^{\varphi(p)} - 1)(g - i - jc)) \bmod p$ для всех чисел $i \in \{0; \dots; g\}$ и $j(i) \in \{0; \dots; \left[\frac{g-i}{c} \right]\}$;

6) $f = g - \sum_{k=0}^g \prod_{i=0}^k (1 - \prod_{j=0}^{\left[\frac{g-i}{c} \right]} sgn(|H_{i,j}| - H_{i,j}))$.

Тогда $frob(a, b, c) = df + (d - 1)c$.

Перед доказательством теоремы 2 заметим, что, выражая последовательно согласно 1) – 6) через буквы a, b, c величины $d, p, q, g, H_{i,j}, f$ и $frob(a, b, c)$, мы получим алгоритмическую формулу числа Фробениуса тройки чисел a, b, c , в которой, кроме знаков операций, использованы только буквы a, b и c . В таком виде формула не приводится, так как она не размещается наглядно на одной странице.

Доказательство. Рассмотрим случай, когда $g \geq 0$. Для краткости введём обозначения $\{0; \dots; g\} = \mathbb{I}$ и $\{0; \dots; \left\lfloor \frac{g-i}{c} \right\rfloor\} = \mathbb{J}(i)$ при $i \in \mathbb{I}$. Отмечаем, что при $g \geq 0$ множества \mathbb{I} и $\mathbb{J}(i)$ при $i \in \mathbb{I}$ не являются пустыми. По теореме Эйлера $q^{\varphi(p)-1} \bmod p = \frac{1}{q} \bmod p$ (здесь $\varphi(n)$ – функция Эйлера при $n \in \mathbb{N}$), то есть $(q^{\varphi(p)-1}(g-i-jc)) \bmod p = \frac{g-i-jc}{q} \bmod p$ и поэтому в 5) получим, что $H_{i,j} = \left\lfloor \frac{g-i-jc}{q} \right\rfloor - \left(\frac{g-i-jc}{q} \bmod p \right)$ для всех $i \in \mathbb{I}$ и $j \in \mathbb{J}(i)$. Согласно теореме 1 при $r = c$ и $f = g - i$ уравнение (i) $px + qy + cz = g - i$, где $i \in \mathbb{I}$, не имеет решений в $\mathbb{N} - 1$ тогда и только тогда, когда $H_{i,j} < 0$ для всех $j \in \mathbb{J}(i)$. Далее под «разрешимостью» уравнения (i) будем по умолчанию понимать его «разрешимость в $\mathbb{N} - 1$ ». Ясно, что $\text{sgn}(|H_{i,j}| - H_{i,j}) = \begin{cases} 1, & \text{если } H_{i,j} < 0 \\ 0, & \text{если } H_{i,j} \geq 0 \end{cases}$. Положим $1 - \prod_{j=0}^{\left\lfloor \frac{g-i}{c} \right\rfloor} \text{sgn}(|H_{i,j}| - H_{i,j}) = \mathbb{K}(i)$. Тогда для числа $\mathbb{K}(i)$ следует

$$\mathbb{K}(i) = \begin{cases} 0, & \text{если } H_{i,j} < 0 \text{ для всех значений } j \in \mathbb{J}(i) \\ 1, & \text{если при некотором } j \in \mathbb{J}(i) \text{ имеем } H_{i,j} \geq 0 \end{cases}, \text{ то есть по-}$$

лучаем, что $\mathbb{K}(i) = \begin{cases} 0, & \text{если (i) не разрешимо} \\ 1, & \text{если (i) разрешимо} \end{cases}$. Теперь пусть $k \in \mathbb{I}$. По-

нятно, что $\prod_{i=0}^k \mathbb{K}(i) = \begin{cases} 0, & \text{если (i) не разрешимо при некотором } i \in \{0; \dots; k\} \\ 1, & \text{если (i) разрешимо для всех } i \in \{0; \dots; k\} \end{cases}$. Пусть i_0 – наименьшее значение среди $i \in \mathbb{I}$, для которых уравнение (i) является неразрешимым. Тогда $g - i_0 = \text{frob}(p, q, c)$. Также выполняются равенства: $\prod_{i=0}^0 \mathbb{K}(i) = \dots = \prod_{i=0}^{i_0-1} \mathbb{K}(i) = 1$, $\prod_{i=0}^{i_0} \mathbb{K}(i) = \dots = \prod_{i=0}^g \mathbb{K}(i) = 0$. Откуда следует $\sum_{k=0}^g \prod_{i=0}^k \mathbb{K}(i) = i_0$, то есть при $f = g - \sum_{k=0}^g \prod_{i=0}^k \mathbb{K}(i)$ окончательно получаем, что $f = \text{frob}(p, q, c)$. Равенство $\text{frob}(a, b, c) = df + (d-1)c$ следует из известной формулы Джонсона [4].

Осталось рассмотреть случай, когда $g < 0$. Так как $g = pq - p - q$ и $p, q \in \mathbb{N}$, то $g \geq -1$ и в нашем случае $g = -1$. Понятно, что в любом наборе из n натуральных чисел ($n \geq 2$) присутствует единица тогда и только тогда, когда число Фробениуса этого набора равно -1 . Поэтому в нашем случае имеем $p = 1$ или $q = 1$. Замечаем, что в пункте 5) возникает «неприятность» – величина $H_{i,j}$ не определена в силу невыполнимости условий $i \in \{0; 1; \dots; g\}$ и $j(i) \in \{0; 1; \dots; \left\lfloor \frac{g-i}{c} \right\rfloor\}$. В пункте 6) в таком случае полагаем, что

величина $\sum_{k=0}^g \prod_{i=0}^k (1 - \prod_{j=0}^{\left\lfloor \frac{g-i}{c} \right\rfloor} \text{sgn}(|H_{i,j}| - H_{i,j}))$ равна нулю, то есть согласно 6) $f = g$ и $f = \text{frob}(p, q, c) = -1$, а значит, $\text{frob}(a, b, c) = cd - c - d = \text{frob}(d, c)$, что вполне соответствует определению числа Фробениуса

тройки a, b, c в рассматриваемом исключительном случае. Теорема 2 доказана.

Хочется отметить, что указанные теоретическая «неприятность» в последнем абзаце рассуждений в ходе доказательства теоремы 2 не влияет на практическую безошибочную работу приведённой ниже компьютерной программы, написанной непосредственно на основе алгоритмической формулы, изложенной в теореме 2. Для наглядности и краткости код программы пишем курсивом и допускаем расположение нескольких операторов в одной строке. При копировании ниже приведённого кода непосредственно в рабочую среду Pascal ABC.NET работа программы может быть проверена самостоятельно.

```

{1} Var a, b, c, d, f, g, p, q, s, u, v, frob: integer; Lim: array of integer; H:
array [,] of integer;
{2} Function Sgn(w:integer): integer; Begin If w= 0 Then Result:= 0
Else Result:= w div (abs(w)); End;
Function Z(w:real): integer; Begin If Trunc(w) <= w Then Result:=
Trunc(w)
Else Result:= Trunc(w) - 1; End;
Function Gsd(w1, w2:integer): integer; Begin While w1 - w2 <> 0 Do If
w1 > w2
Then w1:= w1 - w2 Else w2:= w2 - w1; Result:= w1; End;
{3} Begin Write('a= '); Read(a); Write('b= '); Read(b); Write('c= ');
ReadLn(c);
d:= Gsd(a, b); p:= a div d; q:= b div d; g:= p * q - p - q;
{4} For Var i:= 1 To p Do If (i * q) mod p = 1 Then Begin s:= i; Break;
End;
SetLength(Lim, g+1); For Var i:= 0 To g Do Lim[i]:= Z((g - i) / c);
SetLength(H, g+1, Trunc(g / c)+1); For Var i:= 0 To g Do For Var j:= 0
To Lim[i]
Do H[i, j]:= Z((g - i - j * c) / q) - ((s * (g - i - j * c)) mod p);
{5} f:= g; For Var k:= 0 To g Do Begin v:= 1; For Var i:= 0 To k Do
Begin u:= 1;
For Var j:= 0 To Lim[i] Do u:= u * Sgn(Abs(H[i, j]) - H[i, j]); v:= v * (1
- u); End;
f:= f - v; End; frob:= d * f+(d - 1) * c; WriteLn('frob(a;b;c) = ', frob);
End.

```

Прокомментируем отдельные части кода программы.

В {1} приводится описание типов переменных, используемых для написания кода программы. В {2} для работы программы нам понадобятся функции: $Sgn(w)$ (сигнум числа w), $Z(w)$ (целая часть числа w) и $Gsd(w1, w2)$ (наибольший общий делитель двух натуральных чисел $w1$ и $w2$). В {3} начинается работа основной части программы: вводятся взаимно

простые натуральные числа a, b, c и реализуются пункты 1) – 4), изложенные в формулировке теоремы 2. В {4} находится число $s = q^{\varphi(p)-1} \bmod p = \frac{1}{q} \bmod p$; определяется строка Lim максимальных значений индексов $j(i)$ по формуле $Lim(i) = \left\lfloor \frac{g-i}{c} \right\rfloor$ при всех $i \in \{0; \dots; g\}$; а также находятся величины $H_{i,j}$, определённые в пункте 5), которые размещаются как элементы в матрице H размеров $(g + 1) \times \left(\left\lfloor \frac{g}{c} \right\rfloor + 1\right)$. В {5} находим число $f = \text{frob}(p, q, c)$ по формуле из пункта 6) теоремы 2 и окончательно по формуле Джонсона вычисляем и печатаем $\text{frob}(a, b, c)$.

В заключение отметим, что эта статья является результатом совместной работы творческого коллектива, созданного в рамках кружка «Вычислительные алгоритмы элементарной математики» на малом математическом факультете, образованном на базе факультета математики и компьютерных наук (ФМ и КН) Куб ГУ. В состав коллектива вошли доцент факультета (Г.Н. Титов), студентка факультета (Т.В. Зинченко) и школьник СОШ № 103 г. Краснодара (Д.Р. Скибицкий). Теоремы 1 и 2 получены Г.Н. Титовым. Написание кода программы, иллюстрирующей алгоритмическую формулу из теоремы 2, и тестирование программы осуществляли все участники коллектива. Т.В. Зинченко и Д.Р. Скибицкий докладывали некоторые результаты работы на студенческой научной конференции ФМ и КН Куб ГУ в апреле 2023 года.

Библиографический список

1. Савельев В.П. Алгоритм вычисления числа Фробениуса для трёх натуральных чисел / В.П. Савельев // Сборник научных трудов 83-й Международной конференции Евразийского Научного Объединения. – М.: ЕНО, 2022, - С. 19 – 22.
2. Фомичев В.М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трёх аргументов: Прикладная дискретная математика / В.М. Фомичев. – М.: ПДМ, 2014, - С. 88 – 96.
3. Ramirez Alfonsin J.L. The Diophantine Frobenius Problem. Oxford University Press, 2005. – 243 p.
4. Johnson S.M. A Linear Diophantine Problem. Canadian Journal of Mathematics 12 (1960), P. 390 – 398.

Е.Г. Толкачева, В.Ф. Пуляев

О СПЕКТРЕ ЛИНЕЙНЫХ НЕПРЕРЫВНЫХ ОПЕРАТОРОВ

Рассмотрены некоторые условия, устанавливающие связь между спектром линейного непрерывного оператора и спектром его сужения на инвариантное подпространство. Для некоторых линейных непрерывных операторов, действующих в пространстве непрерывных и ограниченных на полуоси функций (или в пространстве ограниченных последовательностей) показано совпадение их спектра со спектром сужения на пространство непрерывных функций, имеющих конечный предел на бесконечности и на пространство непрерывных функций, имеющих предел на бесконечности равный нулю (на пространство последовательностей, имеющих конечный предел и на пространство последовательностей, имеющих конечный предел равный нулю).

Ключевые слова: линейный непрерывный оператор, полунорма, инвариантное подпространство, спектр, пространство непрерывных и ограниченных на полуоси функций, пространство ограниченных последовательностей.

Some conditions of establishing the connection between the spectrum of linear continuous operator and the spectrum of its restriction on some invariant subspace were analyzed. For some linear continuous operators which map the space of continuous bounded on the semiline functions (or the space of bounded sequences) into itself it is shown that their spectra coincide with the spectra of their restrictions on the space of continuous functions which have finite limit at infinity, the space of continuous functions which have zero limit at infinity (or the space of sequences which have finite limit, the space of sequences which have zero limit).

Keywords: Linear continuous operator, seminorm, invariant subspace, spectrum, space of continuous bounded functions, space of bounded sequences.

Пусть E – комплексное банахово пространство; A – непрерывный линейный оператор, действующий из E в E ; X – замкнутое подпространство E , инвариантное относительно A , и \tilde{A} – сужение оператора A на X , $\sigma(A)$ – спектр оператора A , $\sigma(\tilde{A})$ – спектр оператора \tilde{A} соответственно.

Обозначим через S – множество полунорм $\{p_\alpha(x)\}$ на E . Пусть S удовлетворяет условиям:

для любого x из E :

а) $p_\alpha(x) \leq p_\beta(x)$, если $\alpha \leq \beta$;

б) если $p_\alpha(x) = 0$ для любых $\alpha = 1, 2, \dots$, то $x = 0$.

В работе приведены некоторые условия на X и A , при которых $\sigma(\tilde{A}) \subset \sigma(A)$. Указаны также условия, обеспечивающие включение

$\sigma(A) \setminus \{0\} \subset \sigma(\tilde{A})$. Полученные результаты применены затем к конкретным операторам.

Определение. Последовательность $\{x^n\}$ из S –сходится к элементу x , если $\sup \|x_n\| < \infty$ и $\forall \alpha \in N: p_\alpha(x_n) \rightarrow p_\alpha(x), n \rightarrow \infty$.

Пусть X есть прямая сумма подпространств X_0 и F , где F имеет конечную размерность m .

Пусть S удовлетворяет следующим условиям:

1. Подпространство X_0 всюду плотно в E относительно S –сходимости
2. Если последовательность $\{x_n\}$ S –сходится к $x \in X_0$, то $\{x_n\}$ слабо сходится к x , где $\{x_n\} \subset X_0$.

Возьмем в F нормированный базис $\{e_j\}, j=1, \dots, m$.

Пусть в системе полунорм $\{p_\alpha(x)\}$ существует подмножество $\{p_j(x)\}, j=1, \dots, m$, удовлетворяющее условиям: $p_j(X_0) = \{0\}$ и $p_j(e_i) = \delta_{ij}$, где δ_{ij} – символ Кронекера, $i, j=1, \dots, m$.

Обозначим через $\{y_{ik}\}, k=1, 2, \dots$ некоторую последовательность из X_0 , S –сходящуюся к e_j и положим $z_{jk} = e_j - y_{jk}$. Тогда $\{z_{jk}\}$ S –сходится к нулю.

Теорема 1. Пусть выполнены условия 1 и 2 и оператор A непрерывен относительно S –сходимости. Тогда $\sigma(\tilde{A}) \subset \sigma(A)$.

Кроме того, если множество S тотально и каждую слабо фундаментальную последовательность из X оператор A переводит в последовательность, S –сходящуюся в E , то $\sigma(A) \setminus \{0\} \subset \sigma(\tilde{A})$.

Доказательство. Покажем, что $\sigma(\tilde{A}) \subset \sigma(A)$.

Пусть $\lambda \notin \sigma(A), z \in X$. Выберем последовательность $\{x_k\}$ из X_0 , S –сходящуюся к решению уравнения $(\lambda I - A)x = z$.

Тогда последовательность $\{(\lambda I - A)x_k\}$ S –сходится к z и существует $\lim_{k \rightarrow \infty} p_j(Ax_k)$. Положим $t_k = \sum_{j=1}^m q_j (\lambda I - A)z_{jk}$, где вектор q – решение уравнения $(\lambda I - A)q = w$, а координаты вектора w определяются из условий:

$w_i = \lim_{k \rightarrow \infty} p_j(z + Ax_k)$. Очевидно, последовательность $\{t_k\}$ S –сходится к нулю, $\varphi_i(t_k) \rightarrow \lambda q - \sum_{j=1}^m b_{ij} q_j = w_i$ при $k \rightarrow \infty$. Положим $d_k = t_k + (\lambda I - A)x_k$. Тогда последовательность $\{d_k\}$ S –сходится к z и $\lim_{k \rightarrow \infty} p_j(d_k) = p_j(z)$. Поэтому последовательность $\{d_k\}$ слабо сходится к z .

Таким образом, подпространство $(\lambda I - A)X$ слабо плотно в X , а так как оно замкнуто, то $(\lambda I - A)X = X$. Отсюда следует, что $\sigma(\tilde{A}) \subset \sigma(A)$.

Покажем теперь, что имеет место включение $\sigma(A) \setminus \{0\} \subset \sigma(\tilde{A})$. Пусть $\lambda \notin \sigma(\tilde{A})$ и $\lambda \neq 0$. Рассмотрим уравнение $\lambda x = Ax + y$, где $y \in E$, и покажем, что в E оно имеет единственное решение.

Пусть $\{y_k\}$ – последовательность из X_0 , S –сходящаяся к y , и $\lambda x_k = \tilde{A}x_k + y_k$. По условию 2 последовательность $\{y_k - y_p\}$ слабо сходится к нулю при $k, p \rightarrow \infty$. Тогда из равенства $x_k - x_p = (\lambda I - \tilde{A})^{-1} (y_k - y_p)$ следует, что $\{x_k - x_p\}$ также слабо сходится к нулю при $k, p \rightarrow \infty$. Это означает, что последовательность $\{x_k\}$ слабо

фундаментальна, поэтому по условию теоремы последовательность $\{Ax_k\}$ S -сходится к некоторому элементу $y_0 \in E$. В силу равенства $\lambda x_k = \tilde{A}x_k + y_k$ последовательность $\{x_k\}$ S -сходится к элементу $x_0 = \lambda^{-1}(y + y_0)$ и $\lambda x_0 = Ax_0 + y$.

Убедимся, что уравнение $\lambda x = Ax + y$ имеет в E единственное решение. Допустим, что $\lambda z = Az$, где $z \in E$. Выберем в X_0 последовательность $\{z_k\}$, S -сходящуюся к z . Тогда последовательность $\{r_k\}$, $r_k = (\lambda I - A)z_k$ S -сходится к нулю. Положим $t_k = \sum_{j=1}^m q_j (\lambda I - A)z_{jk}$, где вектор q – решение уравнения $(\lambda I - A)q = w$, а координаты вектора w определяются из условий: $w_i = \lim_{k \rightarrow \infty} \varphi_j(r_k)$. Последовательность $\{r_k - t_k\}$ слабо сходится к нулю. Но тогда слабо сходится к нулю последовательность $\{z_k - \sum_{j=1}^m q_j z_{jk}\}$. А так как она S -сходится к z , то, в силу тотальности S , решение $z = 0$. Теорема 1 доказана.

Теорема 1 может быть применена для исследования связи между спектрами различных операторов и их сужений. Ниже приводятся соответствующие утверждения для интегральных операторов, действующие в пространстве непрерывных ограниченных на полуоси функций, и операторов, действующих в пространстве ограниченных последовательностей. Аналогичные результаты справедливы также так же для операторов в пространстве измеримых ограниченных (с весом) функций.

Введем обозначения $BC^n[0, \infty)$ – пространство непрерывных и ограниченных на $[0, \infty)$ функций со значениями в C^n и $\|x\| = \sup_{t \geq 0} |x(t)|$;

$$C_0^n[0, \infty) = \left\{ x \in BC^n[0, \infty) : \lim_{t \rightarrow \infty} x(t) = 0 \right\};$$

$$A_0^n[0, \infty) = C_0^n[0, \infty) \oplus C^n$$

Пусть $K(t, s)$ – матрица $n \times n$, определена в области $\{(t, s) : t \geq 0, s \geq 0\}$, суммируема по s на $[0, \infty)$ при любом $t \geq 0$ и удовлетворяет условиям:

$$1) \sup_{t \geq 0} \int_0^\infty \|K(t, s)\| ds < \infty;$$

$$2) \lim_{h \rightarrow 0} \int_0^\infty \|K(t+h, s) - K(t, s)\| ds = 0 \text{ для любого } t \geq 0.$$

В этом случае оператор $Kx = \int_0^\infty K(t, s) ds$ переводит пространство $BC^n[0, \infty)$ в себя. Допустим, что подпространство $A_0^n[0, \infty)$ ($C_0^n[0, \infty)$) инвариантно относительно оператора K . Тогда справедлива

Теорема 2. Спектр оператора K совпадает со спектром его сужения \tilde{K} на подпространство $A_0^n[0, \infty)$ ($C_0^n[0, \infty)$).

Доказательство. Воспользуемся теоремой 1. Положим $E = BC^n[0, \infty)$; $X_0 = C_0^n[0, \infty)$; $F = C^n$; $S = \{p_{ii}\}$, где полунормы p_{ii} определяются равенством $p_{ii}(x) = |x_i(t)|$, $x = (x_1, \dots, x_n) \in BC^n[0, \infty)$. Заметим, что S – сходящиеся последовательности совпадают с ограниченными последовательностями, сходящимися поточечно на $[0, \infty)$ к непрерывной функции.

Так как, каждая функция из $BC^n[0, \infty)$ есть поточечный предел на $[0, \infty)$ ограниченной последовательности функций из $C_0^n[0, \infty)$, то $C_0^n[0, \infty)$ плотно в

$BC^n[0, \infty)$ относительно S – сходимости. Слабая сходимость в $A_0^n[0, \infty)$ совпадает с поточечной сходимостью на $[0, \infty)$ (при условии ограниченности последовательности). Отсюда следует, что выполняется условие 2.

Покажем, что оператор K удовлетворяет условиям теоремы 1. Непрерывность K относительно S – сходимости следует из теоремы Лебега о предельном переходе под знаком интеграла (см. [1]). Если последовательность $\{x^m\}$ из $A_0^n[0, \infty)$ слабо фундаментальна, то $\{x^m\}$ ограничена и сходится поточечно на $[0, \infty)$ к некоторой функции $x(t)$. Поэтому последовательность $\{Kx^m\}$ ограничена и сходится на $[0, \infty)$ к функции $Kx \in BC^n[0, \infty)$. Заметим также, что нуль принадлежит спектрам K и \tilde{K} . Отсюда и из теоремы 1 следует что $\sigma(\tilde{K}) = \sigma(K)$. Теорема 2 доказана.

Аналогичное утверждение справедливо для операторов, действующих в пространстве l_∞ – ограниченных комплексных последовательностей $x = (x_1, x_2, \dots)$ с $\|x\| = \sup_i |x_i|$. Обозначим $a_0 = \{x \in l_\infty : \exists \lim_{i \rightarrow \infty} x_i\}$; $c_0 = \{x \in l_\infty : \exists \lim_{i \rightarrow \infty} x_i = 0\}$.

Пусть оператор $Ax = (\sum_{j=1}^{\infty} a_{1j}x_j, \sum_{j=1}^{\infty} a_{2j}x_j, \dots)$ переводит l_∞ в себя и подпространство a_0 (c_0) инвариантно относительно A . Заметим, что при этом $\sup_i \sum_{j=1}^m |a_{ij}| < \infty$ (см. [1]). Справедлива

Теорема 3. Спектр оператора A совпадает со спектром его сужения на подпространство a_0 (c_0).

Доказательство. Для оператора A будут выполнены условия теоремы 1, если положить $X_0 = c_0$; $F = \{x \in l_\infty : x_i = x_1, i = 2, 3, \dots\}$; $S = \{p_i\}$, где $p_i(x) = |x_i|$.

Заметим, что оператор $I-A$ также удовлетворяет условиям теоремы 1. Поэтому, если $0 \notin \sigma(\tilde{A})$, то $1 \notin \sigma(I-\tilde{A})$, и в силу теоремы 1, $1 \notin \sigma(I-A)$, т.е. $0 \notin \sigma(A)$. Поэтому, по теореме 1 $\sigma(A) = \sigma(\tilde{A})$. Теорема 3 доказана.

Замечание. Условиям теоремы 2 удовлетворяют интегральные операторы с ядром $K(t,s)$, где $K(t) \in L(-\infty, \infty)$. Для таких операторов утверждение теоремы 2 известно (см. [2]). Для интегральных операторов Вольтера подобные вопросы рассматривались в [3 – 5].

Библиографический список

1. Данфорд Н., Шварц Дж. Т. Линейные операторы. Общая теория. Editorial URSS., 2010.
2. Рудин У. Функциональный анализ. – Лань, 2005.
3. Гохберг И. Ц., Фельдман И. А. Уравнения в свертках и проекционные методы их решения. М., 1971.

4. Цалюк З. Б. О допустимости некоторых пар пространства для интегральных операторов и уравнений Вольтерра. // Диф. уравнения. 1977. Т. 19. № 11. С 2096 – 2098.

5. Пуляев В.Ф., Цалюк З. Б. К вопросу о допустимости некоторых пар пространств для линейных операторов и уравнений Вольтера. // Диф. уравнения. 1983. Т. 19. № 4. С 684 – 682.

Е.А. Христюк, В.Н. Савин

ТЕСТИРОВАНИЕ ГЕНЕРАТОРОВ

ПОСЛЕДОВАТЕЛЬНОСТЕЙ СЛУЧАЙНЫХ ЧИСЕЛ

В данной статье рассмотрены графические и статистические методы оценки качества генераторов последовательностей случайных чисел.

Ключевые слова: генераторы последовательностей случайных чисел, статистические тесты.

This article discusses graphical and statistical methods for evaluating the quality of random number sequence generators.

Key words: random number sequence generators, statistical tests.

Программные генераторы последовательностей случайных чисел (ГПСЧ) нашли самое широкое применение от игровой компьютерной индустрии до математического моделирования и криптологии [4;5;6]. Основные требования к таким генераторам: независимость элементов генерируемой числовой последовательности, их равномерное распределение и скорость. Реализуя некоторый алгоритм, программные генераторы вырабатывают числа в зависимости от предшествующих значений, поэтому полученные числовые последовательности не являются истинно случайными.

На сегодняшний день разработано достаточно большое количество различных ГПСЧ [3;4]. Для демонстрации их статистических свойств использовались различные подходы к статистическому тестированию. Чаще всего набор и методику тестирования предлагал сам разработчик генератора.

Существует множество способов проверки ГПСЧ. Чаще всего, оценивают близость псевдослучайной последовательности к истинно случайной. Методы, как правило, подразделяются на:

- статистические;
- графические.

К графическим относятся тесты, которые в качестве результата выводят диаграммы и гистограммы [4].

Исследование качества ГПСЧ ведётся активно и в настоящее время, например, см. [2]. Следует отметить, что некоторые генераторы, встроенные в ядра компиляторов и процессоров, были изменены после того, как они не

прошли новые статистические тесты. При этом тестирование ГПСЧ также может использоваться для проверки самих тестов качества генератора, так как если известно, что ГПСЧ выдаёт некачественный набор данных, в каком-то смысле, то тест должен забраковывать эти результаты.

Ряд тестов выявляет отсутствие случайности только путем построения статистики, которая измеряет неравномерность распределения случайных N -последовательностей координат в N -мерном пространстве. Эта неравномерность может быть устранена только тогда, когда пространство начинает заполняться точками с некоторой плотностью. К сожалению, количество точек, требуемое для заполнения такого пространства, масштабируется по степени измерения, а это означает, что очень трудно разрешить этот конкретный вид корреляции.

По всем этим причинам разработка и внедрение тестов на случайность числовых последовательностей, генерируемых различными ГПСЧ с реальными или воображаемыми достоинствами, является важной задачей в статистических вычислениях.

Известно, что при хэшировании (алгоритм нахождения контрольной суммы, предназначенный для проверки целостности данных) незначительное изменение аргумента приводит к значительному изменению результата, поэтому можно исследовать хэш-функции в качестве ГПСЧ. Например, в работе [1] рассматриваются хэш-функции SHA-1 и MD5, но там использовались только графические тесты.

В данной работе исследовались последовательности чисел, сгенерированные методом CRC32, SHA и SHA512. Для сравнения рассматривались также последовательности, полученные генератором mt19937 (вихрь Мерсенна, создатели Матсумото и Нишимура, 1998), линейный конгруэнтный генератор randu от IBM (вошедший в употребление в 1960-х). Каждым методом генерировалась последовательность из 32 миллионов чисел, которая исследовалась с помощью графических тестов и набора статистических тестов Dieharder (пакет программ с открытым кодом, реализованный на различных платформах).

Рассмотрим диаграмму распределения на плоскости для mt19937, представленную на рисунке 1. Точки расположены хаотично, можно сделать вывод что тест пройден успешно. При рассмотрении трехмерного графика тоже никаких узоров/полос не было найдено. На рисунке представлен один из видов куба.

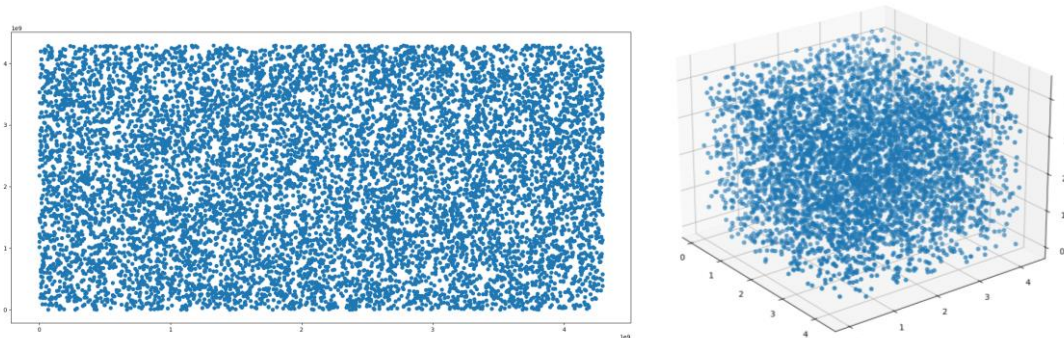


Рис. 1. Диаграмма распределения на плоскости и в пространстве для mt19937

Теперь рассмотрим randu: на графике на плоскости на рисунке 2 можно увидеть полосы.

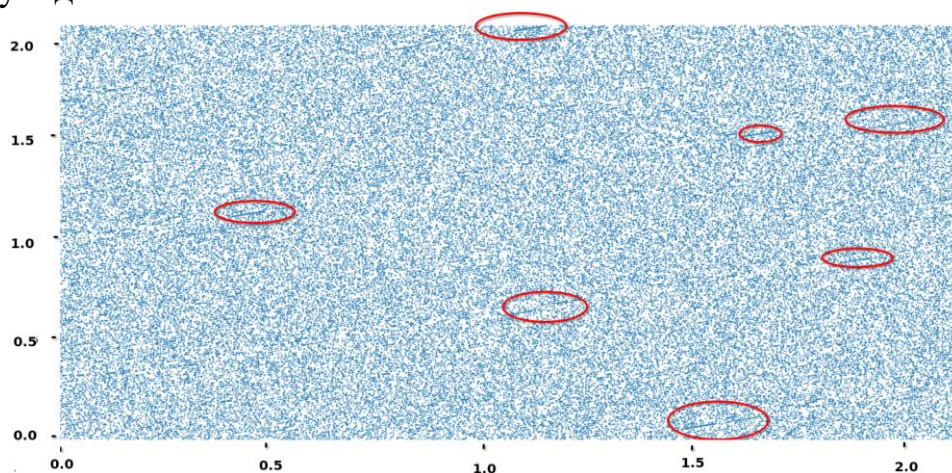


Рис. 2. Диаграмма распределения на плоскости randu

В пространстве на первый взгляд все в порядке, на рисунке 3 (слева) точки расположены хаотично. Однако стоит немного покрутить трехмерный куб как точки образуют несколько полос (рис.3 справа). Теперь уже можно говорить наверняка, что randu не проходит графический тест на однородность ГПСЧ.

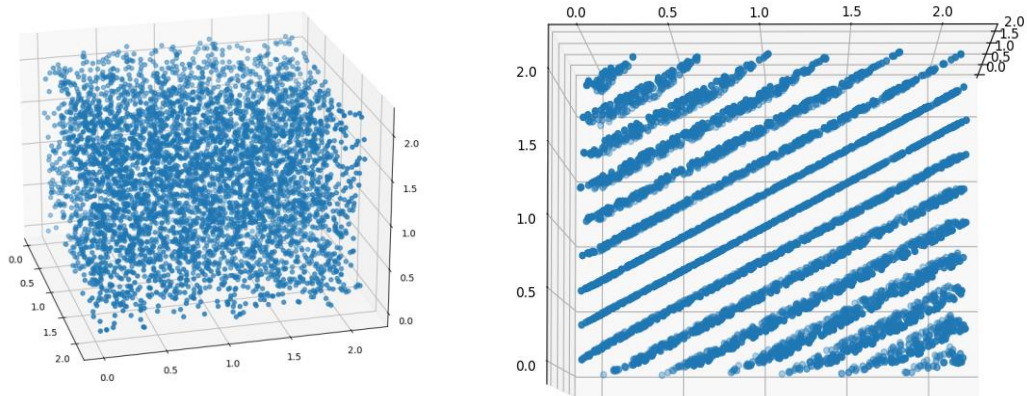


Рис. 3. Диаграмма распределения в пространстве randu

На рисунке 4 представлены графические тесты для алгоритма CRC32, как ГПСЧ. Результаты тестирования демонстрируют неудовлетворительное выполнение поставленных задач. Вместо однородного заполнения видны четкие узоры и линии.

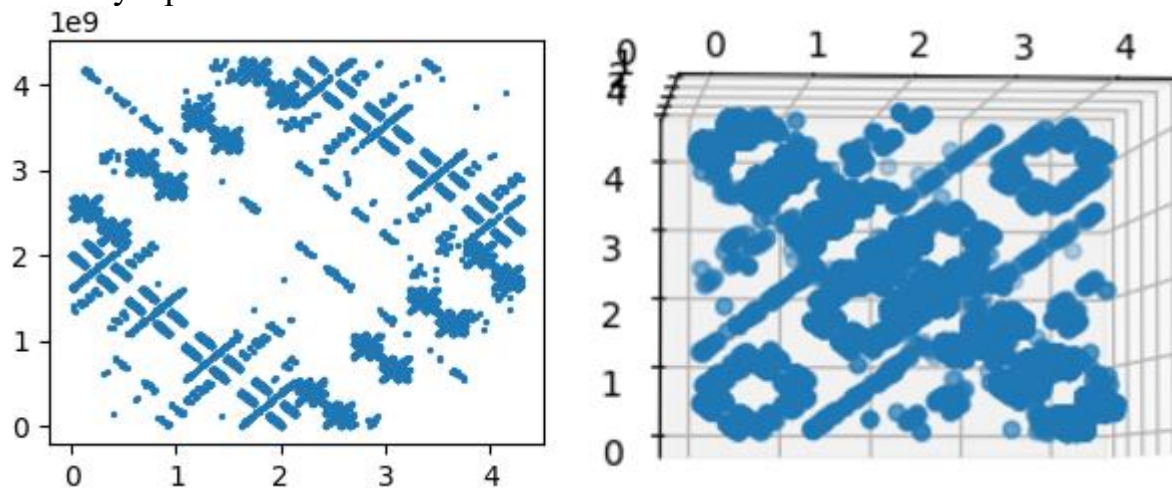


Рис. 4. Диаграммы распределения в пространстве и на плоскости CRC32

На рисунке 5 представлены графические тесты для алгоритма SHA, как ГПСЧ. Результаты тестирования – удовлетворительные, заполнено всё пространство, хотя видны некоторые «пустые» области. SHA512 так же не выдал сильных отклонений на диаграммах при прохождении графических тестов.

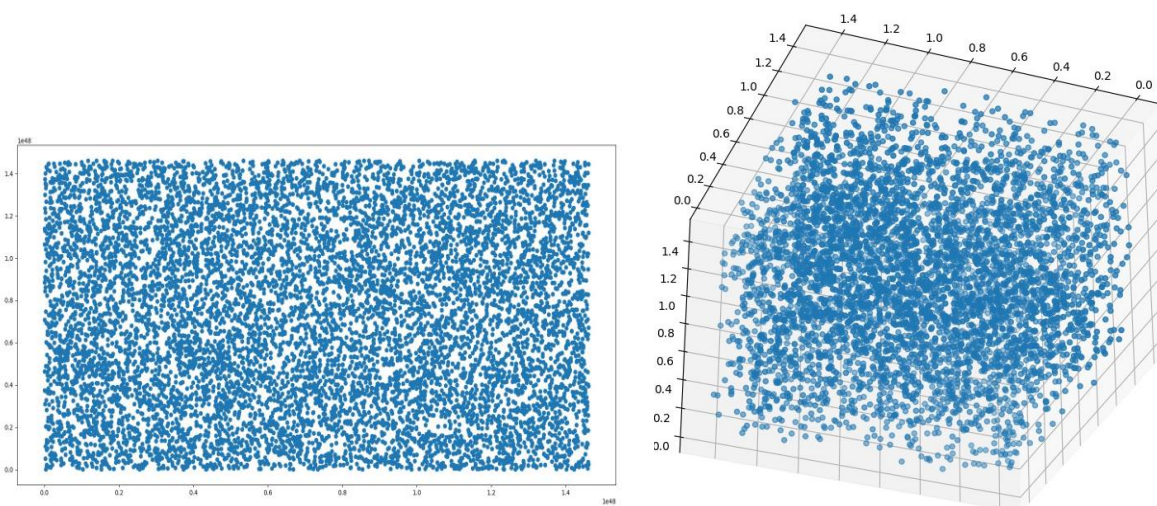


Рис. 5. Диаграммы распределения в пространстве и на плоскости для SHA

Недостатком графического теста является отсутствие точного определения «однородности» заполнения и выбора угла просмотра для трехмерного случая.

Теперь исследуем эти же генераторы с помощью набора Dieharder: допускается слабый результат не более чем в двух тестированиях из ста и провал не более двух тестирований из тысячи.

Всего 2 теста пройдено mt19937 слабо, но все равно не провалены. Это хороший результат. Для генератора randu результат ожидаемый – успешно пройдено всего пару тестирований, слабо 2, все остальное провалено. Статистические тесты подтвердили результат, полученный ранее. Для CRC32 также результат был подтвержден, успешно пройдено только 4 из 114 тестов, а 6 показали слабый результат. Для SHA, к сожалению, результат не был подтвержден, успешно пройдено только 6, слабый - 5 из 114 тестов, тем самым подтверждая более строгие статистические требования для ГПСЧ. SHA512 так же полностью провалил тестирование Dieharder: 6 – успешно, 6 слабо, остальное провалено.

После проведения тестирования пяти алгоритмов с использованием последовательности значений, состоящей из 32 миллионов элементов, можно сделать вывод о их качестве. Для выявления «плохого» генератора достаточно провести простые графические тесты распределения в пространстве и на плоскости. Однако, для определения, является ли алгоритм условно однородным, необходимо прибегнуть к тестированию с использованием статистических пакетов. К сожалению, на сегодняшний день нет единого подхода к оцениванию качества ГПСЧ. В том числе не существует единого мнения о том, как оценивать близость генерируемой последовательности к истинно случайной.

Таким образом, генератор randu, хэш-функции CRC32, SHA и SHA512 не проходят статистический тест на однородность и не могут использоваться в качестве генератора последовательностей случайных чисел, только генератор mt19937 (вихрь Мерсенна) успешно прошёл и графические и статистические тесты на однородность.

Библиографический список

1. Аتماшкин, М. И. Исследование генераторов псевдослучайных последовательностей, построенных на основе хэш-функций / М. И. Аتماшкин, С. В. Белим // Математические структуры и моделирование. – 2009. – № 20. – С. 134-140. – EDN QLIZXL.

2. Григорьев, А. Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей / Григорьев, А. Ю. // Ученые записки УлГУ. Серия: Математика и информационные технологии. – 2017. – № 1. – С. 22-28.

3. Дональд Кнут. Искусство программирования, том 2. Получисленные алгоритмы (The Art of Computer Programming, vol.2. Seminumerical Algorithms.) – 3-е изд. – М.: «Вильямс», 2018. – С. 832. – ISBN 5-8459-0081-6.

4. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

5. Методы генерации и тестирования случайных последовательностей/ М. Б. Будько, М. Ю. Будько, А. В. Гирик, В. А. Грозов. – Санкт-Петербург: Университет ИТМО, 2019. – 70 с.

6. Слеповичев И.И. Генераторы псевдослучайных чисел. – Саратов: СГУ, 2017. – 118 с.

Д.И. Шашков, М.И. Дроботенко ФИЗИКО-МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА СИНТЕЗА НАНОЧАСТИЦ СЕРЕБРА

В статье рассматривается физико-математическая модель процесса синтеза наночастиц серебра методом кавитационно-диффузионного фотохимического восстановления. Исследовано влияние мощности ультрафиолетового излучения на скорость синтеза наночастиц. Установлено, что при уменьшении мощности УФ излучения увеличивается общая длительность синтеза наночастиц серебра. Также уменьшается скорость самих химических реакций из-за уменьшения количества OH^\cdot и, как следствие, уменьшения концентрации e^- .

Ключевые слова: наночастицы серебра, синтез, математическое моделирование, ультрафиолет.

The article considers a physical and mathematical model of the synthesis of silver nanoparticles by the method of cavitation-diffusion photochemical reduction. The influence of the power of ultraviolet radiation on the rate of nanoparticle synthesis has been studied. It has been established that with a decrease in the power of UV radiation, the total duration of the synthesis of silver nanoparticles increases. Also, the rate of the chemical reactions themselves decreases due to a decrease in the amount of OH- and, as a result, a decrease in the concentration of e-. Keywords: silver nanoparticles, synthesis, mathematical modeling, ultraviolet.

В последние годы значительно выросло производство и использование металлических наночастиц. В частности, серебряные наночастицы нашли широкое применение в медицине для диагностики, доставки лекарств, лечения раковых заболеваний. Это обусловлено свойствами подобных наночастиц, в связи с чем благодаря их высокой активности они все шире используются для придания антимикробных свойств раневым повязкам, шовному материалу, различным медицинским полимерам[1]. Необходимо учитывать, что свойства синтезируемых наночастиц будут различаться в зависимости от условий их синтеза, физико-химических свойств используемых веществ [2]. Определение оптимальных условий синтеза, для получения наночастиц с определенными свойствами является актуальной задачей, возможности математического моделирования и численного эксперимента позволяют решить данную задачу.

Для описания процесса синтеза наночастиц серебра была разработана физико-математическая модель метода кавитационно-диффузионного фотохимического восстановления [3], при этом был сделан ряд упрощений: температура постоянна, все параметры усреднены по пространству (зависимость от пространственных переменных не рассматривается).

Уравнение для описания зависимости концентрации ионов H^+ от времени:

$$\frac{\partial}{\partial t} n_{H^+}(t) = K_D n_{H_2O}(t) + K_{hv} n_{H_2O}(t) n_{hv}(t) - K_R n_{H^+}(t) n_{OH^-}(t) - K_e n_{AgNH_3}(t) n_e(t) n_{H^+}(t).$$

$$\frac{\partial}{\partial t} n_{H^+} + K_D n_{H_2O} + K_{hv} n_{H_2O} n_{hv} - K_R n_{H^+} n_{OH^-} - K_e n_{AgNH_3} n_e n_{H^+}$$

Уравнение для описания зависимости концентрации ионов OH^- от времени:

$$\frac{\partial}{\partial t} n_{OH^-}(t) = K_D n_{H_2O}(t) + K_{hv} n_{H_2O}(t) n_{hv}(t) - K_R n_{H^+}(t) n_{OH^-}(t) - 4K_{OH} n_{OH^-}(t).$$

$$\frac{\partial}{\partial t} n_{OH^-} = K_D n_{H_2O} + K_{hv} n_{H_2O} n_{hv} - K_R n_{H^+} n_{OH^-} - 4K_{OH} n_{OH^-}.$$

Уравнение для описания зависимости концентрации электронов e^- от времени:

$$\frac{\partial}{\partial t} n_e(t) = 4K_{OH}n_{OH^-}(t) - K_e n_{AgNH_3}(t)n_e(t)n_{H^+}(t).$$

$$\frac{\partial}{\partial t} n_e = 4K_{OH}n_{OH^-} - K_e n_{AgNH_3} n_e n_{H^+}.$$

Уравнение для описания зависимости концентрации аммиачного комплекса $[Ag(NH_3)_2]OH$ от времени:

$$\frac{\partial}{\partial t} n_{AgNH_3}(t) = -K_e n_{AgNH_3}(t)n_e(t)n_{H^+}(t).$$

$$\frac{\partial}{\partial t} n_{AgNH_3} = -K_e n_{AgNH_3} n_e n_{H^+}.$$

Уравнение для описания зависимости концентрации атомов серебра Ag^0 от времени:

$$\frac{\partial}{\partial t} n_{Ag^0}(t) = K_e n_{AgNH_3}(t)n_e(t)n_{H^+}(t) - 2K_{Ag_2}n_{Ag^0}^2(t).$$

$$\frac{\partial}{\partial t} n_{Ag^0} = K_e n_{AgNH_3} n_e n_{H^+} - 2K_{Ag_2}n_{Ag^0}^2.$$

Уравнение для описания зависимости концентрации димеров Ag_2 от времени:

$$\frac{\partial}{\partial t} n_{Ag_2}(t) = K_{Ag_2}n_{Ag^0}^2(t).$$

$$\frac{\partial}{\partial t} n_{Ag_2} = K_{Ag_2}n_{Ag^0}^2.$$

где:

n_{H_2O} - концентрация воды (количество на единицу объема, соответствующее 100%-й концентрации);

n_{H^+} - концентрация ионов H^+ в воде;

n_{OH^-} - концентрация ионов OH^- в воде;

n_{hv} - концентрация УФ-квантов;

n_e - концентрация электронов;

n_{AgNH_3} - концентрация аммиачного комплекса $[Ag(NH_3)_2]OH$;

n_{Ag} - концентрация атомов серебра Ag ;

n_{Ag_2} - концентрация димеров серебра Ag_2 .

K_D - константа диссоциации воды при заданной температуре;

K_R - константа рекомбинации воды при заданной температуре;

K_{hv} - константа диссоциации воды при поглощении фотона;

K_{OH} - константа рекомбинации ионов OH^- ;

K_e - константа поглощения электронов;

K_{Ag_2} - константа образования димеров серебра Ag_2 .

Задача 1-12 была решена с помощью стандартных численных методов, в частности методом Рунге-Кутты первого порядка. Для вычислений

использовалась программа, разработанная авторским коллективом (свидетельство о регистрации № 2023664915).

С помощью описанной выше физико-математической модели процесса кавитационно-диффузионного фотохимического восстановления были получены графики зависимости концентрации аммиачного комплекса, атомарного серебра и димеров серебра от времени (рисунки 1-4) при различной величине ультрафиолетового излучения. Значение 1 интенсивности УФ излучения соответствует величине 5850 люкс.

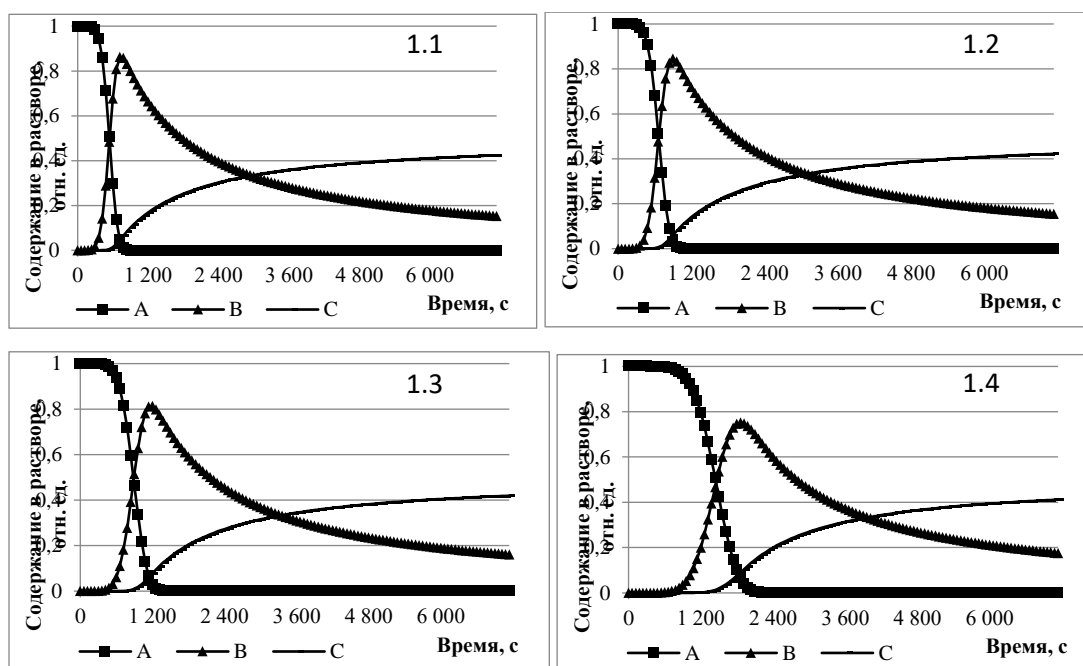


Рис. 1. Зависимость концентрации от времени при изменении интенсивности УФ излучения

Примечание: 1.1 – при 1 интенсивности УФ; 1.2 – при 0,75 интенсивности УФ; 1.3 – при 0,5 интенсивности УФ; 1.4 – при 0,25 интенсивности УФ; А – Зависимость концентрации аммиачного комплекса от времени; В – Зависимость концентрации атомарного серебра от времени; С – Зависимость концентрации димеров серебра от времени)

Из рисунка 1.1 видно, что процесс восстановления серебра происходит быстро, концентрация аммиачного комплекса (А) падает до нуля в первые 15 минут синтеза, это означает, что все серебро в растворе перешло в атомарную форму. Концентрация атомарного серебра (В) вначале резко возрастает, до момента падения концентрации аммиачного комплекса до нуля, а затем плавно снижается в процессе формирования наночастиц. Концентрация димеров серебра (С) и, как следствие, наночастиц серебра практически не растет до момента насыщения раствора атомарным серебром. В дальнейшем при снижении концентрация атомарного серебра (В), процесс формирования наночастиц практически останавливается.

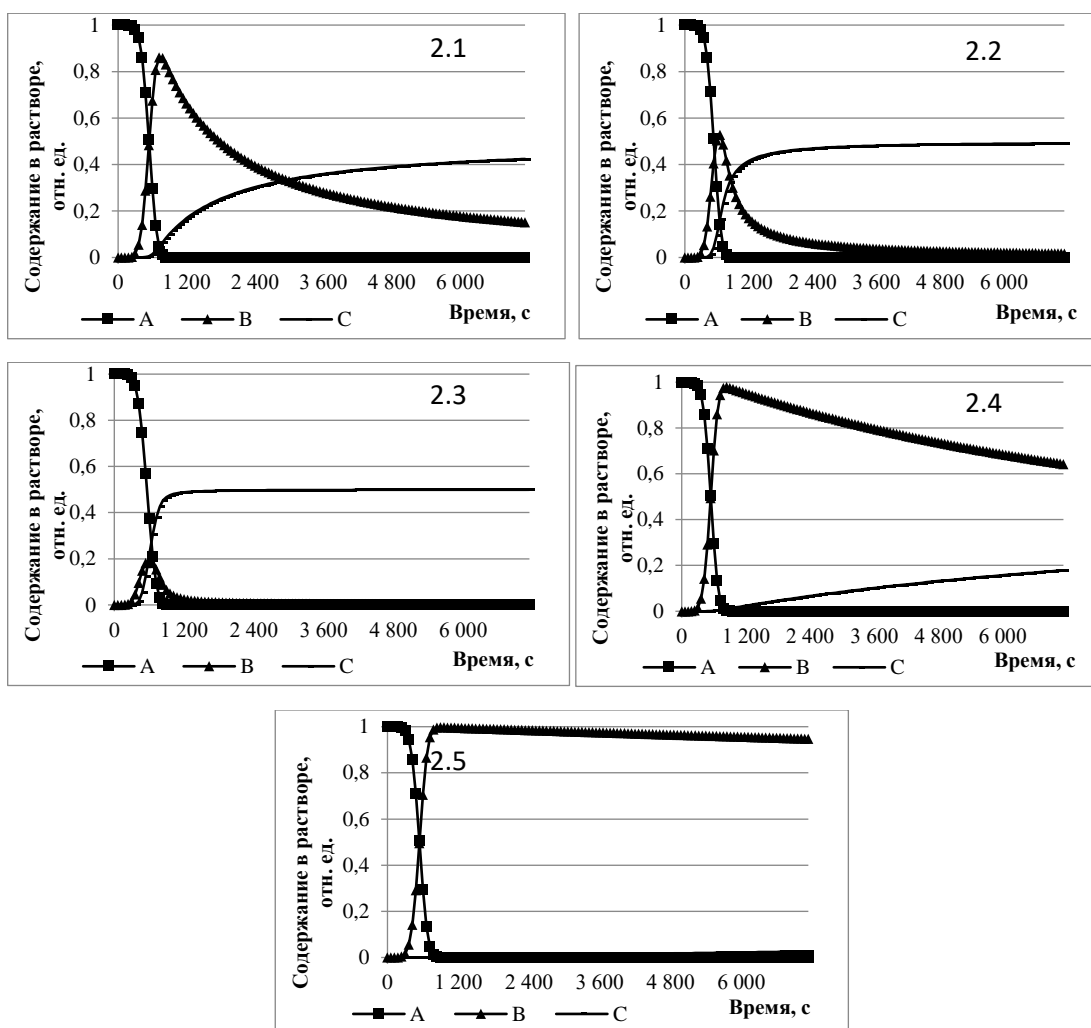


Рис. 2. Зависимость концентрации наночастиц от времени при изменении концентрации аммиачного комплекса серебра

Примечание: 2.1 – при исходной концентрации; 2.2 – при увеличении исходной концентрации в 10 раз; 2.3 – при увеличении исходной концентрации в 100 раз; 2.4 – при уменьшении исходной концентрации в 10 раз; 2.5 – при уменьшении исходной концентрации в 100 раз; А – Зависимость концентрации аммиачного комплекса от времени; В – Зависимость концентрации атомарного серебра от времени; С – Зависимость концентрации димеров серебра от времени).

Из рисунков 2.1-2.5 видно исходная концентрация аммиачного комплекса оказывает различное воздействие на процесс формирования наночастиц серебра. Кроме того, она вызывает увеличение вероятности взаимодействия частиц и как следствие скорость формирования синтезируемых частиц. Уменьшение концентрации приводит к резкому увеличению времени синтеза наночастиц серебра.

Разработанная физико-математическая модель позволит исследовать и улучшить процесс синтеза наночастиц серебра, применяемых для придания шовным материалам антисептических свойств, в том числе в отношении возбудителей бактериальных инфекций. Кроме того, перспективным направлением применения подобных наночастиц может являться разработка раневых покрытий на основе волокон из различных материалов, обработанных раствором, содержащим наночастицы серебра, полученные методом кавитационно-диффузионного фотохимического восстановления. При синтезе наночастиц данным методом более половины наночастиц имеют диаметр до 5 нм, что будет способствовать разрушению биопленок, сформированных на поверхности инфицированных ран.

Работа выполнена при финансовой поддержке государственного задания Минобрнауки Кубанскому государственному университету (FZEN-2023-0006).

Библиографический список

1. Джимаков С.С., Малышко В.В., Горячко А.И., Соколов М.Е., Басов А.А., Моисеев А.В., Шашков Д.И., Копытов Г.Ф., Барышев М.Г., Исаев В.А. / Сорбционная активность наночастиц серебра // Известия вузов. Физика. 2019. Т. 62. № 2 (734). С. 114-122.

2. Шашков Д.И., Копытов Г.Ф., Малышко В.В., Лыкова А.В., Моисеев А.В., Демин Н.Н., Джимаков С.С., Барышев М.Г. / Влияние циклической заморозки на динамику нанокластеров серебра на поверхности полипропиленовых и полиэфирных волокон // Известия вузов. Физика. 2022. Т. 65. № 2 (771). С. 121-125.

3. Малышко В.В., Джимаков С.С., Ломакина Л.В., Басов А.А., Шашков Д.И. Способ повышения количества и антибактериальной активности наночастиц серебра на шовном материале из шелка. Патент на изобретение 2770277 С1, 15.04.2022. Заявка № 2021125044 от 23.08.2021.

СЕКЦИЯ 4. Междисциплинарные проблемы подготовки специалистов

В.Ю. Барсукова, А.В. Бочаров, М.В. Цалюк О ПРОБЛЕМАХ ПРЕПОДАВАНИЯ ДИСЦИПЛИНЫ «ФУНКЦИОНАЛЬНЫЙ АНАЛИЗ» НА ФАКУЛЬТЕТЕ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ НАУК КУБГУ

Раскрываются проблемы преподавания дисциплины «Функциональный анализ», предлагаются пути решения имеющихся проблем, обобщается имеющийся опыт преподавания данной дисциплины в Кубанском государственном университете.

Ключевые слова: функциональный анализ, проблемы преподавания.

The problems of teaching the discipline “Functional Analysis” are revealed, ways to solve existing problems are proposed, and the existing experience of teaching this discipline at Kuban State University is generalized.

Key words: functional analysis, teaching problems.

Дисциплина функциональный анализ, наравне с математическим анализом, алгеброй, комплексным анализом и др., является дисциплиной первого уровня для получения фундаментальной подготовки студентами математических направлений. К тому же, приложения функционального анализа находят применения в различных областях науки, в частности, в достаточно популярной и бурно растущей сегодня сфере машинного обучения, нейронных сетей и искусственного интеллекта. В связи с этим становится острым вопрос получения студентами в должном объеме необходимых компетенций по дисциплине функциональный анализ.

Можно отметить несколько важных аспектов, затрудняющих освоение студентами указанной выше дисциплины. Во-первых, в последние годы, несмотря на относительно неплохие баллы ЕГЭ по математике поступающих на факультет, реальный общий уровень математической подготовки неуклонно снижается, старшеклассников в школе прежде всего натаскивают на задачи ЕГЭ, а некоторые темы, которые должны изучаться в рамках школьного курса математики, но не входят в КИМы единого госэкзамена, часто учителями просто игнорируются. Почти все поступающие на факультет абитуриенты практически не имеют навыков доказательств математических утверждений.

Во-вторых, к сожалению, студент слабо мотивирован к изучению данной дисциплины, он считает ее теоретической и не понимает какой сильный инструмент с точки зрения приложений получает в результате ее освоения.

Особенно это относится к студентам, обучающимся на направлении «Математика и компьютерные науки», которые видят себя в будущем разработчиками ПО и другими специалистами в IT сфере.

Наконец, в связи с тем, что в государственных стандартах ФГОС 3++ отсутствуют требования к количеству часов аудиторной нагрузки, в соответствии с локальными актами КубГУ произошло их постепенное снижение с 32 академических часов до 26 часов в неделю. Это повлекло за собой сокращение объема лекционных часов, в том числе и по математическим дисциплинам. Также, в связи с пересмотром режима занятий студентов уменьшен и сам академический час с 45 минут до 40 минут. Данное сокращение негативно сказывается на очном обучении.

Анализ учебных планов других ВУЗов, реализующих направления подготовки 01.03.01 «Математика» и 02.03.01 «Математика и компьютерные науки» показал, что дисциплина функциональный анализ традиционно изучается на 3 курсе. Ее продолжительность от одного до трех семестров. Объем лекционных и семинарских часов сильно различается. Так, в Воронежском государственном университете для направления подготовки 01.03.01 «Математика» предусмотрено 34 часа лекций и 102 часа семинарских занятий в течении трех семестров, а для того же направления в Южном федеральном университете – 54 часа лекций и всего 18 часов семинарских занятий, курс длится один семестр. В КубГУ в настоящее время на направлении 01.03.01 «Математика» на изучение функционального анализа за два семестра отведено 66 лекционных часов и 66 часов семинарских занятий, на направлении 02.03.01 «Математика и компьютерные науки» – за 2 семестра 50 часов лекций и 52 часа семинарских занятий, для специальности 01.05.01 «Фундаментальная математика и механика» – 52 часа лекций и 68 часов лабораторных занятий в течение двух семестров.

Таким образом, возникают следующие противоречия: между слабой школьной базой студентов математического факультета и высокими требованиями стандарта к пониманию материала; между относительно небольшим количеством академических часов и требованиями к получению необходимых для дальнейшего применения компетенций в полном объеме, а также, между проявлением изначально слабой заинтересованности студентов в изучении данной теоретической дисциплины и реальной картиной приложений ее после полного освоения курса.

Наиболее критичной в последние годы представляется ситуация с получением компетенций, связанных с основным, присущим именно математикам, умением аргументированно доказывать. Следуя структуре учебных планов для всех образовательных программ, реализуемых на факультете, предполагается, что за первые два года обучения в ВУЗе студент, регулярно тренируя это умение на основных математических предметах, к третьему курсу уже готов к освоению такого непростого теоретического и абстрактного курса, как функциональный анализ. И так до определенного момента и

было. В последнее же время наши студенты зачатую впервые сталкиваются с доказательными рассуждениями на лекциях первого года обучения и, естественно, двух лет им никак не хватает. Они слабо понимают, что значит разобрать доказательство, некоторые учат их как стихи, наизусть. И если, например, в математическом анализе или линейной алгебре это в некоторой мере нивелируется более понятным и привычным материалом, то в функциональном анализе возникает множество проблем.

За время работы в дистанционном формате у нас накопились некоторые видеозаписи лекций, и мы предложили их студентам в качестве дополнительного материала для учебы. Для тех, кто не был на лекции, например. Через некоторое время студенты стали спрашивать, нет ли у нас записей и по другим темам тоже. Это привело к мысли о том, что даже присутствующие на лекции студенты в основном сосредоточены на том, чтобы все записать, а не на том, чтобы понять. А когда доходит очередь до понимания, нужная лекция была уже в далеком прошлом и все, сказанное лектором в комментариях, прочно забыто.

Еще одной причиной возникающих сложностей является их неумение читать учебники. Эта проблема является всеобъемлющей и тянется еще из начального школьного образования. Дети, выросшие в период широкого распространения гаджетов, перестали воспринимать и понимать печатный текст. Поэтому, попытка компенсировать отсутствующие лекционные часы, просто вынося некоторые темы на самостоятельное изучение, не приведет к успеху.

Наших студентов нужно учить читать учебники грамотно, разбирая не только то, что написано, но и то, что авторы посчитали очевидным или простым и не прописали явно, подразумевая определенный уровень математической грамотности читающего. В связи с этим мы решили дополнительно к основной, аудиторной форме обучения реализовать интерактивный курс «Читаем функциональный анализ вместе». Это будет несколько видеоуроков, каждый из которых будет содержать разбор доказательства одной теоремы из курса. К каждому видеоуроку прилагается список основных понятий и теорем, которые необходимо повторить для изучения данной темы. Это позволит студенту продуктивно подготовиться к восприятию материала, освежив в памяти необходимую теорию. На каждом видеоуроке предполагается рассказывать студентам как читать то или иное доказательство из какого-либо учебника, например [1, 2]. Не будучи ограничен временем лекционного занятия, преподаватель может рассказывать не только само доказательство, но и его идею, структуру, помочь студентам понять, как его разобрать и выучить. Поскольку это не печатный текст, а живая, не книжная, подача материала, возможно, он будет восприниматься студентами лучше. Более того, поделенный на маленькие части курс, позволяет работать с ним в удобное время, в наиболее доступной для сегодняшней молодежи форме.

Отметим, что эта форма обучения может рассматриваться только как дополнительная, но никак не как основная, поскольку, при таком обучении очень слабой является обратная связь. Поэтому в комплекте с ним в обязательном порядке должны идти консультативные часы, на которых в очном формате студенты могут задать вопросы преподавателю или даже попытаться самостоятельно воспроизвести доказательство, отвечая на вопросы своих однокурсников и преподавателя как на экзамене.

Этот курс призван помочь студентам заполнить вынужденные пробелы при классическом лекционном варианте подачи материала, вызванные дефицитом аудиторных часов, а также научить и приучить их добывать знания самостоятельно. Преподаватель же будет иметь возможность (вне необходимости объять необъятное) обсуждать со студентами на лекциях основные понятия курса, для лучшего понимания иллюстрируя их примерами.

Любой лекционный материал требует подкрепления на семинарских занятиях, и здесь имеется еще одна сложность. Существующие классические задачки относятся к 60-70 годам прошлого века и содержат, в основном, теоретические задачи высокого уровня сложности. В них мало простых задач и упражнений на отработку базовых определений и понятий функционального анализа. Еще в 1980 году профессором Цалюком З.В. и доцентом Пуляевым В.Ф. на кафедре был создан задачник по функциональному анализу, адаптированный под содержание курса, читаемого авторами в то время. К 2010 году задачник был доработан, переиздан [3] и все эти годы активно использовался в учебном процессе. Однако и он не в полной мере удовлетворяет текущему уровню математической подготовки студентов.

Для решения этой проблемы в 2022 году на кафедре был издан практикум по функциональному анализу (авторы Барсукова В.Ю., Бочаров А.В., Солодкова С.С., Цалюк М.В.) [4]. Практикум включает основные разделы, отвечающие классическому курсу функционального анализа. Сборник содержит задачи и упражнения по следующим темам: линейные нормированные пространства, гильбертовы пространства, линейные непрерывные операторы, принцип сжимающих отображений, обратимые операторы, спектр, а также линейные интегральные уравнения Фредгольма. Каждая тема имеет сводку теоретических фактов, необходимых при решении задач, к каждому типу заданий приведены подробные решения, что облегчает процесс самостоятельного изучения. Каждая задача приводится в 20 вариантах примерно одинакового уровня сложности, что студенту позволяет тренироваться в решении основных типов задач, а преподавателю – использовать сборник для составления контрольных работ и индивидуальных заданий. Практикум был апробирован в учебном процессе в отдельных группах, изучающих функциональный анализ. Его использование позволило в некоторой степени поднять минимальный уровень освоения основных понятий дисциплины.

Таким образом, учитывая потребность в математически грамотных специалистах, в том числе и для цифровых отраслей, современному образованию приходится адаптироваться к реалиям времени, менять подходы к обучению и технологиям подачи материала, стараясь при этом не потерять в математической строгости изложения.

Библиографический список

1. Колмогоров, А. Н. Элементы теории функций и функционального анализа: учебное пособие / А. Н. Колмогоров, С. В. Фомин. – М.: ФИЗМАТЛИТ, 2009. – 572 с.
2. Цалюк З.Б., Цалюк М.В. Функциональный анализ. – Краснодар: Просвещение-Юг, 2014. – 79 с.
3. Цалюк З.Б., Пуляев В.Ф. Сборник задач по функциональному анализу. – М. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2010 – 152 с. ISBN 978-5-93972-828-7.
4. Функциональный анализ: практикум/ авторы: В.Ю. Барсукова, А.В. Бочаров, С.С. Солодкова, М.В. Цалюк; – Краснодар: Кубанский гос. ун-т, 2022. – 168 с. ISBN 978-5-8209-2185-8.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный университет»
Факультет математики и компьютерных наук

Уважаемые коллеги!

Приглашаем Вас принять участие во Всероссийской
научно - практической конференции

**«МАТЕМАТИЧЕСКИЕ МЕТОДЫ И МОДЕЛИ В РЕШЕНИИ
ПРИКЛАДНЫХ ЗАДАЧ»**

Цели конференции: обмен опытом между ведущими специалистами отрасли, образовательными организациями высшего образования, дополнительного профессионального образования по вопросам развития, внедрения и модернизации математических методов, моделей, систем искусственного интеллекта.

НАПРАВЛЕНИЯ РАБОТЫ КОНФЕРЕНЦИИ:

Секция 1. Инженерное дело, робототехника и искусственный интеллект.

Секция 2. Экономика и социальная сфера. Задачи цифровизации в современном обществе.

Секция 3. Естественнонаучные задачи и альтернативные направления исследований.

Секция 4. Междисциплинарные проблемы подготовки специалистов

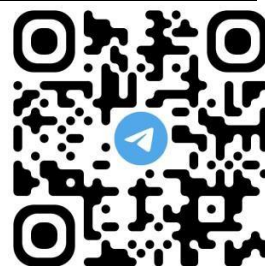
Круглый стол. Актуальные вопросы организации научно-исследовательской работы учебного заведения.

ОРГКОМИТЕТ:

Эл.почта: conference.fmcs@gmail.com.

Телеграмм-канал конференции:

<https://t.me/+MIPaEZ9ungNiYTgy>.



Для заметок

Для заметок

Для заметок

Для заметок

Научное издание

**МАТЕМАТИЧЕСКИЕ МЕТОДЫ И МОДЕЛИ
В РЕШЕНИИ ПРИКЛАДНЫХ ЗАДАЧ**

Материалы
Всероссийской научно-практической конференции

Публикуются в авторской редакции

Подписано в печать _____.____.2023. Выход в свет

Формат 60 × 84 1/16.

Уч.-изд. л. 7,2. Тираж 500 экз. Заказ №

Кубанский государственный университет
350040, г. Краснодар, ул. Ставропольская, 149

Издательско-полиграфический центр
Кубанского государственного университета
350040, г. Краснодар, ул. Ставропольская, 149

