№5-2020

ISSN 1999-9429

ИЗВЕСТИЯ ЮФУ

ТЕХНИЧЕСКИЕ НАУКИ

- Алгоритмы обработки информации
- Моделирование процессов, устройств и систем
- Информационный анализ

ИЗВЕСТИЯ ЮФУ. ТЕХНИЧЕСКИЕ НАУКИ
IZVESTIYA SFedU. ENGINEERING SCIENCES

Свидетельство о регистрации средства массовой информации
ПИ № ФС77-28889 от 12.07.2007
Научно-технический и прикладной журнал
Издается с 1995 года, до середины 2007 года под названием «Известия ТРТУ»
Подписной индекс 41970

№ 5 (215). 2020 г.

Журнал включен в «Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук».

Учредитель Южный федеральный университет.
Издатель Южный федеральный университет.
Ответственный за выпуск Самойлов А.Н.
Технический редактор Ярошевич Н.В.
Оригинал-макет выполнен Ярошевич Н.В.

Подписано к печати . Формат $70\times108\,{}^{1}\!/_{16}$. Бумага офсетная.

Офсетная печать. Усл. печ. л. – 16,9. Уч.-изд. л. – 14,5.
Заказ № . Тираж 250 экз.

Адрес издателя: 344091, г. Ростов-на-Дону, пр. Стачки, 200/1. Тел. 8(863)2478051.

Адрес типографии: Отпечатано в отделе полиграфической, корпоративной и сувенирной продукции Издательско-полиграфического комплекса КИБИ МЕДИА ЦЕНТРА ЮФУ. 344090, г. Ростов-на-Дону, пр. Стачки, 200/1, тел. 8 (863) 247-80-51.

Адрес редколлегии: 347922, г. Таганрог, ул. Чехова, 22, ЮФУ, тел. +7 (928) 909-57-82, e-mail: iborodyanskiy@sfedu.ru, http://izv-tn.tti.sfedu.ru/.

16+ Цена свободная

ISSN 1999-9429 (Print)
ISSN 2311-3103 (Online)

СОДЕРЖАНИЕ

РАЗДЕЛ I. АЛГОРИТМЫ ОБРАБОТКИ ИНФОРМАЦИИ

РАЗДЕЛ II. МОДЕЛИРОВАНИЕ ПРОЦЕССОВ, УСТРОЙСТВ И СИСТЕМ

РАЗДЕЛ III. ИНФОРМАЦИОННЫЙ АНАЛИЗ

CONTENT

SECTION I. INFORMATION PROCESSING ALGORITHMS

SECTION II. PROCESS MODELING, DEVICES AND SYSTEMS

SECTION III. INFORMATION ANALYSIS

Раздел I. Алгоритмы обработки информации

УДК 004.056.55 DOI 10.18522/2311-3103-2020-5-6-16

Л.К. Бабенко, А.С. Шумилин, Д.М. Алексеев

АЛГОРИТМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ХРАНЕНИЯ И ОБРАБОТКИ РЕЗУЛЬТАТОВ ОБСЛЕДОВАНИЙ*

Цели исследования состоят в разработке и оценке эффективности структуры облачной платформы хранения, обработки и систематизации медицинских данных, определении метода защиты, в частности, обеспечения конфиденциальности при передаче и хранении результатов обследований. Для достижения поставленной цели решаются задачи анализа существующих моделей информационных процессов и структур в предметной области, особенности средств накопления и обработки медицинских данных, хранящихся в электронных информационных системах учёта пациентов, разрабатывается архитектура облачной платформы распределенного хранения данных и алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде в форме исходных физиологических сигналов (ЭЭГ, ЭКГ, ЭМГ, ЭОГ и т.д.), регистрируемых при проведении обследований пациентов; создается интегрируемая облачная платформа распределенного хранения, анализа и систематизации медицинских данных и система обеспечения безопасности с использованием разработанного метода защиты; анализируется эффективность предложенного алгоритма защиты конфиденциальной медицинской информации в условиях интеграции в разработанную облачную платформу. Предлагаемый способ защиты медицинской информационной системы подразумевает использование исходного файла формата DICOM и впоследствии преобразованного изображения в формате PNG, которое подвергается алгоритму шифрования пикселей. Для шифрования изображения применяется алгоритм на основе теории хаоса. Возможности систем хаоса позволяют значительно повысить производительность. Иерархичное разделение потоков данных на уровни и стандартизация протоколов передачи данных, а также форматов их хранения позволяют сформировать универсальную, гибкую и надежную медицинскую информационную систему. Предлагаемая архитектура имеет возможность интеграции в существующие медицинские системы. В ходе работы установлено, что рассматриваемый метод защиты является эффективным способом обеспечения конфиденциальности данных медицинской системы.

Шифрование; медицинская информационная система; конфиденциальность; облачные вычисления; информационная безопасность; обработка данных; систематизация данных; большие данные.

L.K. Babenko, A.S. Shumilin, D.M. Alekseev

ALGORITHM OF ENSURING THE SECURITY OF CONFIDENTIAL DATA OF THE MEDICAL INFORMATION SYSTEM FOR STORAGE AND PROCESSING OF EXAMINATION RESULTS

The objectives of the study are to develop and assess the effectiveness of the structure of a cloud platform for storing, processing and organizing medical data, determining a method of protection, in particular, ensuring confidentiality when transferring and storing examination results. To achieve this goal, the tasks of analyzing existing models of information processes and structures in the subject area are being solved, the features of the means for accumulating and pro-

* Работа выполнена при финансовой поддержке РФФИ в рамках проекта № 20-37-90138 – аспиранты.

cessing medical data stored in electronic information systems for patient registration, the architecture of a cloud platform for distributed data storage and an algorithm for ensuring the safety of medical data stored in the cloud are being developed. the platform in electronic form in the form of initial physiological signals (EEG, ECG, EMG, EOG, etc.) recorded during patient examinations; an integrated cloud platform for distributed storage, analysis and systematization of medical data and a security system using the developed protection method are being created; the effectiveness of the proposed algorithm for protecting confidential medical information is analyzed in the context of integration into the developed cloud platform. The proposed method for protecting a medical information system involves the use of an original DICOM file and subsequently a converted PNG image, which is subjected to a pixel encryption algorithm. An algorithm based on chaos theory is used to encrypt the image. The capabilities of chaos systems can significantly increase productivity. Hierarchical division of data streams into levels and standardization of data transfer protocols, as well as their storage formats, allow to form a universal, flexible and reliable medical information system. The proposed architecture has the ability to integrate into existing medical systems. In the course of the work, it was found that the considered protection method is an effective way to ensure the confidentiality of medical system data.

Encryption; medical information system; privacy; cloud computing; information security; data processing; systematization of data; big data.

Введение. В век всеобщей информатизации и активного развития информационных технологий медицинские учреждения в ходе выполнения диагностических исследований обрабатывают и систематизируют значительные объемы данных для последующей реабилитации и лечения пациентов. Эффективность оказываемой медицинской помощи прямо пропорциональна оперативности и удобству использования данной информации специалистами медицинских организаций. Наличие задач, связанных с хранением, систематизацией и обработкой увеличивающихся объемов данных обуславливает актуальность разработки и интеграции в медицинские учреждения медицинских информационных систем (МИС). Возможность оперирования данными в электронном виде обеспечивает оперативность получения врачом необходимой информации о пациенте, что увеличивает скорость принятия решения о постановке диагноза и методах лечения [1].

Одним из актуальных направлений в области разработки и реализации систем хранения, систематизации и обработки медицинских данных является использование возможностей облачных сервисов.

Основной целью реализации облачной платформы является создание единого информационного пространства для сбора, хранения и предоставления результатов медицинских исследований, с использованием распределенной команды квалифицированных медицинских специалистов. К категории медицинских исследований относятся результаты медицинских исследований, проведенных с использованием диагностического оборудования различных производителей.

Полученные данные могут использоваться как медицинскими учреждениями, так и научно-исследовательскими организациями. Пациент может предоставлять результаты собственных медицинских исследований другим пользователям облачной платформы или группам квалифицированных медицинских специалистов. Данные могут быть использованы медицинским персоналом, который оказывает комплекс услуг по их исследованию, анализу или экспертизе, после чего предоставляет результаты исследований.

Анализ проблемы. Медицинские организации в силу законодательства являются операторами персональных данных своих пациентов. Они принимают непосредственное участие в сборе, систематизации, накоплении, хранении, уточнении, обновлении, изменении, распространении и уничтожении такой информации.

Одной из проблем при проектировании медицинских информационных систем является необходимость интеграции механизмов защиты конфиденциальной информации. К категории конфиденциальной информации относят: фамилия, имя,

отчество пациента, месяц, дата и место рождения, серия и номер паспорта, адрес регистрации и фактического проживания, идентификационный номер налогоплательщика (ИНН), страховое свидетельство государственного пенсионного страхования (СНИЛС), семейное, социальное положение, образование, профессия, должность, специальность, серия и номер страхового медицинского полиса и его действительность и др. В связи с тем, что данная категория информации представляет собой, как правило, текстовую форму, ее защита обеспечивается стандартными методами и средствами шифрования [19, 20]. К категории персональных медицинских данных, требующих нетрадиционных подходов к их защите, относят результаты медицинских обследований пациентов, хранящихся в форме сигналов (например, сигналов электроэнцефалограммы).

Постановка задачи. В связи с тем, что требованиями законодательства установлена необходимость защиты персональных данных, ключевой задачей при реализации облачной системы хранения, систематизации и обработки медицинских данных является обеспечение безопасности хранимой информации. В рамках работы цель исследований заключается в разработке и оценке эффективности общей схемы облачной платформы, обеспечивающей выполнение определенного спектра задач, а также в выборе способа обеспечения защиты медицинских данных пациентов, в частности, обеспечения защиты результатов обследований, хранимых в электронном виде в форме сигналов ЭЭГ. **Целью работы** является повышение эффективности работы систем безопасности (блокировки злоумышленных действий) при хранении, систематизации и передаче информации в распределённых медицинских системах, имеющих облачную архитектуру.

Для достижения указанной цели в рамках работы необходимо решить следующие **задачи**:

- ♦ разработать архитектуру облачной платформы распределенного хранения данных, позволяющую взаимодействовать с различными аппаратными системами для проведения медицинских обследований;
- ♦ разработать алгоритм обеспечения безопасности медицинских данных, хранимых в облачной платформе в электронном виде в форме исходных физиологических сигналов (ЭЭГ, ЭКГ, ЭМГ, ЭОГ и т.д.), регистрируемых при проведении обследований пациентов;
- ♦ проанализировать эффективность предложенного алгоритма защиты конфиденциальной медицинской информации в условиях интеграции в разработанную облачную платформу.

Анализ современного состояния исследований. В работе [11] Котяшичев И.А. и Бырылова Е.А. рассматривают возможность использования облачных технологий с целью повышения эффективности внедрения информационных систем в различные отрасли медицины. Среди наиболее распространённых способов обеспечения безопасности данных авторы выделяют шифрование. Однако в ходе работы отмечается неотъемлемая проблема симметричных систем шифрования – проблема распределения ключей, что осложняет процесс работы с такими системами. Проблема заключается в том, что хранение ключей на облачном сервере нецелесообразно, поскольку пользователь, имеющий доступ к облачным серверам, получает доступ к ключу, а следовательно, и к расшифрованным данным.

Керейтова М.Р. и Малыш В.Н. в работе [12] отмечают проблему обеспечения информационной безопасности конфиденциальных данных пациентов как одну из наиболее важных при создании и проектировании медицинских информационных систем. Вопрос защиты информации рассматривается на примере распределенной информационной системы Департамента охраны здоровья населения Кемеровской области, охватывающей все лечебно-профилактические учреждения (ЛПУ) Кемеровской области. Авторы предлагают комплексный подход к решению проблемы:

ввести контроль за рабочими станциями на предмет необычно высокой активности, в полной мере использовать антивирусную защиту, следить за всеми обновлениями для имеющихся операционных систем, использовать многоуровневую аутентификацию пользователей, предполагающую использование USB-ключей, смарт-карт, паролей, файловых ключей. Однако предлагаемый авторами подход не учитывает механизмов обеспечения защиты данных в аспекте предотвращения их утечки и/или несанкционированного доступа при передаче и хранении информации в системах с архитектурой клиент-сервер. Таким образом, в рамках данной работы рассмотрены способы и средства, обеспечивающие защиту на уровне доступа к рабочим станциям пользователям системы, при этом не учтены

Бойченко И. В. в работе [13] отмечает важность проблемы реализации прав граждан в области защиты персональных данных пациентов. Автор рассматривает возможность использования медицинских информационно-аналитических центров в структуре здравоохранения, акцентируя внимание лишь на правовом и юридическом аспектах проблемы. Предварительный анализ, проведенный автором, позволяет сделать вывод о большом потенциале использования облачных технологий в решении задач современного здравоохранения. Однако для их повсеместного внедрения требуется грамотное техническое решение, направленное на разработку методов обеспечения безопасности передаваемой информации и конфиденциальности персональных данных пациентов.

В работе [14] Rohan Jathanna отмечает уязвимость облачных систем к атакам со стороны злоумышленников (DDoS-атаки, атаки с целью проникновения на сервер, несанкционированный доступ к базам данных). Для предотвращения потери доступа к конфиденциальным данным автор предлагает использовать возможности средств резервного копирования. Противодействие несанкционированному доступу достигается путём использования алгоритмов шифрования. Предлагаемые автором подходы имеют существенные недостатки. Система резервного копирования требует большого количества дополнительных вычислительных ресурсов и ресурсов памяти, а также обеспечения нового объекта защиты (ресурса с резервной копией). Эффективность используемых алгоритмов шифрования снижается в связи с наличием проблемы распределения ключей: необходимо предусмотреть возможность передачи ключа от клиента на сервер по защищенному каналу связи. Последствием компрометации ключа шифрования является потеря доступа к конфиденциальным данным [17].

В работе [15] Кривошеева Д.А. выделяет основные недостатки использование ассиметричных систем шифрования в медицинских облачных платформах: большие затраты вычислительных ресурсов, а также времени, которое требуется для реализации вычислительных процессов. Автор предлагает альтернативный подход к созданию симметричного ключа шифрования, основанный на использовании физиологического сигнала пациента в качестве «физиологической» подписи. Существенным недостатком предлагаемого метода является тот факт, что физиологические сигналы (электрокардиограмма, фотоплетизмограмма, электроэнцефалограмма и др.) могут изменяться в течение жизни человека. Соответственно, ключ шифрования, сформированный ранее, спустя определённое время может стать недействительным и, как следствие, доступ к персональным данным станет невозможен [16, 18].

Не менее важной проблемой предлагаемого метода видится возможность доступа к данным только со стороны их обладателя (пациента, который предоставил физиологический сигнал для формирования ключа шифрования). Таким образом, возможность получения доступа к результатам обследования другими лицами (например, лечащим доктором, родственниками пациента, аналитиком системы здравоохранения и др.) затрудняется или вовсе исключается.

Подводя итоги, стоит отметить, что в работах, доступных в открытом доступе в научной литературе и электронных библиотеках, имеются различные недостатки, основными из которых являются: проблема распределения ключей, высокие требования к вычислительным ресурсам, ресурсам времени и памяти. Предлагаемый в рамках текущего проекта подход направлен на исключение указанных выше недостатков за счет применения систем шифрования, ключевой особенностью которых является возможность реализации обработки зашифрованной информации без её расшифровки. К такой информации относятся конфиденциальные данные пациентов, представляющие собой результаты медицинских обследований, которые располагаются в глобальном хранилище на уровне хранения данных. Таким образом, появляется возможность производить вычисления с зашифрованными данными без их предварительного дешифрования.

Разработка платформы медицинской информационной системы. Для решения задачи хранения, систематизации и обработки медицинских данных разработана облачная платформа, общая схема которой представлена на рис. 1.

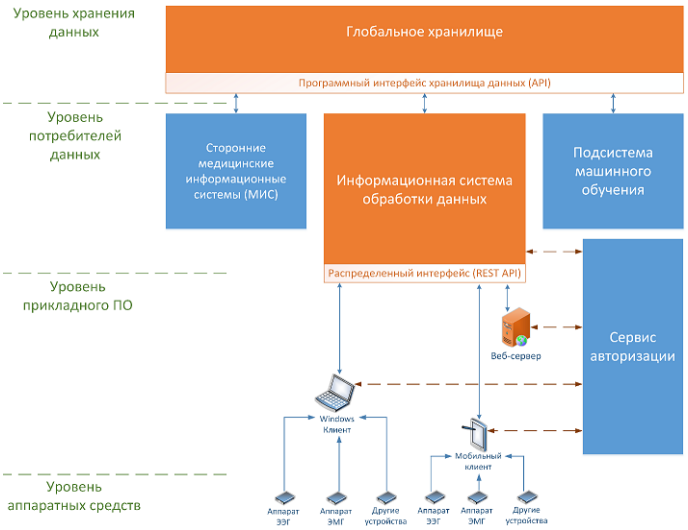

Рис. 1. Общая схема облачной платформы хранения, систематизации и обработки медицинских данных

Разработанная облачная система включает 4 основных уровня:

Уровень хранения данных: глобальное хранилище данных, которое включает в себя базу данных для хранения исходных данных обследований и отчетов, а также антропометрическая, диагностическая, демографическая информация о пациентах. Хранилище содержит полный объем информации для исследований и обучения машинных алгоритмов, но идентификация пациента возможна только по защищенному идентификатору.

Уровень потребителей данных – слой, включающий системы, которые принимают и обрабатывают данные из Глобального хранилища или передают в него новые данные. Этот уровень связан с уровнем хранения данных через стандартизированный программный интерфейс (Storage API). Потребителями данных могут быть: сторонние медицинские информационные системы; исследовательские системы; информационная система обработки данных – содержит базу персональных данных пациентов, соответствует требованиям безопасности и защиты персональных данных и медицинских данных (Федеральный закон РФ от 27 июля 2006 года

№ 152-ФЗ «О персональных данных»; Федеральный закон от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Health Insurance Portability and Accountability Act of 1996, HIPAA) [2]. Данный модуль обеспечивает взаимодействие с конечными клиентскими приложениями по средствам распределенного интерфейса (REST API).

Уровень прикладного ПО – уровень, содержащий программные средства конечных клиентов, где формируются и/или отображаются медицинские данные (обследования в виде сигналов, отчетные и персональные данные пациента): Windows клиенты – программное обеспечение для ОС семейства Windows; Вебсервер – предоставляет пользователю возможность доступа через web browser, в соответствии с назначенными этому пользователю ролями; Мобильный клиент – предоставляет доступ в информационную систему обработки данных используя мобильные устройства (Android, iOS).

Уровень аппаратных средств – физические устройства для проведения обследований. В общем случае могут быть различных видов: электроэнцефалографы, кардиографы, системы биологической обратной связи, носимые фитнес трекеры и т.д.

Экспериментальная часть. Реализация механизмов защиты при передаче данных медицинских обследований посредством облачной платформы. В ходе исследований была разработана МИС, одним из механизмов которой является обеспечение безопасности передаваемых медицинских данных. Информация, циркулирующая в системе, разделяется на два вида: текстовая информация (ФИО пациентов, паспортные данные и др.), обеспечение защиты которой достигается за счет стандартных механизмов шифрования (симметричное блочное шифрование), а также результаты медицинских обследований, хранимых в форме электроэнцефалографических сигналов. Для обеспечения защиты второй категории данных предлагается подход, основанный на конвертации исходных цифровых сигналов в формат изображений.

Разработанный механизм защиты МИС предполагает использование исходного файла DICOM и файла изображения в формате PNG, подверженного алгоритму шифрования пикселей.

Файл DICOM (Digital Imaging and Communications in Medicine) – объектно-ориентированный файл с теговой организацией: пациент → исследование → серия → изображение (кадр или серия кадров) [3, 8].

Файл содержит структурированную информацию, в том числе, медицинские изображения для их дальнейшего сохранения в виде файла PNG и данные пациента в виде текстового файла.

Предполагается использование MATLAB для извлечение медицинских изображений из файла DICOM. Язык программирования JAVA используется для исполнения кода MATLAB и для программной реализации алгоритма шифрования медицинского изображения на основе теории хаоса. Шифрование изображений предполагается выполнять на уровне прикладного ПО, непосредственно перед отправкой в глобальное хранилище. Затем зашифрованное изображение будет загружено через протокол TCP/IP в облачную систему, в которой будет храниться информация о пациенте (зашифрована с использованием блочного алгоритма шифрования) и непосредственно зашифрованное изображение в файле. Для сохранения в секрете факта передачи зашифрованной информации используются методы стеганографии.

В связи со сложной структурой файла DICOM, а также содержанием в нем разнородной информации (текст, изображение сигнала, логотип больницы, тип медицинского устройства визуализации), его обработка представляет собой сложный процесс.

Разделение файла DICOM:

Входные данные: DICOM-файл;

Выходные данные: медицинское изображение в формате .png и текстовая медицинская информация.

Шаг 1. Чтение DICOM-файла;

Шаг 2. Разделение данных пикселей медицинского изображения и связанной с ними медицинской метаинформации;

Шаг 3. Сохранение медицинской метаинформации в текстовом файле;

Шаг 4. Сохранение пикселей медицинского изображения в формате .png с 24-битной глубиной.

Таким образом, медицинское изображение будет сохранено в формате PNG в целях упрощения обработки пикселей в процессе шифрования.

Для шифрования медицинского изображения используется алгоритм на основе теории хаоса, базирующийся на традиционной криптографической архитектуре [4, 5]. Данный алгоритм, применяемый к полученному медицинскому изображению PNG, будет выполняться попиксельно: для каждого пикселя медицинского изображения.

На рис. 2 показан пример обработки медицинского изображения алгоритмом шифрования.

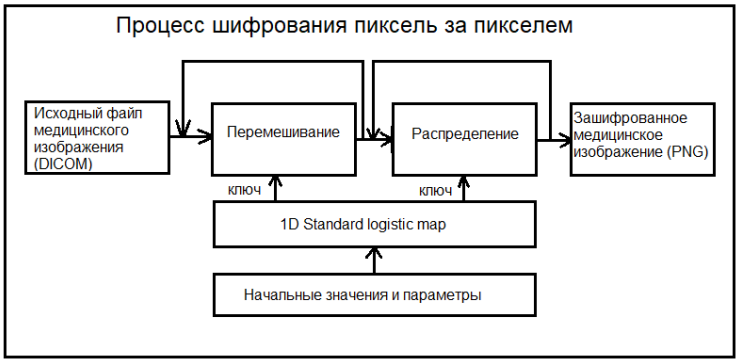

Рис. 2. Схема процесса шифрования медицинского изображения

Перемешивание пикселей означает реорганизацию расположения пикселей исходного медицинского изображения; цель шага - уменьшение высокой степени корреляции между соседними пикселями.

Следующим шагом является распределение, которое относится к изменению значений пикселей медицинского изображения путем выполнения некоторых преобразований значений пикселей. Следовательно, добавление пикселям новых значений повысит безопасность операции шифрования и отменит корреляцию между пикселями, в результате чего будет получено зашифрованное изображение с однородной гистограммой. Генератор ключей в этом процессе является одной из широко известных одномерных карт теории хаоса, известных как «1D Standard Logistic Map (SLM)» [7]. SLM имеет переменную X в качестве выходных данных, начальное условие X_n и один управляющий параметр μ, которые дают различные результаты и свойства при изменении его значения в качестве входных данных. Обычно эту карту можно описать следующим образом: $X_n + 1 = \mu X_n (1 – X_n)$ for n = 0, 1, 2, 3.

Экспериментальные результаты этой карты показывают хаотичное состояние системы, когда Xnє[0;1], управляющий параметр μє[0, 4]. Для большей точности логистическая карта всегда хаотична и имеет аппозитивный показатель Ляпунова

при 3,58≤μ≤4 [8]. В рамках работы SLM используется в качестве генератора ключей для перемешивания и распределения пикселей медицинского изображения в пространственной области, где использование SLM повторяется для всех пикселей изображения, чтобы получить произвольные значения, которые будут использоваться для шифрования пикселя [9, 10].

Шифрование медицинского изображения:

Входные данные: PNG-файл медицинского изображения;

Выходные данные: зашифрованный PNG-файл медицинского изображения.

Шаг 1. Чтение медицинского изображения и его сохранение в 2-х мерный массив пикселей;

Шаг 2. Использование стандартной логистической карты в качестве генератора случайных ключей, его начального состояния и управляющего параметра в качестве секретного ключа шифрования изображения;

Шаг 3. Перемешивание пикселей изображения (перестановка положения пикселей) в зависимости от сгенерированных значений из SLM;

Шаг 4. Распределение пикселей изображения путем изменения их значений в зависимости от ключа, сгенерированного SLM;

Шаг 5. Сохранение значения секретного ключа в том же текстовом файле, в котором хранится медицинская метаинформация, полученная из раздела DICOM-файла.

Заключение. Оценка эффективности разработанной облачной платформы хранения, систематизации и обработки медицинских данных:

Иерархичное разделение потоков данных на уровни, стандартизация протоколов передачи данных и форматов их хранения обеспечивают создание универсальной, гибкой и надежной медицинской информационной системы. Разработанная архитектура позволяет быстро интегрироваться в существующие медицинские системы. Единое пространство для хранения данных дает возможность осуществлять исследование значительного массива классифицированной медицинской информации средствами машинного обучения.

Разработанный механизм защиты МИС предполагает использование исходного файла DICOM и файла изображения в формате PNG, подверженного алгоритму шифрования пикселей. Для шифрования медицинского изображения используется алгоритм на основе теории хаоса, базирующийся на традиционной архитектуре криптографии, созданной Фридрихом. Данный алгоритм, применяемый к полученному медицинскому изображению PNG, выполняется попиксельно: для каждого пикселя медицинского изображения.

Возможности систем хаоса, которые используются для шифрования медицинских изображений, позволяют значительно повысить производительность, поскольку удовлетворяют требованиям цифровых изображений. Применение предложенного механизма шифрования медицинских данных является эффективным способом защиты информации в облачной платформе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Митькина П.А.* Особенности хранения медицинской информации // Современные научные исследования и инновации. – 2017. – № 5. – URL: http://web.snauka.ru/issues/2017/05/82546 (дата обращения: 07.10.2019).
2. Health Insurance Portability and Accountability Act. – URL: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountabilit y_Act (дата обращения: 08.10.2019).
3. DICOM. – URL: https://ru.wikipedia.org/wiki/DICOM (дата обращения 08.10.2019).
4. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images // The Journals of systems and software. – 2013. – Vol. 86. – P. 716-727.

5. *M.G. a. R.D. Jessica Fridrich*, "Detecting LSB Steganography in Color and Gray-Scale Images," Binghamton.
6. *N.A. H.A.-C. Fatma E.-Z. A. Elgamal*. Secure Medical Images Sharing over Cloud Computing environment // International Journal of Advanced Computer Science and Applications. – 2013. – Vol. 4. – P. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment," in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
7. Logistic map.– URL: https://en.wikipedia.org/wiki/Logistic_map (дата обращения 08.10.2019).
8. *Abdulrahman Alsalmany*. Cloud System for Encryption and Authentication Medical Images // IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727. – Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018). – P. 65-75. – https://www.researchgate.net/ publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (дата обращения: 29.09.2019).
9. *Плотников А.В., Прилуцкий Д.А., Селищев С.В.* Стандарт DICOM в компьютерных медицинских технологиях. – URL: https://mks.ru/library/article/1997/dicom.html (дата обращения 08.10.2019).
10. Визуальная криптография. – URL: http://cryptowiki.net/index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (дата обращения 08.10.2019).
11. *Котяшичев И.А., Бырылова Е.А*. Защита информации в «Облачных технологиях» как предмет национальной безопасности // Молодой ученый. – 2015. – № 6.4 (86.4). – С. 30-34. – URL: https://moluch.ru/archive/86/16357/ (дата обращения: 09.06.2020).
12. *Керейтова М.Р., Малыш В.Н.* Информационная безопасность в медицинских информационных системах // НиКа. – 2012. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 11.06.2020).
13. *Бойченко И.В.* Построение ИТ-инфраструктуры здравоохранения на основе парадигмы облачных вычислений // Врач и информационные технологии. – 2011. – № 3. – URL: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (дата обращения: 09.06.2020).
14. *Rohan Jathanna*. Int. Journal of Engineering Research and Application www.ijera.com ISSN: 2248-9622. – June 2017. – Vol. 7, Issue 6, (Part - 5). – P. 31-38 (дата обращения: 10.06.2020).
15. *Кривошеева Дарина*. Модель угроз безопасности в системах дистанционного мониторинга состояния человека // Правовая информатика. – 2016. – № 3. – URL: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (дата обращения: 11.06.2020).
16. *Назаренко Г.И., Михеев А.Е., Горбунов П.А., Гулиев Я.И., Фохт И.А., Фохт О.А*. Особенности решения проблем информационной безопасности в медицинских информационных системах // Врач и информационные технологии. – 2007. – № 4. – URL: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).
17. *Горбунов П.А., Фохт И.А.* Проблемы информационной безопасности в медицинских информационных системах – теоретические решения и практические разработки. Программные системы: теория и приложения / под ред. С.М. Абрамова. В 2-х т. Т. 1. – М.: Физматлит, 2006. – С. 107-112.
18. *Назаренко Г.И, Гулиев Я.И., Ермаков. Д.Е.* Медицинские информационные системы: теория и практика / под ред. Г.И. Назаренко, Г.С. Осипова. – М.: Физматлит, 2005. – 320 с.
19. *Михеев В.А.* Основы построения подсистемы защиты информации многофункциональной информационной системы // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 165-167.
20. *Клепиков Е.А., Ясько А.О.* Вопросы защиты конфиденциальной медицинской информации о пациенте в медицинских информационных системах // Символ науки. – 2016. – № 9-1. – URL: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (дата обращения: 16.10.2020).

REFERENCES

1. *Mit'kina P.A.* Osobennosti khraneniya meditsinskoy informatsii [Features of storing medical information], *Sovremennye nauchnye issledovaniya i innovatsii* [Modern scientific research and innovations], 2017, No. 5. Available at: http://web.snauka.ru/issues/2017/05/82546 (accessed 07 October 2019).
2. Health Insurance Portability and Accountability Act. Available at: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act (accessed 08 October 2019).
3. DICOM. Available at: https://ru.wikipedia.org/wiki/DICOM (accessed 08 October 2019).
4. *L.-Y. T. a. M.-S. H. Li-Chin Huangc.* A reversible data hiding method by histogram shifting in high quality medical images, *The Journals of systems and software*, 2013, Vol. 86, pp. 716-727.
5. *M.G. a. R.D. Jessica Fridrich.* Detecting LSB Steganography in Color and Gray-Scale Images, Binghamton.
6. *N.A. H.A.-C. Fatma E.-Z. A. Elgamal*. Secure Medical Images Sharing over Cloud Computing environment, *International Journal of Advanced Computer Science and Applications*, 2013, Vol. 4, pp. 130-138. A. B. K. R. G. a. J. P. S. Digvijay Singh Chauhan, "Double Secret Key Based Medical Image Watermarking for Secure Telemedicine in Cloud Environment," in 2017 40th International Conference on Telecommunications and Signal Processing (TSP), 2017.
7. Logistic map. Available at: https://en.wikipedia.org/wiki/Logistic_map (accessed 08 October 2019).
8. *Abdulrahman Alsalmany.* Cloud System for Encryption and Authentication Medical Images, *IOSR Journal of Computer Engineering (IOSR-JCE)* e-ISSN: 2278-0661, p-ISSN: 2278-8727, Vol. 20, Issue 1, Ver. II (Jan.-Feb. 2018), pp. 65-75. Available at: https://www.researchgate.net/publication/332571801_Cloud_System_For_Encryption_And_Authentication_Medical_Images (accessed 29 September 2019).
9. *Plotnikov A.V., Prilutskiy D.A., Selishchev S.V.* Standart DICOM v komp'yuternykh meditsinskikh tekhnologiyakh [DICOM standard in computer medical technologies]. Available at: https://mks.ru/library/article/1997/dicom.html (accessed 08 October 2019).
10. Vizual'naya kriptografiya [Visual cryptography]. Available at: http://cryptowiki.net/index.php?title=%D0%92%D0%B8%D0%B7%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F (accessed 08 October 2019).
11. *Kotyashichev I.A., Byrylova E.A.* Zashchita informatsii v «Oblachnykh tekhnologiyakh» kak predmet natsional'noy bezopasnosti [Information protection in "Cloud technologies" as a subject of national security], *Molodoy uchenyy* [Young scientist], 2015, No. 6.4 (86.4), pp. 30-34. Available at: https://moluch.ru/archive/86/16357/ (accessed 09 June 2020).
12. *Kereytova M.R., Malysh V.N.* Informatsionnaya bezopasnost' v meditsinskikh informatsionnykh sistemakh [Information security in medical information systems], *NiKa* [NIK], 2012. Available at: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-meditsinskih-informatsionnyh-sistemah (accessed 11 June 2020).
13. *Boychenko I.V.* Postroenie IT-infrastruktury zdravookhraneniya na osnove paradigmy oblachnykh vychisleniy [Building IT infrastructure for healthcare based on the paradigm of cloud computing], *Vrach i informatsionnye tekhnologii* [Doctor and information technologies], 2011, No. 3. Available at: https://cyberleninka.ru/article/n/postroenie-it-infrastruktury-zdravoohraneniya-na-osnove-paradigmy-oblachnyh-vychisleniy (accessed 09 June 2020).
14. *Rohan Jathanna*. Int. Journal of Engineering Research and Application www.ijera.com ISSN: 2248-9622, June 2017, Vol. 7, Issue 6, (Part - 5), pp. 31-38 (accessed 10 June 2020).
15. *Krivosheeva Darina.* Model' ugroz bezopasnosti v sistemakh distantsionnogo monitoringa sostoyaniya cheloveka [Model of security threats in systems of remote monitoring of human condition], *Pravovaya informatika* [Legal informatics], 2016, No. 3. Available at: https://cyberleninka.ru/article/n/model-ugroz-bezopasnosti-v-sistemah-distantsionnogo-monitoringa-sostoyaniya-cheloveka (accessed 11 June 2020).
16. *Nazarenko G.I., Mikheev A.E., Gorbunov P.A., Guliev Ya.I., Fokht I.A., Fokht O.A.* Osobennosti resheniya problem informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh [Features of solving information security problems in medical information systems], *Vrach i informatsionnye tekhnologii* [Doctor and information technology], 2007, No. 4. Available at: https://cyberleninka.ru/article/n/osobennosti-resheniya-problem-informatsionnoy-bezopasnosti-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

17. *Gorbunov P.A., Fokht I.A.* Problemy informatsionnoy bezopasnosti v meditsinskikh informatsionnykh sistemakh – teoreticheskie resheniya i prakticheskie razrabotki. Programmnye sistemy: teoriya i prilozheniya [Information security problems in medical information systems - theoretical solutions and practical developments. Software systems: theory and applications], ed. by S.M. Abramova. In 2nd vol. Vol. 1. Moscow: Fizmatlit, 2006, pp. 107-112.
18. *Nazarenko G.I, Guliev Ya.I., Ermakov. D.E.* Meditsinskie informatsionnye sistemy: teoriya i praktika [Medical information systems: theory and practice], ed. by G.I. Nazarenko, G.S. Osipova. Moscow: Fizmatlit, 2005, 320 p.
19. *Mikheev V.A.* Osnovy postroeniya podsistemy zashchity informatsii mnogofunktsional'noy informatsionnoy sistemy [Fundamentals of building a subsystem of information security for a multifunctional information system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 8 (85), pp. 165-167.
20. *Klepikov E.A., Yas'ko A.O.* Voprosy zashchity konfidentsial'noy meditsinskoy informatsii o patsiente v meditsinskikh informatsionnykh sistemakh [Issues of protecting confidential medical information about a patient in medical information systems], *Simvol nauki* [Symbol of Science], 2016, No. 9-1. Available at: https://cyberleninka.ru/article/n/voprosy-zaschity-konfidentsialnoy-meditsinskoy-informatsii-o-patsiente-v-meditsinskih-informatsionnyh-sistemah (accessed 16 October 2020).

Статью рекомендовал к опубликованию д.э.н. Е.Н. Тищенко.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: lkbabenko@sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: +79054530191; д.т.н.; профессор.

Шумилин Александр Сергеевич – e-mail: ashumilin@sfedu.ru; тел.: +79081773495; м.н.с.

Алексеев Дмитрий Михайлович – e-mail: dalekseev@sfedu.ru; тел.: +79515069532; ассистент.

Babenko Lyudmila Klimentievna – Southern Federal University; e-mail: lkbabenko@sfedu.ru, 2, Chekhov street, Taganrog, 347922, Russia; phone: +79054530191; dr. of eng. sc.; professor.

Shumilin Alexander Sergeevich – e-mail: ashumilin@sfedu.ru; phone: +79081773495; junior researcher.

Alekseev Dmitry Mikhailovich – e-mail: dalekseev@sfedu.ru; phone: +79515069532; assistant.

УДК 004.056.55 DOI 10.18522/2311-3103-2020-5-16-30

С.В. Поликарпов, В.А. Прудников, К.Е. Румянцев

ВЫЧИСЛИТЕЛЬНО ЭФФЕКТИВНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ УСРЕДНЁННЫХ ЛИНЕЙНЫХ СВОЙСТВ ПСЕВДО-ДИНАМИЧЕСКИХ ПОДСТАНОВОК

Псевдо-динамические подстановки PD-sbox могут стать эффективной заменой фиксированных подстановок в псевдо-случайных функциях, так как обладают положительными свойствами как фиксированных подстановок (малый расход вычислительных ресурсов), так и динамических подстановок (способных кардинально усложнять применение статистических методов криптоанализа). Проблемой активного внедрения псевдо-динамических подстановок является, в том числе, отсутствие вычислительно эффективного метода определения усреднённых линейных свойств для всего множества генерируемых при помощи PD-sbox эквивалентных подстановок, при этом в большинстве случаев интересует только определение максимальных значений преобладания (смещения) bias(α, β) от идеального значения 1/2. Для решения этой проблемы предлагается оригинальный метод, состоящий в том, что максимальные значения преобладания рассчитываются только для относительно небольших фиксированных подстановок, входящих в состав PD-sbox, а результирующие максимальные значения преобладания получаются путём итерационного вычисления с использованием логико-вероятностного выражения для операции Исключаю-

щего ИЛИ-НЕ (XNOR). Эффектом применения предложенного метода является кардинальное снижение вычислительных операций и, соответственно, возможность определения на типовом персональном компьютере максимальных значений преобладания bias(α, β) для 16-элементных PD-sbox, состоящих из 8-битовых фиксированных подстановок (что является недостижимым при использовании тривиального метода).

Псевдо-случайные функции; линейный криптоанализ; псевдо-динамические подстановки.

S.V. Polikarpov, V.A. Prudnikov, K.E. Rumyantsev

COMPUTATIONALLY EFFICIENT METHOD FOR DETERMINING THE AVERAGE LINEAR PROPERTIES OF PSEUDO-DYNAMIC SUBSTITUTIONS

Pseudo-dynamic substitutions PD-sbox can become an effective replacement for fixed substitutions in pseudo-random functions, since they have the positive properties of both fixed substitutions (low consumption of computational resources) and dynamic substitutions (which can radically complicate the application of statistical cryptanalysis methods). The problem of active implementation of pseudo-dynamic substitutions is, inter alia, the absence of a computationally efficient method for determining the averaged linear properties for the entire set of equivalent substitutions generated using PD-sbox, while in most cases, only the determination of the maximum values of the prevalence (bias) bias (α, β) from the ideal value 1/2. To solve this problem, an original method is proposed, which consists in the fact that the maximum dominance values are calculated only for relatively small fixed substitutions included in the PD-sbox, and the resulting maximum dominance values are obtained by iterative calculation using a logical-probabilistic expression for the Exclusive OR operation -NO (XNOR). The effect of using the proposed method is a dramatic reduction in computational operations and, accordingly, the possibility of determining on a typical personal computer the maximum values of the prevalence bias (α, β) for 16-element PD-sboxes consisting of 8-bit fixed substitutions (which is unattainable when using a trivial method).

Pseudo-random functions; linear cryptanalysis; pseudo-dynamic substitutions.

Введение. Одной из серьёзных проблем при создании симметричных криптографических алгоритмов является удовлетворение требований их устойчивости к статистическим методам криптоанализа, среди которых наиболее опасными и часто используемыми являются линейный и дифференциальный криптоанализ (и их производные) [1–8]. Если рассматривать линейный криптоанализ, то его целью является попытка упрощения сложности криптографического преобразования путём замены (аппроксимации) нелинейных элементов на линейные функции. В качестве нелинейных элементов, в большинстве случаев, выступают операции подстановки (замены), имеющие небольшую размерность (обычно 4 или 8 бит).

Как известно [9], реальные фиксированные подстановки не могут обладать идеальными свойствами и имеют ограниченный предел нелинейности (для своей размерности). По этой причине симметричные криптоалгоритмы имеют итерационную структуру, позволяющую «накопить» необходимую нелинейность за счёт количества итераций (раундов) преобразования и, тем самым, противодействовать статистическим методам криптоанализа.

Одним из известных и практически нереализованных путей противодействия статистическим методам криптоанализа является использование динамических подстановок. Однако, динамические подстановки не нашли широкого применения. Исключением является криптоалгоритм RC4, но и он переведён в разряд устаревших и ненадёжных [10]. Недостатками динамических подстановок являются: кардинальное увеличение затрачиваемых ресурсов и малое количество исследований по принципам обновления содержимого подстановок.

Возможным решением проблемы удовлетворения требованиям по одновременной минимизации затрачиваемых аппаратных ресурсов и минимизации задержки при преобразовании информации является применение псевдо-динамических подстановок *PD-sbox* [11–18].

Проведённые ранее исследования, на основе вычислительного эксперимента, показали [11, 14], что псевдо-динамические подстановки при работе в динамическом режиме (когда изменяются значения на управляющем входе) обладают идеальными усреднёнными линейными и дифференциальными свойствами (при усреднении свойств по всему множеству эквивалентных подстановок). Однако, при работе в статическом режиме (когда значение на управляющем входе фиксировано, но зависит от секретного параметра) псевдо-динамические подстановки, в общем случае, не обладают идеальными усреднёнными линейными и дифференциальными характеристиками.

Так, в [12, 13] осуществлено первичное исследование линейных характеристик псевдо-динамических подстановок *PD-sbox*. Предложена методика расчёта линейных свойств псевдо-динамических подстановок *PD-sbox*, позволяющая исследовать линейные свойства в зависимости от свойств и количества составляющих её фиксированных подстановок. Предложенная методика позволяет фактически оценить линейные свойства всего множества порождаемых при помощи *PD-sbox* подстановок. Это выгодно отличает данную работу от большинства работ, по применению зависимых от ключа и динамических подстановок.

В [13] приведены результаты, показывающие, что путём случайного формирования можно получить полноразмерные псевдо-динамические подстановки *PD-sbox*, обладающие экстремально низкими значениями смещения (преобладания) вероятности линейной аппроксимации $bias(\alpha,\beta)$. Стоит отметить, что в работе осуществлялась оценка *среднего* значения преобладания для большого количества *PD-sbox* и эта оценка производилась на основе *экстраполяции* результатов малоразмерных псевдо-динамических подстановок. Приведённый метод *не позволяет* осуществлять точное определение линейных свойств конкретных полноразмерных псевдо-динамических подстановок.

В противовес этому, для определения усреднённых дифференциальных характеристик был найден способ, позволяющий осуществлять исследование таких свойств на обычном персональном компьютере. Приведённый в [15] вычислительно-эффективный метод показывает, что существует *принципиальная* возможность определения усреднённых дифференциальных свойств для полноразмерных псевдо-динамических подстановок, используя только дифференциальные свойства маленьких фиксированных подстановок, входящих в состав *PD-sbox*. Кроме того, в [16] показано существование класса псевдо-динамических подстановок *PD-sbox*, которые в статическом режиме работы имеют идеальное усреднённое распределение дифференциалов.

Таким образом, существует актуальная проблема поиска вычислительно-эффективного метода определения линейных характеристик псевдо-динамических подстановок.

В данной работе предлагается вычислительно-эффективный метод определения линейных свойств (усреднённых по всему множеству эквивалентных подстановок) полноразмерных псевдо-динамических подстановок. Что позволяет закрыть пробел в наличии эффективных средств анализа линейных параметров и, соответственно, синтеза псевдо-динамических подстановок.

Существующие подходы. Метод линейной аппроксимации подстановок был предложен в [19]. В соответствии с определением, линейные свойства определяются количеством совпадений подстановки с набором линейных (аффинных) функций:

$$NSbox(\alpha,\beta) \stackrel{\text{def}}{=} \#\left\{X|0 \le X < 2^M, \left(\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha[i])\right) = \left(\bigoplus_{j=0}^{N-1}(Sbox(X)[j]\cdot\beta[j])\right)\right\}, \quad (1)$$

где $Sbox()$ – выходное значение подстановки; $[j]$ – конкретный бит выходного значения подстановки; x – входные значения подстановки; $[i]$ – конкретный бит входного значения подстановки; 2^M – количество входных комбинаций; M – количество входных бит; N – количество выходных бит; α – битовая маска для входного значения; β – битовая маска для выходного значения; $\cdot$ – операция побитового логического умножения; $\oplus$ – операция сложения по модулю 2. Фактически α и β задают вариант линейной функции.

Вероятность аппроксимации линейной функцией заданной подстановки определяется выражением:

$$p(\alpha,\beta) = \frac{NSbox(\alpha,\beta)}{2^M}. \quad (2)$$

Эффективность аппроксимации часто представляют в виде смещения (преобладания):

$$bias(\alpha,\beta) = \left|p(\alpha,\beta) - \frac{1}{2}\right|, \quad (3)$$

которое показывает, на сколько отличается вероятность аппроксимации от равновероятного (идеального) значения 0,5.

С точки зрения криптографической стойкости, идеальным случаем будет $bias(\alpha,\beta) = 0$ при всех значениях α и β, кроме $\alpha = 0$ и $\beta = 0$. Однако, фиксированных подстановок с такими идеальными свойствами не существует [9].

Таким образом, данный метод требует вычисления количества совпадений всех возможных комбинаций линейных функций с оцениваемой подстановкой. Размерность результирующей таблицы для $NSbox$ будет составлять 2^M строк и 2^N столбцов.

В [12] приведённый метод был расширен для исследования псевдо-динамических подстановок [11].

Псевдо-динамическая подстановка (*PD-sbox*) – структура из фиксированных подстановок и операций сложения по модулю 2 (побитового XOR), обладающая свойствами как динамических, так и фиксированных подстановок (рис. 1).

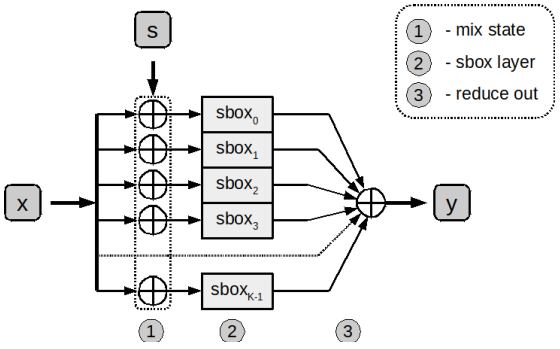

Рис. 1. Структура PD-sbox

Выражение, описывающее псевдо-динамическую подстановку:

$$Y = \bigoplus_{i=0}^{K-1} Sbox_i(X \oplus S^i), \quad (4)$$

где $Sbox$ – фиксированные подстановки; K – количество фиксированных подстановок; X – входные биты; Y – выходные биты; S – биты состояния псевдо-динамической подстановки; M – размерность фиксированных подстановок, входа x и выхода y.

Задавая конкретное значение состояния S – задаём одну эквивалентную подстановку. Всего будет 2^{MK} эквивалентных подстановок (M – размерность входа).

Как было указано [12–14], псевдо-динамические подстановки в динамическом режиме работы обладают идеальными усреднёнными линейными и дифференциальными свойствами (происходит взаимная компенсация значений $bias(\alpha,\beta)$ при усреднении по всему множеству формируемых эквивалентных подстановок).

Поэтому, интерес представляет исследование линейных свойств для статического режима работы псевдо-динамических подстановок *PD-sbox* –когда значения состояния S фиксированы и задаются криптографическим ключом.

Тривиальный метод. Для этого случая тривиальным методом оценки линейных свойств является представление *PD-sbox* в виде *большой* эквивалентной подстановки, заменяющая собой все параллельно включенные фиксированные подстановки из состава *PD-sbox*. Например, *большая* эквивалентная подстановка для *PD-sbox* из двух фиксированных подстановок получается перебором всех возможных входных комбинаций $\{X \oplus S^0, X \oplus S^1\}$ и вычислением соответствующих выходных значений Y (рис. 2.).

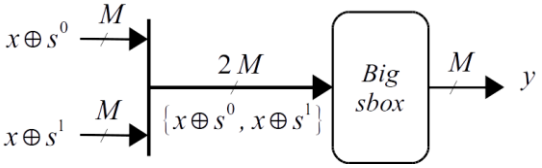

Рис 2. Представление PD-sbox в виде большой эквивалентной подстановки

После этого производится вычисление линейных свойств *большой* эквивалентной подстановки с использованием выражения из [19]. Недостаток метода – для полноразмерных *PD-sbox большая* эквивалентная подстановка будет иметь неприемлемую для вычислений размерность, так как размерность результирующей таблицы для $NSbox(\alpha,\beta)$ будет составлять 2^{MK} строк и 2^M столбцов. Например, 8-элементная *PD-sbox*, сформированная из 4-битных фиксированных подстановок, потребует вычисления таблицы для $NSbox(\alpha,\beta)$, состоящей из $2^{8\cdot4}$ или 2^{32} строк.

Метод на основе аналитического выражения. В работе [12] получены выражения для определения линейных свойств псевдо-динамических подстановок *PD-sbox* для случая, когда значения состояния S фиксированы и задаются криптографическим ключом:

$$p(\alpha,\beta) = \frac{NSbox(\alpha,\beta)}{2^M \cdot \prod_{i=0}^{(K-1)} 2^M} = \frac{NSbox(\alpha,\beta)}{2^{M(1+K)}},$$

Итоговое выражение, описывающее набор линейных функций, аппроксимирующих псевдо-динамическую подстановку *PD-sbox* с произвольным количеством K фиксированных подстановок, выглядит следующим образом:

$$\bigoplus_{k=0}^{K-1}\left(\bigoplus_{i=0}^{M-1}(S^k[i]\cdot\alpha^k[i])\right) = \left(\bigoplus_{j=0}^{N-1}(Y[j]\cdot\beta[j])\right) \oplus \bigoplus_{k=0}^{K-1}\left(\bigoplus_{i=0}^{M-1}(X[i]\cdot\alpha^k[i])\right),$$

где i – номер фиксированной подстановки, перед которой добавляется значение состояния S^i; M – количество бит в значении состояния S^i; K – количество фиксированных подстановок в *PD-sbox*.

Недостаток метода – аналогичен предыдущему случаю, определение таблицы $NSbox(\alpha,\beta)$ для полноразмерных *PD-sbox* будет иметь неприемлемую для вычислений размерность (размерность таблицы для $NSbox(\alpha,\beta)$ будет составлять 2^{MK} строк и 2^M столбцов).

Постановка задачи. Введём следующие обозначения:

K – количество фиксированных подстановок в составе *PD-sbox*;

M – размерность входа и выхода этих фиксированных подстановок;

N_{rows} – количество строк в таблице $P(\alpha,\beta)$;

$N_{columns}$ – количество столбцов в таблице $P(\alpha,\beta)$;

N_{count} – количество операций подсчёта совпадений *одной* линейной функции (задаваемой масками α и β) и исследуемой подстановки (на основе формулы (1)), соответствует количеству входных комбинаций.

Под вычислительной эффективностью будем понимать количество операций и объём памяти, затрачиваемых при определении (расчёте) линейных свойств подстановок.

Для тривиального метода (используя большую эквивалентную подстановку) получаем: $K \cdot M$ – размерность входа в битах; $N_{rows} = 2^{K \cdot M}$; $N_{columns} = 2^M$; $N_{count} = 2^{K \cdot M}$. Суммарное количество проходов в соответствии с формулой (1):

$$N_{bigSbox} = N_{rows} \cdot N_{columns} \cdot N_{count} = 2^{K \cdot M} \cdot 2^M \cdot 2^{K \cdot M} = 2^{M(2 \cdot K+1)}$$

Итогом вычислений будет таблица значений $NSbox(\alpha,\beta)$ размерностью $2^{K \cdot M} \times 2^M$ строк и столбцов. На основе этой таблицы рассчитываются таблицы $P(\alpha,\beta)$ и $bias(\alpha,\beta)$ с такой же размерностью. После чего по таблице $bias(\alpha,\beta)$ осуществляется поиск максимальных значений.

Например, для *PD-sbox* с $K = 8$ и $M = 4$ мы получим $N_{bigSbox} = 2^{4(2 \cdot 8+1)} = 2^{68}$ проходов в соответствии с формулой (1) и таблицу значений $NSbox(\alpha,\beta)$ размерностью $2^{32} \times 2^4$, что уже является непреодолимой задачей для типовых персональных компьютеров (не рассматривая последующие этапы расчёта).

Как показывает анализ публикаций по теме линейного криптоанализа [1, 8], в большинстве случаев для подстановок (и других нелинейных элементов) определяются только максимальные отклонения значений преобладания $bias(\alpha,\beta)$ от идеального значения $(1/2)$.

Таким образом, ставится задача поиска метода, позволяющего вычислять на типовых персональных компьютерах максимальные значения $bias(\alpha,\beta)$ для – элементных псевдо-динамических подстановок *PD-sbox* с $K \leq 16$ и $M \leq 8$.

Предлагаемый подход. Заключается в том, что оцениваются только максимальные значения преобладания $bias(\alpha,\beta)$ для каждого из вариантов битовой маски для выходного значения β (т. е., для каждого столбца $NSbox(\alpha,\beta)$ или $P(\alpha,\beta)$), при этом *не* рассчитываются все варианты битовой маски для входного значения α (имеющее 2^{MK} комбинаций). Вместо этого, вычисляются таблицы $P_i(\alpha^i,\beta)$ для отдельных фиксированных подстановок, а результирующие значения для $P(\alpha,\beta)$ вычисляется с использованием логико-вероятностного выражения, эквивалентному операции Исключающее ИЛИ-НЕ (XNOR).

Линейные свойства 2-элементной *PD-sbox*. Рассмотрим пример определения таблицы вероятностей линейной аппроксимации $P(\alpha,\beta)$ для 2-элементной *PD-sbox*, представленной на рис. 3.

Зададим параметры *PD-sbox*:

- $N = 3$ – размерность входа, бит;
- $M = 3$ – размерность выхода, бит;
- $K = 2$ – количество фиксированных подстановок;
- $sbox_0(x) = [0,4,3,2,7,1,5,6]$ – первая подстановка;
- $sbox_1(x) = [5,0,4,3,2,1,6,7]$ – вторая подстановка.

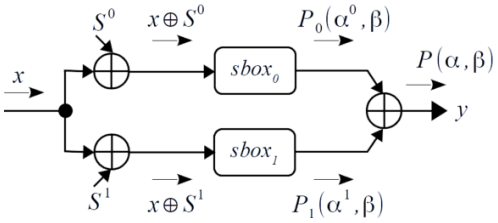

Рис. 3. Пример 2-элементной PD-sbox

Используя (1-2) определим значения $NSbox(\alpha, \beta)$ и $P(\alpha, \beta)$ для каждой фиксированной подстановки (табл. 1, 2).

Таблица 1

Значения $NSbox(\alpha, \beta)$ для $sbox_0$ и $sbox_1$

$NS_0(\alpha_0, \beta)$	β 0	1	2	3	4	5	6	7
α_0 0	8	4	4	4	4	4	4	4
1	4	2	4	6	4	6	4	6
2	4	4	6	6	4	4	6	2
3	4	6	2	4	4	6	6	4
4	4	6	4	6	6	4	2	4
5	4	4	4	4	6	2	6	6
6	4	6	6	4	2	4	4	6
7	4	4	6	2	6	6	4	4

$NS_1(\alpha_1, \beta)$	β 0	1	2	3	4	5	6	7
α_1 0	8	4	4	4	4	4	4	4
1	4	6	4	2	2	4	2	4
2	4	4	6	2	6	6	4	4
3	4	2	2	4	4	6	2	4
4	4	4	6	6	4	4	2	6
5	4	2	6	4	2	4	4	2
6	4	4	4	4	2	6	6	6
7	4	2	4	2	4	2	4	6

Таблица 2

Значения $P(\alpha, \beta)$ для $sbox_0$ и $sbox_1$.

$P_0(\alpha_0, \beta)$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.25	0.5	0.75	0.5	0.75	0.5	0.75
2	0.5	0.5	0.75	0.75	0.5	0.5	0.75	0.25
3	0.5	0.75	0.25	0.5	0.5	0.75	0.75	0.5
4	0.5	0.75	0.5	0.75	0.75	0.5	0.25	0.5
5	0.5	0.5	0.5	0.5	0.75	0.25	0.75	0.75
6	0.5	0.75	0.75	0.5	0.25	0.5	0.5	0.75
7	0.5	0.5	0.75	0.25	0.75	0.75	0.5	0.5

$P_1(\alpha_1, \beta)$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.75	0.5	0.25	0.25	0.5	0.25	0.5
2	0.5	0.5	0.75	0.25	0.75	0.75	0.5	0.5
3	0.5	0.25	0.25	0.5	0.5	0.75	0.25	0.5
4	0.5	0.5	0.75	0.75	0.5	0.5	0.25	0.75
5	0.5	0.25	0.75	0.5	0.25	0.5	0.5	0.25
6	0.5	0.5	0.5	0.5	0.25	0.75	0.75	0.75
7	0.5	0.25	0.5	0.25	0.5	0.25	0.5	0.75

Используя тривиальный метод вычислим *большую* эквивалентную подстановку, соответствующую двум параллельно включенным фиксированным подстановкам. Для этого переберём все возможные входные комбинации $x \oplus S^0 \,||\, x \oplus S^1$ и вычислим соответствующие выходные значения y. Размерность входа составит $N = 3 \cdot 2$ или $N = 6$ бит, а размерность выхода будет $M = 3$ бита.

В нашем случае *большая* эквивалентная подстановка будет иметь вид:

$$bigSbox(x) = [5, 1, 6, 7, 2, 4, 0, 5, 1, 6, 7, 2, 4, 0, 3, 0, 4, 3, 2, 7,$$
$$1, 5, 6, 4, 0, 7, 6, 3, 5, 1, 2, 3, 7, 0, 1, 4, 2, 6, 5, 2, 6, 1,$$
$$0, 5, 3, 7, 4, 1, 5, 2, 3, 6, 0, 4, 7, 6, 2, 5, 4, 1, 7, 3, 0, 7, 3, 4, 5, 0, 6, 2, 1].$$

Используя (1-2) определим значения $NSbox(\alpha,\beta)$ и $P(\alpha,\beta)$ для *большой* эквивалентной подстановки $bigSbox$. Для экономии места приведём только часть строк таблицы (табл. 3, 4).

Таблица 3

Значения $NSbox(\alpha,\beta)$ для $bigSbox$.

$\alpha\backslash\beta$	0	1	2	3	4	5	6	7
0	64	32	32	32	32	32	32	32
1	32	32	32	32	32	32	32	32
…	…	…	…	…	…	…	…	…
9	32	24	32	24	32	32	32	32
10	32	32	32	24	32	32	24	32
11	32	40	32	32	32	32	24	32
12	32	40	32	24	24	32	40	32
…	…	…	…	…	…	…	…	…
63	32	32	32	40	32	24	32	32

Таблица 4

Значения $P(\alpha,\beta)$ для $bigSbox$.

$\alpha\backslash\beta$	0	1	2	3	4	5	6	7
0	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
…	…	…	…	…	…	…	…	…
9	0.5	0.375	0.5	0.375	0.5	0.5	0.5	0.5
10	0.5	0.5	0.5	0.375	0.5	0.5	0.375	0.5
11	0.5	0.625	0.5	0.5	0.5	0.5	0.375	0.5
12	0.5	0.625	0.5	0.375	0.375	0.5	0.625	0.5
…	…	…	…	…	…	…	…	…
63	0.5	0.5	0.5	0.625	0.5	0.375	0.5	0.5

Обратим внимание на следующие значения $P(\alpha,\beta)$ для $bigSbox$:

1) $\alpha = 9; \beta = 4; P(9,4) = 0.5;$
2) $\alpha = 9; \beta = 1; P(9,1) = 0.375;$
3) $\alpha = 11; \beta = 1; P(11,1) = 0.625.$

Согласно указанному принципу вычисления $bigSbox$ соответствие между значениями масок $bigSbox$, $sbox_0$ и $sbox_1$ будет иметь следующий вид:

$$\alpha = \{\alpha^0 || \alpha^1\} = \alpha^0 \cdot 2^M + \alpha^1, \quad (5)$$

где $||$ – операция конкатенации двух битовых слов.

Таким образом, мы имеем следующее соответствие между масками:

1) $\alpha = 9 = 1 \cdot 8 + 1 \rightarrow \alpha^0 = 1, \alpha^1 = 1;$
2) $\alpha = 9 = 1 \cdot 8 + 1 \rightarrow \alpha^0 = 1, \alpha^1 = 1;$
3) $\alpha = 11 = 1 \cdot 8 + 3 \rightarrow \alpha^0 = 1, \alpha^1 = 3.$

С учётом этого, указанные выше значения $P(\alpha,\beta)$ для $bigSbox$ зависят от следующих значений $P(\alpha,\beta)$ фиксированных подстановок $sbox_0$ и $sbox_1$:

1) $P(9,4) = 0.5 : P_0(\alpha^0 = 1, \beta = 4) = 0.5$ и $P_1(\alpha^1 = 1, \beta = 4) = 0.25$;
2) $P(9,1) = 0.375 : P_0(\alpha^0 = 1, \beta = 1) = 0.25$ и $P_1(\alpha^1 = 1, \beta = 1) = 0.75$;
3) $P(11,1) = 0.625 : P_0(\alpha^0 = 1, \beta = 1) = 0.25$ и $P_1(\alpha^1 = 3, \beta = 1) = 0.25$.

Обозначим функцию, которая связывает $P(\alpha,\beta)$ с $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$ как $F()$:

$$P(\alpha,\beta) = F(P_0(\alpha^0,\beta), P_1(\alpha^1,\beta)).$$

Тогда приведённые выше варианты можно записать в следующем виде:

1) $F(0{,}5; 0{,}25) = 0{,}5$;
2) $F(0{,}25; 0{,}75) = 0{,}375$;
3) $F(0{,}25; 0{,}25) = 0{,}625$.

Выражение для первого случая сразу наводит на мысль, что мы имеем зависимость, аналогичную операции XOR (Исключающее ИЛИ). Как известно [20], логико-вероятностное выражение для XOR является «терминатором» – если на любом из входов будет равновероятное значение $(x = 0{,}5)$, то на выходе также будет равновероятное значение: $Pxor(0{,}5; any) = 0{,}5$.

Выражения для второго и третьего случая позволяют уточнить вид зависимости. Найденное авторами выражение, описывающее зависимость между $P(\alpha,\beta)$, $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$, имеет следующий вид:

$$p(\alpha,\beta) = F(p_0,p_1) = 1 - ((1-p_0)\cdot p_1 + p_0\cdot(1-p_1)), \quad (6)$$

где $p_0 = P_0(\alpha^0,\beta)$; $p_1 = P_1(\alpha^1,\beta)$.

Легко проверить, что данное выражение соответствует операции Исключающее ИЛИ-НЕ (XNOR) – путём подстановки значений «0» и «1» в выражение для $F(p_0,p_1)$ в соответствии с таблицей истинности XNOR.

То, что операции XOR на выходе *PD-sbox* соответствует логико-вероятностное выражение само по себе не вызывает вопросы. Теория логико-вероятностных выражений развивается много лет и находит применение, в том числе, для расчёта надёжности сложных систем [20].

Очень интересным фактом выступает то, что здесь логико-вероятностное выражение описывает связь между вероятностями аппроксимации подстановок линейными функциями, причём эта зависимость имеет инверсный характер – на выходе *PD-sbox* расположена операция XOR, а выражение для $P(\alpha,\beta)$ соответствует логико-вероятностной форме операции XNOR (рис. 3).

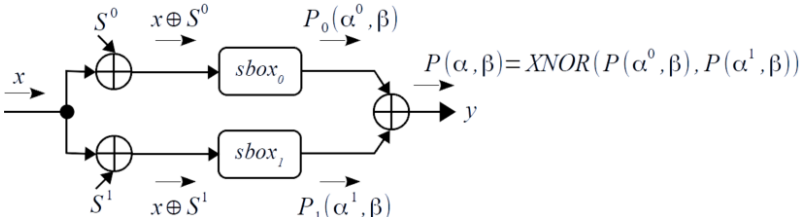

Рис. 4. Пояснения формирования $P(\alpha,\beta)$

Таким образом, мы получили **первый важный вывод**: для вычисления таблицы вероятностей $P(\alpha,\beta)$ для 2-элементной *PD-sbox* достаточно только таблиц вероятностей $P_0(\alpha^0,\beta)$ и $P_1(\alpha^1,\beta)$ соответствующих фиксированных подстановок $sbox_0$ и $sbox_1$ (входящих в состав *PD-sbox*) и вычисления по формуле (6) результирующих значений таблицы вероятностей $P(\alpha,\beta)$.

Однако, с точки зрения вычислительной эффективности данный вывод пока не даёт преимуществ, так как для расчёта результирующей таблицы вероятностей $P(\alpha,\beta)$ потребуется проход 2^{2M} значений $\alpha = \alpha^0||\alpha^1$.

Линейные свойства K-элементной *PD-sbox*. Рассмотрим пример определения таблицы вероятностей линейной аппроксимации $P(\alpha,\beta)$ для 3-элементной *PD-sbox*. В соответствии с правилами булевой алгебры, мы можем представить операцию XOR от 3 переменных в виде двух последовательных операций XOR от 2 переменных. Данный вариант *PD-sbox* представлен на рис. 5.

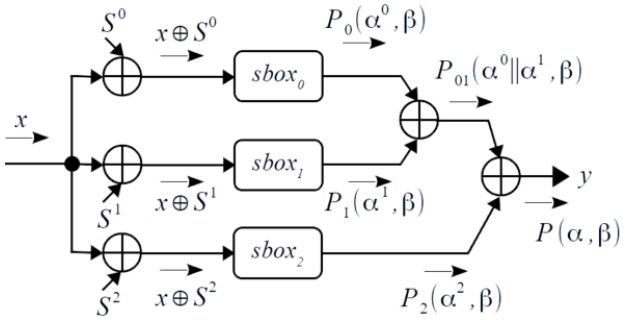

Рис. 5. Пример 3-элементной PD-sbox

Проведённые исследования показали, что для этого случая также походит выражение (6), только в качестве p_0 подставляется результат вычисления $P_{01}(\alpha^0 \parallel \alpha^1,\beta) = F(P_{01}(\alpha^0,\beta), P_1(\alpha^1,\beta))$ для двух фиксированных подстановок:

$$P(\alpha,\beta) = F(p_0,p_1) = 1 - ((1-p_0)\cdot p_1 + p_0\cdot(1-p_1)), \quad (7)$$

где $p_0 = P_{01}(\alpha^0 \parallel \alpha^1,\beta)$; $p_1 = P_2(\alpha^2,\beta)$.

Очевидно, что таким итерационным способом мы можем вычислять таблицы вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox*. Таким образом, мы получили **второй важный вывод**: для вычисления таблицы вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox* достаточно только таблиц вероятностей $P_0(\alpha^0,\beta)...P_{K-1}(\alpha^{K-1},\beta)$ соответствующих фиксированных подстановок $sbox_0...sbox_{K-1}$ (входящих в состав *PD-sbox*) и итерационного попарного вычисления по формуле (7) значений таблицы вероятностей $P(\alpha,\beta)$.

Итоговое итерационное выражение, позволяющее определить результирующее значения вероятностей $P(\alpha,\beta)$ для K-элементных *PD-sbox* можно записать в следующем виде:

$$P(\alpha^0 \parallel \alpha^i,\beta)|_{imax=K-1} = 1 - \left(1 - P(\alpha^0 \parallel \alpha^{i-1},\beta)\right)\cdot P(\alpha^i,\beta) + \\ + P(\alpha^0 \parallel \alpha^{i-1},\beta)\cdot\left(1 - P(\alpha^i,\beta)\right). \quad (8)$$

Как и в предыдущем случае, с точки зрения вычислительной эффективности данный вывод пока не даёт преимуществ, так как для расчёта результирующей таблицы вероятностей $P(\alpha,\beta)$ потребуется проход 2^{KM} значений маски $\alpha = \alpha^0 \parallel \alpha^1 \parallel \ldots \parallel \alpha^{K-1}$.

Поиск максимальных значений $bias(\alpha,\beta)$. С точки зрения стойкости к линейному криптоанализу в большинстве случаев важно только определение максимальных отклонений значений преобладания $bias(\alpha,\beta)$ от идеального значения $(1/2)$.

В соответствии с выражением (3) значения преобладания $bias(\alpha,\beta)$ показывают отклонение вероятности аппроксимации подстановки линейными функциями $P(\alpha,\beta)$ от равновероятного значения 0,5. Если проанализировать выражение (6),

то мы увидим, что максимальное значение на выходе $F(p_0, p_1)$ будет в случае, если на входах будут значения p_0 и p_1, максимально отличающиеся от значения 0,5. Иными словами, максимальное значение $bias(\alpha, \beta)$ задаётся максимальными значениями исходных фиксированных подстановок $bias(\alpha^0, \beta)$ и $bias(\alpha^1, \beta)$.

Вернёмся к нашему примеру с 2-элементными *PD-sbox*. Так как нам нужны максимальные значения $bias(\alpha, \beta)$ для всех вариантов выходной маски β, то для поиска максимальных значений $bias(\alpha, \beta)$ вместо *полных* таблиц $bias(\alpha^0, \beta)$ и $bias(\alpha^1, \beta)$ нам достаточно только по одной строке с максимальными значениями из этих таблиц. Например:

$row_{maxbias}(\alpha^0, \beta) =$
$\{bias_{max}(\alpha^0, 0); bias_{max}(\alpha^0, 1); bias_{max}(\alpha^0, 2); \ldots; bias_{max}(\alpha^0, 2^{M-1})\},$
$row_{maxbias}(\alpha^1, \beta) =$
$\{bias_{max}(\alpha, 0); bias_{max}(\alpha^1, 1); bias_{max}(\alpha^1, 2); \ldots; bias_{max}(\alpha^1, 2^{M-1})\}.$

Для нашей 2-элементной *PD-sbox* строки будут иметь следующий вид:

$P_{max}(\alpha^0, \beta)$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
max	0.5	0.25	0.75	0.75	0.75	0.75	0.75	0.75

$P_{max}(\alpha^1, \beta)$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
max	0.5	0.75	0.75	0.25	0.75	0.75	0.25	0.75

$bias(\alpha^0, \beta) = |P_0(\alpha^0, \beta) - 0{,}5|$

$\alpha_0 \backslash \beta$	0	1	2	3	4	5	6	7
max	0	0.25	0.25	0.25	0.25	0.25	0.25	0.25

$bias(\alpha^1, \beta) = |P_1(\alpha^1, \beta) - 0{,}5|$

$\alpha_1 \backslash \beta$	0	1	2	3	4	5	6	7
max	0	0.25	0.25	0.25	0.25	0.25	0.25	0.25

При попарной подстановке значений $P_{max}(\alpha^0, \beta)$ и $P_{max}(\alpha^1, \beta)$ в выражение XNOR (6) мы получим строку с максимальными значениями $P_{max}(\alpha^0 \parallel \alpha^1, \beta)$:

$\alpha^0 \parallel \alpha^1 \backslash \boldsymbol{\beta}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
max	0,5	0,375	0,625	0,375	0,625	0,625	0,375	0,625

Или, если перевести в значения $bias_{max}(\alpha^0 \parallel \alpha^1, \beta)$:

$\alpha^0_{max} \parallel \alpha^1_{max} \backslash \boldsymbol{\beta}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
max	0	0,125	0,125	0,125	0,125	0,125	0,125	0,125

Полученные максимальные значения *совпадают* с максимальными значениями при расчёте *полных* таблиц $P(\alpha, \beta)$, $P_0(\alpha^0, \beta)$ и $P_1(\alpha^1, \beta)$.

Используя выражение (8) приведённый пример можно расширить на вычисление максимальных значений $P_{max}(\alpha, \beta)$ и $bias_{max}(\alpha, \beta)$ для K-элементных подстановок *PD-sbox*:

$$P_{max}(\alpha^0 \parallel \alpha^i, \beta)|_{imax=K-1} = 1 - ((1 - P_{max}(\alpha^0 \parallel \alpha^{i-1}, \beta)) \cdot P_{max}(\alpha^i, \beta) + \\ + P_{max}(\alpha^0 \parallel \alpha^{i-1}, \beta) \cdot (1 - P_{max}(\alpha^i, \beta))). \quad (9)$$

Сравнение вычислительной эффективности. Для предложенного метода вычислительные затраты будут складываться из следующих составляющих:

1. Расчёт таблиц $P_0(\alpha^0, \beta) \ldots P_{K-1}(\alpha^{K-1}, \beta)$ и преобладания $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ для фиксированных подстановок, входящих в состав *PD-sbox*. Для одной фиксированной подстановки потребуется:

$$N_{Sbox} = N_{rows} \cdot N_{columns} \cdot N_{count} = 2^M \cdot 2^M \cdot 2^M = 2^{3 \cdot M}$$

проходов в соответствии с формулой (1).

2. Поиск максимальных значений по столбцам в таблице $bias(\alpha, \beta)$ и составление строки максимальных значений. Для одной фиксированной подстановки всего требуется $N_{find\_max} = N_{rows} \cdot N_{columns} = 2^M \cdot 2^M = 2^{2 \cdot M}$ операций просмотра и определения максимальных значений.

3. Итоговый расчёт вероятности $P(\alpha, \beta)$ и преобладания $bias(\alpha, \beta)$ используя итерационное выражение (9). Для K-элементной *PD-sbox* всего потребуется $N_{iter} = K - 1$ итераций вычисления функции Исключающее ИЛИ-НЕ $F(\alpha, \beta)$.

Например, для *PD-sbox* с $K = 8$ и $M = 4$ мы получим $K \cdot N_{Sbox} = K \cdot 2^{3 \cdot M} = 8 \cdot 2^{12}$ проходов в соответствии с формулой (1) для вычисления таблиц $NSbox(\alpha, \beta)$ всех фиксированных подстановок. Такое же количество уйдёт на вычисление значений вероятностей и преобладания по формулам (2) и (3).

Кроме этого, потребуется $K \cdot N_{find\_max} = K \cdot 2^{2 \cdot M} = 8 \cdot 2^8$ операций просмотра и определения максимальных значений для всех фиксированных подстановок и $N_{iter} = 7$ итераций вычисления функции Исключающее ИЛИ-НЕ $F(\alpha, \beta)$.

В табл. 4 приведено сравнение тривиального и предложенного методов по двум наиболее ресурсоёмким показателям.

Таблица 4

Эффективность предложенного метода поиска $bias_{max}(\alpha, \beta)$

	Тривиальный метод		**Предложенный метод**	
***PD-sbox*:**	$N_{bigSbox}$	$sizeNsbox(\alpha, \beta)$	$K \cdot N_{Sbox}$	$sizeNsbox(\alpha, \beta)$
$K = 2$ и $M = 4$	2^{20}	$2^8 \times 2^4$	2^{13}	$2 \times 2^4 \times 2^4$
$K = 4$ и $M = 4$	2^{36}	$2^{16} \times 2^4$	2^{14}	$4 \times 2^4 \times 2^4$
$K = 8$ и $M = 4$	2^{68}	$2^{32} \times 2^4$	2^{15}	$8 \times 2^4 \times 2^4$
$K = 16$ и $M = 4$	2^{132}	$2^{64} \times 2^4$	2^{16}	$16 \times 2^4 \times 2^4$
$K = 2$ и $M = 8$	2^{40}	$2^{16} \times 2^8$	2^{25}	$2 \times 2^8 \times 2^8$
$K = 4$ и $M = 8$	2^{72}	$2^{32} \times 2^8$	2^{26}	$4 \times 2^8 \times 2^8$
$K = 8$ и $M = 8$	2^{136}	$2^{64} \times 2^8$	2^{27}	$8 \times 2^8 \times 2^8$
$K = 16$ и $M = 8$	2^{264}	$2^{128} \times 2^8$	2^{28}	$16 \times 2^8 \times 2^8$

Как видно, данная задача является решаемой при использовании типовых персональных компьютеров.

Заключение. Таким образом, представлен вычислительно эффективный метод определения усреднённых линейных свойств псевдо-динамических подстановок, заключающийся в поиске максимальных значений преобладания (смещения) вероятности линейной аппроксимации $bias(\alpha, \beta)$ для K-элементных *PD-sbox*, который состоит из следующих этапов:

1. Расчёт таблиц значений вероятности $P_0(\alpha^0, \beta) \ldots P_{K-1}(\alpha^{K-1}, \beta)$ и преобладания $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ для фиксированных подстановок, входящих в состав *PD-sbox*.

2. Для каждой из полученных таблиц $bias_0(\alpha^0, \beta) \ldots bias_{K-1}(\alpha^{K-1}, \beta)$ формируется строка максимальных значений $bias_{maxi}(\alpha^i, \beta)$, содержащая максимальные значения преобладания для всех комбинаций маски b.

3. Для каждой из полученных таблиц $P_0(\alpha^0,\beta)\ldots P_{K-1}(\alpha^{K-1},\beta)$ формируется аналогичная строка значений $P_{maxi}(\alpha^i,\beta)$, с соответствующими п.2 значениями вероятностей.

4. Расчёт промежуточных и итоговых максимальных значений $P_{max}(\alpha,\beta)$ и $bias_{max}(\alpha,\beta)$ используя итерационное выражение (9).

Предложенный метод, в противовес известным подходам, позволяет определять максимальные значения $bias_{max}(\alpha,\beta)$ используя приемлемые вычислительные ресурсы.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Preneel B.* Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. – Berlin Heidelberg NewYork London Paris Tokyo Hong Kong Barcelona Budapest: Springer-Verlag, 2004.
2. *Matsui M.* The first experimental cryptanalysis of the data encryption standard / Y. Desmedt (ed.), CRYPTO // Lecture Notes in Computer Science. – Vol. 839. – Springer, 1994. – P. 1-11.
3. *Harpes C., Kramer G.G., Massey J.L.* A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma / L.C. Guillou, J.-J. Quisquater (eds.), EUROCRYPT // Lecture Notes in Computer Science. – Vol. 921. – Springer, 1995. – P. 24-38.
4. *Selçuk A.A.* On probability of success in linear and differential cryptanalysis // J. Cryptology. – 2008. – Vol. 21 (1). – P. 131-147.
5. *Bogdanov A., Rijmen V.* Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography. – Springer, US, 2012. – P. 1-15.
6. *Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen.* Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard // Information Processing Letters. – 2014. – Vol. 114, Issue 6. – P. 322-330. – https://doi.org/10.1016/j.ipl.2014.01.007.
7. *Andrey Bogdanov, Elif Bilge Kavun, Elmar Tischhauser, Tolga Yalçın.* Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis // Journal of Computational and Applied Mathematics. – 2014. – Vol. 259, Part B. – P. 592-598. – https://doi.org/10.1016/j.cam.2013.10.020.
8. *Eichlseder M., Leander G., & Rasoolzadeh S.* (Accepted/In press). Computing Expected Differential Probability of (Truncated) Differentials and Expected Linear Potential of (Multidimensional) Linear Hulls in SPN Block Ciphers. In Progress in Cryptology - IndoCrypt 2020.
9. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: Московский центр непрерывного математического образования, 2004. – 470 с.
10. Security Advisory 2868725: Recommendation to disable RC4. Security Research and Defense Blog. – URL: http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx.
11. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Псевдо-динамические таблицы подстановки: основа современных симметричных криптоалгоритмов // Научное обозрение. – 2014. – № 12. – С. 162-166. – URL: http://www.sced.ru/ru/files/7_12_1_2014/7_12_1_2014.pdf.
12. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Исследование линейных характеристик псевдо-динамических подстановок // Известия ЮФУ. Технические науки. – 2015. –№ 5 (166). – С. 111-123.
13. *Поликарпов С.В., Кожевников А.А.* Псевдо-динамические подстановоки: исследование линейных свойств // Известия ЮФУ. Технические науки. – 2015. – № 8 (169). – С. 19-31.
14. *Поликарпов С.В., Румянцев К.Е., Кожевников А.А.* Псевдо-динамические таблицы подстановки: исследование дифференциальных характеристик // Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках: сборник материалов международного научного е-симпозиума. – Электрон. текстовые дан. – Россия. – г. Москва. – 2014 г. – Киров: МЦНИП, 2015. – С. 77-89.
15. *Sergey Polikarpov, Konstantin Rumyantsev and Dmitry Petrov.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions // AIP Conference Proceedings 1952, 020091. 2018.

16. *Polikarpov S., Petrov D., Kozhevnikov A.* On A Class Pseudo-Dynamic Substitutions PD-Sbox, With A Perfect Averaged Distribution of Differentials in Static Mode of Work // Proceedings of the 2017 International Conference on Cryptography, Security and Privacy. – Wuhan, China: ACM, 2017. – P. 17-21. – (ICCSP 17). – ISBN 978-1-4503-4867-6. – DOI: 10.1145/3058060.3058087. – URL: http://doi.acm.org/10.1145/3058060.3058087.
17. *Kozhevnikov A.A., Polikarpov S.V., Rumyantsev K.E*. On differential properties of a symmetric cryptoalgorithm based on pseudo-dynamic substitutions // Математические вопросы криптографии. – 2016. – Т. 7:2. – С. 91-102. – URL: https://doi.org/10.4213/mvk186.
18. *Поликарпов С.В., Кожевников А.А., Румянцев К.Е., Прудников В.А.* Псевдослучайная функция PCOLLAPSER, обеспечивающая экстремальный параллелизм обработки информации // Известия ЮФУ. Технические науки. – 2019. – № 5 (207). – С. 88-100.
19. *Matsui Mitsuru.* Linear Cryptoanalysis Method for DES Cipher // Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. – 1993. – P. 386-397. – URL: http://dx.doi.org/10.1007/3-540-48285-7_33.
20. *Рябинин И.А.* Логико-вероятностный анализ проблем и надежности, живучести и безопасности: очерки разных лет. ЮРГТУ, 2009. – 599 с. – https://books.google.ru/books?id=7ACRkgAACAAJ.

REFERENCES

1. *Preneel B.* Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. Berlin Heidelberg NewYork London Paris Tokyo Hong Kong Barcelona Budapest: Springer-Verlag, 2004.
2. *Matsui M.* The first experimental cryptanalysis of the data encryption standard, Y. Desmedt (ed.), CRYPTO, *Lecture Notes in Computer Science*, Vol. 839. Springer, 1994, pp. 1-11.
3. *Harpes C., Kramer G.G., Massey J.L*. A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma, L.C. Guillou, J.-J. Quisquater (eds.), EUROCRYPT, *Lecture Notes in Computer Science*, Vol. 921. Springer, 1995, pp. 24-38.
4. *Selçuk A.A.* On probability of success in linear and differential cryptanalysis, *J. Cryptology*, 2008, Vol. 21 (1), pp. 131-147.
5. *Bogdanov A., Rijmen V*. Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography. Springer, US, 2012, pp. 1-15.
6. *Long Wen, Meiqin Wang, Andrey Bogdanov, Huaifeng Chen.* Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard, *Information Processing Letters*, 2014, Vol. 114, Issue 6, pp. 322-330. Available at: https://doi.org/10.1016/j.ipl.2014.01.007.
7. *Andrey Bogdanov, Elif Bilge Kavun, Elmar Tischhauser, Tolga Yalçın.* Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis, *Journal of Computational and Applied Mathematics*, 2014, Vol. 259, Part B, pp. 592-598. Available at: https://doi.org/10.1016/j.cam.2013.10.020.
8. *Eichlseder M., Leander G., & Rasoolzadeh S.* (Accepted/In press). Computing Expected Differential Probability of (Truncated) Differentials and Expected Linear Potential of (Multidimensional) Linear Hulls in SPN Block Ciphers. In Progress in Cryptology - IndoCrypt 2020.
9. *Logachev O.A., Sal'nikov A.A., Yashchenko V.V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean functions in coding theory and cryptology]. Moscow: Moskovskiy tsentr nepreryvnogo matematicheskogo obrazovaniya, 2004, 470 p.
10. Security Advisory 2868725: Recommendation to disable RC4. Security Research and Defense Blog. Available at: http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx.
11. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Psevdo-dinamicheskie tablitsy podstanovki: osnova sovremennykh simmetrichnykh kriptoalgoritmov [Pseudo-dynamic substitutions: the basis of modern symmetric cryptoalgorithms], *Nauchnoe obozrenie* [Scientific Review], 2014, No. 12, pp. 162-166. Available at: http://www.sced.ru/ru/files/7_12_1_2014/7_12_1_2014.pdf.

12. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Issledovanie lineynykh kharakteristik psevdo-dinamicheskikh podstanovok [Investigation of linear characteristics of pseudo-dynamic substitutions], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 111-123.
13. *Polikarpov S.V., Kozhevnikov A.A.* Psevdo-dinamicheskie podstanovoki: issledovanie lineynykh svoystv [Pseudo-dynamic substitutions: investigation of linear propertie], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 8 (169), pp. 19-31.
14. *Polikarpov S.V., Rumyantsev K.E., Kozhevnikov A.A.* Psevdo-dinamicheskie tablitsy podstanovki: issledovanie differentsial'nykh kharakteristik [Pseudo-dynamic substitutions: research of differential characteristics], *Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma* [Physical and mathematical methods and information technologies in natural science, engineering and humanities: collection of materials of the international scientific e-symposium]. Electron. text data. Russia. Moscow, 2014. Kirov: MTSNIP, 2015, pp. 77-89.
15. *Sergey Polikarpov, Konstantin Rumyantsev and Dmitry Petrov.* Computationally efficient method for determining averaged distribution of differentials for pseudo-dynamic substitutions, *AIP Conference Proceedings* 1952, 020091. 2018.
16. *Polikarpov S., Petrov D., Kozhevnikov A.* On A Class Pseudo-Dynamic Substitutions PD-Sbox, With A Perfect Averaged Distribution of Differentials in Static Mode of Work, *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*. Wuhan, China: ACM, 2017, pp. 17-21. (ICCSP 17). ISBN 978-1-4503-4867-6. DOI: 10.1145/3058060.3058087. Available at: http://doi.acm.org/10.1145/3058060.3058087.
17. Kozhevnikov A.A., Polikarpov S.V., Rumyantsev K.E. On differential properties of a symmetric cryptoalgorithm based on pseudo-dynamic substitutions, *Matematicheskie voprosy kriptografii* [Mathematical questions of Cryptography], 2016, Vol. 7:2, pp. 91-102. Available at: https://doi.org/10.4213/mvk186.
18. *Polikarpov S.V., Kozhevnikov A.A., Rumyantsev K.E., Prudnikov V.A.* Psevdosluchaynaya funktsiya PCOLLAPSER, obespechivayushchaya ekstremal'nyy parallelizm obrabotki informatsii [Pseudo-random function PCOLLAPSER providing extreme parallelism of information processing], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2019, No. 5 (207), pp. 88-100.
19. *Matsui Mitsuru.* Linear Cryptoanalysis Method for DES Cipher, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, 1993, pp. 386-397. Available at: http://dx.doi.org/10.1007/3-540-48285-7_33.
20. *Ryabinin I.A.* Logiko-veroyatnostnyy analiz problem i nadezhnosti, zhivuchesti i bezopasnosti: ocherki raznykh let [Logical-probabilistic analysis of problems and reliability, survivability and safety: essays from different years]. YURGTU, 2009. 599 p. Available at: https://books.google.ru/books?id=7ACRkgAACAAJ.

Статью рекомендовала к опубликованию к.т.н. К.Б. Дахкильгова.

Поликарпов Сергей Витальевич – Южный федеральный университет; e-mail: polikarpovsv@sfedu.ru; 347900, г. Таганрог, ул. Чехова, 2, корпус «И»; тел.: 89085159762; к.т.н.

Прудников Вадим Александрович – e-mail: pruvad@yandex.ru; тел.: 89198961427.

Румянцев Константин Евгеньевич – e-mail: rke2004@mail.ru, тел.: 89281827209; д.т.н.; профессор.

Polikarpov Sergey Vitalievich – Southern Federal University; e-mail: polikarpovsv@sfedu.ru; 347900, Taganrog, 2, Chekhov street; phone: +79085159762; cand. of eng. sc.

Prudnikov Vadim Aleksandrovich – e-mail: pruvad@yandex.ru; phone: +79198961427.

Rumyantsev Konstantin Evgenyevich – e-mail: rke2004@mail.ru; phone: +79281827209; dr. of eng. sc.; professor.

УДК 615.47:616-072.7 DOI 10.18522/2311-3103-2020-5-31-40

М. Рагеб Ага

ПРИНЦИПЫ ФОРМИРОВАНИЯ БАЗЫ ЗАПИСЕЙ ЭКГ СИГНАЛОВ И ИХ ФРАГМЕНТОВ ДЛЯ ОЦЕНКИ ХАРАКТЕРИСТИК НОСИМЫХ ЦИФРОВЫХ ON-LINE МОНИТОРОВ

Электрокардиографические (ЭКГ) сигналы обладают рядом свойств, которые могут значительно дополнить существующие и более устоявшиеся биометрические методы. Некоторые из наиболее заметных свойств - это тот факт, что сигналы могут быть получены непрерывно с использованием минимально навязчивых настроек, не склонны к созданию скрытых паттернов и обеспечивают естественное обнаружение живости, открывая новые возможности в области разработки биометрических систем. В статье предложены методы формирования базы данных ЭКГ-сигналов и их фрагментов для оценки характеристик портативных цифровых он-лайн мониторов. В методе дискретного вейвлет-преобразования (DWT) позволяет с высокой точностью определить наличие RR-интервалов и их сегментов. Это позволяет использовать данный метод для классификации ЭКГ-сигналов, формирования базы записей данных сигналов и генерирования тестовых сигналов, предназначенных для оценки характеристик носимых цифровых ONLINE-мониторов. В этой статье представлен улучшенный и более эффективный алгоритм генерация сигналов электрокардиограммы (ЭКГ) под Непрерывным Вейвлет-Преобразованием от архива PhysioBank для проверки работоспособности ЭКГ аппарата ,

Дискретного вейвлет-преобразования ДВП; вейвлет-преобразование ВП; электрокардиография ЭКГ; непрерывного вейвлет-преобразования НВ; MIT Physionet.

M. Ragheb Agha

PRINCIPLES OF FORMING A DATABASE OF ECG SIGNALS AND THEIR FRAGMENTS FOR EVALUATING THE CHARACTERISTICS OF WEARABLE DIGITAL ON-LINE MONITORS

Electrocardiographic (ECG) signals have several properties that can greatly complement the existing, and more established biometric modalities. Some of the most prominent properties are the fact that the signals can be continuously acquired using minimally intrusive setups, are not prone to produce latent patterns, and provide intrinsic liveliness detection, opening new opportunities within the area of biometric systems development. The paper proposes methods for forming a database of ECG signals and their fragments for assessing the characteristics of portable digital on-line monitors. In the method of discrete wavelet transform (DWT) it allows to determine with high accuracy the presence of RR-intervals and their segments. This makes it possible to use this method for classifying ECG signals, forming a database of signal data records and generating test signals designed to assess the characteristics of wearable digital ONLINE monitors. This article presents an improved and more efficient algorithm by Discrete Wavelet Transform for generating electrocardiogram (ECG) signals from the PhysioBank archive to test the performance of an ECG machine.

Electrocardiography ECG; wavelet transform WT; discrete wavelet transform DWT; continuous wavelet transform CWT; MIT Physionet.

Введение. В работе предложены методы формирования базы записей ЭКГ сигналов и их фрагментов для оценки характеристик носимых цифровых on-line мониторов. Проведено сравнение различных методов обнаружения RR-интервалов ЭКГ-сигнала на рис. 1.

Для распознавания отклонений ЭКГ-сигнала от нормы могут применяться решающие правила, функции расстояния и правдоподобия, дисперсионный анализ, нейронные сети, статистические классификаторы и другие методы [2].

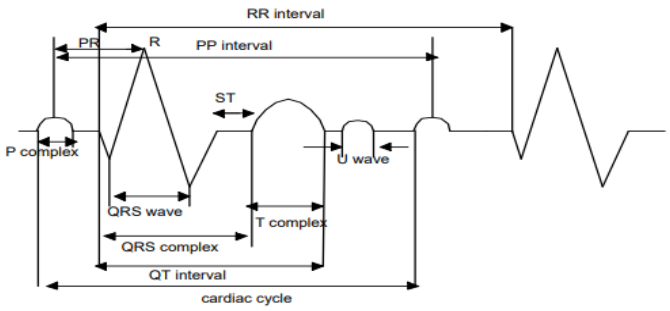

Рис. 1. Обнаружение различных волн в ЭКГ-сигнале

Таблица 1

Наименования амплитудно-временных параметров элементов ЭКГ-сигнала

Сегмент	Описание	Длительность
RR	интервал между соседними R-колебаниями	0.6-1.2 s
P	первое короткое восходящее движение ЭКГ	80 ms
PR	измеряется от начала зубца P до начала комплекса QRS	120-200 ms
QRS	колебание обычно начинается с отклонения вниз зубца Q, значительного отклонения вверх зубца R и заканчивается нисходящим отклонением зубца S	80-120 ms
J- точка	Точка, в которой заканчивается комплекс QRS и начинается сегмент ST, называется J-точкой.	/ /
PR	соединяет волну P и комплекс QRS	50-120 ms
ST	соединяет комплекс QRS и зубец T	80-120 ms
T	обычно незначительный восходящий сигнал	160 ms
ST	измеряется от точки J до конца зубца T	320 ms
QT	измеряется от начала комплекса QRS до конца зубца T	420 ms
U	обычно имеет низкую амплитуду и часто полностью отсутствует	/ /

Биомедицинские сигналы, такие как сигналы ЭКГ человеческого организма, являются нелинейными и нестационарными. Из-за нестационарной природы сигналов ЭКГ преобразование Фурье не подходит для них;

Вейвлет-преобразование (Wavelet Transform – WT). Это метод, который позволяет провести анализ ЭКГ-сигнала во временной и частотной областях одновременно с многократным анализом исследуемой функции [4].

WT (ВП) состоит из непрерывного вейвлет-преобразования (CWT) Continuous Wavelet Transform и дискретного вейвлет-преобразования (DWT) Discrete Wavelet Transform / (ДВП).

Во многих аспектах DWT можно использовать для извлечения признаков сигнала ЭКГ.

DWT определяется следующей формулой [4]:

$$DWT_X(j,k) = \int_{-\infty}^{+\infty} x(t)\psi_{j,k}(t)dt$$

$$\psi_{j,k}(t) = \frac{1}{\sqrt{s}}\,\psi\left(\frac{t-2^j k}{2^j}\right),$$

где ψ j, k (t) – вейвлет-функция, $x(t)$ – это сигнал ЭКГ; DWT используется для извлечения статистических характеристик. Каждое отдельное сердцебиение ЭКГ делится на пять поддиапазонов с использованием ψ(t) – материнского вейвлета [3].

С помощью данного метода в среде Matlab была создана система, позволяющая исследовать ЭКГ-сигналы, выделять в них фрагменты, определять наличие заболеваний по виду сигнала. Для формирования базы данных ЭКГ-сигналов были использованы данные 300 ЭКГ-сигналов из базы MIT Physionet [1].

Эти данные могут быть использованы для формирования тестовых сигналов для оценки характеристик носимых цифровых Online-мониторов. В каждом сигнале содержится 3600 отсчётов. Сигнал разбивается на 8-9 интервалов. Каждый интервал содержит около 250–300 отсчётов [7].

Таблица 2

В качестве примера можно рассмотреть ЭКГ-сигнал с частотой 50 Гц. В таком случае результаты преобразования будут выглядеть следующим образом:

Наименование интервала	Уровень	Диапазон частот, Гц
D1	1	50-25
D2	2	25-12.5
D3	3	12.5-6.25
D4	4	3.125-1.5625
D5	5	1.5625-0.78125
D6 …. D9	6….9	0.78125-0.390625

function[d1,d2,d3,d4,d5,d6,d7,d8,cleanecg]=wavelettransform(ecg)

Вейвлет-преобразование при обработке сигналов ЭКГ может быть использовано как инструмент для выделения признаков, шумоподавления и распознавания сердцебиения. В данном случае DWT использовался в качестве метода выделения признаков [6].

$$W_{\varphi}(s,t) = \int_{-\infty}^{+\infty} x(t)\psi_{s,t}(t)dt$$

$$\psi_{s,t}.(t) = \frac{1}{\sqrt{s}}\,\psi\,\left(\frac{1-t}{s}\right),$$

где $\psi_{j,k}(t)$ – вейвлет-функция, $x(t)$ это сигнал ЭКГ

Особенности распознавания интервала RR. Зубец R – это точка, соответствующая наивысшему пику кривой ЭКГ, а интервал RR – время между последовательными комплексами QRS. Сигнал ЭКГ имеет нелинейное динамическое поведение, и во время аритмии нелинейные динамические компоненты изменяются более значительно, чем линейные аналоги.

Интервал RR характеризуется тем, что его достаточно просто определить, легко рассчитать, а также данный интервал менее подвержен шуму, чем другие интервалы [12].

Четыре типа признаков интервала RR, а именно RR_{pre} – предыдущий RR-интервал, RR_{post} – последующий RR-интервал, RR_{ave} – средний RR-интервал и RR_{local} – локальный RR-интервал, были получены из последовательности нескольких RR-интервалов, чтобы характеризовать динамические особенности сердцебиения. При расчете этих функций используются следующие формулы [9]:

$$RR_{pre}(i) = R(i) - R(i-1),$$

$$RR_{post}(i) = R(i+1) - R(i),$$

$$RR_{local} = \frac{1}{10}\sum_{I=-5}^{5} RR(i),$$

$$RR_{ave} = \frac{1}{N_{RR}}\sum_{I=1}^{N_{RR}} RR(i),$$

где i – номер местоположения текущего пика R, а RRpre, RRpost, R-Rlocal и RRave представляют предыдущий, последующий, локальный и средний интервал RR соответственно. R (i) – текущий R-пик, R (i - 1) и R (i + 1) представляют предыдущий и последующий R-пики соответственно.

На рис. 3 изображено сравнение графиков результата дискретного вейвлет-преобразования и исходного ЭКГ-сигнала [5].

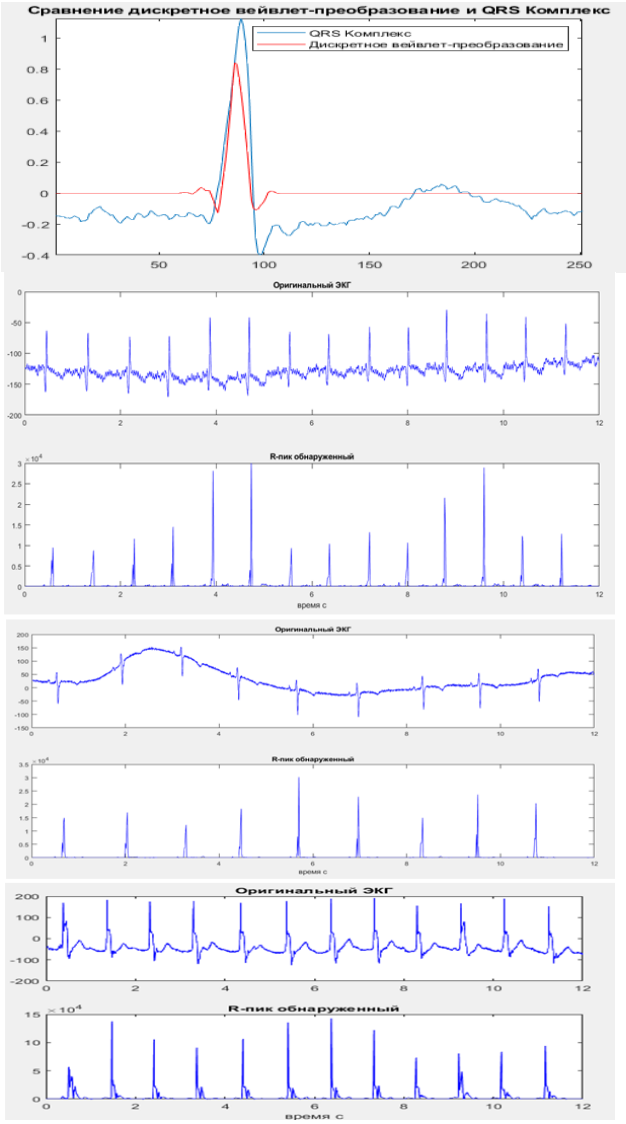

Рис. 3. Сравнение графиков результата дискретного вейвлет-преобразования и исходного ЭКГ-сигнала

Как видно, дискретное вейвлет-преобразование обладает высокой чувствительностью к распознаванию RR-интервала и его сегментов. Это даёт возможность использовать данный метод для формирования базы записей ЭКГ-сигналов, характерных для нормальной работы сердца и при наличии заболеваний [9].

Алгаритм формирования базы записей ЭКГ-сигналов. На рис. 4 изображена структурная схема процесса формирования базы записей ЭКГ-сигналов. Исходный ЭКГ-сигнал берётся из базы данных (например, MIT-BIH, Алмазова и др.) [10].

Рис. 4. Структурная схема процесса формирования базы записей ЭКГ-сигналов

В данном случае используется база MIT-BIH. Затем сигнал предварительно обрабатывается: анализируется спектр, определяется амплитуда, частота и диапазон частот. Далее происходит сегментация ЭКГ-сигнала и к каждому сегменту применяется ДВП. В результате применения ДВП происходит распознавание RR-интервала. Затем выделяются признаки интервала (Q R S T U P) и по ним определяется принадлежность исследуемого ЭКГ-сигнала к определённому классу сигналов (классификация ЭКГ-сигнала). Записи сигналов оформляются и хранятся в системе в виде таблицы. На рис. 5 данная база записей впоследствие может быть использована для оценки характеристики носимых цифровых ONLINE-мониторов путём использования генератора тестового ЭКГ-сигнала displayWaveformLabels(data,true,1000) [14].

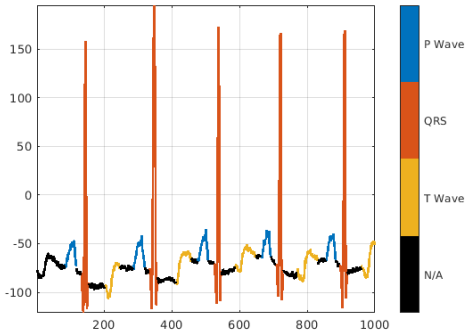

Рис. 5. Генератора тестового ЭКГ-сигнала

Пиковый детектор комплекса QRS. Другим методом, позволяющим выявить RR-интервал [17], является использование пикового детектора применительно к комплексу QRS. Структурная схема процесса оценки комплекса QRS и обнаружение его пиковых значений (зубца R) изображена на рис. 7. Результат применения пикового детектора в среде Matlab изображён на рис. 6 [11].

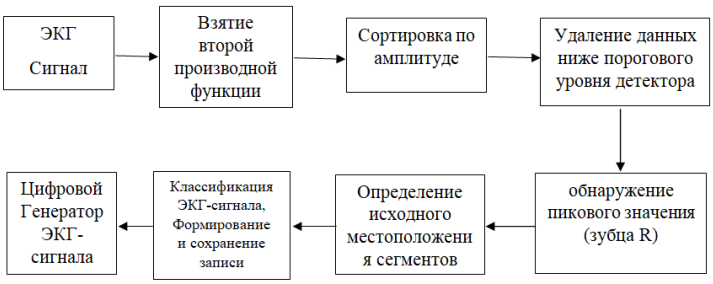

Рис. 6. Структурная схема процесса оценки комплекса QRS и обнаружение его пиковых значений

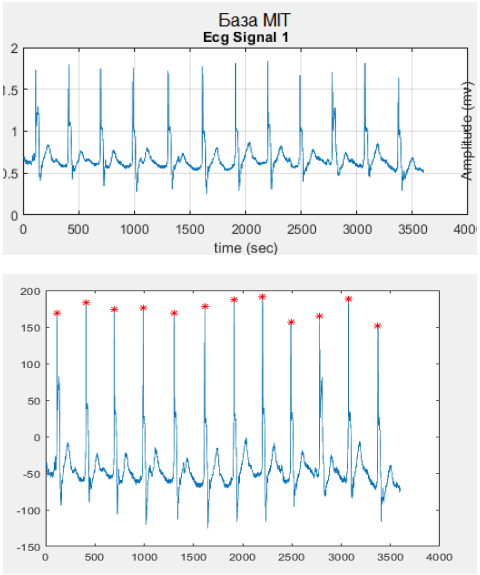

Рис. 7. Обнаружения пика R для сигнала 102mt.mat (пороговый коэффициент = 0,7)

Пиковые индексы детектора QRS. Данный метод похож на предыдущий. Отличие заключается в том, что для определения пика используются значения, которые близки к пороговому уровню [16, 20].

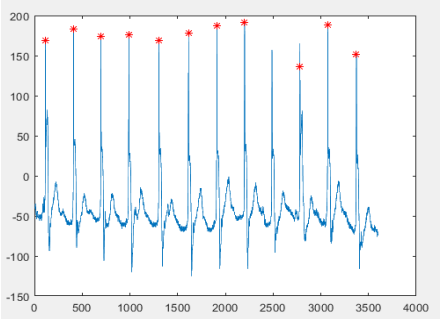

Рис. 7. Обнаружения пика R для сигнла 102mt.mat (пороговый коэффициент = 0,7)

Сравнение методов обнаружения сегментов ЭКГ-сигнала. Для оценки точности обнаружения сегментов ЭКГ-сигнала необходимо использовать такие количественные параметры, как чувствительность, специфичность, точность и средняя ошибка времени [14].

Чувствительность – это отношение количества верно не найденных R-зубцов (т.е. их нет и на самом деле) к сумме количества верно не найденных R-зубцов и ошибок второго рода (R-зубец обнаружен, но его нет на самом деле). Специфичность – это отношение количества верно найденных R-зубцов (т.е. они есть и на самом деле) к сумме количества верно найденных R-зубцов и ошибок первого рода (R-зубец не обнаружен, но на самом деле он есть).

Точность (Precision) обнаружения RR-интервала – это отношение количества верно не найденных R-зубцов к сумме количества верно не найденных R-зубцов и количества ошибок первого рода [15, 21].

Точность (Accuracy) обнаружения RR-интервала – это отношение суммы количества верно найденных пиков и количества верно не найденных к сумме количества верно найденных и верно не найденных пико и количества ошибок первого и второго рода.

Средняя ошибка времени – это отношение суммы модулей разности момента времени, в который алгоритмом был обнаружен пик, и действительному моменту времени пика к TP – количеству верно не найденных пиков[22].

Эти параметры рассчитываются с использованием следующих формул:

$$\text{чувствительность} = \frac{TP}{TP + FN}$$

$$\text{специфичность} = \frac{TN}{TN + FP}$$

$$\text{Точность } (Accuracy) = \frac{TP + TN}{TP + FN + TN + FP}$$

$$\text{Точность } (Precision) = \frac{TP}{TP + FP}$$

$$\text{Средняя ошибка времени} = \frac{\sum|\text{обнаруженное в. } QRS - \text{в реальное в. } QRS|}{TP},$$

где TN – количество верно найденных пиков (количество найденных верно пиков); FN – количество ошибок второго рода (когда пик найден, но на самом деле его нет); FP – количество ошибок первого рода (когда пик не найден, но на самом деле он есть); TP – количество верно не найденных пиков (их нет на самом деле) [19] [18, 19].

Таблица 3

Рассмотреть сравнения все методы определить наличие RR-интервалов и их сегментов следующим образом:

Метод	Чувствительность	Специфичность	Точность (Accuracy)	Точность (Precision)	Средняя ошибка времени
DWT	0,975	0,991	0,988	0,985	3,56
Пиковый детектор	0,931	0,955	0,947	0,954	6,9
Пиковые индексы детектора	0,901	0,945	0,953	0,957	7,1

Заключение. В результате проделанной работы было выявлено, что метод дискретного вейвлет-преобразования (DWT) позволяет с высокой точностью определить наличие RR-интервалов и их сегментов. Это позволяет использовать данный метод для классификации ЭКГ-сигналов, формирования базы записей данных сигналов и генерирования тестовых сигналов, предназначенных для оценки характеристик носимых цифровых ONLINE-мониторов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Интернет-портал PhysioNet. – URL: https://www.physionet.org.
2. *Ту Дж., Гонсалес Р.* Принципы распознавания образов: пер. И.П. Гуревича / под ред. Ю.И. Журавлева. – М.: Мир, 1978. – С. 410-415.
3. *Бейтс Р.А., Хилтон М.Ф., Годфри К.Р. и Чаппелл М.Дж.* Сравнение методов гармонического вейвлет-анализа вариабельности сердечного ритма. – 1998. – С. 278-299.
4. *Эрчелеби Э.* Удаление шума сигналов электрокардиограммы с использованием дискретного вейвлет-преобразования на основе подъема. – 2004. – С. 479-493.
5. *Пиньомарк А., Лимсакул К., Пхукпаттаранонт П.* Оптимальные вейвлет-функции в вейвлет-шумоподавлении для многофункционального миоэлектрического управления // ECTI Transactions по электротехнике, электронике и коммуникациям. – ECTI, 2010. – С. 43-52.
6. *Чуакри S.* Вейвлет-шумоподавление сигнала электрокардиограммы на основе оценки искаженного шума // Компьютеры в кардиологии. – 2005, IEEE.
7. *Хаберл Р., Джиге Г., Пултер Р., Стейнбек Г.* Спектральное картирование электрокардиограммы с преобразованием Фурье для идентификации пациентов с устойчивой желудочковой тахикардией и ишемической болезнью сердца. – С. 310-326.
8. *Месте О., Рикс Х., Каминал П., Такор Н.* Характеристика поздних потенциалов желудочков в частотно-временной области с помощью вейвлет-преобразования // Транзакция IEEE по биомедицинской инженерии. – 1994. – С. 625-633.
9. *Морлет Д., Кудерк Дж. П., Тубул П., Рубель П.* Вейвлет-анализ ЭКГ высокого разрешения у пациентов после инфаркта: роль основного вейвлета и анализируемого отведения. – 1995. – С. 308-330.
10. *Симсон М.Б., Эйлер Д., Майкельсон Э.* Обнаружение задержки активации желудочков на поверхности тела у собак. – 1981. – С. 362-372.
11. *Симсон М.Б.* Использование сигнала терминального комплекса QRS для идентификации пациентов с желудочковой тахикардией после инфаркта миокарда. – 1981. – С. 230-244.
12. *Эберт Х.* Легкая ЭКГ. Интерпретация дифференциальных диагнозов. – Штутгарт; Нью-Йорк: Тиме, 2005. – С. 138-140.
13. *Авдеева Д.К., Казаков В.Ю., Наталинова Н.М., Иванов М.Л.* Результаты моделирования воздействия фильтра высокой частоты и фильтра низкой частоты на качество регистрации микропотенциалов на электрокардиограмме. – 2013. – С. 318.
14. *Рангайян Р.М.* Анализ биомедицинских сигналов. Практический подход. – 2007. – С. 438-444.
15. *Смоленцев Н.К.* Основы теории вейвлетов. Вейвлеты в MatLab. – 2005. – С. 304-310.
16. *Дроздов Д.В.* Влияние фильтрации на диагностические свойства биосигналов // Функциональная диагностика. – 2011. – С. 75-78.
17. *Дубровин В.И., Твердохлеб Ю.В., Харченко В.В.* Автоматизированная система анализа и интерпретации ЭКГ // Радиоэлектроника, информатика, управление. – 2014. – С. 148-160.
18. Сайт «PhysioBank Archive Index». – http://www.physionet.org/physiobank/database/.
19. *Гольденберг Л.М.* Справочник. Цифровая обработка сигналов. – М.: Радио и связь, 1985. – С. 310-314.
20. *Гайдышев И.* Анализ и обработка. – СПб., 2006. – С. 750-754.
21. *Монахова О.А.* Регистрация каррдиоинтервалограммы по вейвлетному спектру электрокардиограммы. – Саратов, 2009. – С. 10-17.
22. *Монахова О.А.* Исследование тонкой структуры электрокардиографического сигнала методами вейвлетного анализа. – Саратов, 2009. – С. 119-132.

REFERENCES

1. Internet-portal PhysioNet [The Internet portal PhysioNet]. Available at: https://www.physionet.org.
2. *Tu Dzh., Gonsales R.* Printsipy raspoznavaniya obrazov [Principles of image recognition]: translated by I.P. Gurevicha, ed. by Yu.I. Zhuravleva. Moscow: Mir, 1978, pp. 410-415.
3. *Beyts R.A., Khilton M.F., Godfri K.R. i Chappell M.Dzh.* Sravnenie metodov garmonicheskogo veyvlet-analiza variabel'nosti serdechnogo ritma [Comparison of methods of harmonic wavelet analysis of heart rate variability], 1998, pp. 278-299.
4. *Erchelebi E.* Udalenie shuma signalov elektrokardiogrammy s ispol'zovaniem diskretnogo veyvlet-preobrazovaniya na osnove pod"ema [Noise removal of electrocardiogram signals using discrete lift-based wavelet transform], 2004, pp. 479-493.
5. *Pin'omark A., Limsakul K., Pkhukpattaranont P.* Optimal'nye veyvlet-funktsii v veyvlet-shumopodavlenii dlya mnogofunktsional'nogo mioelektricheskogo upravleniya [Optimal wavelet functions in wavelet noise reduction for multifunctional myoelectric control], *ECTI Transactions po elektrotekhnike, elektronike i kommunikatsiyam* [ECTI Transactions in Electrical engineering, Electronics and Communications]. ECTI, 2010, pp. 43-52.
6. *Chuakri S.* Veyvlet-shumopodavlenie signala elektrokardiogrammy na osnove otsenki iskazhennogo shuma [Wavelet noise reduction of the electrocardiogram signal based on the assessment of distorted noise], *Komp'yutery v kardiologii* [Computers in Cardiology], 2005, IEEE.
7. *Khaberl R., Dzhige G., Pulter R., Steynbek G.* Spektral'noe kartirovanie elektrokardiogrammy s preobrazovaniem Fur'e dlya identifikatsii patsientov s ustoychivoy zheludochkovoy takhikardiey i ishemicheskoy bolezn'yu serdtsa [Spectral mapping of a fourier transform electrocardiogram for the identification of patients with sustained ventricular tachycardia and ischemic heart disease], pp. 310-326.
8. *Meste O., Riks Kh., Kaminal P., Takor N.* Kharakteristika pozdnikh potentsialov zheludochkov v chastotno-vremennoy oblasti s pomoshch'yu veyvlet-preobrazovaniya [Characterization of late ventricular potentials in the time-frequency domain using a wavelet transform], *Tranzaktsiya IEEE po biomeditsinskoy inzhenerii* [IEEE transaction on biomedical engineering], 1994, pp. 625-633.
9. *Morlet D., Kuderk Dzh. P., Tubul P., Rubel' P.* Veyvlet-analiz EKG vysokogo razresheniya u patsientov posle infarkta: rol' osnovnogo veyvleta i analiziruemogo otvedeniya [High-resolution ECG wavelet analysis in patients after a heart attack: the role of the main wavelet and the analyzed lead], 1995, pp. 308-330.
10. *Simson M.B., Eyler D., Maykel'son E.* Obnaruzhenie zaderzhki aktivatsii zheludochkov na poverkhnosti tela u sobak [Detection of delayed ventricular activation on the body surface in dogs], 1981, pp. 362-372.
11. *Simson M.B.* Ispol'zovanie signala terminal'nogo kompleksa QRS dlya identifikatsii patsientov s zheludochkovoy takhikardiey posle infarkta miokarda [Using the signal of the terminal complex QRS to identify patients with ventricular tachycardia after myocardial infarction], 1981, pp. 230-244.
12. *Ebert Kh.* Legkaya EKG. Interpretatsiya differentsial'nykh diagnozov [Light ECG. Interpretation of differential diagnoses]. Shtutgart; N'yu-York: Time, 2005, pp. 138-140.
13. *Avdeeva D.K., Kazakov V.Yu., Natalinova N.M., Ivanov M.L.* Rezul'taty modelirovaniya vozdeystviya fil'tra vysokoy chastoty i fil'tra nizkoy chastoty na kachestvo registratsii mikropotentsialov na elektrokardiogramme [Results of modeling the effect of a high-frequency filter and a low-frequency filter on the quality of recording micro-potentials on an electrocardiogram], 2013, pp. 318.
14. *Rangayyan R.M.* Analiz biomeditsinskikh signalov. Prakticheskiy podkhod [Analysis of biomedical signals. Practical approach], 2007, pp. 438-444.
15. *Smolentsev N.K.* Osnovy teorii veyvletov. Veyvlety v MatLab [Fundamentals of wavelet theory. Wavelets in MatLab], 2005, pp. 304-310.
16. *Drozdov D.V.* Vliyanie fil'tratsii na diagnosticheskie svoystva biosignalov [Influence of filtering on diagnostic properties of biosignals], *Funktsional'naya diagnostika* [Functional diagnostics], 2011, pp. 75-78.
17. *Dubrovin V.I., Tverdokhleb Yu.V., Kharchenko V.V.* Avtomatizirovannaya sistema analiza i interpretatsii EKG [Automated system of analysis and interpretation of ECG], *Radioelektronika, informatika, upravlenie* [Radioelectronics, informatics, managemen], 2014, pp. 148-160.
18. Cayt «PhysioBank Archive Index» [The Website "PhysioBank Archive Index"]. Available at: http://www.physionet.org/physiobank/database/.
19. *Gol'denberg L.M.* Spravochnik. TSifrovaya obrabotka signalov [Guide. Digital signal processing]. Moscow: Radio i svyaz', 1985, pp. 310-314.

20. *Gaydyshev I.* Analiz i obrabotka [Analysis and processing]. Saint Petersburg, 2006, pp. 750-754.
21. *Monakhova O.A.* Registratsiya karrdiointervalogrammy po veyvletnomu spektru elektro-kardiogrammy [Check cardiointervalogram in the wavelet spectrum of the electro-cardiogram]. Saratov, 2009, pp. 10-17.
22. *Monakhova O.A.* Issledovanie tonkoy struktury elektrokardiograficheskogo signala metodami veyvletnogo analiza [Investigation of the fine structure of the electrocardiographic signal by wavelet analysis methods]. Saratov, 2009, pp. 119-132.

Статью рекомендовал к опубликованию д.т.н., профессор З.М. Юлдашев.

Рагеб Ага Мохамад – Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»; e-mail: aga.mod@hotmail.co.uk; 197376, Санкт-Петербург, ул. проф. Попова, 5; тел.: 88122343059; кафедра биотехнических систем; аспирант.

Ragheb Agha Mokhamed – Saint Petersburg Electrotechnical University “LETI”; e-mail: aga.mod@hotmail.co.uk; 5, prof. Popova street, Saint Petersburg, 197376, Russia; phone: +78123464487; the department of biotechnical systems; graduate student.

УДК 681.324 DOI 10.18522/2311-3103-2020-5-40-51

В.И. Потапов

ПРИМЕНЕНИЕ ЗАПРЕЩЕННЫХ ФИГУР В ЗАДАЧЕ РАСКРАСКИ ГРАФА ПРИ ПРОЕКТИРОВАНИИ ПЕЧАТНЫХ ПЛАТ

Проектирование конструкции печатных плат в виде плоских структур без перемычек является одной из самых сложных задач на этапе схемотехнического проектирования. Задача в такой постановке особенно актуальна микросборок и для электронных модулей контрольно-проверочной, бортовой аппаратуры, выполненных по технологии поверхностного монтажа, где, например, по причине металлического теплоотвода или керамического основания, структура соединений возможна только в одном слое. В работе рассматривается задача проектирования печатных плат в виде синтеза плоских структур электронных схем. Целью является расположение соединений на печатной плате без пересечений, что облегчает условия проведения трасс любому трассировщику современных программ проектировании. Для её решения предложено большое число различных алгоритмов, основным недостатком которых является заложенный в них принцип последовательного и фрагментарного просмотра коммутационного пространства. Сложность алгоритмов синтеза подобных структур обусловлена также необходимостью учета большого числа различных требований, связанных со спецификой их изготовления и особенностями разрабатываемого конструктивно-технологического решения. В настоящей работе предлагается выполнить проектирование печатной платы с высокой эффективностью трассировки соединений за счет решения задачи расслоения исходного графа-схемы и построения плоского графа-схемы как на стороне установки ЭРЭ, так и на обратной стороне платы - стороне пайки, исключая запрещенные фигуры по теореме Потрягина-Куратовского. Критерием является минимизация переходных отверстий, а также минимизация проводников (ребер) на одной стороне печатной платы. Задача расслоения представляет собой задачу раскраски графа в два цвета с использованием принципов характеризационного управления, решение которой базируется на теореме Кенига, определяющей запрещенную фигуру в виде циклов нечетной длины. Для проектирования печатных плат разработаны алгоритм и методика построения планарных графов и расслоения графа на две стороны печатной платы с уменьшением количества неразведенных ребер. Точное решение принимает вид полиномиальной зависимости не выше 5-й степени, позволяет получить результат за приемлемое время и повысить эффективность трассировки на 5–15 %.

Плоские структуры электронных средств; графо-теоретический подход; запрещенные фигуры; трассировка в одном слое; граф; ребро графа; планарность; алгоритм; анализ; синтез; электро-радиоэлемент.

V.I. Potapov

APPLICATION OF FORBIDDEN SHAPES IN THE GRAPH COLORING PROBLEM WHEN DESIGNING PRINTED CIRCUIT BOARDS

Designing a printed circuit board in the form of flat structures without jumpers is one of the most difficult tasks at the stage of circuit design. The task in this formulation is especially relevant for micro-assemblies for electronic modules of control and verification, on-board equipment, made using surface-mount technology, where, for example, due to a metal heat sink or a ceramic base, the structure of connections is possible only in one layer. The paper deals with the problem of designing printed circuit boards in the form of synthesis of flat structures of electronic circuits. The goal is to position the connections on the PCB without overlapping, making it easier for any router in modern design programs to route. To solve it, a large number of different algorithms have been proposed, the main disadvantage of which is the principle of sequential and fragmentary viewing of the switching space inherent in them. The complexity of the algorithms for the synthesis of such structures is also due to the need to take into account a large number of different requirements associated with the specifics of their manufacture and the features of the developed constructive and technological solution. In this paper, it is proposed to design a printed circuit board with a high efficiency of routing connections by solving the problem of stratifying the original graph-scheme and constructing a flat graph-scheme both on the installation side of the electrical radio elements and on the reverse side of the board - the soldering side, excluding forbidden figures according to Potryagin's theorem - Kuratovsky. The criterion is to minimize vias as well as minimize conductors (fins) on one side of the PCB. The bundle problem is a graph coloring problem in two colors using the principles of characterization control, the solution of which is based on the Koenig theorem, which defines a forbidden figure in the form of cycles of odd length. For the design of printed circuit boards, an algorithm and method for constructing planar graphs and stratifying the graph into two sides of the printed circuit board with a decrease in the number of undistributed edges have been developed. The exact solution takes the form of a polynomial dependence not higher than the 5th degree, it allows you to get the result in a reasonable time and increase the tracing efficiency by 5–15 %.

Flat structure of electronic means; graph-theoretical approach; prohibited figures; trace in a single layer; graph; an edge of the graph; planarity prohibited figure; algorithm; analysis; synthesis; electric radio element.

Введение. Проектирование конструкции печатных плат без перемычек является одной из самых сложных задач на этапе конструирования. Задача в такой постановке особенно актуальна для бортовых электронных модулей, выполненных по технологии поверхностного монтажа, где, например, по причине металлического теплоотвода или керамического основания, структура соединений возможна только в одном или двух слоях.

Для её решения предложено большое число различных алгоритмов [1–3, 5, 9–11], основным недостатком которых является заложенный в них принцип последовательного и фрагментарного просмотра коммутационного пространства. Сложность алгоритмов синтеза подобных структур обусловлена также необходимостью учета большого числа различных требований, связанных со спецификой их изготовления и особенностями разрабатываемого конструктивно-технологического решения.

Конечная задача – получение 100 % трассировки соединений на печатной плате, для достижения которой необходимо учитывать следующие характерные свойства:

- ♦ большая размерность;
- ♦ необходимость контроля на промежуточных и окончательных стадиях, обусловленная значительным временем решения или вмешательством человека;
- ♦ недопустимость пересечения трасс, принадлежащих разным электрическим цепям;
- ♦ связь топологических ограничений со схемотехническими и теплофизическими ограничениями.

Теоретическая часть. В алгоритмическом плане задача заключается в построении для всех цепей схемы оптимальных монтажных соединений. Алгоритмические методы трассировки печатных соединений в зависимости от конструкции коммутационного поля делятся на две основные группы: топографические и графо-теоретические.

Топографические методы наиболее эффективны для трассировки двусторонних и многослойных печатных плат, подложек БИС, а также твердотельных БИС с несколькими слоями коммутации.

На первом этапе формируется список цепей, определяющий группы эквипотенциальных выводов. Здесь главной задачей является предварительное определение порядка соединений выводов внутри отдельных цепей. Такое упорядочение осуществляется с помощью алгоритмов построения минимальных деревьев.

На втором и третьем этапах решаются вопросы, на каком из слоев будет осуществляться трассировка соединений и в каком порядке. Большинство известных методов расслоения соединений основаны на анализе взаимного расположения всей совокупности соединений на одной плоскости с целью распределения конфликтующих между собой соединений по отдельным слоям. Поскольку подавляющее большинство алгоритмов трассировки принадлежит к алгоритмам последовательного типа, то порядок прокладки соединений определяется заранее.

Графо-теоретические методы трассировки предполагают предварительный анализ планарности схемы, представленной в виде графовой модели, и последующую ликвидацию пересечений с помощью технологических приемов. Окончательная фаза состоит в получении эскиза топологии схемы при оптимальном распределении функций между конструктором и САПР. Практическая реализация связана со сложностью учета различных метрических ограничений на расположение элементов и соединений. Кроме того, для корректного проведения топологического анализа необходимо применять адекватные топологические модели элементов, электрических соединений и конструкции коммутационной схемы. В этой группе методов центральное место отводится алгоритмам определения планарности графов. С точки зрения удобства реализации выделяются следующие: алгоритм Бадера-Фишера, алгоритм Дана и Чена и др.

Попытки применить графо-теоретические методы к проектированию топологии печатных плат нашли наиболее яркое отражение в работе Ауслендера и Трента. Была представлена модель, позволяющая в принципе расположить схему соединений любой сложности в двух слоях с переходами между ними, при условии, что метрические параметры коммутационного поля не влияют на возможность такой раскладки. Но если межслойные переходы могут быть выполнены лишь по контактным площадкам (КП) устанавливаемых элементов, то возникает задача расположения соединений в минимальном числе слоев. В топологическом плане она сводится к нахождению минимального планарного разбиения графа схемы (задача расслоения). Однако ввиду указанных выше сложностей для практического использования наиболее приемлемыми оказались эвристические последовательные процедуры выделения планарных подграфов из исходного графа.

Расслоение осуществляется с целью распределения "конфликтующих" соединений по отдельным слоям для наиболее эффективного использования площади коммутационного поля. Алгоритмическое расслоение может выполняться до, после и в процессе трассировки отдельных соединений.

Расслоение до трассировки основано на выявлении возможностей разбиения графа схемы на минимальное число планарных подграфов с последующей реализацией этих подграфов на отдельных слоях. Основная сложность такого подхода состоит в построении точных математических моделей схемы с учетом метриче-

ских параметров коммутационного поля. Но в большинстве случаев расслоение выполняется после размещения элементов и более простой путь состоит в учете "взаимодействия" отдельных соединений или связывающих деревьев при условии их одновременного расположения на одной плоскости. При этом учитываются метрические параметры соединений, так как положение КП на коммутационном поле уже известно. Наиболее распространенным приемом является выделение некоторых приоритетных направлений, группирование соединений в соответствии с выбранными направлениями и разнесение этих групп на отдельные слои.

Фундаментальные теоретические основы указанного подхода заложены работами Кодреса и Вайссмана. Задача Кодреса заключается в ликвидации минимального числа пересечений таким образом, чтобы было возможно реализовать соединение без пересечений в двух слоях. Для каждой цепи предварительно строится минимальное дерево и связь между слоями возможна только в точках, соответствующих выводам элементов, а неизбежные пересечения устраняются с учетом дополнительных конструктивных возможностей (проход между выводами элементов). Системе проводников на плоскости ставится в соответствие граф пересечений $\Gamma = (X, L)$, вершины которого $x \in X$ соответствуют отдельным проводникам, а ребра $l \in L$ – их пересечениям. Ищется такая двухцветная раскраска графа Г, при которой суммарное количество ребер, соединяющих одноцветные вершины будет минимально (количество неустраненных пересечений). При этом вершины одного цвета соответствуют проводникам, расположенным в одном слое. Такая задача выделения в графе Г максимального по числу ребер бихроматического подграфа решается методами линейного программирования.

Аналогичная задача состоит в ликвидации минимального числа проводников для получения двухслойного разложения.

Расслоение проводников сводится к получению раскраски вершин графа пересечений $U = (X, L)$ в минимальное число цветов. Особенностью задачи является то обстоятельство, что для каждой пары выводов требуется выбрать по одному пути таким образом, чтобы обеспечить разложение всей системы соединений в минимальное число слоев. Для отдельных модификаций метода Вайссмана характерно отсутствие ограничений на геометрию соединений, но реализация метода связана с большими временными затратами, увеличивающимися с ростом размерности задачи.

В силу этих обстоятельств он послужил теоретической основой для построения приближенных процедур расслоения. В ряде работ при ортогональной трассировке соединений предлагается тривиальное распределение проводников на два слоя, когда все горизонтальные отрезки помещаются в одном слое, а вертикальные – в другом. В точках изгибов соединений размещаются контактные переходы. Однако в этом случае возникает избыточное число переходов. Алгоритм дает сокращение числа переходов до 60 % по сравнению с чисто ортогональным расслоением. Получение точного решения такой задачи представляется весьма проблематичным ввиду ее большой размерности. В этой связи предложен ряд эвристических процедур минимизации числа переходов. В частности, локальная минимизация числа переходов в процессе трассировки многослойных соединений. Определенный интерес также представляют алгоритмы Хейса и Джейера, в которых процессы трассировки и расслоения совмещены. Исходя из проведенного выше анализа следует, что предварительное расслоение является эффективным для многослойных схем, в которых ограничено число межслойных переходов. В этом случае существенно сокращается время трассировки (по сравнению с процессом последовательного заполнения слоев, при котором осуществляются попытки трассировки заведомо не разводимых в данном слое соединений). Кроме того, предварительное

расслоение дает лучшее использование коммутационного поля и уменьшение числа слоев. А для двухслойных схем с ортогональной коммутацией наиболее эффективна трассировка, включающая построение совмещенной топологии схемы и последующее расслоение с минимизацией числа переходов.

В последние годы получили развитие бионические алгоритмы.

Бионические алгоритмы. Ученые не отступают от решения проблемы в виде достижения 100 % трассировки соединений печатной платы. Для этого были разработаны алгоритмы планаризации графов на основе [9, 20, 21]:

- бионических технологий;
- квантовых алгоритмов;
- генетических алгоритмов;
- алгоритм Курапова;
- алгоритм «У».

Известные методы планаризации графов, опирающиеся на то, что оптимизируемая функция обладает набором определенных качеств, например одноэкстремальностью, зачастую не справляются с решением подобных прикладных задач. Поэтому в настоящее время для этих целей используются принципиально отличающиеся от них стохастические многоагентные алгоритмы бионического класса в виде алгоритмов:

- муравьиный алгоритм (Ant Colony Optimization (ACO)),
- алгоритм умных капель (Intelligent Water Drops (IWDs)),
- генетический алгоритм (Genetic Algorithm (GA или ГА)),
- адаптивный ГА (adaptive GA),
- эвристика Лин-Кернигана для решения задач комбинаторной оптимизации.

Задача планаризации графа относится к классу NP-полных задач. Одним из методов решения задач оптимизации является локальный спуск, в частности алгоритм 3-замены (3-opt). Суть алгоритма состоит в том, что относительно текущего решения, представленного циклическим графом f со значением целевой функции c(f), рассматривается его окрестность, то есть множество циклических графов, которые можно получить из f удалением не более 3х ребер и заменой другими 3-мя ребрами. Если в этом множестве существует граф g, целевая функция которого $c(g)=\phi(c(f))$, то g назначается текущим решением. Процедура повторяется до тех пор, пока текущее решение не перестанет изменяться.

Сравнительные результаты нахождения экстремального значения целевой функции для рассматриваемых алгоритмов: 3-замена, ACO, IWDs, GA, Adaptive GA, отклонение достигнутого значения от лучшего, составило, соответственно в %: 9.27; 0.22; 6.37; 14.35; 15.10.

Таким образом, для решения исходной задачи, помимо классических алгоритмов, могут быть использованы бионические алгоритмы комбинаторной оптимизации. Была исследована эффективность этих алгоритмов на задаче комбинаторики, проведен сравнительный анализ работы данных алгоритмов. Результаты исследования констатируют, что рассмотренные алгоритмы находят приближенное решение построения планарного графа.

Алгоритмы построения плоского графа. Существует ряд других алгоритмов определения плоского графа и укладки планарных графов:

1. Алгоритмы, основанные на добавлении пути («path additional algorithm»);
2. Алгоритмы, основанные на добавлении вершин («vertex additional algorithm»);
3. Алгоритм плоской укладки графов был предложен Ауслендером и Партером;
4. Хопкрофт и Тарьян смогли улучшить оценку времени работы алгоритма, предложив алгоритм на основе добавления простого пути на каждом шаге;

5. Алгоритм на основе добавления на каждом шаге новой вершины был представлен Лемпелем и Кедербаумом;

6. Алгоритм Буса и Люкера позволяет не только проверить граф на планарность, но и построить плоскую укладку на плоскости;

7. Гамма – алгоритм. Алгоритм представляет собой процесс последовательного присоединения к уложенному подграфу G' графа G новой цепи, оба конца которой принадлежат G';

8. Алгоритм укладки графа на плоскости на основе PQ – деревьев. Алгоритм плоской укладки графов предложили Чибой Н. и Нижезеки Т. и основан на подходе добавления на каждом шаге новой вершины графа;

9. Алгоритм для поиска st – нумерации был предложен в 1976 году Тарьяном Р. и Ивеном Ш.;

10. Алгоритм, предложенный Ивеном и Кедербаумом, который проверяет граф на планарность, используя такую структуру данных как PQ - дерево;

11. Алгоритм, предложенным Бусом и Люкером, PQ - деревья представляют все возможные перестановки и обращения элементов (вершин) баш – формы B_k.

12. Алгоритм ENTIRE – EMBEDED, позволяем расширить укладку A_u(v) графа D_u в укладку A исходного графа G.

Наблюдается приближенное решение и экспоненциальная зависимость трудоемкости выполнения алгоритмов и максимальная достижимость эффективности трассировки соединений, равная 90.1%

Экспериментальная часть. Рассмотрим классический подход к разработке печатных плат, использующих электро-радиоэлементы (ЭРЭ) с «жесткой» логикой функционирования. В начале разрабатывается принципиальная электрическая схема, а затем создается конструкция за счет решения задач размещения ЭРЭ и трассировки соединений на монтажном поле. Этот подход сложился исторически за счет того, что каждый вывод ЭРЭ несет свое функциональное значение. На основе анализа проведенного в [2, 3, 6, 9, 14, 17–19] для решения данной задачи будем использовать графо - теоретический метод, который предполагает планаризацию графа, расслоение графа на две стороны для ДПП и предварительный анализ планарности графа схемы с последующей ликвидацией пересечений, назначая конфликтное звено трассы на обратную сторону печатной платы.

Основной задачей создания топологии схемы соединений выводов ЭРЭ является необходимость расположения соединений на плоскости без пересечений, что облегчает условия проведения трасс любому трассировщику современных программ проектирования.

Задача трассировки соединений выводов элементов в схеме заключается в синтезе плоского графа схемы, не содержащего подграфов гомеоморфных К 5 или К 3,3.

В [2, 6, 14, 17–19] приведен алгоритм планаризации графа из теории характеризационного управления, основанный на нахождении запрещенных фигур и перевода их из класса запрещенных в класс разрешенных.

Основным требованием, предъявляемым к системам автоматизированного проектирования плоских конструкций печатных плат с различным количеством слоев, является обеспечение 100 % эффективности трассировки соединений, под которой понимается отношение количества реализованных соединений на одном слое к общему количеству соединений.

В настоящей работе предлагается выполнить проектирование печатной платы с высокой эффективностью трассировки соединений за счет решения задачи расслоения исходного графа-схемы и построения плоского графа-схемы как на стороне установки ЭРЭ, так и на обратной стороне платы – стороне пайки, исключая запрещенные фигуры по теореме Потрягина-Куратовского [6]. Критерием является

минимизация переходных отверстий или минимизация количества проводников (ребер) на одной стороне печатной платы. Задача расслоения представляет собой задачу раскраски графа в два цвета, реализация которой основана на семантическом подходе с использованием принципов теории характеризационного управления. Идея реализации подробно изложена в [6, 7, 9, 14–19], и основана на теореме Кенига, определяющей запрещенную фигуру в виде циклов нечетной длины. Граф является двухцветным тогда и только тогда, когда он не содержит циклов нечетной длины [2, 3, 14, 18, 19].

Алгоритм расслоения ребер на две стороны.

1. Поиск запрещенных фигур (циклов нечетной длины).
2. Построение семантической таблицы.
3. Нахождение минимального покрытия строк таблицы столбцами. Все строки таблицы покрыты хотя бы одним столбцом? Если да, то переход к п. 7. Иначе к п.4.
4. Нахождение компоненты запрещенной фигуры для приведения исходной модели к интерпретируемому виду.
5. Удаление компоненты из исходного графа на основании семантической таблицы минимального покрытия.
6. Переход к п.1.
7. Полученное минимальное покрытие является оптимальным решением, удаление этих компонент (сигнатур) переводит запрещенные фигуры в класс разрешенных, т.е. формирует двухцветный граф.
8. Конец алгоритма.

Рассмотрим пример преобразования графа, изображенного на рис. 1, в двухцветный. Функционал качества – минимум удаленных ребер.

По теории характеризационного управления отыскиваем все запрещенные фигуры – это циклы нечетной длины. Строим семантическую таблицу (таблица1), в которой строки отражают запрещенные фигуры, а столбцы – компоненты (ребра) этих фигур.

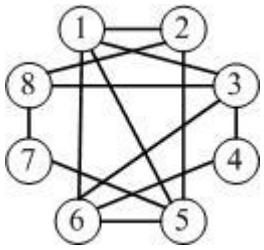

Рис. 1. Исходный граф

Минимальное покрытие строк столбцами первой таблицы указывает, какие компоненты запрещенной фигуры должны быть изменены при приведении исходной модели к интерпретируемому виду. Это компонента – ребро 38. Удаление этого ребра (рис. 2) приводит к началу алгоритма и построению второй таблицы (табл. 2). Аналогично первой таблицы, здесь также находится компонента при минимальном покрытии строк столбцами (ребро 15). Удаление этого ребра (рис. 3), приводит к началу алгоритма и построению третьей таблицы (табл. 3). Минимальное покрытие в последней таблице (ребро 36) приводит к оптимальному решению – двухцветному графу (рис. 4).

Таблица 1

Семантическая таблица

Ребра / З.Ф.	12	13	15	16	25	28	34	36	38	46	57	78
1251	1		1		1							
1361		1		1			1					
3463							1	1		1		
138751		1	1						1		1	1
16387521	1			1	1			1	1		1	1
283152		1	1		1	1			1			
163821	1			1		1		1	1			
16438751			1	1			1		1	1	1	1

Таблица 2

Семантическая таблица после удаления компоненты (ребро 38)

Ребра / З.Ф.	12	13	15	16	25	28	34	36	46	57	78
1251	1		1		1						
1361		1		1				1			
3463							1	1	1		
157821	1		1			1				1	1

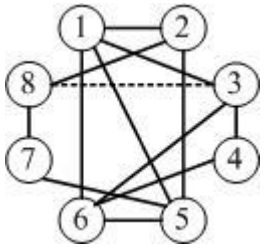

Рис. 2. Граф после удаления компоненты 38

Таким образом, ребра 38, 15, 36 переводят запрещенные фигуры (циклы нечетной длины) в класс разрешенных, а исходный граф к двухцветному виду. Этот процесс на много порядков менее трудоёмок, чем процесс фактической генерации всех эквивалентных структур при поиске минимального решения известными подходами [2, 3, 9, 11, 14–19]. Трудоемкость алгоритма не превышает полином 5 степени при достижении точного решения.

При проектировании двухсторонних печатных плат разработана методика построения планарных графов и расслоения графа на две стороны печатной платы с уменьшением количества неразведенных ребер.

Таблица 3

Семантическая таблица после удаления очередной компоненты

Ребра / З.Ф.	13	16	34	36	46
1361	1	1		1	
3463			1	1	1

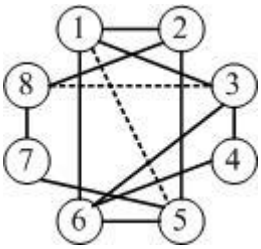

Рис. 3. Граф после очередного удаления компоненты

Рис. 4. Плоский граф: а – со стороны пайки; б – со стороны установки ЭРЭ

Основным критерием эффективности построения плоских структур является 100 % трассировка соединений между элементами структуры в одном или нескольких слоях. Оценим результаты синтеза плоских структур электронных схем, построенных с применением разработанной модели и алгоритма. Для проведения эксперимента по трассировке соединений использовался современный пакет прикладных программ Altium Designer (P-CAD) со специализированным программным обеспечением (СПО).

Проведенный сравнительный анализ, представленных результатов трассировки (возможность 100 % трассировки) применяемых САПР, полученных «До» (без участия планаризации) и «После» (планаризации) использования предлагаемого подхода планаризации исходных графов для проектирования плоских структур электронных схем, позволяет повысить эффективность трассировки соединений в среднем на 5–15 %. Информация представлена в табл. 4, а на рис. 5 показана зависимость эффективности трассировки (в процентах) в обычном режиме и после проведения планаризации относительно установленной на предприятии нормированной трудоемкости выполнения работ, связанной с размещением, трассировкой и последующей доработкой. Количество связей в исходной схеме на момент проведения исследований – 920 шт.

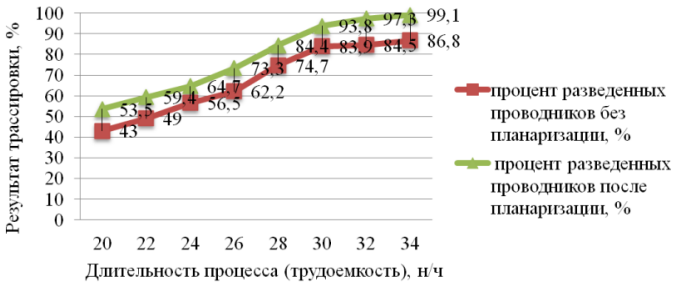

Рис. 5. График зависимости трассировки в обычном режиме и после проведения планаризации относительно длительности процесса

Таблица 4

Зависимость результата трассировки без планаризации и с планаризацией

N	Время процесса (трудоемкость), н/ч	Процент разведенных проводников без планаризации, %	ПРОЦЕНТ разведенных проводников после планаризации, %
1	20	43	53,5
2	22	49	59,4
3	24	56,5	64,7
4	26	62,2	73,3
5	28	74,7	84,4
6	30	83,9	93,8
7	32	84,5	97,3
8	34	86,8	99,1

Заключение. При проектировании двухсторонних печатных плат разработана методика построения планарных графов и расслоения графа на две стороны печатной платы с уменьшением количества неразведенных ребер, основанная на теории характеризационного управления. Трудоемкость получения точного решения задачи принимает вид полиномиальной зависимости не выше 5-й степени и позволяет получить результат за приемлемое время при этом эффективность трассировки вырастает на 5–15 %.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. *Алексеев О.В., Головков А.А., Пивоваров И.Ю.* Автоматизация проектирования радиоэлектронных средств. – М.: Высшая школа, 2000. – 479 с.
2. *Горбатов В.А.* Фундаментальные основы дискретной математики. Информационная математика. – М.: Наука, Физматлит, 2000. – 544 с.
3. *Горбатов В.А., Смирнов М.И., Хлытчиев И.С.* Логическое управление распределенными системами. – М.: Энергоатомиздат, 1991. – 287 с.
4. *Шеин А.Б, Лазарева Н.М.* Методы проектирования электронных устройств. – М.: Инфра-инженерия, 2011. – 456 с.
5. *Муромцев Д.Ю., Тюрин И.В., Белоусов О.А., Курносов Р.Ю.* Проектирование функциональных узлов и модулей радиоэлектронных средств. – СПб.: Лань, 2018. – 251 с.
6. *Берж К.* Теория графов и ее применение. – М.: Иностранная литература, 1962. – 320 с.
7. *Норенков И.П.* Основы автоматизированного проектирования. – М.: МГТУ им. Баумана, 2009. – 430 с.
8. *Юрков Н.К.* Технология радиоэлектронных средств. – Пенза: ПГУ, 2012. – 640 с.
9. *Гладков Л.А., Курейчик В.В., Курейчик В.М.* Дискретная математика. – М.: Физматлит, 2014. – 496 с.
10. *Курейчик В.М., Лебедев О.Б., Лебедев Б.К.* Поисковая адаптация. – М.: Физматлит, 2006. – 270 с.
11. *Петров Ю.В.* Методы математического моделирования радиотехнических систем. – СПб.: Балт. гос. техн. ун-т, 2005. – 111 с.
12. *Пирогова Е.В.* Проектирование и технология печатных плат. – М.: Форум, 2005. – 559 с.
13. *Муромцев Ю.Л., Муромцев Д.Ю., Тюрин И.В.* Информационные технологии проектирования радиоэлектронных средств. – М.: Академия, 2010. – 384 с.
14. *Потапов В.И., Сускин В.В., Шевченко В.Ф.* Теория характеризационного управления в конструировании плоских структур радиоэлектронных средств. – Рязань: ООО «Экотекст», 2017. – 92 с.
15. *Потапов В.И., Сускин В.В.* Об одном подходе к синтезу плоских структур электронных средств с жесткой логикой функционирования // Вестник Рязанского государственного радиотехнического университета. – 2016. – № 56. – С. 83-89.

16. *Потапов В.И., Сускин В.В.* Модели и алгоритмы проектирования плоских структур электронных средств на основе гибкой элементной базе // Вестник Рязанского государственного радиотехнического университета. – 2017. – № 62. – С 79-88.
17. *Потапов В.И.* Задача синтеза структуры электронных модулей, построенных с использованием принципов характеризационного управления // Сб. статей Всероссийской научно-практической конференции «Стратегия научно-технологического развития России: проблемы и перспективы реализации. МЦНП «Новая наука». – Петрозаводск, 2020. – С. 18-30.
18. *Потапов В.И., Сускин В.В., Филаткин С.В.* Принцип построения плоских конструкций электронных схем с учетом запрещенных фигур // IOP Conference Series: Materials Science and Engineering (MSE), 2020.
19. *Потапов В.И.* Запрещенные фигуры в проектировании конструкций электронных модулей // XXV Юбилейная Всероссийская научно-техническая конференция студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях (НИТ-2020): Тез. докл. Рязан. гос. радиотехн. ун-т. Рязань, 2020.
20. *Гуменникова А.В., Емельянова М.Н., Семенкин Е.С., Сопов Е.А.* Об эволюционных алгоритмах решения сложных задач оптимизации // Вестник СибГАУ. – 2003. – № 4. – С. 14-23.
21. *Онищенко Т.Ю., Марасанов В.В.* Характеризационный анализ как оптимизационный метод контроля и прогнозирование работоспособности электронных схем // Вестник ХНТУ. – 2013. – № 3. – С. 12-19.

REFERENCES

1. *Alekseev O.V., Golovkov A.A., Pivovarov I.Yu.* Avtomatizatsiya proektirovaniya radioelektronnykh sredstv [Automation of design of radio-electronic means]. Moscow: Vysshaya shkola, 2000, 479 p.
2. *Gorbatov V.A.* Fundamental'nye osnovy diskretnoy matematiki. Informatsionnaya matematika [Fundamental foundations of discrete mathematics. Information Mathematics]. Moscow: Nauka, Fizmatlit, 2000, 544 p.
3. *Gorbatov V.A., Smirnov M.I., Khlytchiev I.S.* Logicheskoe upravlenie raspredelennymi sistemami [Logical management of distributed systems]. Moscow: Energoatomizdat, 1991, 287 p.
4. *Shein A.B, Lazareva N.M.* Metody proektirovaniya elektronnykh ustroystv [Design methods for electronic devices]. Moscow: Infra-inzheneriya, 2011, 456 p.
5. *Muromtsev D.Yu., Tyurin I.V., Belousov O.A., Kurnosov R.Yu.* Proektirovanie funktsional'nykh uzlov i moduley radioelektronnykh sredstv [Design of functional units and modules of radio-electronic means]. Saint Petersburg: Lan', 2018, 251 p.
6. *Berzh K.* Teoriya grafov i ee primenenie [Graph theory and its application]. Moscow: Inostrannaya literatura, 1962, 320 p.
7. *Norenkov I.P.* Osnovy avtomatizirovannogo proektirovaniya [Computer-aided design basics]. Moscow: MGTU im. Baumana, 2009, 430 p.
8. *Yurkov N.K.* Tekhnologiya radioelektronnykh sredstv [The technology of radio electronic means]. Penza: PGU, 2012, 640 p.
9. *Gladkov L.A., Kureychik V.V., Kureychik V.M.* Diskretnaya matematika [Discrete Mathematics]. Moscow: Fizmatlit, 2014, 496 p.
10. *Kureychik V.M., Lebedev O.B., Lebedev B.K.* Poiskovaya adaptatsiya [Search adaptation]. Moscow: Fizmatlit, 2006, 270 p.
11. *Petrov Yu.V.* Metody matematicheskogo modelirovaniya radiotekhnicheskikh system [Methods of mathematical modeling of radio engineering systems]. Saint Petersburg: Balt. gos. tekhn. un-t, 2005, 111 p.
12. *Pirogova E.V.* Proektirovanie i tekhnologiya pechatnykh plat [Design and technology of printed circuit boards]. Moscow: Forum, 2005, 559 p.
13. *Muromtsev Yu.L., Muromtsev D.Yu., Tyurin I.V.* Informatsionnye tekhnologii proektirovaniya radioelektronnykh sredstv [Information technologies for designing radio-electronic equipment]. Moscow: Akademiya, 2010, 384 p.
14. *Potapov V.I., Suskin V.V., Shevchenko V.F.* Teoriya kharakterizatsionnogo upravleniya v konstruirovanii ploskikh struktur radioelektronnykh sredstv [Theory of characterization control in the design of flat structures of radioelectronic devices]. Ryazan': OOO «Eko-tekst», 2017, 92 p.

15. *Potapov V.I., Suskin V.V.* Ob odnom podkhode k sintezu ploskikh struktur elektronnykh sredstv s zhestkoy logikoy funktsionirovaniya [About one approach to the synthesis of planar structures of electronic devices with function of rigid logic], *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Bulletin of the Ryazan State Radio Engineering University], 2016, No. 56, pp. 83-89.
16. *Potapov V.I., Suskin V.V.* Modeli i algoritmy proektirovaniya ploskikh struktur elektronnykh sredstv na osnove gibkoy elementnoy baze [Models and algorithms for designing flat structures of electronic devices based on a flexible element base], *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Bulletin of the Ryazan State Radio Engineering University], 2017, No. 62, pp. 79-88.
17. *Potapov V.I.* Zadacha sinteza struktury elektronnykh moduley, postroennykh s ispol'zovaniem printsipov kharakterizatsionnogo upravleniya [The task of synthesizing the structure of electronic modules built using the principles of characterization management], *Sb. statey Vserossiyskoy nauchno-prakticheskoy konferentsii «Strategiya nauchno-tekhnologicheskogo razvitiya Rossii: problemy i perspektivy realizatsii. MTSNP «Novaya nauka»* [Collection of articles of the all-russian scientific and practical conference " strategy of scientific and technological development of Russia: problems and prospects of implementation. MCNP "New science"]. Petrozavodsk, 2020, pp. 18-30.
18. *Potapov V.I., Suskin V.V., Filatkin S.V.* Printsip postroeniya ploskikh konstruktsiy elektronnykh skhem s uchetom zapreshchennykh figur [The principle of constructing flat structures of electronic circuits taking into account forbidden figures], *IOP Conference Series: Materials Science and Engineering (MSE), 2020*.
19. *Potapov V.I.* Zapreshchennye figury v proektirovanii konstruktsiy elektronnykh moduley [Prohibited figures in the design of electronic module structures], *XXV Yubileynaya Vserossiyskaya nauchno-tekhnicheskaya konferentsiya studentov, molodykh uchenykh i spetsialistov «Novye informatsionnye tekhnologii v nauchnykh issledovaniyakh (NIT-2020): Tez. dokl. Ryazan. gos. radiotekhn. un-t. Ryazan', 2020* [XXV Anniversary All-Russian Scientific and Technical Conference of Students, Young Scientists and Specialists " New Information Technologies in Scientific Research (NIT-2020): Abstracts of reports of the Ryazan State Radio Engineering University. Ryazan, 2020].
20. *Gumennikova A.V., Emel'yanova M.N., Semenkin E.S., Sopov E.A.* Ob evolyutsionnykh algoritmakh resheniya slozhnykh zadach optimizatsii [On evolutionary algorithms for solving complex optimization problems], *Vestnik SibGAU* [Vestnik. SibGAU], 2003, No. 4, pp. 14-23.
21. *Onishchenko T.Yu, Marasanov V.V.* Kharakterizatsionnyy analiz kak optimizatsionnyy metod kontrolya i prognozirovanie rabotosposobnosti elektronnykh skhem [Characterization analysis as an optimization method for monitoring and predicting the performance of electronic circuits], *Vestnik KhNTU* [Vestnik HNTU], 2013, No. 3, pp. 12-19.

Статью рекомендовал к опубликованию к.т.н. Р.В. Шевченко.

Потапов Вадим Игоревич – Филиал АО «РКЦ «Прогресс – ОКБ «Спектр»; e-mail: v.i.potapov@mail.ru; 390005, г. Рязань, ул. Гагарина, 59а; тел.: +79056934100; начальник опытно-экспериментального производства.

Potapov Vadim Igorevich – Joint stock company "Rocket space center "Progress" – branch special design Bureau "SPECTR"; e-mail: v.i.potapov@mail.ru; 59a, Gagarina street, Ryazan, 390005, Russia; phone: +79056934100; head of the experimental production.

УДК 004.067 DOI 10.18522/2311-3103-2020-5-52-60

Ю.А. Брюхомицкий

ВЕРИФИКАЦИЯ ДИНАМИЧЕСКИХ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ЛИЧНОСТИ НА ОСНОВЕ ВЕРОЯТНОСТНОЙ НЕЙРОННОЙ СЕТИ

Биометрическая верификация личности используются преимущественно при доступе в компьютерные и мобильные системы, а также для удаленной (голосовой) верификации. При этом наибольшее распространение получили системы биометрической верификации по фиксированной парольной фразе, которые достаточно просты в реализации, но очень уязвимы для атак воспроизведения скомпрометированного короткого текста. Для устранения этого недостатка верификацию личности предлагается осуществлять по произвольному в отношении объема, содержания и языка тексту (текстонезависимая биометрическая верификация). В данной работе предлагается обобщенный подход к решению задачи верификации личности по динамическим биометрическим параметрам разной модальности (клавиатурный почерк, рукопись, голос). Представление сигналов динамической биометрии осуществляется путем преобразования их в последовательности информационных единиц, каждая из которых содержит одинаковое количество отсчетов биометрического сигнала соответствующей модальности. Решение поставленной задачи осуществляется путем контроля степени концентрации близко расположенных информационных единиц (кластеров) в определенных точках многомерного признакового пространства. Реализуется такой контроль на вероятностной нейронной сети, осуществляющей статистическую оценку плотности вероятности распределения информационных единиц в соответствующих кластерах с последующим определением суммарной плотности вероятности для всего класса объектов. Преимуществами предлагаемого подхода являются: обобщение существенно различных методов текстонезависимой верификации личности по динамическим биометрическим параметрам разной модальности; возможность принимать верификационное решение за фиксированное время поступления биометрических данных, определяемое размером используемого эталона; возможность задавать точность верификации путем изменения размерности слоя образцов вероятностной сети. Недостатком предлагаемого подхода является необходимость программной реализации нейронной сети большой размерности. Однако этот недостаток быстро нивелируется с повышением производительности средств вычислительной техники.

Текстонезависимая биометрическая верификация личности по динамическим биометрическим параметрам; кластеризация биометрических данных в признаковом пространстве; вероятностная нейронная сеть; статистическая оценка плотности вероятности распределения информационных единиц.

Yu.A. Bryuhomitsky

VERIFICATION OF DYNAMIC BIOMETRIC PARAMETERS OF A PERSONALITY BASED ON A PROBABLE NEURAL NETWORK

Biometric identity verification is used primarily for access to computer and mobile systems, as well as for remote (voice) verification. In fact, the most widespread systems are biometric verification systems based on a fixed passphrase, which are quite simple to implement, but very vulnerable to attacks of reproduction of a compromised short text. To eliminate this drawback, it is proposed to carry out identity verification using a text that is arbitrary in terms of volume, content and language (text-independent biometric verification). This paper proposes a generalized approach to solve the problem of identity verification by dynamic biometric parameters of different modality (keyboard writing, handwriting, voice). The presentation of dynamic biometrics signals is carried out by converting them into a sequences of information units, each of which contains the same number of counts of biometric signal of corresponding modality. The solution to this problem is carried out by monitoring the degree of concentration of closely located information units (clusters) at certain points of the multidimensional feature space. Such control is implemented on a probabilistic neural network that

statistically evaluates the probability density of the distribution of information units in the corresponding clusters with the subsequent determination of the total probability density for the entire class of objects. The advantages of the proposed approach are: generalization of substantially different methods of text-independent identity verification by dynamic biometric parameters of different modality; the ability to make a verification decision for a fixed time of receipt of biometric data, determined by the size of the model used; the ability to set the verification accuracy by changing the dimension of the layer of probabilistic network samples. The disadvantage of the proposed approach is the need for software implementation of a large-scale neural network. However, this drawback is quickly leveled with an increase in the productivity of computer technology.

Text-independent biometric identity verification based on dynamic biometric parameters; clustering of biometric data in the feature space; probabilistic neural network; statistical estimation of the probability density of the distribution of information units.

Введение. Динамические системы биометрической идентификации личности (динамическая биометрия) основаны на анализе индивидуальных особенностей хорошо заученных подсознательных движений человека. Практическое применение в настоящее время получили системы анализа голоса [1–3], рукописи [4–8] и клавиатурного почерка [9–13]. Системы биометрической идентификации личности используются в информационной безопасности преимущественно как средство аутентификации личности при входе в компьютерные и мобильные системы, а также для удаленной (голосовой) аутентификации.

Наибольшее распространение получили системы биометрической аутентификации по фиксированной короткой фразе (обычно парольной). Они достаточно просты в реализации, но уязвимы для атак воспроизведения скомпрометированного короткого текста. Для устранения этого недостатка возможен переход к аутентификации личности по произвольному в отношении объема, содержания и языка тексту (тектонезависимые системы биометрической аутентификации).

В текстонезависимых биометрических системах аутентификации эталоны личностей строятся на основе достаточно больших образцов текста соответствующей модальности. При этом возникает ряд принципиальных проблем, связанных с трудностью их формирования, анализа и сопоставления с предъявляемыми образцами биометрии. Вместе с тем эти проблемы можно удовлетворительно решить в других классах задач, информационной безопасности, связанных с обработкой динамических биометрических образов личности. Примерами таких задач являются: скрытная верификация работающих пользователей компьютерных систем (на основе клавиатурной биометрии); скрытное выявление инсайдеров (на основе клавиатурной биометрии); скрытное выявление отклонений в психофизическом состоянии личности (на основе голосовой, рукописной, клавиатурной биометрии); аудит безопасности компьютерных систем на основе интерактивного взаимодействия администратора системы с пользователями по каналам связи биометрической модальности (голосовой, рукописной, клавиатурной), сводящийся к иной реализации полиграфа, и другие подобные задачи.

Постановка задачи. В текстонезависимой динамической биометрии исходные данные представлены сигналами (функциями времени), структура которых содержит необходимые индивидуальные особенности личности. Для выявления этих особенностей входные биометрические данные предлагается представлять и обрабатывать в виде последовательностей информационных единиц фиксированного размера. Такое представление используется, в частности, при массово-параллельной децентрализованной обработке данных, принятой в искусственных иммунных системах (ИИС) [14–20].

В отличие от иммунологического подхода в данной работе решение задачи основано на том, что в определенных точках признакового пространства осуществляется контроль степени концентрации близко расположенных точек, образую-

щих кластеры. Реализуется такой контроль путем приближенной статистической оценки плотности вероятности распределения близких по воспроизведению информационных единиц в соответствующих кластерах информационного пространства признаков с последующим определением суммарной плотности вероятности для всего класса объектов.

Для решение указанной задачи предлагается использовать вероятностную нейронную сеть (PNN – Probabilistic Neural Network), являющейся модификацией нейронной сети радиально-базисных функций (RBF-сеть) [21–22].

Решение поставленной задачи. Воспроизведение произвольного текста средствами динамической биометрии любой модальности реализуется совокупностью заученных подсознательных движений, которые преобразуются в электрические сигналы (функции времени) В общем случае эти сигналы являются многомерными: $\boldsymbol{x}(t) = x_1(t), x_2(t), \dots, x_n(t)$.

На этапе предварительной обработки сигналы $\boldsymbol{x}(t)$ оцифровываются $\boldsymbol{x}(t) \to \boldsymbol{x}(t_i),\ i = 1, 2, \dots$, масштабируются, из них исключаются длительные паузы, не обусловленные индивидуальными особенностями воспроизведения текста. В голосовой биометрии исключаются также неинформативные с точки зрения распознавания голоса фонемы шипящих звуков.

Отсчеты сигнала $\boldsymbol{x}(t_i),\ i = 1, 2, \dots$ можно рассматривать как точки метрического пространства E^n, представленные векторами признаков $\boldsymbol{x_i} = x_{1i}, x_{2i}, \dots, x_{ni}$, а сам сигнал $\boldsymbol{x}(t_i)$, – как последовательность $\{\boldsymbol{x}(t_i)\}_{i=1}^{\infty} = \{\boldsymbol{x}_i\}_{i=1}^{\infty} = \boldsymbol{x}_1, \boldsymbol{x}_2, \dots$ элементов, представленных векторами признаков: $\boldsymbol{x}_i$. В математическом смысле последовательность $\{\boldsymbol{x}_i\}_{i=1}^{\infty}$ «пробегает» конечное множество Ψ_x векторов признаков $\boldsymbol{x_i}$ биометрии данной личности.

Исследования [19–20], показывают, что индивидуальные особенности динамической биометрии личности в наибольшей степени проявляются при воспроизведении не одиночных символов текста или фонем речи, а синтаксически связанных фрагментов текста или речи, обладающих существенно большей индивидуальностью. Использование этого феномена при анализе позволяет строить системы биометрической идентификации личности с существенно более высокими характеристиками по точности.

Для использования указанного феномена последовательность $\{\boldsymbol{x}_i\}_{i=1}^{\infty}$ расчленяется на фрагменты $\{\boldsymbol{x}_i\}_{i=1}^{r}$ одинакового размера по r отсчетов в каждом фрагменте. Результатом будет новая последовательность $\{\boldsymbol{y}_j\}_{j=1}^{\infty} = \boldsymbol{y}_1, \boldsymbol{y}_2, \dots\ ,\ j = 1, 2, \dots$, каждый элемент $\boldsymbol{y}_j$ которой содержит r векторов $\boldsymbol{x}_i$ исходной последовательности $\{\boldsymbol{x}_i\}_{i=1_i}^{\infty}$:

$$\{\boldsymbol{y}_j\}_{j=1}^{\infty} = \boldsymbol{y}_1, \boldsymbol{y}_2, \dots, \qquad \boldsymbol{y}_j = \{\boldsymbol{x}_i\}_{i=1}^{r}, \qquad i = 1, 2, \dots, r, \qquad j = 1, 2, \dots.$$

Совокупность векторов $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_r$ каждого элемента $\boldsymbol{y}_j$ можно представить как один s-мерный вектор $\boldsymbol{y}_j$, содержащий $s = n \times r$ компонент:

$$\boldsymbol{y}_j = \begin{bmatrix} y_{11} & y_{12} & \cdots & y_{1r} \\ y_{21} & y_{22} & \cdots & y_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ y_{n1} & y_{n2} & \cdots & y_{nr} \end{bmatrix}.$$

В итоге образ динамической биометрии личности будет представлен последовательностью $\{\boldsymbol{y}_j\}_{j=1}^{\infty}$ s-мерных векторов признаков $\boldsymbol{y}_j$ в пространстве признаков E^s.

Последовательность $\{\boldsymbol{y}_j\}_{j=1}^{\infty}$, ограниченная N_y элементами

$$\{\boldsymbol{y}_j\}_{j=1}^{N_y} = \boldsymbol{y}_1, \boldsymbol{y}_2, \dots\ , \boldsymbol{y}_{N_y},\ j = 1, 2, \dots N_y,$$

можно трактовать как биометрический эталон данной личности **P**. При этом распределение биометрических данных личности в пространстве признаков E^s будет представлено множеством *s*-мерных областей (кластеров), каждая из которых отражает распределение определенных фрагментов $\boldsymbol{y}_j$ биометрических данных личности. Число областей (кластеров) будет соответствовать числу фрагментов $\boldsymbol{y}_j$, эталонной последовательности $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$.

Режим верификации предполагает наличие единственного биометрического эталона личности $\mathbf{P} = \{\boldsymbol{y}_{Pj}\}_{j=1}^{N_y}$, соответствующего легитимному пользователю информационной системы – «своему». Любая последовательность $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$, не соответствующая эталону **P**, считается принадлежащей нелегитимному пользователю – «чужому». Это позволяет оптимизировать пространство признаков E^s в рабочее пространство $E_{\text{р}}^s$ путем анализа и использования минимаксных значений данных $\boldsymbol{y}_{Pj}$ по координатам *s*.

Последующая реализация операции верификации биометрических данных личности осуществляется на основе модифицированной PNN-сети.

Вероятностная нейронная сеть представляет собой параллельную реализацию статистических методов Байеса [21–22] и ориентирована на задачи классификации образцов разных классов. В PNN образцы классифицируются на основе оценок их близости к соседним образцам. При этом используется ряд критериев статистических методов, на основе которых принимается решение о том, к какому классу отнести неизвестный образец. Формальным правилом при классификации является то, что класс с наиболее плотным распределением в области неизвестного образца, а также – с более высокой априорной вероятностью, а также – с более высокой ценой ошибки классификации, будет иметь преимущество по сравнению с другими классами.

Оценка стоимости ошибки классификации и априорной вероятности предполагает хорошее знание решаемой задачи и данной задаче выбираются одинаковыми. Для оценки функции плотности распределения вероятностей применяют метод Парцена (Parzen), в соответствии с которым для каждого учебного образца рассматривается некоторая весовая функция, называемая функцией потенциала или ядром. В качестве учебных образцов в данной задаче выступают элементы биометрической последовательности $\{\boldsymbol{y}_j\}_{j=1}^{\infty}$личности, а качестве функции потенциала – упрощенная функция Гаусса

$$\varphi(\boldsymbol{y}_j) = \exp\left(-\frac{\|\boldsymbol{y}-\boldsymbol{y}_j\|^2}{2\sigma^2}\right), \quad \textbf{(1)}$$

где $\boldsymbol{y}_j$ – *j*-й образец последовательности $\{\boldsymbol{y}_j\}_{j=1}^{\infty}$; $\boldsymbol{y}$ – неизвестный образец; σ параметр, задающий ширину функции и определяющий ее влияние.

Используемая функция Гаусса отличается от классической отсутствием коэффициента $1/\sigma\sqrt{2\pi}$ перед экспонентой, что позволяет получить максимальное значение функции плотности распределения вероятностей, равное единице, а не величине указанного коэффициента.

В данной работе решается задача верификации личности, представленной своим биометрическим эталоном **P**. Поэтому функция плотности распределения вероятностей для эталонной последовательности $\mathbf{P} = \{\boldsymbol{y}_j\}_{j=1}^{N_y}$, определится как сумма функций Гаусса для всех элементов эталона **P**:

$$\varphi^{\mathbf{P}}(\boldsymbol{y}) = \sum_{j=1}^{N_y} \exp\left(-\frac{\|\boldsymbol{y}-\boldsymbol{y}_j\|^2}{2\sigma^2}\right). \quad (2)$$

Вариант структуры PNN-сети для решения задачи верификации личности показан на рис. 1.

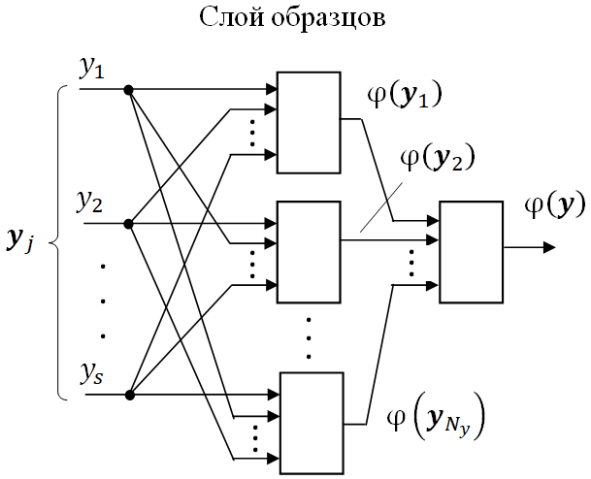

Рис. 1. Вариант структуры PNN-сети для решения задачи верификации личности

На входы сети последовательно поступают s-мерные векторы $\boldsymbol{y}_j$ последовательности $\mathbf{P} = \{\boldsymbol{y}_j\}_{j=1}^{N_y}$. Слой образцов содержит N_y нейронов по числу образцов входного вектора $\boldsymbol{y}_j$ из обучающей выборки $\mathbf{P}$. Веса матрицы связей $\mathbf{W}$ слоя образцов определяются значениями компонент соответствующего образца входного вектора $\boldsymbol{y}_j$. Для входных векторов $\boldsymbol{y}_j$, содержащих s компонент и представленных N_y образцами, матрица связей $\mathbf{W}$ имеет вид

$$\mathbf{W} = \begin{Vmatrix} w_{11} & w_{12} & \cdots & w_{1N_y} \\ w_{21} & w_{22} & \cdots & w_{2N_y} \\ \cdots & \cdots & \cdots & \cdots \\ w_{s1} & w_{s2} & \cdots & w_{sN_y} \end{Vmatrix} = \begin{Vmatrix} y_{11} & y_{12} & \cdots & y_{1N_y} \\ y_{21} & y_{22} & \cdots & y_{2N_y} \\ \cdots & \cdots & \cdots & \cdots \\ y_{s1} & y_{s2} & \cdots & y_{sN_y} \end{Vmatrix}. \quad (3)$$

В (3) каждый j-нейрон слоя образцов имеет набор из s весов, соответствующих s компонентам входного вектора, (j-столбец матрицы $\mathbf{W}$).

На выходах нейронов слоя образцов будут значения плотностей вероятностей $\varphi^{\mathbf{P}}(\boldsymbol{y}_1)$, $\varphi^{\mathbf{P}}(\boldsymbol{y}_2)$, …, $\varphi^{\mathbf{P}}\left(\boldsymbol{y}_{N_y}\right)$ распределения образцов $\{\boldsymbol{y}_j\}_{j=1}^{N_y}$ в соответствующих кластерах $j = 1, 2, \ldots, N_y$. Выходной нейрон реализует суммирование плотностей вероятностей $\varphi^{\mathbf{P}}(\boldsymbol{y}_1), \varphi^{\mathbf{P}}(\boldsymbol{y}_2), \ldots, \varphi^{\mathbf{P}}\left(\boldsymbol{y}_{N_y}\right)$ в итоговую плотность $\varphi^{\mathbf{P}}(\boldsymbol{y})$ распределения всей эталонной последовательности $\mathbf{P} = \{\boldsymbol{y}_j\}_{j=1}^{N_y}$ в рабочем пространстве признаков E_{p}^{s}.

В соответствии с принципом формирования матрицы связей (3) заменим в (1) векторы образцов $\boldsymbol{y}_j$ на соответствующие им векторы весов $\boldsymbol{w}_j^{\mathrm{T}}$. Тогда функция активности j-нейрона слоя образцов приобретает вид

$$\varphi^{\mathbf{P}}(\boldsymbol{y}_j) = \exp\left(-\frac{\left\|\boldsymbol{y} - \boldsymbol{w}_j^{\mathrm{T}}\right\|^2}{2\sigma^2}\right),$$

или в покомпонентном представлении

$$\varphi^{\mathbf{P}}(\boldsymbol{y}_j) = \exp\left[-\frac{1}{2\sigma^2}\sum_{i=1}^{s}(y_i - w_{ji})^2\right], \tag{4}$$

В PNN-сети необходимо провести предварительную нормализацию входных векторов. Это выполняется путем деления каждой компоненты входного вектора на его длину:

$$y_i^{\mathrm{H}} = y_i \Big/ \sqrt{\sum_{i=1}^{s} y_i^2}. \tag{5}$$

Такая операция превращает входной вектор $\boldsymbol{y}$ в вектор единичной длины $\boldsymbol{y}^{\mathrm{H}}$ в пространстве признаков $\mathrm{E}_{\mathrm{p}}^{\mathrm{s}}$. Исходя из соответствия между векторами весов $\boldsymbol{w}_j^{\mathrm{T}}$ и векторами образцов $\boldsymbol{y}_j$, нормализацию следует провести также и для весов

$$w_{ji}^{\mathrm{H}} = w_{ji} \Big/ \sqrt{\sum_{i=1}^{s} w_{ji}^2}.$$

Введение в выражение (4) для функции активности j-нейрона слоя образцов нормализованных значений компонент y_i и w_{ji} позволяет преобразовать его к более простой для вычислений форме:

$$\varphi^{\mathbf{P}}(\boldsymbol{y}_j) = \exp\left[-\frac{1}{2\sigma^2}\sum_{i=1}^{s}\left(y_i - w_{ji}\right)^2\right] =$$

$$= \exp\left(-\frac{1}{2\sigma^2}\sum_{i=1}^{\boldsymbol{s}} 2y_i \cdot w_{ji} \Big/ \sqrt{\sum_{i=1}^{s} y_i^2} \cdot \sqrt{\sum_{i=1}^{s} w_{ji}^2}\right) = \exp\left(\frac{1}{\sigma^2}\sum_{i=1}^{\boldsymbol{s}} y_i^{\mathrm{H}} \cdot w_{ji}^{\mathrm{H}} - 1\right)$$

Функция активности $\varphi^{\mathbf{P}}(\boldsymbol{y})$ выходного нейрона определяет значение плотности распределения вероятностей всей эталонной последовательности $\mathbf{P} = \{\boldsymbol{y}_j\}_{j=1}^{N_y}$ в рабочем пространстве признаков E_{p}^{s}. После нормализации она вычисляется по формуле

$$\varphi^{\mathbf{P}}(\boldsymbol{y}) = \sum_{j=1}^{N_y} \exp\left(\frac{1}{\sigma^2}\sum_{i=1}^{\boldsymbol{s}} y_i^{\mathrm{H}} \cdot w_{ji}^{\mathrm{H}} - 1\right).$$

Обучение PNN-сети сводится к тому, что векторы образцов $\boldsymbol{y}_j$ эталонной последовательности $\mathbf{P} = \{\boldsymbol{y}_j\}_{j=1}^{N_y}$ предварительно нормализуются предъявляются на входы сети и вычисляется значение $\varphi^{\mathbf{P}}(\boldsymbol{y})$ плотности распределения вероятностей всей эталонной последовательности $\mathbf{P}$. Длительность обучения определяется одним циклом прогона последовательности $\mathbf{P}$.

В рабочем режиме через обученную сеть пропускается биометрическая последовательность априори неизвестной личности $\mathbf{X}$ того же размера N_y, что и эталонная $\mathbf{P}$, и вычисляется значение $\varphi^{\mathbf{X}}(\boldsymbol{y})$ плотности распределения вероятностей для этой последовательности.

Для принятия верификационного решения, исходя из допустимой величины ошибки первого рода, устанавливается пороговая величина невязки $\Delta_{\text{Т}} = \varphi^{\mathbf{P}}(\boldsymbol{y}) - \varphi^{\mathbf{X}}(\boldsymbol{y})$, на основании которой неизвестную личность $\mathbf{X}$ следует признать «своим» $\mathbf{X}^{\text{С}}$или «чужим» $\mathbf{X}^{\text{Ч}}$:

$$\mathbf{X} \equiv \begin{cases} \mathbf{X}^{\text{С}}, \text{если } \Delta < \Delta_{\text{Т}}; \\ \mathbf{X}^{\text{Ч}}, \text{если } \Delta \geq \Delta_{\text{Т}}. \end{cases}$$

Заключение. Предлагаемый подход позволяет обобщить существенно различные существующие методы верификации личности по динамическим биометрическим параметрам разной модальности – голоса, рукописи и клавиатурного набора.

Преимуществами предлагаемого подхода являются:

♦ возможность текстонезависимого анализа динамической биометрии различной модальности, произвольного объема и содержания;

♦ возможность принимать верификационное решение за фиксированное время работы пользователя, определяемое размером эталона **P**;

♦ возможность задавать точность работы системы верификации путем изменения размерности слоя образцов PNN-сети.

Недостатком предлагаемого подхода является необходимость программной реализации нейронной сети большой размерности. Вместе с тем этот недостаток быстро нивелируется за счет повышения производительности средств вычислительной техники.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ахмад Х.М., Жирков В.Ф.* Введение в цифровую обработку речевых сигналов. – Владимир: Изд-во Владим. гос. ун-та, 2007. – 192 с.
2. *Матвеев Ю.Н.* Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н.Э. Баумана, серия Приборостроение. – 2012. – № 2. – С. 46-61.
3. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers // IEEE Trans. Speech Audio Process. – 2002. – Vol. 10, No. 4. – P. 205-212.
4. *Анисимова Э.С.* Идентификация онлайн-подписи с помощью оконного преобразования Фурье и радиального базиса // Компьютерные исследования и моделирование. – 2014. – Т. 6, № 3. – С. 357-364.
5. *Jain A.K., Friederike D.G., Connel S.D.* On-line signature verification // Pattern Recognition. – 2002. – Vol. 35 (12). – P. 2963-2972.
6. *Plamondon R., Srihari S.* On-line and Off-line Handwriting Recognition: A Comprehensive Survey // IEEE Trans. PAMI. – 2000. – Vol. 22 (1). – P. 63-84.
7. *Иванов А.И.* Биометрическая идентификация личности по динамике подсознательных движений: монография. – Пенза: Изд-во Пенз. гос. ун-та, 2000. – 188 с.
8. *Брюхомицкий Ю.А., Казарин М.Н.* Система аутентификации личности по почерку // Сб. трудов научно-практической конференции с международным участием «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2002. – С. 22-29.
9. *Мазниченко Н.И., Гвозденко М.В.* Анализ возможностей систем автоматической идентификации клавиатурного почерка // Вестник Национального технического университета «Харьковский политехнический институт». Серия “Информатика и моделирование». – 2008. – Вып. № 24. – С. 77-82.
10. *Скубицкий А.В.* Анализ применимости метода реконструкции динамических систем в системах биометрической идентификации по клавиатурному почерку // Инфокоммуникационные технологии. – 2008. – Т. 6, № 1. – С. 51-53.
11. *Брюхомицкий Ю.А., Казарин М.Н.* Метод биометрической идентификации пользователя по клавиатурному почерку на основе разложения Хаара и меры близости Хэмминга // Известия ТРТУ. – 2003. – № 4 (33). – С. 141-149.
12. *Брюхомицкий Ю.А.* Цепочный метод клавиатурного мониторинга // Известия ЮФУ. Технические науки. – 2009. – № 11. – С. 135-145.

13. *Брюхомицкий Ю.А., Казарин М.Н.* Методы многосвязного представления клавиатурного почерка // Матер. III Международной конференции «Нелокальные краевые задачи и родственные проблемы математической биологии, информатики и физики». Нальчик, 5-8 декабря 2006 г. – С. 68-69.
14. *Dasgupta D.* Artificial Immune Systems and Their Applications, Ed., Springer-Verlag, 1999.
15. *De Castro L.N., Timmis, J.I.* Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000. – 357 p.
16. *Hofmeyr S. and Forrest S.* Architecture for an Artificial Immune System // Evolutionary Computation. – 2000. – No. 8 (4). – P. 443-473.
17. *Specht D.F.* Probabilistic neural networks // Neural Networks. – 1990. – No. 3. – P. 109-118.
18. *Чернышев Ю.О., Венцов Н.Н., Григорьев Г.В.* Искусственные иммунные системы: обзор и современное состояние // Программные продукты и системы. – 2014. – № 4. – С. 136-142.
19. *Зайцев С.А., Субботин С.А.* Обобщенная модель искусственной иммунной системы / Proceedings. – Berlin–Heidelberg: Springer-Verlag, 2003. – Ser. LNCS 2723. – P. 195-206.
20. *Литвиненко В.И., Дидык А.А., Захарченко Ю.А.* Компьютерная система для решения задач классификации на основе модифицированных иммунных алгоритмов // ААЭКС. – 2008. – № 2 (22).
21. *Spech D.F.* Probailistic neural networks // Neural Networks. – 1990. – No. 3. – P. 109-118.
22. *Каллан Р.* Основные концепции нейронных сетей. – Вильямс, 2001. – 291 с.

REFERENCES

1. *Akhmad Kh.M., Zhirkov V.F.* Vvedenie v tsifrovuyu obrabotku rechevykh signalov [Introduction to digital speech signal processing]. Vladimir: Izd-vo Vladim. gos. un-ta, 2007, 192 p.
2. *Matveev Yu.N.* Tekhnologii biometricheskoy identifikatsii lichnosti po golosu i drugim modal'nostyam [Technologies of biometric identification of the person by voice and other modalities], *Vestnik MGTU im. N.E. Baumana, seriya Priborostroenie* [Bulletin of Bauman Moscow state technical University, instrument Engineering series], 2012, No. 2, pp. 46-61.
3. *Campbell W., Assaleh K., Broun C.* Speaker recognition with polynomial classifiers, *IEEE Trans. Speech Audio Process*, 2002, Vol. 10, No. 4, pp. 205-212.
4. Anisimova E.S. Identifikatsiya onlayn-podpisi s pomoshch'yu okonnogo preobrazovaniya Fur'e i radial'nogo bazisa [Identification of an online signature using a window Fourier transform and a radial basis], *Komp'yuternye issledovaniya i modelirovanie* [Computer research and modeling], 2014, Vol. 6, No. 3, pp. 357-364.
5. *Jain A.K., Friederike D.G., Connel S.D.* On-line signature verification, *Pattern Recognition*, 2002, Vol. 35 (12), pp. 2963-2972.
6. *Plamondon R., Srihari S.* On-line and Off-line Handwriting Recognition: A Comprehensive Survey, *IEEE Trans. PAMI*, 2000, Vol. 22 (1), pp. 63-84.
7. *Ivanov A.I.* Biometricheskaya identifikatsiya lichnosti po dinamike podsoznatel'nykh dvizheniy: monografiya [Biometric identification of a person by the dynamics of subconscious movements: a monograph]. Penza: Izd-vo Penz. gos. un-ta, 2000, 188 p.
8. *Bryukhomitskiy Yu.A., Kazarin M.N.* Sistema autentifikatsii lichnosti po pocherku [System of identity authentication by handwriting], *Sb. trudov nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem «Informatsionnaya bezopasnost'»* [Collection of proceedings of the scientific and practical conference with international participation "Information security"]. Taganrog: Izd-vo TRTU, 2002, pp. 22-29.
9. *Maznichenko N.I., Gvozdenko M.V.* Analiz vozmozhnostey sistem avtomaticheskoy identifikatsii klaviaturnogo pocherka [Analysis of the capabilities of automatic identification systems for keyboard handwriting], *Vestnik Natsional'nogo tekhnicheskogo universiteta «KHar'kovskiy politekhnicheskiy institut». Seriya "Informatika i modelirovanie»* [Bulletin of the national technical University "Kharkiv Polytechnic Institute". Series "Informatics and modeling"], 2008, Issue No. 24, pp. 77-82.
10. *Skubitskiy A.V.* Analiz primenimosti metoda rekonstruktsii dinamicheskikh sistem v sistemakh biometricheskoy identifikatsii po klaviaturnomu pocherku [Analysis of the applicability of the method of reconstruction of dynamic systems in systems of biometric identification by keyboard handwriting], *Infokommunikatsionnye tekhnologii* [Information and communication technology], 2008, Vol. 6, No. 1, pp. 51-53.

11. *Bryukhomitskiy Yu.A., Kazarin M.N.* Metod biometricheskoy identifikatsii pol'zovatelya po klaviaturnomu pocherku na osnove razlozheniya Khaara i mery blizosti Khemminga [The method of biometric identification of the user by keyboard handwriting based on the Haar decomposition and the Hamming proximity measure], *Izvestiya TRTU* [Izvestiya TSURE], 2003, No. 4 (33), pp. 141-149.
12. *Bryukhomitskiy Yu.A.* TSepochnyy metod klaviaturnogo monitoringa [Chain method of keyboard monitoring], *Izvestiya YuFU. Tekhnicheskie* nauki [Izvestiya SFedU. Engineering Sciences], 2009, No. 11, pp. 135-145.
13. *Bryukhomitskiy Yu.A., Kazarin M.N.* Metody mnogosvyaznogo predstavleniya klaviaturnogo pocherka [Methods of multi-linked representation of keyboard handwriting], *Mater. III Mezhdunarodnoy konferentsii «Nelokal'nye kraevye zadachi i rodstvennye problemy matematicheskoy biologii, informatiki i fiziki. Nal'chik, 5-8 dekabrya 2006 g.* [Proceedings of the III International conference "non-Local boundary value problems and related problems of mathematical biology, computer science and physics". Nalchik, December 5-8, 2006], pp. 68-69.
14. *Dasgupta D.* Artificial Immune Systems and Their Applications, Ed., Springer-Verlag, 1999.
15. *De Castro L.N., Timmis, J.I.* Artificial Immune Systems: A New Computational Intelligence Approach, London: Springer-Verlag, 2000, 357 p.
16. *Hofmeyr S. and Forrest S.* Architecture for an Artificial Immune System, *Evolutionary Computation*, 2000, No. 8 (4), pp. 443-473.
17. *Specht D.F.* Probabilistic neural networks, *Neural Networks*, 1990, No. 3, pp. 109-118.
18. *Chernyshev Yu.O., Ventsov N.N., Grigor'ev G.V.* Iskusstvennye immunnye sistemy: obzor i sovremennoe sostoyanie [Artificial immune systems: review and current state], *Programmnye produkty i sistemy* [Software products and systems.], 2014, No. 4, pp. 136-142.
19. *Zaytsev S.A., Subbotin S.A.* Obobshchennaya model' iskusstvennoy immunnoy sistemy [Generalized model of the artificial immune system], *Proceedings.* Berlin–Heidelberg: Springer-Verlag, 2003. Ser. LNCS 2723, pp. 195-206.
20. *Litvinenko V.I., Didyk A.A., Zakharchenko Yu.A.* Komp'yuternaya sistema dlya resheniya zadach klassifikatsii na osnove modifitsirovannykh immunnykh algoritmov [Computer system for solving classification problems based on modified immune algorithms], *AAEKS* [AAEKS], 2008, No. 2 (22).
21. *Spech D.F.* Probailistic neural networks, *Neural Networks*, 1990, No. 3, pp. 109-118.
22. *Kallan R.* Osnovnye kontseptsii neyronnykh setey [Basic concepts of neural networks]. Vil'yams, 2001, 291 p.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Брюхомицкий Юрий Анатольевич – Южный федеральный университет; e-mail: bryuhomitskiy@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; с.н.с.; доцент.

Bryuhomitsky Yuriy Anatoly – Southern Federal University; e-mail: bryuhomitskiy@sfedu.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; senior researcher; associate professor.

УДК 519.6 DOI 10.18522/2311-3103-2020-5-60-67

В.В. Семенистый, И.Э. Гамолина

ИССЛЕДОВАНИЕ СПОСОБОВ ОРГАНИЗАЦИИ ПАРАЛЛЕЛЬНОГО РЕШЕНИЯ ВНЕШНИХ ЗАДАЧ АЭРОДИНАМИКИ НА ОСНОВЕ СХЕМ РАСЩЕПЛЕНИЯ

Целью работы является исследование способов организации параллельного решения внешних задач аэродинамики и разработка гибридного параллельно-конвейерного способа организации численного решения двумерных задач, моделирующих течение вязких сжимаемых жидкостей и обтекание объектов сложной формы. Рассматривается параболизованная система уравнений Навье-Стокса, для численного решения которой выбран конечно-

разностный алгоритм. В силу своих особенностей, которыми являются экономичность и устойчивость в исследовании пограничных слоев движущихся тел и корректного решения задач с дозвуковыми зонами данный алгоритм предпочтителен обычного маршевого метода. Для реализации нелинейной конечно-разностной схемы в каждом маршевом сечении используются внутренние итерации. Разработанный параллельный алгоритм конструктивно состоит из вложенных итерационных циклов. Система уравнений решается на каждой внутренней итерации последовательно в два этапа. На первом этапе решаются уравнения количества движения и энергии; на втором этапе по найденным значениям скоростей и давления находится плотность. На каждом дробном шаге внутренней итерации рассчитываются одномерные массивы данных. В работе используется метод расщепления оператора по физическим процессам. Для численного решения задачи проводится факторизация стабилизирующего оператора. Приводится схема организации процесса решения задачи на внутренней итерации. В работе предложен принцип организации параллельных вычислений, где используется внутренний параллелизм решаемой физической задачи. Для реализации параллельного алгоритма выбрана вычислительная среда, содержащая решающее поле соединенных коммутационными связями вычислительных устройств, каждое из которых обладает собственной оперативной памятью, и устройство управления, поддерживающее работу системы. Алгоритм использует различную топологию связи между рабочими процессорами. Уменьшение размерности задачи позволяет сэкономить время на межпроцессорном обмене данными. В работе проведены временные оценки эффективности разработанного параллельного алгоритма для каждой внутренней итерации. Использование метода параллельной прогонки, предложенный принцип организации параллельных вычислений позволяют увеличить скорость расчета физической задачи для каждой внутренней итерации по сравнению с ранее используемыми алгоритмами для такого класса задач.

Параболизованная система уравнений Навье-Стокса; методы расщепления; организация параллельных вычислений; временные оценки алгоритма.

V.V. Semenistyy, I.E. Gamolina

STUDY OF PARALLEL SOLUTION ORGANIZATION FOR EXTERNAL AERODYNAMICS PROBLEMS BASED ON SPLITTING SCHEMES

The aim of this work is to study the ways to organize parallel solutions of external aerodynamics problems. A hybrid parallel-conveyor method for numerical solution of two-dimensional problems is considered. It allows to simulate the flow of viscous compressible fluids around objects of complex shape. A parabolized system of Navier-Stokes equations is considered, for the numerical solution a finite-difference algorithm is chosen. Due to its features (cost-effectiveness and stability in the study of boundary layers of moving bodies) this algorithm was preferred. To implement a nonlinear finite-difference scheme, the internal iterations are used in each main section. The developed parallel algorithm consists constructively of nested iterative loops. The system of equations is solved at each internal iteration. It is organized in two stages. At the first stage the equations of motion are solved; at the second stage the density is determined. At each fractional step of the internal iteration, one-dimensional data arrays are calculated. The paper uses the method of splitting the operator by physical processes. For the numerical solution of the problem, the factorization of the stabilizing operator is carried out. The scheme of the organization of the process of problem solving is given in each internal iteration. The paper proposes the principle of organizing parallel computing. The internal parallelism of the physical problem is used here. To implement the parallel algorithm, a computing environment is specially selected. It contains a decisive field of computing devices connected by switching connections, each of computing device has its own RAM. Besides computing environment contains a control device. The parallel algorithm uses a communication topology between worker processors. Reducing the dimension of the problem (to 2d) allows to save time on data exchange between the processors. In this paper, time estimates of the effectiveness of the developed parallel algorithm for each internal iteration are carried out. The use of the parallel run method and the proposed principle of organizing parallel calculations allow to increase the effectiveness of solving problems of such class.

Parabolized system of Navier-Stokes equations; splitting methods; organization of parallel computations; time calculation estimates of the algorithm.

Введение. Моделирование двумерных задач аэрогидродинамики на многопроцессорных вычислительных комплексах [1, 2] расширяет возможности конструирования экономичных параллельных алгоритмов, что в конечном счете приводит к ускорению расчетов без потери численной устойчивости. Это происходит благодаря параллельному вычислению больших по размерности независимых фрагментов алгоритма, которые распределяются по ветвям параллельного процесса. Такой крупноблочный принцип распараллеливания позволяет создавать перспективные параллельные алгоритмы [3, 14].

Выбранный численный конечно-разностный алгоритм по применению метода глобальных для решения параболизованной системы уравнений Навье-Стокса, предложенный в работе [4], моделирует широких класс вязких сжимаемых течений. Способ организации параллельного решения задачи заключается в последовательном отображении численного алгоритма на структуру параллельной модели вычислительной среды. Особенности численного алгоритма состоят в том, что он, во-первых, является экономичным и устойчивым алгоритмом исследования пограничных слоев движущихся тел, а во-вторых конструктивно состоит из вложенных итерационных циклов позволяющих строить различные эффективные параллельные вычислительные алгоритмы. При решении разностной задачи можно организовать конвейерные вычисления по одним итерационным параметрам и параллельные по другим.

Если провести анализ пригодности и эффективности метода глобальных итераций [4, 5] при его параллельной реализации на современных многопроцессорных вычислительных структурах, то можно выделить ряд его преимуществ по сравнению с методом установления. Уменьшение размерности задачи позволяет сэкономить время на межпроцессорном обмене данными, т.е. уменьшается время накладных расходов. Возрастает внутренний параллелизм модели, т.к. прогонка по одному из направлений заменяется методом бегущего счета.

Для реализации параллельного алгоритма выбрана вычислительная среда [10, 12], которая архитектурно содержит решающее поле вычислительных устройств, соединенных коммутационными связями и устройство управления, поддерживающее работу системы. Каждое вычислительное устройство обладает собственной оперативной памятью для проведения арифметических расчетов. Решение двумерных задач аэрогидродинамики позволяет более гибко использовать топологию связи между рабочими процессорами.

Основная часть. Для численной организации параллельного решения параболизованной системы уравнений Навье-Стокса методом глобальных итераций в сеточной области $Q=\{(x_n,y_j),1\le n\le N,1\le j\le M\}$ выбрана следующая конечно-разностная схема [4]:

$$A_1^n\frac{f_j^n-f_j^{n-1}}{h_1}+A_2^n\frac{(f_*^{n+1})^{\upsilon-1}-f_j^n}{h_1}+B_h^n f_j^n=L_h^n f_j^n+F_h^n, \quad (1)$$

$$\sigma\frac{(\rho u)_j^n-(\rho u)_j^{n-1}}{h_1}+(1-\sigma)\frac{((\rho u)_*^{n+1})^{\upsilon-1}-(\rho u)_j^n}{h_1}+\Lambda^{\pm}(\rho v)_j^n=0, \quad (2)$$

где

$$A_1=\begin{pmatrix}\sigma u & 0 & (1-\sigma)/\rho\\ 0 & \sigma u & 0\\ \sigma\gamma p & 0 & \sigma u\end{pmatrix},\quad A_2=\begin{pmatrix}(1-\sigma)u & 0 & \sigma/\rho\\ 0 & (1-\sigma)u & 0\\ (1-\sigma)\gamma p & 0 & (1-\sigma)u\end{pmatrix},$$

$$\sigma=\begin{cases}1 & u\ge 0\\ 0 & u<0\end{cases},$$

$(f_*^n)^{\upsilon-1} = 0{,}5((f_{j+1}^n)^{\upsilon-1} + (f_{j-1}^n)^{\upsilon-1}),$ $\upsilon -$ номер текущей глобальной итерации.

Разностные операторы B_h^n, L_h^n и $\Lambda^{\pm}$ аппроксимируют соответствующие дифференциальные операторы.

Для реализации нелинейной разностной схемы (1), (2) в каждом n-ом маршевом сечении $\upsilon -$ глобальной итерации используются внутренние итерации

$$\frac{f_j^{s+1} - f_j^s}{\tau} + A_1^s \frac{f_j^{s+1} - f_j^{n-1}}{h_1} + A_2^s \frac{(f_*^{n+1})^{\upsilon-1} - f_j^{s+1}}{h_1} + B_h^s f_j^{s+1} = L_h^s f_j^{s+1} + F_h^s \quad (3)$$

$$\frac{\rho_j^{s+1} - \rho_j^s}{\tau} + \sigma \frac{(\rho u)_j^{s+1} - (\rho u)_j^{n-1}}{h_1} + (1-\sigma) \frac{((\rho u)_*^{n+1})^{\upsilon-1} - (\rho u)_j^{s+1}}{h_1} + \Lambda^{\pm}(\rho v)^{s+1} = 0 \cdot \quad (4)$$

Система (3), (4) отличается от системы (1), (2) добавлением слагаемых, которые участвуют во внутренних итерациях. При сходимости итераций по s мы получим решение исходной системы.

Система уравнений (3), (4) в течении $\upsilon -$ глобальной итерации решается на каждой внутренней (по s) итерации последовательно в два этапа. На первом этапе решаются уравнения количества движения и энергии (3) методом расщепления по физическим процессам[6]. На втором этапе по найденным значениям скоростей и давления из уравнения (4) находится плотность.

Исследования. Решение разностной схемы (3), (4) зависит от трех параметров: номера S, отвечающего за число внутренних итераций, которые продолжаются до установления значений газодинамических переменных в одном маршевом сечении; номера n -количества маршевых сечений, зависящего от изменения значений характеристик течения вниз по потоку и номера υ, числа глобальных итераций необходимого для установления давления в дозвуковых областях пограничного слоя.

В работе [11] определен порядок организации параллельных вычислений по схеме (3), (4) и подробно исследованы конвейерные вычисления на последовательности глобальных итераций (по υ). Получены временные оценки параллельного алгоритма.

Учитывая, что многопроцессорные вычислительные системы имеют свои внутренние характеристики t_a (время одной арифметической операции в тактах) и t_o (время операции обмена) [7] при прохождении одной глобальной итерации процессору на арифметические вычисления потребуется время равное [11]:

$$T_\upsilon = NJM \sum_{l_1}^{k_1} t_{l_1} + NM \sum_{l_2}^{k_2} t_{l_2} + M \sum_{l_3}^{k_3} t_{l_3}.$$

Здесь N и M – параметры, соответствующие размерности по координатам, а J – число внутренних итераций.

Учитывая, что

$$\sum_{l_m}^{k_m} t_{l_m} = c_m t_a, \quad m = 1,2,3$$

получаем

$$T_\upsilon = (c_1 NJM + c_2 NM + c_3 M) t_a.$$

Здесь t_{lm} - время выполнения в одном расчетном узле сетки всех арифметических операций для l_m операторов тела соответствующего цикла.

Для используемого численного алгоритма $c_1 \approx 425,\ c_2 \approx 12,\ c_3 \approx 12.$

В настоящей работе продолжаем исследовать эффективность параллельного алгоритма [16, 17], используя внутренний параллелизм задачи, сильнее погружая физическую задачу в вычислительную среду.

Рассмотрим решение системы (3), (4) на внутренней итерации (по s). Для этого систему уравнений запишем в каноническом виде [8, 13]:

$$K^s \frac{(f_j^{s+1} - f_j^s)}{\tau} = -\Omega^s, \tag{5}$$

где

$$K^s = E + \frac{\tau}{h_1}(A_1^s - A_2^s) + \tau B_h^s - \tau\Lambda_h^s,$$

$$\Omega^s = A_1^s \frac{f_j^s - f_j^{n-1}}{h_1} + A_2^s \frac{(f_*^{n+1})^{\upsilon-1} - f_j^s}{h_1} + B_h^s f_j^s - \Lambda_h^s f_j^s - F_h^s.$$

При решении системы (5) используется метод расщепления оператора B_h^s по физическим процессам [6]. Для численного решения системы (5) факторизуем стабилизирующий оператор K^s:

$$K^s \approx \Pi_1^s \cdot \Pi_2^s \cdot \Pi_3^s, \tag{6}$$

где

$$\Pi_1^s = E + \frac{\tau}{h_1}(A_1^s - A_2^s), \quad \Pi_1^s = E + \tau B_1^s - \tau\Lambda_1^s, \quad \Pi_3^s = E + \tau B_2^s.$$

С учетом (6) система (5) может быть записана в виде следующей схемы в дробных шагах[4]:

$$\Pi_1^s \xi^{\frac{1}{3}} = -\Omega^s, \quad \Pi_2^s \xi^{\frac{2}{3}} = \xi^{\frac{1}{3}}, \quad \Pi_3^s \xi^{s+1} = \xi^{\frac{2}{3}}, \quad f^{s+1} = f^s + \tau\xi^{s+1}.$$

Для организации параллельного процесса решения задачи на внутренней итерации представим численный алгоритм с помощью следующей структурной схемы (рис. 1) [11].

Рис. 1. Организация процесса решения задачи на внутренней итерации

Так как после расщепления оператора K^s на каждом дробном шаге внутренней итерации рассчитываются одномерные массивы данных размерности M, то при параллельной организации вычислений воспользуемся решением задачи, рас-

смотренной в статье [16]. Использование метода параллельной прогонки [9, 18] позволяет улучшить временную оценку расчета внутренней итерации (T_s). Вместо оценки времени $T_s = t_1 M$, полученной в [11], имеем новую, улучшенную, оценку:

$$T_s \approx (20m + 8p - 32)t_a + (3p - 2)t_0.$$

Здесь M=mp, где p – число процессоров, участвующих в расчете внутренней итерации.

Новая организация параллельных вычислений позволяет увеличить скорость расчета физической задачи для каждой внутренней итерации приблизительно в $K_y \approx \frac{8M}{20m + (8 + 3\alpha)p}$, $\alpha = \frac{t_0}{t_a}$ раз.

Заключение. Применение новых вычислительных технологий включает и разработку параллельных алгоритмов [15, 19, 20]. В работе моделируется один из таких алгоритмов на основе метода глобальных итераций широко использующегося в вычислительной аэрогидродинамики. Предложенный параллельный алгоритм позволяет более рационально использовать вычислительную среду. Благодаря перестраивающейся коммутационной системе можно одновременно организовать параллельные вычисления на внутренней итерации и конвейерные на внешней глобальной итерации. Такой комбинированный подход позволяет ускорить проведение расчетов по сравнению с используемыми ранее алгоритмами. В статье приведены теоретические оценки для коэффициента ускорения на одной внутренней итерации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Воеводин В.В., Воеводин Вл.В.* Параллельные вычисления. – СПб.: БХВ-Петербург, 2002. – 608 с.
2. *Воеводин В.В.* Модели и методы в параллельных процессах. – М.: Наука, 1986. – 206 с.
3. *Миллер Р., Боксер Л.* Последовательные и параллельные алгоритмы: Общий подход. – М.: Бином. Лаборатория знаний, 2006. – 406 с.
4. *Мелешко С.В., Черный С.Г.* Исследование вязких сжимаемых течений на основе параболизованных уравнений Навье–Стокса. – Новосибирск, 1985. – 48 с. (Препринт/ИТПМ СО РАН; №32-85).
5. *Ковеня В.М., Черный С.С.* Маршевый метод решения стационарных упрощенных уравнений Навье–Стокса // Журнал вычислительной математики и математической физики. – 1983. – Т. 23, № 5. – С. 1186-1189.
6. *Ковеня В.М., Яненко Н.Н.* Метод расщепления в задачах газовой динамики. – Новосибирск: Наука, 1981. – 304 с.
7. *Геркель В.П.* Теория и практика параллельных вычислений: учеб. пособие. – М.: Интуит, БИНОМ. Лаборатория знаний, 2016. – 423 с.
8. *Ковеня В.М.* Алгоритмы расщепления при решении многомерных задач аэрогидродинамики. – Новосибирск. Изд-во СО РАН. 2014. – 280 с.
9. *Яненко Н.Н., Коновалов А.Н., Бугров А.Н., Шустов Г.В.* Об организации параллельных вычислений и распараллеливание прогонки // Численные методы механики сплошных сред. – 1978. – № 7. – С. 136-139.
10. *Семенистый В.В., Гамолина И.Э., Дурягина В.В.* Конструирование эффективных параллельных алгоритмов для решения полной двумерной системы уравнений Навье-Стокса по явной схеме Мак-Кормака // Сб. материалов II международной научно-практической конференции «Исследования и разработки в перспективных научных областях». – Новосибирск, 2017. – С. 88-95.
11. *Семенистый В.В., Гамолина И.Э., Дурягина В.В, Богданов Д.С.* Моделирование и анализ параллельного алгоритма решения задачи обтекания плоской пластины методом глобальных итераций // Сб. материалов XIII международной научно-практической конференции. Ч. 1 «Вопросы современной науки: проблемы, тенденции, перспективы». – М.: Научный журнал «Chronos», 2017. – С. 79-85.

12. *Семенистый В.В., Гамолина И.Э., Дурягина В.В.* Оценка эффективности прямых параллельных методов для задачи течения совершенного газа по каналу переменного сечения // Матер. XIV Всерос. научн.-практ. конф., 15 июня 2018 г. – Краснодар: Краснодарский университет МВД России, 2018. – С. 250-256.
13. *Ковеня В.М.* Об одном алгоритме решения уравнений Навье–Стокса вязкой несжимаемой жидкости // Вычислительные технологии. – 2006. – Т. 11, № 2. – С. 39-51.
14. *Богачев К.Ю.* Основы параллельного программирования. – М.: Бином. Лаборатория знаний, 2003. – 344 с.
15. *Базовкин А.В., Ковеня В.М*. Распараллеливание алгоритма расщепления на многопроцессорных системах при моделировании течений вязкой несжимаемой жидкости // Вестник НГУ. Серия: Математика, механика, информатика. – 2013. – Т. 13. – Вып. 4. – С. 3-15.
16. *Гамолина И.Э., Семенистый В.В.* Параллельная организация вычислений при расчете задач аэрогидродинамики прямыми методами. Международное научное сотрудничество, образование и культура. – Ростов-на-Дону: Summa-Rerum, 2014. – № 3 (4).
17. *Гамолина И.Э., Дурягина В.В., Семенистый В.В.* Дозвуковое обтекание профилей // Известия ЮФУ. Технические науки. – 2013. – № 4. – С. 61-67.
18. *Теренков В.И., Арсении В.Ф., Евсеев Е.Г., Луцкий Я.А., Семенистый В.В.* О корректности и устойчивости алгоритма распараллеливания прогонки // Тр. инт-та прикл. математ. им. И.Н. Векуа Тбилис. ун-та. – Тбилиси, 1985. – С. 298-307.
19. *Деги Д.В., Старченко А.В.* Численное решение уравнений Навье-Стокса на компьютерах с параллельной архитектурой // Вестник Томского государственного университета. Математика и механика. – 2012. – № 2 (18). – С. 88-98.
20. *Dongarra J., Foster I., Fox J. et al.* Sourcebook of Parallel Computing. San Francisco (CA, USA): Elsevier Science, 2003. – 852 p.

REFERENCES

1. *Voevodin V.V., Voevodin Vl.V.* Parallel'nye vychisleniya [Parallel computing]. Saint Petersburg: BKhV-Peterburg, 2002, 608 p.
2. *Voevodin V.V.* Modeli i metody v parallel'nykh protsessakh [Models and methods in parallel processes]. Moscow: Nauka, 1986, 206 p.
3. *Miller R., Bokser L.* Posledovatel'nye i parallel'nye algoritmy: Obshchiy podkhod [Serial and parallel algorithms: General approach]. Moscow: Binom. Laboratoriya znaniy, 2006, 406 p.
4. *Meleshko S.V., Chernyy S.G.* Issledovanie vyazkikh szhimaemykh techeniy na osnove parabolizovannykh uravneniy Nav'e–Stoksa [Investigation of viscous compressible flows based on parabolized Navier-Stokes equations]. Novosibirsk, 1985, 48 p. (Preprint/ITPM SB RAS; No. 32-85).
5. *Kovenya V.M., CHernyy S.S.* Marshevyy metod resheniya statsionarnykh uproshchennykh uravneniy Nav'e–Stoksa [Marching method for solving stationary simplified Navier-Stokes equations], *Zhurnal vychislitel'noy matematiki i matematicheskoy fiziki* [Journal of Computational Mathematics and Mathematical Physics], 1983, Vol. 23, No. 5, pp. 1186-1189.
6. *Kovenya V.M., Yanenko N.N.* Metod rasshchepleniya v zadachakh gazovoy dinamiki [Splitting method in gas dynamics problems]. Novosibirsk: Nauka, 1981, 304 p.
7. *Gerkel' V.P.* Teoriya i praktika parallel'nykh vychisleniy: ucheb. posobie [Theory and practice of parallel computing: a textbook]. Moscow: Intuit, BINOM. Laboratoriya znaniy, 2016, 423 p.
8. *Kovenya V.M.* Algoritmy rasshchepleniya pri reshenii mnogomernykh zadach aerogidrodinamiki [Splitting algorithms for solving multidimensional problems of aerohydrodynamics]. Novosibirsk. Izd-vo SO RAN. 2014, 280 p.
9. *Yanenko N.N., Konovalov A.N., Bugrov A.N., Shustov G.V.* Ob organizatsii parallel'nykh vychisleniy i rasparallelivanie progonki [On the organization of parallel calculations and parallelization of the run], *Chislennye metody mekhaniki sploshnykh sred* [Numerical methods of continuum mechanics], 1978, No. 7, pp. 136-139.
10. *Semenistyy V.V., Gamolina I.E., Duryagina V.V.* Konstruirovanie effektivnykh parallel'nykh algoritmov dlya resheniya polnoy dvumernoy sistemy uravneniy Nav'e-Stoksa po yavnoy skheme Mak-Kormaka [Designing effective parallel algorithms for solving a complete two-dimensional system of Navier-Stokes equations according to the explicit McCormack scheme], *Sb. materialov II mezhdunarodnoy nauchno-prakticheskoy konferentsii «Issledovaniya i razrabotki v perspektivnykh nauchnykh oblastyakh»* [Collection of materials of the II International Scientific and Practical Conference "Research and Development in promising scientific fields"]. Novosibirsk, 2017, pp. 88-95.

11. *Semenistyy V.V., Gamolina I.E., Duryagina V.V, Bogdanov D.S.* Modelirovanie i analiz parallel'nogo algoritma resheniya zadachi obtekaniya ploskoy plastiny metodom global'nykh iteratsiy [Modeling and analysis of a parallel algorithm for solving the problem of flow around a flat plate by the method of global iterations], *Sb. materialov XIII mezhdunarodnoy nauchno-prakticheskoy konferentsii. CH. 1 «Voprosy sovremennoy nauki: problemy, tendentsii, perspektivy»* [Collection of materials of the XIII International Scientific and Practical Conference. Part 1 "Issues of modern science: problems, trends, prospects"]. Moscow: Nauchnyy zhurnal «Chronos», 2017, pp. 79-85.
12. *Semenistyy V.V., Gamolina I.E., Duryagina V.V.* Otsenka effektivnosti pryamykh parallel'nykh metodov dlya zadachi techeniya sovershennogo gaza po kanalu peremennogo secheniya [Evaluation of the effectiveness of direct parallel methods for the problem of perfect gas flow through a channel of variable cross-section], *Mater. XIV Vseros. nauchn.-prakt. konf., 15 iyunya 2018 g.* [Proceedings of the XIV All-Russian Scientific and Practical Conference, June 15, 2018]. Krasnodar: Krasnodarskiy universitet MVD Rossii, 2018, pp. 250-256.
13. *Kovenya V.M.* Ob odnom algoritme resheniya uravneniy Nav'e–Stoksa vyazkoy neszhimaemoy zhidkosti [On an algorithm for solving the Navier-Stokes equations of a viscous incompressible fluid], *Vychislitel'nye tekhnologii* [Computing technologies], 2006, Vol. 11, No. 2, pp. 39-51.
14. *Bogachev K.Yu.* Osnovy parallel'nogo programmirovaniya [Fundamentals of parallel programming]. Moscow: Binom. Laboratoriya znaniy, 2003, 344 p.
15. *Bazovkin A.V., Kovenya V.M.* Rasparallelivanie algoritma rasshchepleniya na mnogoprotsessornykh sistemakh pri modelirovanii techeniy vyazkoy neszhimaemoy zhidkosti [Parallelization of the splitting algorithm on multiprocessor systems in the simulation of viscous incompressible fluid flows], *Vestnik NGU. Seriya: Matematika, mekhanika, informatika* [Bulletin of NSU. Series: Mathematics, Mechanics, Computer science], 2013, Vol. 13, Issue 4, pp. 3-15.
16. *Gamolina I.E., Semenistyy V.V.* Parallel'naya organizatsiya vychisleniy pri raschete zadach aerogidrodinamiki pryamymi metodami. Mezhdunarodnoe nauchnoe sotrudnichestvo, obrazovanie i kul'tura [Parallel organization of calculations in the calculation of problems of aerohydrodynamics by direct methods. International scientific cooperation, education and culture]. Rostov-on-Don: Summa-Rerum, 2014, pp 3 (4).
17. *Gamolina I.E., Duryagina V.V., Semenistyy V.V.* Dozvukovoe obtekanie profiley [Subsonic flow around profiles], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 4, pp. 61-67.
18. *Terenkov V.I., Arsenii V.F., Evseev E.G., Lutskiy Ya.A., Semenistyy V.V.* O korrektnosti i ustoychivosti algoritma rasparallelivaniya progonki [On the correctness and stability of the parallelization algorithm of the run], Tr. int-ta prikl. matemat. im. I.N. Vekua Tbilis. un-ta [Proceedings of the I.N. Vekua Institute of Applied Mathematics]. Tbilisi, 1985, pp. 298-307.
19. *Degi D.V., Starchenko A.V.* Chislennoe reshenie uravneniy Nav'e-Stoksa na komp'yuterakh s parallel'noy arkhitekturoy [Numerical solution of the Navier-Stokes equations on computers with parallel architecture], *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika* [Bulletin of Tomsk State University. Mathematics and mechanics], 2012, No. 2 (18), pp. 88-98.
20. *Dongarra J., Foster I., Fox J. et al.* Sourcebook of Parallel Computing. San Francisco (CA, USA): Elsevier Science, 2003, 852 p.

Статью рекомендовал к опубликованию к. пед. н. Ю.В. Романов.

Семенистый Владимир Васильевич – Южный федеральный университет; e-mail: vlad60sem@gmail.com; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89282135206; кафедра высшей математики; к.ф.-м.н.; доцент.

Гамолина Ирина Эдуардовна – e-mail: iegamolina@sfedu.ru; тел.: 89185190837; кафедра высшей математики; к.т.н.; доцент.

Semenistyy Vladimir Vasil'evich – Southern Federal University; e-mail: vlad60sem@gmail.com; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +79282135206; the department of higher mathematics; cand. of phys.-math. sc.; associate professor.

Gamolina Irina Eduardovna – e-mail: iegamolina@sfedu.ru; phone: +79185190837; the department of higher mathematics; cand. of eng. sc.; associate professor.

Раздел II. Моделирование процессов, устройств и систем

УДК 621.372 DOI 10.18522/2311-3103-2020-5-68-74

А.Н. Зикий, П.Н. Зламан

МОДЕЛИРОВАНИЕ ДВУХ МИКРОПОЛОСКОВЫХ ФИЛЬТРОВ САНТИМЕТРОВОГО ДИАПАЗОНА

Полосовые фильтры являются неотъемлемой составной частью любой радиоприемной аппаратуры. Именно они определяют избирательность приемника по всем каналам приема. Целью настоящей работы является моделирование двух микрополосковых фильтров сантиметрового диапазона волн. Объектом исследования в данной работе являются два микрополосковых фильтра на частоты 5,75 и 4,6 ГГц. Такие фильтры можно использовать в конвертере сантиметрового диапазона волн в качестве сигнального и гетеродинного фильтров. Проведено моделирование двух фильтров в среде Microwave Office. Представлены результаты в виде моделей двух фильтров и четырех амплитудно-частотных характеристик. Даны геометрические размеры фильтров, достаточные для их изготовления на материале RT5870 фирмы Роджерс. Фильтры имеют ширину полосы пропускания 200 МГц и потери в полосе пропускания не более 3 дБ. Потери в полосе заграждения для сигнального фильтра составили не менее 45 дБ, и не менее 35 дБ для гетеродинного фильтра, что является очень хорошим результатом для двухзвенного фильтра. Приемлемые электрические параметры, малые габариты и умеренная стоимость изготовления фильтров позволяет их широко использовать в профессиональной и радиолюбительской аппаратуре. Для повышения технологичности изготовления выбран материал с малой диэлектрической проницаемостью. При этом зазоры и допуски на точность их изготовления получаются приемлемыми. Конструкция фильтров позволяет их легко интегрировать с другими узлами конвертера: малошумящим усилителем, смесителем, усилителем промежуточной частоты, усилителем в гетеродинном тракте.

Микрополосковый фильтр; амплитудно-частотная характеристика; топология; геометрические размеры; моделирование.

A.N. Zikiy, P.N. Zlaman

MODELING OF TWO MICROSTRIP FILTERS OF THE CENTIMETER RANGE

Band-pass filters are an integral part of any radio equipment. They determine the selectivity of the receiver for all channels of reception. The aim of this work is to modelling two microstrip filters of the centimeter wave range. The object of study in this work are two microstrip filters at a frequency of 5.75 GHz and 4.6 GHz. Such filters can be used in the converter of the centimeter wave range as a signal and heterodyne filters. Two filters were simulated in the Microwave Office environment. The results are presented in the form of models of two filters and four amplitude-frequency characteristics. Given are the geometric dimensions of the filters, sufficient for their manufacture on material RT5870 of Rogers company. Filters have a bandwidth of 200 MHz and a loss in bandwidth of not more than 3 dB. Losses in the stop band for the signal filter were at least 45 dB, and at least 35 dB for the heterodyne filter, which is a very good result for a two-pole filter. Acceptable electrical parameters, small dimensions and moderate cost of manufacturing filters allows them to be widely used in professional and amateur radio equipment. To improve the manufacturability of manufacturing, a material with a low dielectric constant was selected. At the same time, gaps and tolerances on the

accuracy of their manufacture are acceptable. The design of the filters allows them to be easily integrated with other components of the converter: a low-noise amplifier, a mixer, an intermediate frequency amplifier, an amplifier in the local oscillator path.

Microstrip filter; amplitude-frequency characteristic; topology; geometric dimensions; modeling.

Введение. При проектировании конвертора сантиметрового диапазона понадобились два фильтра – сигнальный и гетеродинный. Поскольку требования к фильтрам невысокие (табл. 1), было принято решение выполнить их на общей подложке с малошумящим усилителем, смесителем и усилителем промежуточной частоты. Микрополосковые фильтры могут быть выполнены с разной электродинамической структурой:

- на полуволновых резонаторах с четвертьволновыми связями [1];
- на встречных стержнях с четвертьволновыми резонаторами [1];
- гребенчатые фильтры с длиной резонаторов $\lambda/8$ и $\lambda/16$ [1];
- шлейфовые фильтры на однородных резонаторах [1];
- шлейфовые фильтры на неоднородных резонаторах.

Были выбраны фильтры с двумя полуволновыми резонаторами и четвертьволновыми связями [1, 2] на несимметричной микрополосковой линии передачи. Выбранный тип фильтра удобен как в изготовлении, так и в настройке.

К фильтрам предъявляются следующие требования, изложенные в табл. 1.

Таблица 1

Требования к фильтрам

Наименование параметра, размерность	Фильтр 1	Фильтр 2
Диапазон рабочих частот, ГГц	5,65-5,85	4,5-4,7
Потери в полосе пропускания, не более, дБ	3	3
Потери в полосе заграждения зеркальной частоты 3,35-3,55 ГГц не менее, дБ	30	30
Потери в полосе заграждения от 7,3 до 11 ГГц не менее, дБ	30	-
Потери в полосе заграждения от 6 до 9 ГГц не менее, дБ	-	30
Входное и выходное сопротивление, Ом	50	50
Число резонаторов	2	2

Конструкция сигнального фильтра. Топология исследуемого сигнального фильтра показана на рис. 1.

Рис. 1. Топология фильтра 1

Для изготовления конвертора и входящих в него фильтров выбран материал RT5870 фирмы Роджерс [3–6]. Этот материал имеет малые диэлектрические потери, высокую стабильность относительной диэлектрической проницаемости и может работать на исследуемых частотах.

Расчет сигнального фильтра проводился по методике из книги [1]. Результаты расчета приведены в табл. 2. Эти данные будем считать первым приближением, а второе приближение предполагается получить на модели.

Таблица 2

Геометрические размеры сигнального фильтра

Позиционное обозначение	Ширина, мм	Длина, мм	Наименование
w1	1	8.84	подводящий проводник
w2	2.5	8.84	резонатор
w3	2.5	8.84	резонатор
w4	2.5	8.84	резонатор
w5	2.5	8.84	резонатор
w6	1	8.84	подводящий проводник
s1	0.3	8.84	зазор
s2	1.3	8.84	зазор
s3	0.3	8.84	зазор

Конструкция гетеродинного фильтра. Конструкция гетеродинного фильтра такая же, как и сигнального. Результаты расчета гетеродинного фильтра приведены в табл. 3.

Таблица 3

Геометрические размеры гетеродинного фильтра

Позиционное обозначение	Ширина, мм	Длина, мм	Наименование
w1	1	11,2	подводящий проводник
w2	2.5	11,2	резонатор
w3	2.5	11,2	резонатор
w4	2.5	11,2	резонатор
w5	2.5	11,2	резонатор
w6	1	11,2	подводящий проводник
s1	0.3	11,2	зазор
s2	1.3	11,2	зазор
s3	0.3	11,2	зазор

Моделирование. Моделирование двух фильтров проведено в пакете прикладных программ Microwave Office (MWO) [7, 8]. Модель сигнального фильтра приведена на рис. 2.

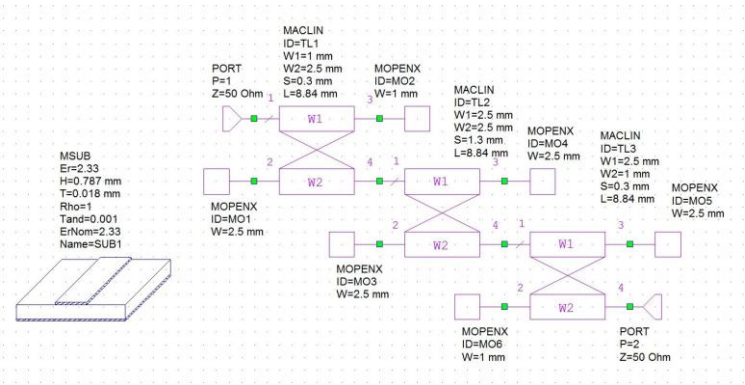

Рис. 2. Модель фильтра 1 из MWO

Для показа ложной полосы пропускания приведена АЧХ сигнального фильтра в полосе от 3 до 12 ГГц (рисю 3). Амплитудно-частотная характеристика этого фильтра из MWO в полосе 5–6,5 ГГц приведена на рис. 4. Анализ гетеродинного фильтра представлен на рис. 5–7.

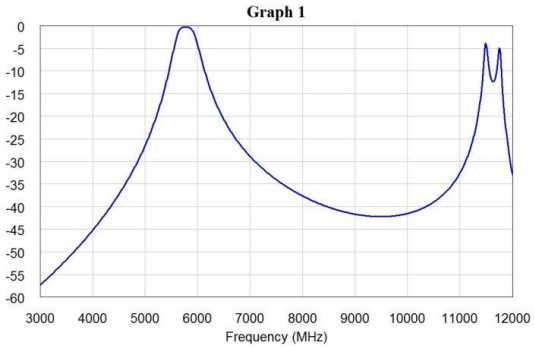

Рис. 3. АЧХ фильтра 1 в полосе 3-12 ГГц

Из рис. 3 видно, что ложная полоса пропускания на частоте $2f_0$ не подавляется, а заграждение на частотах зеркального канала 3,35–3,55 ГГц больше требуемого.

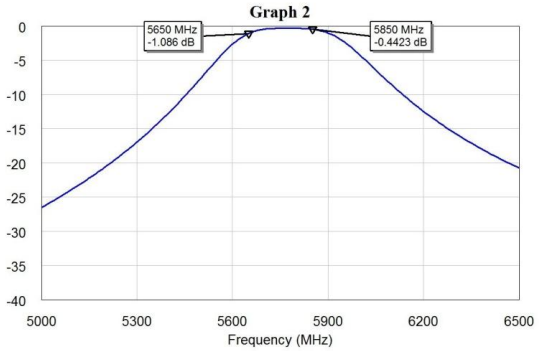

Рис. 4. АЧХ фильтра 1 в полосе 5–6,5 ГГц

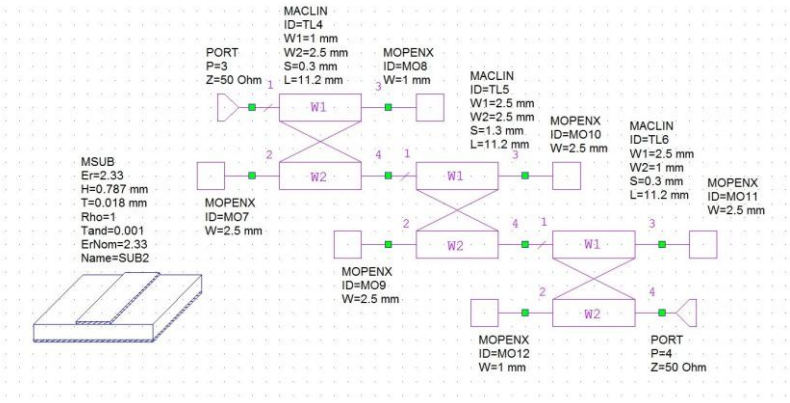

Рис. 5. Модель фильтра 2 из MWO

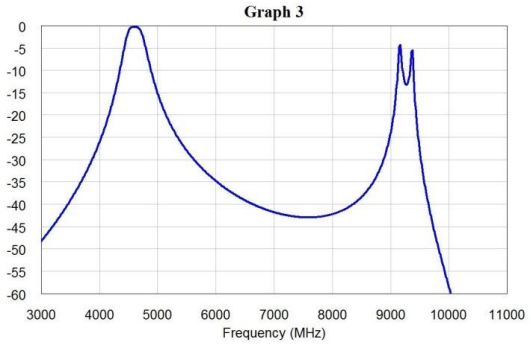

Рис. 6. АЧХ фильтра 2 в полосе 3–11 ГГц

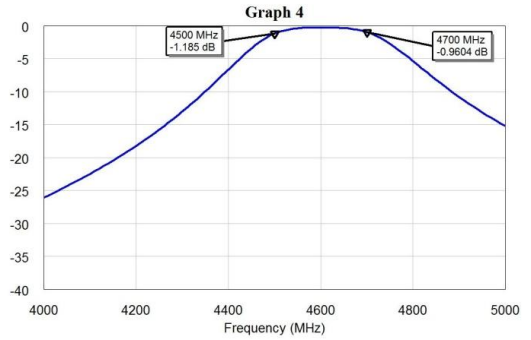

Рис. 7. АЧХ фильтра 2 в полосе 4–5 ГГц

Выводы. Ниже в табл. 4 сведены заданные и достигнутые при моделировании параметры фильтров.

Таблица 4

Основные параметры фильтров

Наименование параметра, размерность	Фильтр 1		Фильтр 2	
	задано	получено	задано	получено
Диапазон рабочих частот, ГГц	5,65–5,85	5,65–5,85	4,5–4,7	4,5–4,7
Потери в полосе пропускания не более, дБ	3	1,5	3	1,5
Потери в полосе заграждения зеркальной частоты 3,35–3,55 ГГц не менее, дБ	30	>45	30	>35
Потери в полосе заграждения от 7,3 до 11 ГГц не менее, дБ	30	>30	-	-
Потери в полосе заграждения от 6 до 9 ГГц не менее, дБ	–	–	30	>35
Входное и выходное сопротивление, Ом	50	50	50	50
Число резонаторов	2	2	2	2

Из этой таблицы видно, что все требования к фильтрам выполняются.

При выполнении данной работы были использованы сведения из статьи [9], а также предыдущий опыт авторов [10–14]. Выбору технического решения способствовало изучение и использование литературы [15–20], особенно примеров расчета.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Маттей Д.Л, Янг Л., Джонс Е.М.Т.* Фильтры СВЧ, согласующие цепи и цепи связи. – М.: Связь, 1971. – Т. 1. – 451 с. Т. 2. – 494 с.
2. *Зелях Э.В., Фельдштейн А.Л., Явич Л.Р., Брилон В.С.* Миниатюрные устройства УВЧ и ОВЧ диапазонов на отрезках линий. – М.: Радио и связь, 1989. – 112 с.
3. Design Equations for Broadside and Edgewise Stripline Couplers. Rogers Corporation. Design 3.2.1. – 2 p.
4. Width and Effective Dielectric Constant Equations for Design of Microstrip Transmission Lines. Rogers Corporation. Design 3.1.2. – 2 p.
5. RT/Duroid 5870/5880 High Frequency Laminates Fabrication Guidelines. Rogers Corporation. – 8 p.
6. RT/Duroid 5870/5880 High Frequency Laminates. Data Sheet. Rogers Corporation. – 2 p.
7. *Разевиг В.Д., Потапов Ю.В., Курушин А.А.* Проектирование СВЧ устройств с помощью Microwave Office. – М.: Солон-Пресс, 2003. – 496 с.
8. *Бахвалова С.А., Романюк В.А.* Основы моделирования и проектирования радиотехнических устройств в Microwave Office: учеб. пособие. – М.: Солон-Пресс, 2016. – 152 с.
9. 6 cm FM ATV-Convertor from Alberto IK8UIF дата обращения 8.05.2020. – http://home.kpn.nl/f2hjnlindeijer/532/6cm%20FMATV%20Converter.htm.
10. *Андрианов А.В., Быков С.А., Зикий А.Н., Пустовалов А.И.* Микрополосковый фильтр на полуволновых резонаторах // Инженерный вестник Дона. – 2017. – № 2.
11. *Андрианов А.В., Быков С.А., Зикий А.Н., Пустовалов А.И.* Моделирование и экспериментальное исследование трактового фильтра сантиметрового диапазона // Инженерный вестник Дона. – 2017. – № 1.
12. *Андрианов А.В., Зикий А.Н., Зламан П.Н.* Моделирование и экспериментальное исследование микрополоскового фильтра на полуволновых резонаторах // Электротехнические и информационные комплексы и системы. – 2016. – № 3. – С. 32-35.
13. *Андрианов А.В., Зикий А.Н., Пустовалов А.И.* Моделирование и экспериментальное исследование трактового фильтра на встречных стержнях // Инженерный вестник Дона. – 2016. – № 4.
14. *Зикий А.Н., Лебедев В.К., Зламан П.Н., Матвиенко Р.Н.* Экспериментальное исследование двух фильтров дециметрового диапазона // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 178-185.
15. *Ханзел Г.* Справочник по расчету фильтров. – М.: Сов. Радио, 1974. – 288 с.
16. *Алексеев Л.В., Знаменский А.Е., Лоткова Е.Д.* Электрические фильтры метрового и дециметрового диапазонов. – М.: Связь, 1976. – 280 с.
17. *Алексеев О.В., Грошев Г.А., Чавка Г.Г.* Многоканальные частотно-разделительные устройства и их применение. – М.: Радио и связь, 1981. – 136 с.
18. *Леонченко В.П., Фельдштейн А.Л., Шепелянский Л.А.* Расчет полосковых фильтров на встречных стержнях. Справочник. – М.: Связь, 1975. – 312 с.
19. *Бова Н.Т., Ефремов Ю.Г., Конин В.В. и др.* Микроэлектронные устройства СВЧ. – Киев: Техника, 1984. – 184 с.
20. Микроэлектронные устройства СВЧ: учеб. пособие / под ред. Г.И. Веселова. – М.: Высшая школа, 1988. – 280 с.

REFERENCES

1. *Mattey D.L, Yang L., Dzhons E.M.T.* Fil'try SVCh, soglasuyushchie tsepi i tsepi svyazi [Microwave filters, impedance-matching networks, and coupling structures]. Moscow: Svyaz', 1971, Vol. 1, 451 p. Vol. 2, 494 p.
2. *Zelyakh E.V., Fel'dshteyn A.L., Yavich L.R., Brilon V.S.* Miniatyurnye ustroystva UVCh i OVCH diapazonov na otrezkakh liniy [Miniature devices of UHF and VHF ranges on line segments]. Moscow: Radio i svyaz', 1989, 112 p.
3. Design Equations for Broadside and Edgewise Stripline Couplers. Rogers Corporation. Design 3.2.1, 2 p.
4. Width and Effective Dielectric Constant Equations for Design of Microstrip Transmission Lines. Rogers Corporation. Design 3.1.2, 2 p.
5. RT/Duroid 5870/5880 High Frequency Laminates Fabrication Guidelines. Rogers Corporation, 8 p.

6. RT/Duroid 5870/5880 High Frequency Laminates. Data Sheet. Rogers Corporation, 2 p.
7. *Razevig V.D., Potapov Yu.V., Kurushin A.A.* Proektirovanie SVCh ustroystv s pomoshch'yu Microwave Office [Design Microwave Devices Using Microwave Office]. Moscow: Solon-Press, 2003, 496 p.
8. *Bakhvalova S.A., Romanyuk V.A.* Osnovy modelirovaniya i proektirovaniya radiotekhnicheskikh ustroystv v Microwave Office: ucheb. posobie [Fundamentals of modeling and design of radio devices in the Microwave Office: tutorial]. Moscow: Solon-Press, 2016, 152 p.
9. 6 cm FM ATV-Convertor from Alberto IK8UIF дата обращения 8.05.2020. Available at: http://home.kpn.nl/f2hjnlindeijer/532/6cm%20FMATV%20Converter.htm.
10. *Andrianov A.V., Bykov S.A., Zikiy A.N., Pustovalov A.I.* Mikropoloskovyy fil'tr na poluvolnovykh rezonatorakh [Microstrip filter on half-wave resonators], *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 2017, No. 2.
11. *Andrianov A.V., Bykov S.A., Zikiy A.N., Pustovalov A.I.* Modelirovanie i eksperimental'noe issledovanie traktovogo fil'tra santimetrovogo diapazona [Modeling and experimental study of a centimeter-range channel filter], *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 2017, No. 1.
12. *Andrianov A.V., Zikiy A.N., Zlaman P.N.* Modelirovanie i eksperimental'noe issledovanie mikropoloskovogo fil'tra na poluvolnovykh rezonatorakh [Modeling and experimental study of a microstrip filter on half-wave resonators], *Elektrotekhnicheskie i informatsionnye kompleksy i sistemy* [Electrical and data processing facilities and systems]. 2016. No. 3, pp. 32-35.
13. *Andrianov A.V., Zikiy A.N., Pustovalov A.I.* Modelirovanie i eksperimental'noe issledovanie traktovogo fil'tra na vstrechnykh sterzhnyakh [Simulation and experimental study of a interdigital path filter], *Inzhenernyy vestnik Dona* [Engineering Journal of Don], 2016, No. 4.
14. *Zikiy A.N., Lebedev V.K., Zlaman P.N., Matvienko R.N.* Eksperimental'noe issledovanie dvukh fil'trov detsimetrovogo diapazona [An experimental study of two decimeter range filters], *Izvestiya YuFU. Tekhnicheskie nauki* [.Izvestiya SFedU. Engineering Sciences], 2014, No. 8, pp. 178-185.
15. *Khanzel G.* Spravochnik po raschetu fil'trov [Filter Calculation Reference]. Moscow: Sov. Radio, 1974, 288 p.
16. *Alekseev L.V., Znamenskiy A.E., Lotkova E.D.* Elektricheskie fil'try metrovogo i detsimetrovogo diapazonov [Electric filters of meter and decimeter ranges]. Moscow: Svyaz', 1976, 280 p.
17. *Alekseev O.V., Groshev G.A., Chavka G.G.* Mnogokanal'nye chastotno-razdelitel'nye ustroystva i ikh primenenie [Multichannel frequency separation devices and their application]. Moscow: Radio i svyaz', 1981, 136 p.
18. *Leonchenko V.P., Fel'dshteyn A.L., Shepelyanskiy L.A.* Raschet poloskovykh fil'trov na vstrechnykh sterzhnyakh. Spravochnik [Calculation of interdigital band-pass filters]. Moscow: Svyaz', 1975, 312 p.
19. *Bova N.T., Efremov Yu.G., Konin V.V. i dr.* Mikroelektronnye ustroystva SVCh [Microelectronic Microwave Devices]. Kiev: Tekhnika, 1984, 184 p.
20. Mikroelektronnye ustroystva SVCh: ucheb. posobie [Microelectronic Microwave Devices: tutorial, ed. by G.I. Veselova. Moscow: Vysshaya shkola, 1988, 280 p.

Статью рекомендовал к опубликованию к.т.н. М.И. Дулин.

Зикий Анатолий Николаевич – Южный федеральный университет; e-mail: zikiy50@mail.ru; 347922, г. Таганрог, ул. Чехова, 2; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; с.н.с.; доцент.

Зламан Павел Николаевич – e-mail: otdel24d@.nkbmius.ru; 347900, г. Таганрог, ул. Петровская, 81; Научно-конструкторское бюро моделирующих и управляющих систем; ведущий инженер-конструктор.

Zikiy Anatoliy Nikolaevich – Southern Federal University; e-mail: zikiy50@mail.ru; 2, Chekhov street, Taganrog, 347922, Russia; the department of information security of telecommunication systems; cand. of eng. sc.; senior researcher; associate professor.

Zlaman Pavel Nikolaevich – e-mail: otdel24d@.nkbmius.ru; 81, Petrovskaya street, Taganrog, 347900, Russia; Research and design Bureau of modeling and control systems; leading design engineer.

УДК 517.524 DOI 10.18522/2311-3103-2020-5-75-85

Н.С. Кривша, В.В. Кривша, С.А. Бутенков

МОДЕЛИРОВАНИЕ СТРУКТУРЫ КУБАТУРНЫХ ФОРМУЛ ДЛЯ ПРОЕКТИРОВАНИЯ ЭФФЕКТИВНЫХ ВЫЧИСЛИТЕЛЬНЫХ СТРУКТУР НА ПЛИС

Предлагается метод построения вычислительных моделей для исследования и оптимизации универсальных вычислительных структур, выполняющих вычисление вычисления сложных кубатурных формул. Теоретической базой для введенных моделей служит теория пространственной грануляции, методы которой разработаны коллективом авторов. Методология пространственной грануляции позволяет переходить от вычислений в точечном метрическом пространстве данных (которое не всегда существует) к вычислениям в аффинном многомерном пространстве, содержащем укрупненные единицы данных (пространственные гранулы). Такое преобразование данных основано на использовании аффинно-инвариантных моделей декартовых гранул и основывается на оптимальных процедурах покрытия точечного пространства выпуклыми гранулами. Такие полезные вычислительные свойства введенных моделей данных позволяют построить вычислительно эффективные процедуры для манипулирования многомерными данными, одним из приложений которых является вычисление многомерных кубатурных формул. Новые модели позволяют создавать наглядные матричные модели данных произвольной размерности для целей планирования структуры вычислительных процессов и построения информационных графов таких процессов. Эффективное и наглядное представление сложных вычислительных формул позволяет выполнять эквивалентные (с численной точки зрения) преобразования таких формул с целью выбора эффективных схемных решений для построения высокопроизводительных вычислительных блоков вычисления кубатур высокой размерности на базе ПЛИС. На основе оптимизированных моделей вычислительных структур строятся схемные решения, реализующие кубатурные формулы на реконфигурируемых вычислительных системах. Сложность решения задачи проектирования на ПЛИС связана с тем, что используемые вычислительные средства содержать поля ПЛИС, проектирование вычислительных структур для которых является вычислительно сложной задачей. Авторы использовали разработанные в организации автоматизированные средства проектирования на полях ПЛИС, такие как язык высокого уровня COLAMO, язык низкого уровня Fire Constructor и сопутствующие программные средства для реализации полученных информационных графов многомерных кубатур и экспериментальной оценки качества полученных результатов. Предлагаемый в работе теоретический подход к моделированию и оптимизации информационных графов вычислительных структур может быть распространен на широкий круг задач вычислительной математики.

Численные методы; кубатурные формулы; теория грануляции; пространственные гранулы; высокопроизводительные вычисления; реконфигурируемые вычислительные системы; ПЛИС.

N.S. Krivsha, V.V. Krivsha, S.A. Butenkov

THE STRUCTURE OF CUBATURE FORMULAS MODELLING FOR THE EFFICIENT FPGA IMPLEMENTATION

In the paper we present the new computing models for the common cubature formulas computing unit design and optimization. The basis of new modeling technique is related with the space granulation theory, developed in our recent papers. The Spatial Granulation Technique allows us to pass from computing in the metrical data points space to affine data space, contains the aggregated data units named as granules. The introduced data transformation based on the affine-invariant Cartesian granule model and on the optimal data points coarsening procedures. The useful properties of new data models allows to provide the very efficient multivariable data management procedures. The one of them is the multivariate cubature formulas calculation. The new theory provides the obvious matrix data processing models for the information graphs design and

optimization. We can perform the equivalent mappings for the complicated information graph models for the efficient structures matching. Optimized models of information graphs are used for the FPGA-based devices implementation. The main problem of FPGA design is the commutation structures complication for the large FPGA fields, obtained as the basic units for the reconfigurable cubature formulas computing units. In this work we use the high-level programming language COLAMO and assembler language Fire Constructor for the computing units implementation. As a result of new technique implementation we can provide the family of adequate and useful graphic representation for a multivariable cubature formulas over the matrix calculation. The provided models are suitable for the optimal design of configurable computing structures, universal and dedicated devices from the FPGA basis. For the device implementation the developed high-level software products are used. For the designed universal devices the testing procedures was performed and examined with the symbolic calculation software for the computing results evaluation.

Cubature formula; theory of space granulation; space granules; high-performance computing; configurable computer; FPGA.

Введение. Одной из классических, но и поныне практически важных задач вычислительной математики является задача вычислении многомерных (или многократных) интегралов. Это область численных методов, изобилующая множеством классических результатов, но предоставляющая обширное поле нерешенных задач [1]. Она имеет широчайшее поле приложений [2, 3] и, в то же время, является обширным полем приложения сил для получения новых теоретических результатов [4, 5]. В настоящее время существенно расширился круг решаемых в этой области вычислительных задач. Потребовалось научиться вычислять интегралы от сложных функций большого числа переменных [4–6]. При этом резко выросли вычислительные возможности: можно использовать десятки тысяч и более узлов интерполяции. Для подобных задач важнейшую роль приобретают методы проектирования эффективных вычислительных структур [7, 8], решающих сложные задачи при оптимальном расходе аппаратных и временных ресурсов [9, 11].

Начальным этапом построения реконфигурируемых высокопроизводительных систем является построение и оптимизация информационных графов вычислительных процессов [9]. На основе получаемых (и оптимизируемых) графов процессов можно строить реализации вычислительных блоков с использованием высокоуровневых средств разработки, таких как специализированный язык COLAMO и другие средства обеспечения процесса проектирования схемных решений [12]. Отметим, что решающим (и пока не автоматизированным) этапом в проектировании информационных графов является переход от алгебраической записи вычислительной формулы к собственно графу вычислительного процесса. Эта задача плохо формализуема и содержит значительную творческую составляющую, подобно задаче составления алгоритма для языков программирования [8, 9]. От результатов построения информационного графа для заданной вычислительной формулы во многом зависят точность, быстродействие и аппаратные затраты полученного схемного решения вычислительной задачи [13], поэтому методология данного этапа является важной при проектировании.

Цели и задачи работы. Целью работы является разработка методологии моделирования кубатурных формул с помощью математического аппарата грануляции для получения моделей, позволяющих изучать свойства различных вычислительных структур для последующей реализации с помощью стандартных программных средств разработки реконфигурируемых вычислительных структур на ПЛИС.

Задачи работы:

1) Построение метода представления кубатурных формул в аппарате гранулированных вычислений;

2) Получение универсальных рабочих структур информационных графов для построения устройств вычисления многомерных кубатур;

3) Изучение возможности реализации полученных графов на стандартных средствах проектирования для ПЛИС;

4) Экспериментальная оценка полученных результатов.

Для решения этих задач в работе использованы базовые теоретические результаты теории пространственной грануляции данных [15–17], высокоуровневые программные средства разработки вычислительных блоков на ПЛИС: алгоритмический язык COLAMO и язык уровня ассемблера Fire Constructor [12], а также средства символьных вычислений пакета MathCAD для оценки точности полученных результатов.

Основы методологии грануляции. Идеология гранулированных вычислений основана на переходе от представления данных в виде точек некоторого векторного пространства [14] к их представлению более сложными математическими структурами. Она объединяет и обобщает широкий круг частных подходов, связанных с кластеризацией, сегментацией, покрытием сетями Кохонена и другими подобными подходами, связанными с укрупнением единиц представления данных (в широком смысле этого слова) [18–20].

В ряде наших работ методология грануляции применена для неточечных объектов в многомерных пространствах с сохранение исходного геометрического смысла и получила название теории пространственной грануляции [15, 19, 20] и др.

В декартовых координатах объект представляется в виде множества элементов в пространстве размерности n [6], каждый из которых задан с помощью определителя с $n+1$ параметром:

$$G_n = \begin{vmatrix} {}^1x^1 & {}^2x^1 & \cdots & {}^nx^1 & (-1)^n \\ {}^1x^2 & {}^2x^2 & \cdots & {}^nx^2 & (-1)^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ {}^1x^n & {}^2x^n & \cdots & {}^nx^n & (-1)^n \\ {}^1x^{n+1} & {}^2x^{n+1} & \cdots & {}^nx^{n+1} & (-1)^n \end{vmatrix}, \quad (1)$$

при этом параметрами элемента являются координаты вершин элемента ${}^ix^j$, $i=1,...,n,\quad j=1,...,(n+1)$ в тензорных обозначениях. Данная алгебраическая модель допускает вычисление целого спектра мер на элементах G_n с помощью миноров (1) согласно [19].

Построение квадратурных формул на моделях гранул. Используем геометрическое содержание введенной модели (1), где определитель рассматривается как аффинный геометрический инвариант, после нормировки, приводится к площади фигуры, образованной точками, проективные координаты которых входят в модель (1).

Для размерности пространства $n=1$ (квадратуры) выберем на отрезке числовой оси $a \le x^1 \le b$ узлы сетки $\omega = \left\{ {}^kx^1 \in [a;b] \right\}$, $0 \le k \le Nx^1$, при этом шаг сетки может быть неравномерным [1]. Согласно [6], мы можем записать базовую квадратурную формулу прямоугольников для интеграла на отрезке в виде

$$\int_a^b f\left(x^1\right)dx^1 = \sum_{k=1}^{Nx^1} \begin{vmatrix} {}^{k-1}x^1 f\left({}^{k-1}x^1\right) & 0 & 1 \\ {}^kx^1 f\left({}^{k-1}x^1\right) & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} + R\left(x^1\right), \quad (2)$$

пригодном для реализации на параллельных и кластерных системах [8, 20].

Используя свойства определителей модели (1), мы можем модифицировать формулу (2) в форме, эффективной при реализации на конвейерных системах:

$$\int_a^b f\left(x^1\right)dx^1 = \begin{vmatrix} \sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 f\left({}^{k-1}x^1\right)\right] & 0 & 1 \\ \sum_{k=1}^{Nx^1}\left[{}^{k}x^1 f\left({}^{k-1}x^1\right)\right] & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} + R\left(x^1\right). \quad (3)$$

Комбинируя модели (2) и (3), мы можем получить формулу более высокого порядка точности (средних прямоугольников) на той же сетке, которая имеет вид:

$$\int_a^b f\left(x^1\right)dx^1 = \begin{vmatrix} 2\sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 \cdot f\left(\frac{{}^{k}x^1 + {}^{k-1}x^1}{2}\right)\right] & 0 & 1 \\ \sum_{k=1}^{Nx^1}\left[\left({}^{k}x^1 + {}^{k-1}x^1\right)\cdot f\left(\frac{{}^{k}x^1 + {}^{k-1}x^1}{2}\right)\right] & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} + R\left(x^1\right). \quad (4)$$

Отметим, что используя свойства определителей и формулы (2) – (4), мы можем построить модели квадратурных формул более высокого порядка точности, например, формулы трапеций для параллельно-конвейерной реализации по [19]:

$$\int_a^b f\left(x^1\right)dx^1 = \begin{vmatrix} \left[\left(\sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 f\left({}^{k-1}x^1\right)\right]\right) - \left(\sum_{k=1}^{Nx^1}\left[{}^{k}x^1 \cdot f\left({}^{k}x^1\right)\right]\right)\right] & 0 & \frac{1}{2} \\ \left[\left(\sum_{k=1}^{Nx^1}\left[{}^{k}x^1 f\left({}^{k-1}x^1\right)\right]\right) - \left(\sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 \cdot f\left({}^{k}x^1\right)\right]\right)\right] & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{vmatrix} + R\left(x^1\right). \quad (5)$$

Повышая порядок составных квадратурных формул, из (5) получаем базовый вариант квадратурной формулы Симпсона для параллельно-конвейерной реализации [5]:

$$\int_a^b f\left(x^1\right)dx^1 = \begin{vmatrix} \left[4\cdot\sum_{k=1}^{Nx^1}\left[2^{k-1}x^1_{k-1} f\left(\frac{{}^{k-1}x^1 + {}^{k}x^1}{2}\right)\right] - \sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 f\left({}^{k-1}x^1\right)\right] + \sum_{k=1}^{Nx^1}\left[{}^{k}x^1 f\left({}^{k}x^1\right)\right]\right] & 0 & \frac{1}{6} \\ \left[4\cdot\sum_{k=1}^{Nx^1}\left[\left({}^{k-1}x^1 + {}^{k}x^1\right) f\left(\frac{{}^{k-1}x^1 + {}^{k}x^1}{2}\right)\right] - \sum_{k=1}^{Nx^1}\left[{}^{k}x^1 f\left({}^{k-1}x^1\right)\right] + \sum_{k=1}^{Nx^1}\left[{}^{k-1}x^1 f\left({}^{k}x^1\right)\right]\right] & 0 & \frac{1}{6} \\ 0 & 1 & 0 \end{vmatrix} + R\left(x^1\right). \quad (6)$$

Построение кубатурных формул на моделях гранул. Введенная модель (1) позволяет развить методологию моделирования формул на гранулах и на случай $n = 2$, т.е. для построения моделей кубатурных формул. Для построения модели кубатурной формулы будем использовать метод ячеек на основе квадратурных формул (2)–(6), поскольку он обеспечивает большую точность, чем метод повторного интегрирования [1]. В случае сетки $a \le x^1 \le b, c \le x^2 \le d$ (возможно, неравномерной) с узлами $\omega = \left\{\left({}^{k1}x^1, {}^{k2}2x^2\right) \in [a;b]\times[c;\mathrm{d}]\right\}$, $0 \le k1 \le Nx^1, 0 \le k2 \le Nx^2$ получим параллельную версию кубатурной формулы прямоугольников в виде:

$$\iint\limits_D f\left(x^1,x^2\right)dx^1dx^2=\sum_{k1=1}^{Nx^1}\begin{vmatrix}\sum\limits_{k2=1}^{Nx^2}\left[{}^{k2-1}x^2\,f\left({}^{k1}x^1,{}^{k2}x^2\right)\right] & 0 & 1\\ \sum\limits_{k2=1}^{Nx^2}\left[{}^{k2}x^2\,f\left({}^{k1}x^1,{}^{k2}x^2\right)\right] & 0 & 1\\ 0 & \left({}^{k1}x^1-{}^{k1-1}x^1\right) & 0\end{vmatrix}+R\left(x^1,x^2\right). \quad (7)$$

Важным свойством введенных кубатур является то, что шаг сетки ω может быть неравномерным по обеим координатам. Это полезно при разработке адаптивных алгоритмов интегрирования [2].

Формула (7) может быть представлена в конвейерной форме как:

$$\iint\limits_D f\left(x^1,x^2\right)dx^1dx^2=\begin{vmatrix}\sum\limits_{k1=1}^{Nx^1}\sum\limits_{k2=1}^{Nx^2}\left[{}^{k2-1}x^2\,f\left({}^{k1}x^1,{}^{k2}x^2\right)\right] & 0 & \dfrac{1}{Nx^1}\\ \sum\limits_{k1=1}^{Nx^1}\sum\limits_{k2=1}^{Nx^2}\left[{}^{k2-1}x^2\,f\left({}^{k1}x^1,{}^{k2}x^2_{k2}\right)\right] & 0 & \dfrac{1}{Nx^1}\\ 0 & \sum\limits_{k1=1}^{Nx^1}\left[{}^{k1}x^1-{}^{k1-1}x^1\right] & 0\end{vmatrix}+R\left(x^1,x^2\right). \quad (8)$$

Модифицируя исходные формулы (2), (3) и (7), получим параллельную реализацию кубатурной формулы трапеций:

$$\iint\limits_D f\left(x^1,x^2\right)dx^1dx^2=\sum_{k1=1}^{Nx^1}\begin{vmatrix}2\cdot\sum\limits_{k2=1}^{Nx^2}\left[{}^{k2-1}x^2\,f\left({}^{k1}x^1,\dfrac{{}^{k2}x^2+{}^{k2-1}x^2}{2}\right)\right] & 0 & 1\\ \sum\limits_{k2=1}^{Nx^2}\left[\left({}^{k2}x^2+{}^{k2-1}x^2\right)f\left({}^{k1}x^1,\dfrac{{}^{k2}x^2+{}^{k2-1}x^2}{2}\right)\right] & 0 & 1\\ 0 & \left({}^{k1}x^1-{}^{k1-1}x^1\right) & 0\end{vmatrix}+R\left(x^1,x^2\right). \quad (9)$$

На основе свойств модели (1) и применяя (2), (3) к (8), можно представить кубатурную формулу трапеций в конвейерной форме:

$$\iint\limits_D f\left(x^1,x^2\right)dx^1dx^2=\begin{vmatrix}2\sum\limits_{k1=1}^{Nx^1}\sum\limits_{k2=1}^{Nx^2}\left[{}^{k2-1}x^2\,f\left({}^{k1}x^1,\dfrac{{}^{k2}x^2+{}^{k2-1}x^2}{2}\right)\right] & 0 & \dfrac{1}{Nx^1}\\ \sum\limits_{k1=1}^{Nx^1}\sum\limits_{k2=1}^{Nx^2}\left[\left({}^{k2}x^2+{}^{k2-1}x^2\right)f\left({}^{k1}x^1,\dfrac{{}^{k2}x^2+{}^{k2-1}x^2}{2}\right)\right] & 0 & \dfrac{1}{Nx^1}\\ 0 & \sum\limits_{k1=1}^{Nx^1}\left[{}^{k1}x^1-{}^{k1-1}x^1_1\right] & 0\end{vmatrix}+R\left(x^1,x^2\right). \quad (10)$$

Аналогичным образом на основе модели (1) могут быть получены многомерные кубатурные формулы для произвольной размерности пространства n [15].

Полученные формулы демонстрируют методику получения и модификации эквивалентных представлений кубатурных формул, позволяющих получать различную структуру и, следовательно, погрешность, сложность и другие показатели процесса вычисления [22].

Рассмотрим теперь структуры, позволяющие реализовывать в виде аналогичных моделей методы произвольного порядка точности в пространстве произвольного порядка n [19].

Универсальные кубатурные формулы на моделях гранул. Очевидно, что с точки зрения вычислительной структуры алгоритма все интерполяционные кубатурные формулы полностью задаются порядком метода и набором весовых и узловых коэффициентов [1]. Это позволяет для полученной в предыдущем разделе оп-

тимальной модели вычислений (2)–(10) получить компактное (свернутое) представление. Введем общие обозначения для узловых коэффициентов U_k, определяющих расположение узлов ${}^k x^i$, где $i = 1, ..., Nx^1$ – тензорный индекс координаты, а $k = 1, ..., N\omega$ – индекс узла сетки по i-й координате. Для обеспечения универсальности в выборе метода введем весовые коэффициенты C_k, соответствующие выбранным узлам сетки ω [22].

Введем индекс для локальных интервалов составной квадратурной формулы $j = 1, ..., Nx^1$. На локальных интервалах $\left[{}^{j-1}x^1, {}^{j}x^1 \right]$ используем модельные формулы (2) – (6) с нормировкой шагов на каждом интервале по массиву значений U_k, а также учитывая веса узлов на локальном интервале как C_k, мы получим универсальную составную квадратурную формулу для моделей (2)–(6), пригодную для реализации с помощью языка проектирования COLAMO [5] в виде:

$$\int_a^b f\left(x^1\right)dx^1 = \frac{1}{C_{met}} \sum_{j=0}^{Nx^1-1} \left[\left({}^{j+1}x^1 - {}^{j}x^1 \right) \sum_{k=0}^{N\omega-1} C_k^1 f\left(\frac{{}^{j+1}x^1 + {}^{j}x^1}{2} + \frac{{}^{j+1}x^1 - {}^{j}x^1}{2} U_k^1 \right) \right] + R\left(x^1\right), \quad (11)$$

где $C_{met} = \sum_{k=0}^{N\omega-1} C_k$ – нормирующий коэффициент заданного метода интегрирования. Число весовых коэффициентов формулы C_k равно числу узловых коэффициентов U_k и равно $N\omega$ (порядку выбранного метода интегрирования) [1].

Распространяя основные обозначения (11) на модельные формулы кубатур (7)–(10), для функции $f\left(x^1, x^2\right)$ на прямоугольнике $\left((a,b);(c,d)\right)$ в плоскости получим универсальную кубатурную формулу вида:

$$\iint_D f\left(x^1, x^2\right)dx^1dx^2 = \frac{1}{C_{met1}C_{met2}} \sum_{j1=0}^{Nx^1-1} \left[C_{j1}^1 \left({}^{j1+1}x^1 - {}^{j1}x^1 \right) \left[\sum_{j2=0}^{Nx^2-1} \left[C_{j2}^2 \left({}^{j2+1}x^2 - {}^{j2}x^2 \right) \left[\sum_{k1=0}^{N\omega1-1} \left[\sum_{k2=0}^{N\omega2-1} \left[f\left(\frac{{}^{j1+1}x^1 + {}^{j1}x^1}{2} + \frac{{}^{j1+1}x^1 - {}^{j1}x^1}{2} U_{k1}^1, \frac{{}^{j2+1}x^2 + {}^{j2}x^2}{2} + \frac{{}^{j2+1}x^2 - {}^{j2}x^2}{2} U_{k2}^2 \right) \right] \right] \right] \right] \right] \right] + R\left(x^1, x^2\right), \quad (12)$$

где C_{met1}, C_{met2} – нормирующие коэффициенты методов интегрирования, Nx^1, Nx^2 – количества разбиений координатных осей, $N\omega1, N\omega2$ – порядки методов для координатных осей 1 и 2, C_i^1, C_j^2 – весовые коэффициенты по координатам, U_i^1, U_j^2 – узловые коэффициенты по координатам.

Отметим, что при использовании формул типа (12) для интегрирования по разным координатным осям могут быть использованы разные методы, отличающиеся порядком, узловыми и весовыми коэффициентами [1]. Такое свойство существенно повышает универсальность предлагаемых формул для случая, когда свойства подынтегральной функции существенно отличаются при изменении вдоль разных координатных осей [2].

На основе формул (11), (12) можно получить многомерные кубатурные формулы для произвольной размерности вмещающего пространства n. Возможно также получение универсальных формул для криволинейных областей На основе формул (11), (12) можно получить также универсальные кубатурные формулы для произвольной размерности вмещающего пространства n [20].

Структурное представление универсальных формул. Полученные в предыдущих разделах формулы позволяют строить информационные универсальных графы кубатурных формул, управляя их реализацией в специализированном языке

COLAMO [12]. В качестве примера разработаем возможные реализации графа вычисления универсальной квадратурной формулы (11). Для упрощения графа введем заранее нормированные весовые коэффициенты метода: $C'_k = C^1_k / Cmet$. Для параллельной схемы вычислений граф приведен на рис. 1.

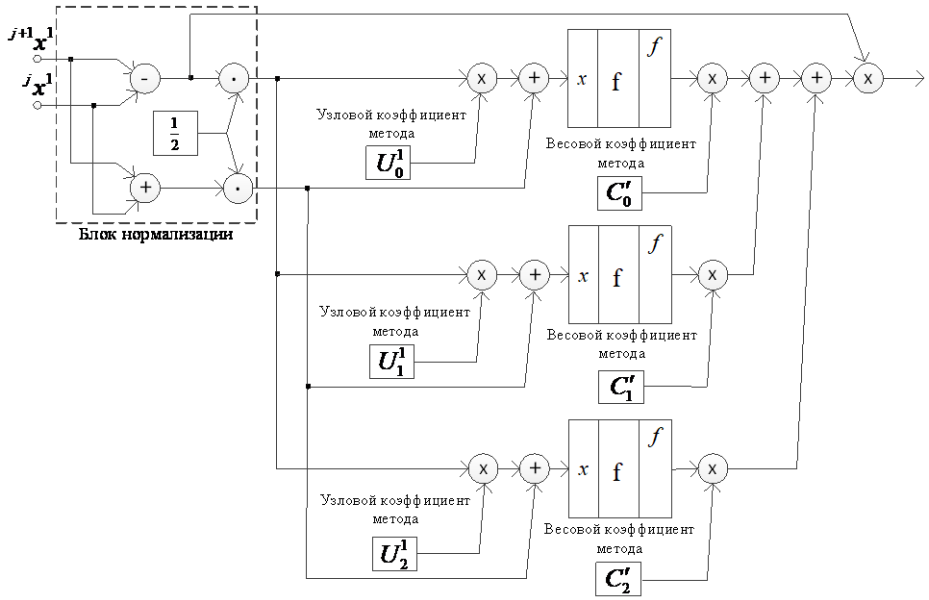

Рис. 1. Базовый граф параллельной схемы вычислений для (11)

По формуле (11) можно также построить информационный граф для конвейерной реализации квадратуры, представленный на рис. 2.

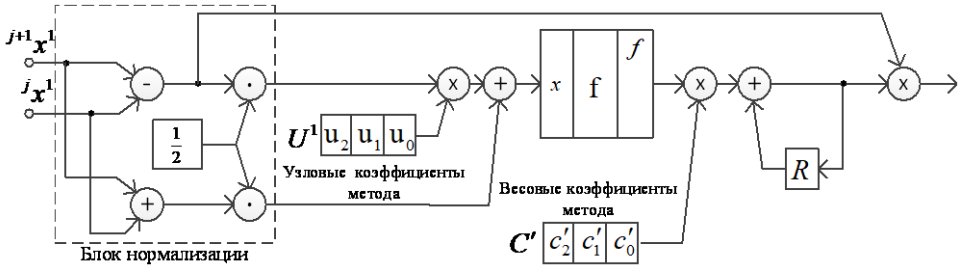

Рис. 2. Базовый граф конвейерной схемы вычислений для (11)

Общая структура РВС на ПЛИС строится с помощью метода параллельно-конвейерного представления информационных графов. Для сборки структур РВС из типовых макросов могут используются разработанные в НИЦ СЭ и НК высокоуровневые средства проектирования: алгоритмический язык COLAMO и язык уровня ассемблера Fire Constructor [9, 12].

Приведенные примеры графов вычислений являются универсальными по отношению к выбору метода и шага интегрирования. Что позволяет создать универсальные блоки интегрирования для ПЛИС, настраиваемые параметрами [8, 11]. Также возможно создание вычислителей кубатурных формул высокой размерности $n > 3$, оптимизированных по структуре вычислений и затрачиваемому ресурсу [13].

Исследование реализаций универсальной формулы. Для оценки погрешности вычисления были организованы символические вычисления в пакете MathCAD для точного значения интеграла. Для оценки погрешности метода в том же пакете вычислялись точные значения квадратуры по выбранному методу. Эти значения сравнивались с результатом, полученным с помощью блоков на ПЛИС. Результаты тестирования приведены в следующей таблице.

Таблица 1

Пор. мет.	$n=1$		$n=2$		$n=3$	
Мет. Ньютона-Котеса	Отн. погр.		Отн. погр.		Отн. погр.	
	Точ. знач.	Выч. знач.	Точ. знач.	Выч. знач.	Точ. знач.	Выч. знач.
	5,6%	6,0%	1,5%	1,3%	0,45%	0,64%
Мет. наив. точности	0,24%	0,32%	0,03%	0,04%	0,002%	0,003%

Изучение таблицы показывает, что полученные значения квадратур практически не отличаются от точных значений квадратур.

Заключение. В работе предлагается математический аппарат представления одного важного класса вычислительных задач (вычисление многомерных кубатурных формул [1]), основанный на представлении исходных формул в виде формул на пространственных гранулах [6]. Такие модели позволяют получать множество вариантов вычислительных структур не эвристическим путем, а с помощью эквивалентных преобразований исходных формул [19]. При преобразованиях изменяется структура, точность, число операций и другие свойства изучаемых формул, что позволяет целенаправленно искать требуемые оптимальные показатели структуры [16] для дальнейшей реализации с помощью стандартных программных средств [9].

Предложенная методика позволяет получить для сложных (многомерных) кубатурных формул большое количество вариантов структуры организации вычислений, лежащих между чисто параллельным и чисто конвейерным представлениями [8] в виде доступной для восприятия матричной модели [6].

В качестве перспектив развития предложенного подхода можно рассматривать распространение полученных теоретических и прикладных результатов на методы решения дифференциальных и интегральных уравнений [2], методы конечных элементов [3] и другие разделы, математически связанные с понятиями интегрирования с целью получения эффективных решений таких классов задач на реконфигурируемых вычислительных системах [8–10].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Соболь И.М.* Многомерные квадратурные формулы и функции Хаара. – М.: Наука, 1969. – 288 с.
2. *Зализняк В.Е.* Основы научных вычислений: Введение в численные методы для физиков. – М.: Едиториал УРСС, 2002.– 378 с.
3. *Самарский А.А., Михайлов А.П.* Математическое моделирование: Идеи. Методы. Примеры. – 2-е изд., испр. – М.: Физматлит, 2001. – 320 с.
4. *Бутенков С.А. Кривша Н.С., Кривша В.В.* Современные процедуры анализа многомерных данных // Современное состояние естественных и технических наук. – 2015. – Вып. XIX. – С. 75-76.
5. *Рогозов Ю.И., Бутенков С.А., Нагоров А.Л., Бесланеев З.О* Модели данных на основе теории информационной грануляции // Сб. трудов Пятой Международной конференции «Системный анализ и информационные технологии» САИТ-2013, Красноярск, 19-25 сентября 2013 г. – Т. 2. – С. 395-398.

6. *Бутенков С.А., Нагоров А.Л., Бесланеев З.О.* Геометрический подход к построению моделей данных на основе теории грануляции // Вестник Дагестанского государственного технического университета. – 2014. – № 1. – Т. 32. – С. 47-55.
7. *Барский А.Б.* Параллельные процессы в вычислительных системах. Планирование и организация. – М.: Радио и связь, 1990. – 256 с.
8. *Бутенков С.А.* Структурная организация гранулированных вычислений при обработке данных на реконфигурируемых вычислительных системах // Известия ЮФУ: Технические науки. – 2018. – № 8 (202). – С. 250-262.
9. *Каляев И.А., Левин И.И., Семерников Е.А., Шмойлов В.И.* Реконфигурируемые мультиконвейерные вычислительные структуры. – Ростов-на-Дону: Изд.-во ЮНЦ РАН, 2009. – 344 с.
10. *Butenkov S., Zhukov A., Nagorov A., Krivsha N.* Granular Computing Models and Methods Based on the Spatial Granulation // XII Int. Symposium «Intelligent Systems», INTELS'16, 5-7 October 2016, Moscow, Russia. Elsevier Procedia Computer Science. – 2017. – Vol. 103. – P. 295-302.
11. *Бутенков С.А.* Высокопроизводительные технические средства и методы для реконфигурируемых вычислительных систем в оптико-электронных системах обработки данных // Матер. V Международной научно-практической конференции «Актуальные вопросы исследований в авионике: теория, обслуживание, разработки» – «АВИАТОР», 15-16 февраля 2018 г., ВУНЦ ВВС «ВВА им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). – С. 112-114.
12. *Левин И.И., Дордопуло А.И., Гудков В.А.* Программирование реконфигурируемых вычислительных узлов на языке COLAMO: учеб. пособие. – Ростов-на-Дону: Изд-во ЮФУ, 2016. – 114 с.
13. *Бутенков С.А., Семерников Е.А.* Оптимизация проектирования вычислительных систем реального времени на основе моделей массового обслуживания // Матер. Третьей Всероссийской научно-технической конференции "Суперкомпьютерные технологии" (СКТ-2014), Геленджик, 29 сентября – 4 октября 2014 г. – Ростов-на-Дону: Изд-во ЮФУ, 2014. – Т. 1. – С. 30-35.
14. *Бутенков С.А., Жуков А.Л.* Информационная грануляция на основе изоморфизма алгебраических систем // Сб. трудов Международной алгебраической конференции, посвященной 80-летию со дня рождения А.И. Кострикина, Нальчик, 12-18 июля 2009 г. – С. 206-209.
15. *Бутенков С.А.* Грануляция и инкапсуляция в системах эффективной обработки многомерной информации // Искусственный интеллект. – 2005. – № 4. – С. 106-115.
16. *Butenkov S., Zhukov A., Nagorov A., Krivsha N.* Granular Computing Models and Methods Based on the Spatial Granulation // XII Int. Symposium «Intelligent Systems», INTELS'16, 5-7 October 2016, Moscow, Russia. Elsevier Procedia Computer Science. – 2017. – Vol. 103. – P. 295-302.
17. *Yao Y.Y.* Granular computing: basic issues and possible solutions // Proceedings of the 5th Joint Conference on Information Sciences. – 2000. – P. 186-189.
18. *Pedrysz W.* Granular Computing – the emerging paradigm // Journal of Uncertain Systems. – 2007. – Vol. 1, No. 1. – P. 38-61.
19. *Бутенков С.А., Кривша В.В., Кривша Н.С., Семененко А.В.* Математические основы гранулирующего подхода к моделированию процессов обработки данных на супервычислительных системах // Матер. Первой Всероссийской конференции «Актуальные проблемы математики и информационных технологий», Махачкала, 3–5 февраля 2020 г. – Махачкала: Изд-во ДГУ, 2020. – С. 54-58.
20. *Бутенков С.А., Кривша Н.С., Кривша В.В*. Численные методы и математические модели гранулированных вычислений // Матер. XXII Международной научно-практической конференции "Academic Science – Problems and Achievements", North Charleston, USA, February 17–18, 2020. – Lulu Press, Inc., 627 Davis Drive, Suite 300, Morrisville, NC, USA, 27560. – P. 49-51.
21. *Бутенков С.А.* Методы информационной грануляции в параллельных вычислениях // Матер. 3-й Всероссийской научно-технической конференции «СКТ-2014», 29 сентября-4 октября 2014 г., Дивноморское, Геленджик. – Т. 1. – С. 99-104.
22. *Бутенков С.А., Нагоров А.Л., Бесланеев З.О., Хатунцев В.Н.* Геометрический подход к оценке квадратурных формул на гранулированных моделях // Известия Кабардино-Балкарского Государственного университета. – 2014. – Т. IV, № 2. – С. 17-22.

REFERENCES

1. *Sobol' I.M.* Mnogomernye kvadraturnye formuly i funktsii Khaara [Multivariable quadrature formulas and Haar functions]. Moscow: Nauka, 1969, 288 p.
2. *Zaliznyak V.E.* Osnovy nauchnykh vychisleniy: Vvedenie v chislennye metody dlya fizikov [Basics of Scientific Computing: Introduction to Numerical methods for the Physicists]. Moscow: Editorial URSS, 2002, 378 p.
3. *Samarskiy A.A., Mikhaylov A.P.* Matematicheskoe modelirovanie: Idei. Metody. Primery [Mathematical Modelling: Basic issues, Techniques, Examples]. 2nd ed. Moscow: Fizmatlit, 2001, 320 p.
4. *Butenkov S.A. Krivsha N.S., Krivsha V.V.* Sovremennye protsedury analiza mnogomernykh dannykh [The Contemporary Techniques of Multivariable Data Analysis], *Sovremennoe sostoyanie estestvennykh i tekhnicheskikh nauk* [Contemporary issues of Natural and Technical Sciences], 2015, Issue XIX, pp. 75-76.
5. *Rogozov Yu.I., Butenkov S.A., Nagorov A.L., Beslaneev Z.O.* Modeli dannykh na osnove teorii informatsionnoy granulyatsii [Data models based on Information Granulation Theory], *Cb. trudov Pyatoy Mezhdunarodnoy konferentsii «Sistemnyy analiz i informatsionnye tekhnologii» SAIT-2013, Krasnoyarsk, 19-25 sentyabrya 2013 g.* [System Analysis and Information Technologies» SAIT-2013, Krasnoyarsk, September 19-25, 2013], Vol. 2, pp. 395-398.
6. *Butenkov S.A., Nagorov A.L., Beslaneev Z.O.* Geometricheskiy podkhod k postroeniyu modeley dannykh na osnove teorii granulyatsii [Basics of geometrical approach to the granulated data models], *Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of Dagestan State Technical University], 2014, No. 1. Vol. 32, pp. 47-55.
7. Barskiy A.B. Parallel'nye protsessy v vychislitel'nykh sistemakh. Planirovanie i organizatsiya [The Parallel Computational Processes: Scheduling and Organization]. Moscow: Radio i svyaz', 1990, 256 p.
8. Butenkov S.A. Strukturnaya organizatsiya granulirovannykh vychisleniy pri obrabotke dannykh na rekonfiguriruemykh vychislitel'nykh sistemakh [The structure of granular computing units for the data processing on the configurable computers], *Izvestiya YuFU: Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2018, No. 8 (202), pp. 250-262.
9. *Kalyaev I.A., Levin I.I., Semernikov E.A., Shmoylov V.I.* Rekonfiguriruemye mul'tikonveyernye vychislitel'nye struktury [Configurable multi-conveyer computing structures]. Rostov-on-Don: Izd.-vo YuNTS RAN, 2009, 344 p.
10. *Butenkov S., Zhukov A., Nagorov A., Krivsha N.* Granular Computing Models and Methods Based on the Spatial Granulation, *XII Int. Symposium «Intelligent Systems», INTELS'16, 5-7 October 2016, Moscow, Russia. Elsevier Procedia Computer Science*, 2017, Vol. 103, pp. 295-302.
11. *Butenkov S.A.* Vysokoproizvoditel'nye tekhnicheskie sredstva i metody dlya rekonfiguriruemykh vychislitel'nykh sistem v optiko-elektronnykh sistemakh obrabotki dannykh [High performance devices and techniques for the reconfigurable computers in optical data processing systems], *Mater. V Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Aktual'nye voprosy issledovaniy v avionike: teoriya, obsluzhivanie, razrabotki» – «AVIATOR», 15-16 fevralya 2018 g., VUNTS VVS «VVA im. prof. N.E. Zhukovskogo i Yu.A. Gagarina» (g. Voronezh)* [In Proc. of V International Conference «Topical Questions of Investigations in Avionics: Theory, Design and Maintenance» – «AVIATOR», February 15-16, 2018, Air Force Academy named after N.E. Zhukovskij and Y.A. Gagarin (Voroneg, Russia)], pp. 112-114.
12. *Levin I.I., Dordopulo A.I., Gudkov V.A.* Programmirovanie rekonfiguriruemykh vy-chislitel'nykh uzlov na yazyke COLAMO: ucheb. posobie [Programming for the Reconfigurable Computers on COLAMO language: the Tutoruial]. Rostov-on-Don: Izd-vo YuFU, 2016, 114 p.
13. *Butenkov S.A., Semernikov E.A.* Optimizatsiya proektirovaniya vychislitel'nykh sistem real'nogo vremeni na osnove modeley massovogo obsluzhivaniya [Real-Time Computers Optimization Based on the Queuing Theory Models], *Mater. Tret'ey Vse-rossiyskoy nauchno-tekhnicheskoy konferentsii "Superkomp'yuternye tekhnologii" (SKT-2014), Gelendzhik, 29 sentyabrya – 4 oktyabrya 2014 g.* [In Proc. of III All-Russian Scientific Conference "Supercomputing Techniques " (SCT-2014), Gelendgik, September 29 – October 4, 2014]. Rostov-on-Don: Izd-vo YuFU, 2014, Vol. 1, pp. 30-35.

14. *Butenkov S.A., Zhukov A.L.* Informatsionnaya granulyatsiya na osnove izomorfizma algebraicheskikh sistem [Information granulation based on the algebraic systems isomorphism], *Sb. trudov Mezhdunarodnoy algebraicheskoy konferentsii, posvyashchennoy 80-letiyu so dnya rozhdeniya A.I. Kostrikina, Nal'chik, 12-18 iyulya 2009 g*. [Proc. of Annual international algebraic conf. dedicated to A.I. Kostrikin jubilee, Nalchik, July 12-18, 2009], pp. 206-209.
15. *Butenkov S.A.* Granulyatsiya i inkapsulyatsiya v sistemakh effektivnoy obrabotki mnogomernoy informatsii [Multivariable Data Processing by the Granulation and Encapsulation], *Iskusstvennyy intellect* [Artificial Intelligence], 2005, No. 4, pp. 106-115.
16. *Butenkov S., Zhukov A., Nagorov A., Krivsha N.* Granular Computing Models and Methods Based on the Spatial Granulation, *XII Int. Symposium «Intelligent Systems», INTELS'16, 5-7 October 2016, Moscow, Russia. Elsevier Procedia Computer Science*, 2017, Vol. 103, pp. 295-302.
17. *Yao Y.Y.* Granular computing: basic issues and possible solutions, *Proceedings of the 5th Joint Conference on Information Sciences*, 2000, pp. 186-189.
18. *Pedrysz W.* Granular Computing – the emerging paradigm, *Journal of Uncertain Systems*, 2007, Vol. 1, No. 1, pp. 38-61.
19. *Butenkov S.A., Krivsha V.V., Krivsha N.S., Semenenko A.V*. Matematicheskie osnovy granuliruyushchego podkhoda k modelirovaniyu protsessov obrabotki dannykh na supervychislitel'nykh sistemakh [Mathematical Issues of Granulated Data Models for the Supercomputing Processing], *Mater. Pervoy Vserossiyskoy konferentsii «Aktual'nye problemy matematiki i informatsionnykh tekhnologiy», Makhachkala, 3–5 fevralya 2020 g.* [In Proc. of I All-Russian Conference «Topic Problems of Mathematics and Information Technologies», Mahachkala, February 3–5, 2020]. Makhachkala: Izd-vo DGU, 2020, pp. 54-58.
20. *Butenkov S.A., Krivsha N.S., Krivsha V.V.* Chislennye metody i matematicheskie modeli granulirovannykh vychisleniy [Numerical method and models of granular computing], *Mater. XXII Mezhdunarodnoy nauchno-prakticheskoy konferentsii "Academic Science – Problems and Achievements", North Charleston, USA, February 17–18, 2020* [Proc. of XXII International conf. "Academic Science – Problems and Achievements", North Charleston, USA, February 17–18, 2020]. Lulu Press, Inc., 627 Davis Drive, Suite 300, Morrisville, NC, USA, 27560, pp. 49-51.
21. *Butenkov S.A.* Metody informatsionnoy granulyatsii v parallel'nykh vychisleniyakh [Information granulation approach for the parallel computers], *Mater. 3-y Vserossiyskoy nauchno-tekhnicheskoy konferentsii «SKT-2014», 29 sentyabrya-4 oktyabrya 2014 g., Divnomorskoe, Gelendzhik* [Proc. of 3-rd All-Russian Conference «SCT-2014», September 29 – October 4, 2014 г., Gelendgik], Vol. 1, pp. 99-104.
22. *Butenkov S.A., Nagorov A.L., Beslaneev Z.O., Khatuntsev V.N.* Geometricheskiy podkhod k otsenke kvadraturnykh formul na granulirovannykh modelyakh [Geometrical Approach to the Quadrature Formulas over the Granulated Data Evaluation], *Izvestiya Kabardino-Balkarskogo Gosudarstvennogo universiteta* [Bulletin of Kabardino-Balkarian State University], 2014, Vol. IV, No. 2, pp. 17-22.

Статью рекомендовал к опубликованию д.ф.-м.н. Г.В. Куповых.

Кривша Наталья Сергеевна – Южный федеральный университет; e-mail: natalie-home@yandex.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: +79185456456; к.т.н.; доцент.

Кривша Виталий Вадимирович – Научно-исследовательский центр супер-ЭВМ и нейрокомпьютеров; e-mail: kvit_ok@mail.ru; г. Таганрог, Итальянский пер., 106; тел.: +79281339489; вед. программист; к.т.н.

Бутенков Сергей Андреевич – e-mail: saabmount@gmail.com; тел.: +79281420088; с.н.с.; к.т.н., доцент.

Krivsha Natalya Sergeevna – Southern Federal University; e-mail: natalie-home@yandex.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +79185456456; cand. of eng; sc.; associate professor.

Krivsha Vitalij Vladimirovich – Supercomputers and Neurocomputers Research Center; e-mail: kvit_ok@mail.ru; Ital'yanskiy, 106, Taganrog, Russia; phone: +79281339489; senior programmer; cand. of eng. sc.

Butenkov Sergey Andreevich – e-mail: saabmount@gmail.com; phone: +79281420088; senior researcher; cand. of eng. sc.; associate professor.

УДК 53.04 DOI 10.18522/2311-3103-2020-5-86-100

А.А. Курносов

ЭФФЕКТЫ НЕЛИНЕЙНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ МОРСКИХ ТЕХНОГЕННЫХ ОБЪЕКТОВ

Применительно к взаимодействию сложных систем рассматриваются вопросы мониторинга информационной обстановки, типы информационных взаимодействий и топологический подход к учёту многосредного взаимодействия сложных систем в подводной среде. Приведена классификация основных эффектов, возникающих при информационном взаимодействии морских техногенных объектов. Выделены три основные группы эффектов, связанные с физикой сред, с особенностями распространения энергии в этих средах и с особенностями собственно взаимодействия двух и более объектов. Приведена схема кластеризации эффектов – неопределённость, несовместимость, нелинейность, релятивистские эффекты, эффекты на границах сред. Внутри указанных кластеров в статье рассмотрены эффекты: роста интенсивности информационного обмена, появления непрогнозируемых новых связей, каузальной несовместимости, антиподов, бликов, подсветок, релятивистские эффекты. Показано, что существуют определенные различия в информационном взаимодействии объектов, находящихся в средах с разными скоростями взаимодействия и диссипацией энергии взаимодействия. Эти различия проявляются в росте интенсивности обмена в плотных средах на некоторых расстояниях «близости». При этом наблюдается появление непрогнозируемых причинно-следственных связей. В ходе обмена информацией в этих областях сингулярности, помимо эффектов, обусловленных особенностями распространения сигналов в воде, наблюдаются эффекты, связанные именно с информационным взаимодействием двух и более объектов. Отмечено, что практически все эффекты способны приводить к существенному искажению воспринимаемой объектами информации и к нарушению процесса принятия решений. Наибольшим катастрофическим потенциалом обладают эффекты несовместимости. При высоких скоростях движения морских техногенных объектов для отдельных наблюдателей возможно нарушение причинности. Показана схема нарушения причинности при взаимодействии объектов, связанная с потерями информации двух типов – релятивистского (за счёт превышения скорости перемещения объектов над скоростью взаимодействия в среде) и геометрического (за счёт выхода «быстрого» объекта из области «медленного» распространения импульса). Сделан вывод о необходимости проведения физического имитационного моделирования с использованием высокопроизводительных систем и современных математических методов на единой критериальной базе.

Сложные системы; неэргодичность; совместимость; взаимодействие; неопределённость; антиподы; блики; подсветки; фактор Лоренца; причинность; физическое имитационное моделирование.

A.A. Kurnosov

EFFECTS OF NONLINEAR INFORMATION INTERACTION OF MARINE TECHNOGENIC OBJECTS

With regard to the interaction of complex systems, the issues of monitoring the information situation, the types of information interactions and the topological approach to taking into account the multimedia interaction of complex systems in the underwater environment are considered. The classification of the main effects arising from information interaction of marine technogenic objects is given. Three main groups of effects associated with the physics of media, with the features of the propagation of energy in these media and with the features of the actual interaction of two or more objects are distinguished. The scheme of clustering of effects is given: uncertainty, incompatibility, nonlinearity, relativistic effects, effects on the boundaries of media. Within these clusters, the article considers the following effects: an increase in the intensity of information exchange, the emergence of unpredictable new connections, causal incompatibility, antipodes, glare, backlights, relativistic effects. It is shown that there are certain differences in the information interaction of objects in media with different interaction rates and dissipation of interaction energy. These differences are manifested in an increase in the intensity of exchange in dense media at some "proximity" distances. In this

case, the emergence of unpredictable causal relationships is observed. During the exchange of information in these regions of the singularity, in addition to the effects caused by the peculiarities of the propagation of signals in water, the effects associated precisely with the information interaction of two or more objects are observed. It is noted that almost all effects can lead to a significant distortion of the information perceived by objects and to a violation of the decision-making process. Incompatibility effects have the greatest catastrophic potential. At high speeds of movement of marine technogenic objects for individual observers, a violation of causality is possible. The scheme of violation of causality in the interaction of objects is shown, associated with the loss of information of two types – relativistic (due to the excess of the speed of movement of objects over the speed of interaction in the medium) and geometric (due to the exit of a "fast" object from the region of "slow" pulse propagation). It is concluded that it is necessary to carry out physical simulation using high-performance systems and modern mathematical methods on a single criterion basis.

Complex systems; non-ergodicity; compatibility; interaction; uncertainty; antipodes; glare; highlights; Lorentz factor; causality; physical simulation.

Введение. Наше стремление создавать конкурентоспособные системы, обладающие всё большей эффективностью, неизбежно ведёт к усложнению создаваемых систем и процессов взаимодействия составляющих компонент. Мы выделяем следующие определяющие характеристики таких систем – сложные неравновесные неэргодические рефлексивные открытые активные многоцелевые системы с динамической структурой, взаимодействующие во множестве трансформируемых сред.

Управление такими, лишь частично совместимыми системами возможно, однако, требует максимально полного учёта физических и информационных аспектов взаимодействия.

Мониторинг полей и сигналов. Учёт физических и информационных аспектов взаимодействия морских техногенных объектов требует создания механизма мониторинга эффективного динамического информационного поля вокруг объектов, с учётом диссипации энергии в среде, квантования по Котельникову-Найквисту, эффектов Допплера, фазовых сдвигов и задержек распространения сигналов, факторов фокусировки энергии, удлинения и бликовой структуры отраженных сигналов , характеристик излучателей и приёмников и т.п. Учёт указанных факторов относится к классу сложнейших научно-технических проблем, реализация механизмов мониторинга, чувствительных к совокупности приведенных эффектов в значимой части спектра, насчитывает в мире единицы успешных реализаций [2]. Одна из таких реализаций разработана в АО «СПМБМ «Малахит», её ядром являются механизмы мониторинга информационной обстановки; схема основных факторов, учитываемых при мониторинге только подводной обстановки представлена на рис. 1.

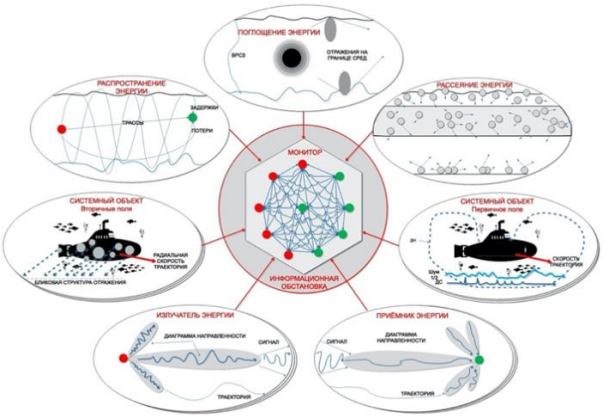

Рис. 1. Факторы, учитываемые при взаимодействии сложных систем в подводной среде (по материалам [1, 2])

Главная сложность при мониторинге информационной обстановки заключается в корректном динамическом учёте факторов изменчивости систем, существующих непрерывно и дискретно в трех измерениях времени – координатном, частотном и структурном.

Типы информационных взаимодействий объектов, учитываемых при мониторинге, на примере трех объектов, размещённых в стратифицированной нелинейной подводной среде показаны на рис. 2.

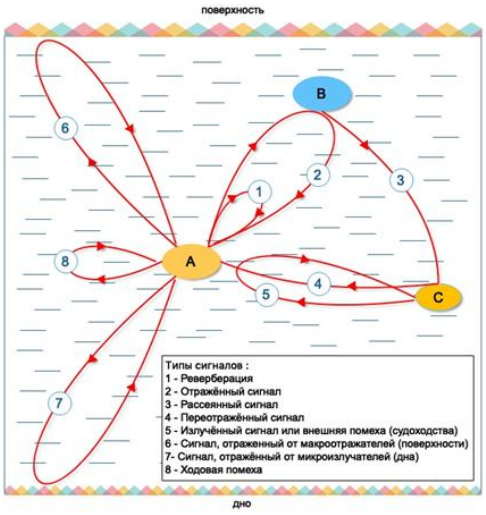

Рис. 2. Типы информационных взаимодействий объектов в одной среде с двумя границами

Более сложные, но аналогичные взаимодействия возникают при реализации многосредных задач. При этом необходимо учитывать, что многосредные системы сами образуют структуры определённой сложности, фактически увеличивающие размерность пространства взаимодействующих объектов за счёт включения в него в качестве таковых границ раздела сред (рис. 3).

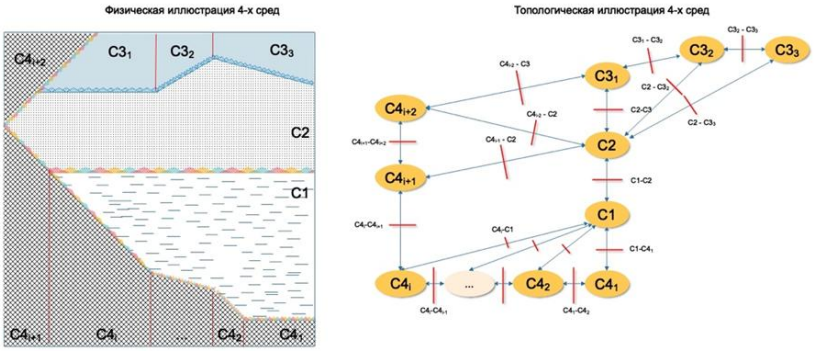

Рис. 3. Иллюстрация сложной топологии многосредных задач

Физические эффекты при информационном взаимодействии. Взаимодействие сложных систем связано с появлением ряда эффектов, обнаруживаемых при мониторинге и требующих обязательного учёта при проектировании сложных систем. К ним относятся в первую очередь эффекты, показанные на рис. 4.

Рис. 4. Основные эффекты при информационном взаимодействии сложных систем

Можно выделить три большие группы эффектов (выделены различными цветами) – связанные с физикой сред (красный цвет), с особенностями распространения энергии в этих средах (синий цвет), а также с особенностями собственно взаимодействия двух и более объектов (чёрный цвет).

Приведенные на рис. 2 основные физические эффекты известны много десятилетий и изучены достаточно хорошо (например, в [3–7]), поэтому их неполный перечень приводится здесь только для лучшего понимания сложности исследуемых процессов взаимодействия, обладающих нелинейной природой.

К рассматриваемым далее эффектам собственно взаимодействия объектов можно отнести эффекты, составляющие 5 подгрупп – неопределённости, несовместимости, релятивистских эффектов и некоторых эффектов, связанных с нелинейностью физических процессов. Все перечисленные эффекты приводят к искажениям помехосигнальной (ПСО) и информационной обстановки (ИО) в той или иной степени влияя на ситуационную осведомлённость.

Неопределённость. Эффекты неопределённости приводят к искажениям ПСО, в первую очередь, за счёт двух взаимосвязанных эффектов – резкого роста интенсивности информационного обмена в определённых ситуациях взаимодействия с высокой «плотностью» процессов взаимодействия – быстротой и необратимостью их протекания, а также непредсказуемого характера появления новых связей. Иллюстрация роста интенсивности информационного обмена, полученного в АО «СПМБМ «Малахит» при проведении имитационного моделирования, приведена на рис. 5.

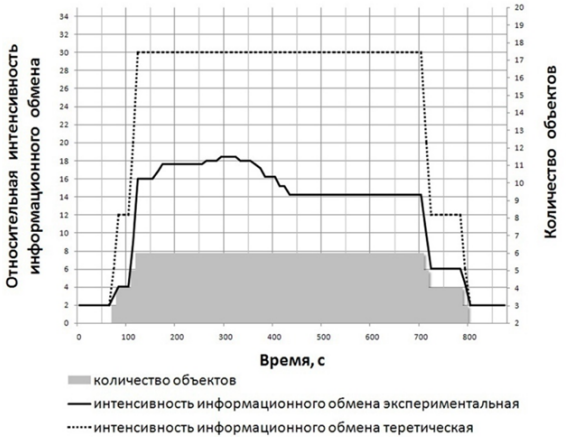

Рис. 5. Изменение интенсивности информационного обмена в зависимости от количества взаимодействующих объектов (диапазон расстояний 0–3 км)

Непредсказуемость появления новых связей обусловлена динамическим характером взаимодействия и различной величиной силы цели в зависимости от углов падения-отражения сигналов. Их предельное количество связано с количеством объектов взаимодействия N зависимостью типа (N^2-N); понятна величина расхождения между ожидаемым количеством связей, обычно ≈ N: так, для 5 объектов и 5-ти ожидаемых связей количество непредсказуемых связей может составить величину порядка 20-ти.

Антиподы. В отдельную подгруппу можно выделить искажения ПСО, вызванные сложным характером формирования отражённых сигналов – так называемые антиподы [8]. Антипод – информационный портрет объекта, полученный при его облучении активными радиолокационными или гидроакустическими сигналами. По существу, радиолокационный/гидроакустический антиподы являются самостоятельными характеристиками информационного портрета корабля.

Эффект появления антиподов связан с физическими особенностями формирования эхосигналов вблизи границ раздела сред; особенность антиподов заключается в том, что уровень сигнала антипода зачастую выше, чем уровень сигнала, отражённого от реального объекта; в зоне прямой видимости величины средней эффективной поверхности рассеяния самого корабля и его антипода одинаковы по порядку величин [10, 11–13]. Распознавание объектов вообще, а морских техногенных объектов – в частности, основывается на анализе их информационных портретов с высоким разрешением по двум координатам. Часть портрета оказывается занята антиподом объекта, так что все процедуры распознавания и определения истинных координат объектов следует проводить с учетом этого фактора.

На рис. 6 приведена схема формирования антипода, а на рис. 7 приведены численные характеристики типового антипода для портрета надводного корабля. Аналогичные эффекты возникают применительно к подводным объектам, находящимся вблизи границ раздела сред.

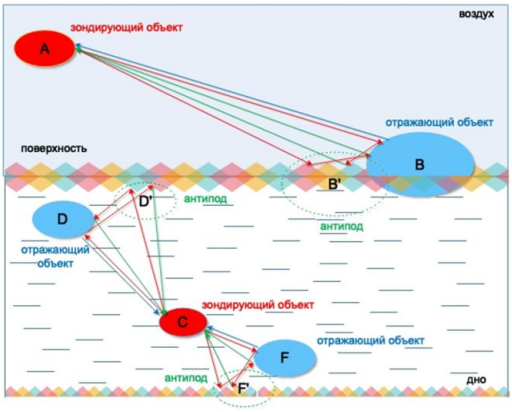

Рис. 6. Схема формирования антиподов у границ раздела сред

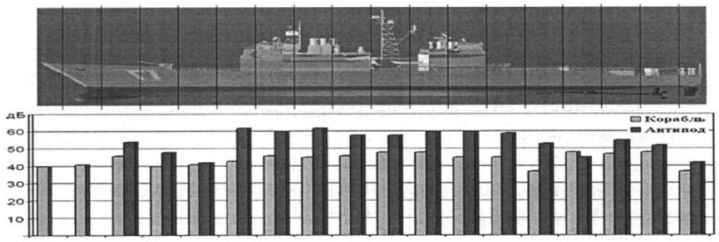

Рис. 7. Гистограммы распределения интенсивности отражений от корабля и его антипода (приводится по данным [8])

Бликовая структура. Этот эффект можно считать очень похожим на эффект антиподов, однако его природа несколько другая. Если появление антиподов связано с наличием границы раздела сред и с тонкими механизмами формирования сигналов, отражающихся квазиодновременно от реального объекта и от границы раздела сред, то появление бликовой структуры в отражённом сигнале связано с различной силой отражений от объекта, неоднородного внутренне.

Обычно модель такого объекта представляют набором n-сфер с эквивалентными радиусами Rn, отстоящими друг от друга на расстояние ln.

Схема формирования отраженного сигнала с бликовой структурой показана на рис. 7; разницу в сигналах, отражённых от подводного объекта с кормового и отличного от кормового и траверзного направлений прихода тонального акустического сигнала иллюстрирует рис. 8 (приводится по данным [9]).

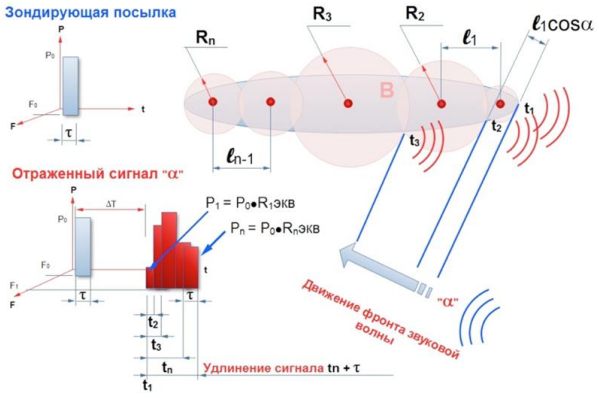

Рис. 8. Схема формирования отражённого сигнала с бликовой структурой

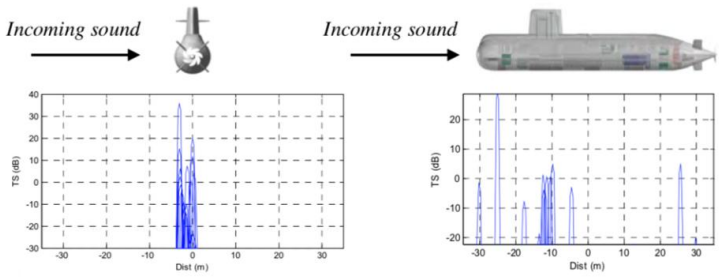

Рис. 9. Иллюстрация сигналов, отраженных подводным объектом с кормового и отличающегося от траверзного направлений (по материалам [9])

Подсветки. Эффект подсветки проявляется в ситуациях взаимодействия как минимум двух, как правило – не менее трех объектов, один из которых является наблюдателем, второй – наблюдаемым, а третий – источником сильных, зачастую ненаправленных сигналов (или помех). В таких случаях наблюдаемые объекты, даже обладающие высокой скрытностью, это качество теряют за счёт отражения сигналов (помех) в сторону объекта-наблюдателя.

Это происходит потому, что энергии сигнала (помех), отражённого от наблюдаемого объекта оказывается достаточно для его подсветки в системах обнаружения объекта-наблюдателя. Иллюстрация схемы подсветки приведена на рис. 10.

Рис. 10. Схема подсветки

Данный эффект может рассматриваться как положительный в задачах поиска скрытных объектов и как отрицательный – в задачах уклонения от обнаружения.

Совместимость. Одним из важнейших следствий взаимодействия является несовместимость систем, вступающих в это взаимодействие, преимущественно информационное; по степени сложности различают атрибутивную, сигнальную и каузальную совместимость. Факторы рискового взаимодействия, приводящие к эффектам несовместимости, составляют 5 групп, показанных на рис. 11.

Эффекты несовместимости носят непредсказуемый динамический характер, близкий по типу к фазовым переходам [14] (рис. 12). В случае проявления системой эмерджентных свойств можно говорить о высокой степени совместимости элементов взаимодействующих систем, вплоть до полной. В случае ухудшения результата (от прогнозируемого) можно говорить о появлении эффектов несовместимости, вплоть до полной. Кроме того, предлагается считать проявления несовместимости свойством, характеризующим именно сложные системы.

Рисунок 12 иллюстрирует изменения состояния системы при переходе из текущего состояния A в желательное состояние C. При отсутствии несовместимости в системе и наличии системы управления с обратной связью, система перейдет в желательное состояние и получит эффект (c-a); при проявлении факторов несовместимости конечный результат может быть непредсказуем и дать один из трех возможных вариантов – «чудесный» F с эффектом (f-a); нежелательный «допустимый» D с ухудшением состояния системы, но в области допустимых состояний (d-a); нежелательный «ужасный» E с резким ухудшением состояния системы за пределами области допустимых состояний (e-a). Координация управления при таком переходе невозможна, неопределённость результата будет расти с ростом количества факторов неопределённости и усложнением системы

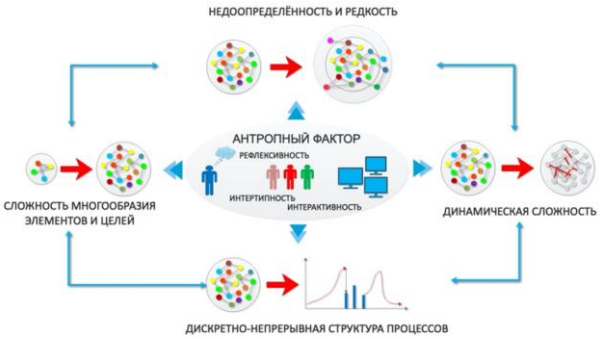

Рис. 11. Факторы рискового взаимодействия сложных систем

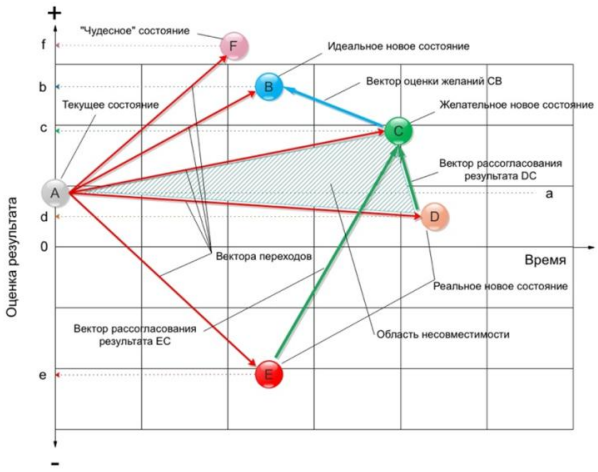

Рис. 12. Характер проявления несовместимости сложных систем

Тем не менее, управление частично совместимыми системами возможно, однако требует максимально полного учёта физических аспектов взаимодействия объектов, образующих сложную систему. Особенно трудоёмкой для исследований и корректировок является каузальная совместимость, требующая высокопроизводительного физического имитационного моделирования динамики каузальных гиперграфов.

Релятивистские эффекты. Специальная теория относительности (СТО) рассматривает ситуации взаимодействия движущихся объектов с сигналами информационного взаимодействия, обладающими постоянной скоростью в среде, которая н е может превышать скорости света. Морские техногенные объекты движутся со скоростями, не превышающими десятков метров в секунду, однако скорость информационного взаимодействия в подводной среде составляет величину порядка $1.5 \times 10^3 \text{м/с}$). То есть в подводной среде, без всяких нарушений положений СТО, возможно перемещение объектов со скоростями, превышающими скорость информационного взаимодействия. Кроме того, объекты других доменов, взаимодействующие с морскими техногенными объектами и движущиеся со скоростями, существенно превышающими скорость звука в воде, по взаимодействию будут связаны именно со скоростью звука в воде (так, например, самолет, получающий информацию о местонахождении подводного объекта от радиогидроакустического буя, реально работает с двухканальной системой, в которой скорость получения информации определяется самым медленным из каналов – гидроакустическим). Таким образом, большое количество объектов, взаимодействующих с морскими техногенными объектами, независимо от их природы, будут привязаны к скорости информационного взаимодействия порядка $1.5 \times 10^3 \text{м/с}$ (см. рис. 13, линии электромагнитного (красным цветом) и гидроакустического (синим цветом) взаимодействия на рис. 13 изображены условно, для того, чтобы подчеркнуть существование различных по скорости и структуре каналов взаимодействия.).

Будем рассматривать три системы координат (СК) в принятой в СТО терминологии «штрихованных» инерциальных систем: неподвижную СК OX; 1-ую подвижную СК OX' (см. рис. 14), связанную непосредственно с движущимся объектом; 2-ую подвижную СК OX'', связанную с излучаемыми гидроакустическими сигналами.

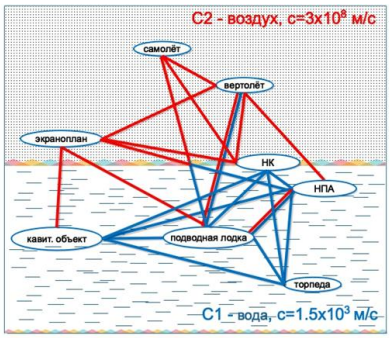

Рис. 13. Взаимодействующие объекты и среды взаимодействия

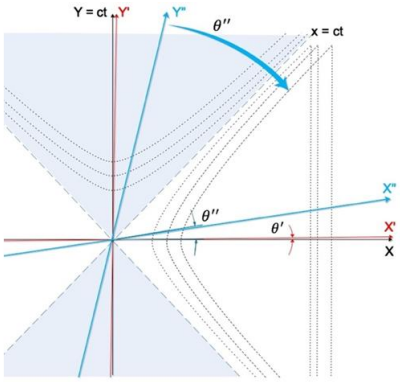

Рис. 14. Системы координат инерциальных систем и гиперболы инварианта Минковского

Рассмотрим следующие скорости некоторых потенциально-взаимодействующих в морской среде объектов [15–22] и соответствующие релятивистские коэффициенты β и γ:

Таблица 1

Скорости объектов и релятивистские коэффициенты

N п/п	Тип объекта	v', м/с	β'	β''	γ'	γ''	θ'	θ''
1	Необитаемый подводный аппарат	3	10^{-8}	$2x10^{-3}$	1	1,000002	$5,73x10^{-7}$	0,12
2	Надводный корабль	15	$5x10^{-8}$	0,01	1	1,00005	$2,86x10^{-6}$	0,57
3	Подводная лодка	20	$6,67x10^{-8}$	0,013	1	1,000084	$3,82x10^{-6}$	0,76
4	Торпеда	30	10^{-7}	0,02	1	1,0002	$5,73\ x10^{-6}$	1,15
5	Вертолёт	75	$2,5x10^{-7}$	0,05	1	1,0012	$1,43\ x10^{-5}$	2,86
6	Экраноплан/ ракетоторпеда / НПА типа «Посейдон»	100	$3,33x10^{-7}$	0,067	1	1,0022	$1,89\ x10^{-5}$	3,81
7	Самолёт	200	$6,66\ x10^{-7}$	0,133	1	1,009	$3,82\ x10^{-5}$	7,41
8	Дозвуковая ракета	300	10^{-6}	0,2	1	1,021	$5,7x10^{-5}$	11.31
9	Суперкавитирующий объект 1	750	$2,5x10^{-6}$	0,5	1	1,155	$1,43\ x10^{-4}$	26,57
10	Сверхзвуковая ракета	900	$3x10^{-6}$	0,6	1	1,25	$1,71x10^{-4}$	30.96
11	Суперкавитирующий объект 2	1500	$5x10^{-6}$	1	1	∞	$2,86\ x10^{-4}$	45

Примечания к табл. 1:

1. Коэффициент $\beta' = \frac{v'}{c}$, где v'– скорость объекта относительно OX, c – скорость электромагнитного взаимодействия в среде C ($c = 3 \times 10^8$), $\beta'' = \frac{v''}{c''}$, где v''– скорость объекта, c'' – скорость гидроакустического взаимодействия в среде C" ($c' = c'' \sim 1.5 \times 10^3$)

2. Лоренц-фактор $\gamma = \frac{1}{\sqrt{1-\beta^2}}$ с индексами, соответствующими индексам β.

3. Углы поворота осей систем координат относительно OX и OX' соответственно: $\theta' = arctg\ \frac{v'}{c}, \theta'' = arctg\ \frac{v''}{c''}$

4. β, γ – соответствуют неподвижной системе координат OX, β', γ' – соответствуют 1-ой подвижной системе координат OX′ (см. рис. 1), связанной непосредственно с движущимся объектом. β'', γ'' – соответствуют 2-ой подвижной системе координат OX″, связанной с излучаемыми объектами гидроакустическими сигналами.

Как и следовало ожидать, между неподвижной OX и подвижной OX′ системами координат релятивистские эффекты практически отсутствуют, сводясь к величинам шестого-седьмого порядков малости; оси систем координат OX и OX′ можно считать взаимно совпадающими (угол $\theta' \sim 0$), поэтому далее можно считать эти оси совпадающими, а под скоростью взаимодействия в среде понимать скорость распространения гидроакустических волн c''.

Однако применительно к осям OX′ и OX″ всё обстоит иначе – поскольку коэффициент β'' для реально взаимодействующих в подводной среде объектов принимает далеко не малые значения; а поворот-сжатие косоугольной системы координат OX″ относительно (OX, OX′) измеряется значительными величинами.

Как следует из СТО [23], в случае, когда β''>1 - инвариант s^2 пространства-времени Минковского, определяемый как $s^2 = c''^2 t^2 - x^2$, принимает отрицательное значение, становясь пространственно-, а не времениподобным. Это ведёт к нарушению причинности, степень которой можно оценивать, например, по значению Лоренц-фактора γ''. При превышении значения β''=1, взаимодействие между объектами становится невозможным в силу превышения объектами скорости звука в воде (области на рис. 14, лежащие за пределами «звукового» конуса).

Причинность же для неподвижного наблюдателя сохраняется, поскольку никакого нарушения положений СТО не происходит – перемещения всех объектов происходит со скоростями, много меньшими скорости света. Но для реальных объектов, взаимодействующих с конечной скоростью взаимодействия c'', и обладающих принципиальной возможностью движения со скоростями, большими, чем скорость взаимодействия, такое нарушение причинности совершенно объяснимо.

Естественно, что большинство реальных взаимодействующих объектов, показанных на рис. 13 и в табл. 1, обладают существенно более низкими скоростями, чем приведенные предельные значения; но даже для них релятивистские эффекты будут достаточно заметны, по крайней мере, несоизмеримо заметнее, чем для типовых моделей, рассматриваемых СТО.

Приведенные простейшие оценки релятивистских искажений, возникающих при взаимодействии относительно быстродвижущихся объектов в подводной среде показывают наличие не ничтожных искажений времён, частот, расстояний и параметров характеристик направленности осцилляторов – фактически, можно считать, что при взаимодействии N объектов возникает (N2-N) «миров», отличающихся указанными параметрами взаимодействия. Если сконцентрировать внимание на проблеме причинности, то можно предположить, что в определённых случаях может иметь место нарушение причинности в связи с «разновремённостью» событий, происходящих в этих «мирах» [24]. Естественно, что нарушение

причинности происходит для конкретного наблюдателя, производящего оценку ситуации; сама сеть отношений между причинно-следственными связями в случае наличия причинно-следственной инвариантности всегда будет одинаковой (если только этот наблюдатель в силу искажённости ситуации для него не изменит саму сеть отношений своими действиями). На рис. 15,а) показан абстрактный причинно-следственный граф как результат событий (синие круги) и процессов (красные стрелки), происходящих в некой системе из N неподвижных объектов (на рисунке не показана); горизонтальные слоения этого графа (красный пунктир) вдоль вертикального направления соответствуют обычному последовательному течению «координатного» времени, все события в одном слое происходят одновременно для всех N-объектов. В случае относительного перемещения объектов (зелёная стрелка) все наблюдатели на объектах испытают индивидуальные последовательности событий, например так, как показано на рис. 15,б). А это значит, что слоение, которое они естественным для себя образом построят, будет отличаться от слоения рис. 15,а,б) – рис. 15,в). Поскольку наблюдателям, перемещающимся по зелёной стрелке, неизвестен «истинный» причинно-следственный граф, то они создадут свои собственные версии, где слоения будут горизонтальными; и чтобы сохранилась основная структура и углы каузального графа, они осуществят скейлинг с масштабным коэффициентом, пропорциональным фактору Лоренца γ – рис. 15,г). Как видно, при этом восприятие наблюдателями последовательности событий становится несколько иным, что не может не оказывать влияния на процесс принятия решения.

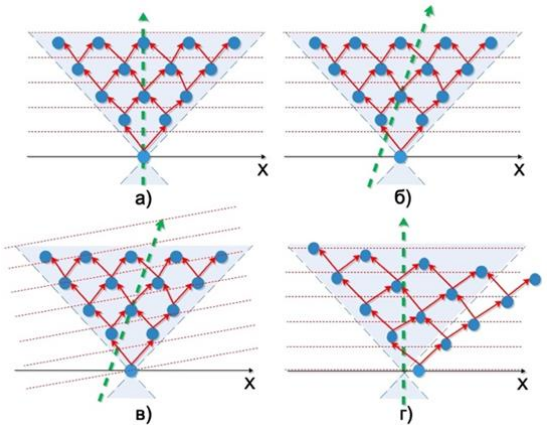

Рис. 15. Схема нарушения причинности за счёт релятивистских эффектов

Несложно показать аналогичным вышеприведенному образом, что для взаимодействующих через подводную среду объектов искажения будут иметь место и для характеристик направленности осцилляторов, продольного и поперечного эффектов Допплера и т.п.

Последний эффект помещён в подраздел релятивистских эффектов постольку, поскольку он тоже связан с понятием relatio (отношения), хотя и рассматривается с позиций Галилеевской механики. Относительно близкие величины скоростей распространения информации и движения морских техногенных объектов приводят при взаимодействии к потере контакта за счёт выхода объекта из зоны локации за время распространения звуковой волны до объекта (такой же эффект имеет место и при отражении сигнала). Также имеют место Допплеровские сдвиги частот за счёт наличия радиальных скоростей взаимного перемещения объектов. Иллюстрация потери контакта приведена на рис. 16.

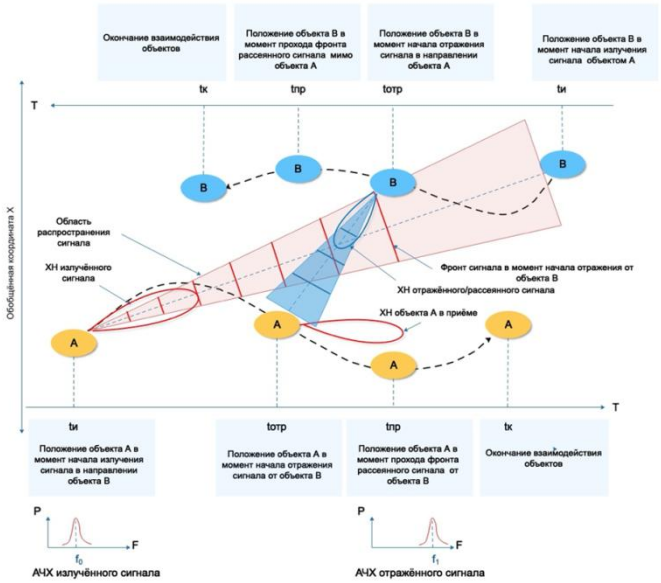

Рис. 16. Информационное взаимодействие двух объектов в подводной среде

Заключение. Существуют определенные различия в информационном взаимодействии объектов, находящихся в средах с разными скоростями взаимодействия и диссипацией энергии взаимодействия. Эти различия проявляются в росте интенсивности обмена в плотных средах на некоторых расстояниях «близости». При этом наблюдается появление непрогнозируемых причинно-следственных связей. В ходе обмена информацией в этих областях сингулярности помимо эффектов, обусловленных особенностями распространения сигналов в воде, наблюдаются эффекты, связанные именно с информационным взаимодействием двух и более объектов.

Необходимо сосредоточиться на проблематике обеспечения управления системами с неполной совместимостью, поскольку именно эффекты несовместимости обладают наибольшим катастрофическим потенциалом.

Существуют искажения ПСО, вызываемые антиподами, бликами и подсветками. А потери информации можно разделить на два типа:

♦ релятивистский – за счёт превышения скорости перемещения объектов над скоростью взаимодействия в среде (в пределах предельной скорости взаимодействия – скорости света);

♦ геометрический – за счёт выхода «быстрого» объекта из области «медленного» распространения импульса.

При высоких скоростях движения морских техногенных объектов для отдельных наблюдателей возможно нарушение причинно-следственных связей.

Практически все эффекты способны приводить к потерям или существенному искажению воспринимаемой объектами информации и к нарушению процесса принятия решений.

Приведенные особенности необходимо учитывать при исследовании процессов информационного взаимодействия объектов в различных средах. Учёт эффектов, возникающих при взаимодействии морских техногенных объектов, представляет собой серьёзную научно-техническую проблему, требующую проведения физического имитационного моделирования с использованием высокопроизводительных систем и современных математических методов на единой критериальной базе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Курносов А.А.* Способ учета каузальной совместимости в сложных технических системах // Сб. трудов 24-й международной конференции «Системный анализ, управление и навигация». – 2019. – С. 109-111.
2. The Sonar Simulation Toolset, Release 4.6: Science, Mathematics, and Algorithms Applied Physic Laboratory University of Washington.
3. *Сташкевич А.П.* Акустика моря. – Л.: Судостроение, 1966. – 350 с.
4. *Урик Р.Дж.* Основы гидроакустики: пер. с англ. / под общ. ред. Е.И. Шендерова. – Л.: Судостроение, 1978. – 448 с.
5. *Румынская И.А.* Основы гидроакустики. – Л.: Судостроение, 1979. – 213 с.
6. *Бреховских Л.М., Годин О.А.* Акустика слоистых сред. – М.: Наука, 1989. – 416 с.
7. *Свердлин Г.М.* Прикладная гидроакустика. – Л.: Судостроение, 1990.
8. *Штагер Е.А*. Радиолокационные антиподы кораблей. – СПб.: ЦНИИ им. А.Н. Крылова, 2011. – 169 с.
9. *Lennart B., Jörgen P. A* fast target strength model and its application with a multipath propagation model // UACE2017 4th Underwater Acoustics Conference and Exhibition. – P. 405-412.
10. *Штагер Е.А.* Отражение радиоволн от кораблей и других морских объектов. – СПб.: ВВМ, 2004. – 418 с.
11. *Штагер Е.А.* Рассеяние радиоволн объектами сложной формы. – М.: Радио и связь, 1986. – 184 с.
12. *Штагер Е.А., Штагер Д.Е.* Область существования эффекта усиления обратного рассеяния волн вблизи шероховатой границы раздела // Радиотехника и электроника. – 1990. – Т. 35, № 2.
13. *Алексеев А.Г., Штагер Е.А., Козырев С.В.* Физические основы технологии Stealth. – СПб.: ВВМ, 2007. – 282 с.
14. *Дорофеев В.Ю., Курносов А.А., Лопота А.В., Половко С.А.* Глобальные цели, принципы проектирования, механизмы взаимодействия, дестабилизирующие эффекты и рациональная организация разработки RIC-систем // Известия ЮФУ. Технические науки. 2019. – № 1 (203). – С. 85-98.
15. Интернет ресурс: https://ru.wikipedia.org/wiki/%D0%A1 %D1%83% D0%BF% D0%B5%D1%80%D0%BA%D0%B0%D0%B2%D0%B8%D1%82%D0%B0% D1%86% D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%82% D0%BE%D1%80% D0%BF%D0%B5%D0%B4%D0%B0_%D1%84%D0%B8% D1%80%D0%BC%D1%8B_ Diehl_BGT_Defence (дата обращения: 08.07.2020).
16. Интернет ресурс: https://wiki.wargaming.net/ru/Navy:%D0%A2%D0%BE% D1%80%D0% BF%D0%B5%D0%B4%D1%8B_%D0%A0%D0%BE%D1%81% D1%81%D0%B8%D0% B8_%D0%B8_%D0%A1%D0%A1%D0%A1%D0%A0 (дата обращения: 08.07.2020).
17. Интернет ресурс: http://brahmos.com/ru-content.php?id=10&sid=10 (дата обращения; 14.07.2020).
18. Интернет ресурс: https://ru.wikipedia.org/wiki/%D0%9E%D0%BD% D0%B8% D0%BA% D1%81%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2%D0%BE%D0%BA%D0 %BE%D1%80%D0%B0%D0%B1%D0%B5%D0%BB% D1%8C% D0%BD%D0%B0% D1%8F_%D1%80%D0%B0%D0%BA%D0%B5% D1%82%D0%B0) (дата обращения: 14.07.2020).
19. Интернет ресурс: https://ru.wikipedia.org/wiki/%D0%9B% D1%83%D0%BD%D1%8C_%D1% 8D%D0%BA%D1%80%D0%B0%D0%BD% D0%BE%D0%BF%D0%BB%D0%B0%D0%BD) (дата обращения: 14.07.2020).
20. *Шахиджанов Е.С., Суслов Ю.В.* Скоростные подводные ракеты подводных лодок // Сб. «Роль российской науки в создании отечественного подводного флота». – М.: Наука, 2007.
21. Интернет ресурс: https://rg.ru/2019/03/19/posejdon-smogut-ispolzovat-dlia-glubinnogo-issledovaniia-mirovogo-okeana.html) (дата обращения: 14.07.2020).
22. Интернет ресурс: https://www.scmp.com/news/china/article/1580226/shanghai-san-francisco-100-minutes-chinese-supersonic-submarine.
23. *Мандельштам Л.И.* Лекции по оптике, теории относительности и квантовой механике. – М.: Наука, 1972. – 440 с.
24. *Вольфрам С.* Путь к фундаментальной теории физики. – https://writings.stephenwolfram.com/2020/04/finally-we-may-have-a-path-to-the-fundamental-theory-of-physics-and-its-beautiful/ (дата обращения: 18.08.2020).

REFERENCES

1. *Kurnosov A.A.* Sposob ucheta kauzal'noy sovmestimosti v slozhnykh tekhnicheskikh sistemakh [Method of accounting for causal compatibility in complex technical systems], *Sb. trudov 24-y mezhdunarodnoy konferentsii «Sistemnyy analiz, upravlenie i navigatsiya»* [Collection of works of the 24th international conference "System analysis, control and navigation"], 2019, pp. 109-111.
2. The Sonar Simulation Toolset, Release 4.6: Science, Mathematics, and Algorithms Applied Physic Laboratory University of Washington.
3. *Stashkevich A.P.* Akustika moray [Acoustics of the sea]. Leningrad: Sudostroenie, 1966, 350 p.
4. *Urik R.Dzh.* Osnovy gidroakustiki [Basics of hydroacoustics]: trans. from English, under the general ed. E.I. Shenderova. Leningrad: Sudostroenie, 1978, 448 p.
5. *Rumynskaya I.A.* Osnovy gidroakustiki [Fundamentals of hydroacoustics]. Leningrad: Sudostroenie, 1979, 213 p.
6. *Brekhovskikh L.M., Godin O.A.* Akustika sloistykh sred [Acoustics of layered media]. Moscow: Nauka, 1989, 416 p.
7. *Sverdlin G.M.* Prikladnaya gidroakustika [Applied hydroacoustics]. Leningrad: Sudostroenie, 1990.
8. *Shtager E.A.* Radiolokatsionnye antipody korabley [Radar antipodes of ships]. Saint Petersburg: TSNII im. A.N. Krylova, 2011, 169 p.
9. *Lennart B., Jörgen P. A* fast target strength model and its application with a multipath propagation model, *UACE2017 4th Underwater Acoustics Conference and Exhibition,* pp. 405-412.
10. *Shtager E.A.* Otrazhenie radiovoln ot korableĭ i drugikh morskikh ob"ektov [Reflection of radio waves from ships and other marine objects].]. Saint Petersburg: VVM, 2004, 418 p.
11. *Shtager E.A.* Rasseyanie radiovoln ob"ektami slozhnoў formy [Scattering of radio waves by objects of complex shape]. Moscow: Radio i svyaz', 1986, 184 p.
12. *Shtager E.A., Shtager D.E.* Oblast' sushchestvovaniya effekta usileniya obratnogo ras-seyaniya voln vblizi sherokhovatoў granitsy razdela [The region of existence of the *effect of amplification of backscattering of waves near a rough interface], Radiotekhnika* i elektronika [Radio engineering and electronics], 1990, Vol. 35, No. 2.
13. *Alekseev A.G., Shtager E.A., Kozyrev S.V.* Fizicheskie osnovy tekhnologii Stealth [Physical bases of Stealth technology]. Saint Petersburg: VVM, 2007, 282 p.
14. *Dorofeev V.Yu., Kurnosov A.A., Lopota A.V., Polovko S.A.* Global'nye tseli, printsipy proektirovaniya, mekhanizmy vzaimodeystviya, destabiliziruyushchie effekty i ratsional'naya organizatsiya razrabotki RIC-sistem [Global aims, design principles, interaction mechanisms, destabilizing effects and rational organization of ric-system development], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2019, No. 1 (203), pp. 85-98.
15. Available at: https://ru.wikipedia.org/wiki/%D0%A1 %D1%83% D0%BF%D0%B5%D1%80%D0%BA%D0%B0%D0%B2%D0%B8%D1%82%D0%B0% D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%82% D0%BE%D1%80%D0%BF%D0%B5%D0%B4%D0%B0_%D1%84%D0%B8% D1%80%D0%BC%D1%8B_Diehl_BGT_ Defence (accessed 08 July 2020).
16. Available at: https://wiki.wargaming.net/ru/Navy:%D0%A2%D0%BE%D1%80%D0%BF%D0%B5%D0%B4%D1%8B_%D0%A0%D0%BE%D1%81% D1%81%D0%B8%D0%B8_%D0%B8_%D0%A1%D0%A1%D0%A1%D0%A0 (accessed 08 July 2020).
17. Available at: http://brahmos.com/ru-content.php?id=10&sid=10 (accessed 14 July 2020).
18. Available at: https://ru.wikipedia.org/wiki/%D0%9E%D0%BD% D0%B8% D0%BA%D1%81%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2%D0%BE%D0%BA%D0%BE%D1%80%D0%B0%D0%B1%D0%B5%D0%BB% D1%8C%D0%BD%D0%B0%D1%8F_%D1%80%D0%B0%D0%BA%D0%B5% D1%82%D0%B0) (accessed 14 July 2020).
19. Available at: https://ru.wikipedia.org/wiki/%D0%9B% D1%83%D0%BD% D1%8C_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD% D0%BE%D0%BF%D0% BB%D0%B0%D0%BD) (accessed 14 July 2020).
20. *Shakhidzhanov E.S., Suslov Yu.V.* Skorostnye podvodnye rakety podvodnykh lodok [High-speed submarine missiles], *Sb. «Rol' rossiyskoy nauki v sozdanii otechestvennogo podvodnogo flota»* [Collection "The role of Russian science in the creation of the domestic submarine fleet"]. Moscow: Nauka, 2007.

21. Available at: https://rg.ru/2019/03/19/posejdon-smogut-ispolzovat-dlia-glubinnogoissledovaniia-mirovogo-okeana.html) (accessed 14 July 2020).
22. Available at: https://www.scmp.com/news/china/article/1580226/shanghai-san-francisco-100-minutes-chinese-supersonic-submarine.
23. *Mandel'shtam L.I.* Lektsii po optike, teorii otnositel'nosti i kvantovoy mekhanike [Lectures on optics, theory of relativity and quantum mechanics]. Moscow: Nauka, 1972, 440 p.
24. *Vol'fram S.* Put' k fundamental'noy teorii fiziki [The Path to the Fundamental Theory of Physics]. Available at: https://writings.stephenwolfram.com/2020/04/finally-we-may-have-a-path-to-the-fundamental-theory-of-physics-and-its-beautiful/ (accessed 18 August 2020).

Статью рекомендовал к опубликованию к.т.н. С.А. Матвеев.

Курносов Андрей Алексеевич – АО «СПМБМ «Малахит», АО ОСК; e-mail: ajkur@mail.ru; 196135, Санкт-Петербург, ул. Фрунзе, 18; тел.: +78122421538; к.т.н.; зам. главного конструктора специализации.

Kurnosov Andrey Alexeevich – SPMDB "Malachite", USBC JSC; e-mail: ajkur@mail.ru; 18 Frunze str., Saint-Petersburg, 196135, Russia; phone: +78122421538; cand. of eng. sc.; deputy chief designer.

УДК 004.9:004.8 DOI 10.18522/2311-3103-2020-5-100-110

Д.М. Елькин, В.В. Вяткин

ПОДХОД К УПРАВЛЕНИЮ ТРАНСПОРТНЫМИ ПОТОКАМИ НА ОСНОВЕ СТАНДАРТА МЭК 61499*

Количество транспортных средств на дорогах общего пользования постоянно увеличивается, а развитие дорожной инфраструктуры происходит низкими темпами, а не качественное управление транспортом влечет за собой повышение стоимости перевозок, увеличение аварийности, уровня шума, а также загрязнение окружающей среды. Вследствие этого, возникает необходимость применения передовых алгоритмов и подходов к управлению транспортом, чтобы максимально использовать существующую дорожную сеть и увеличить пропускную способность дорог. В ходе последних исследований выявлено, что на участках дорожной сети с высокой интенсивностью и изменчивостью трафика, наиболее эффективны адаптивные подходы к управлению дорожным движением. Суть применяемых на сегодняшний день подходов к адаптивному управлению заключается в том что,они основаны на анализе транспортной загруженности и изменяют фазы работы светофора в зависимости от полученных данных в режиме реального времени.. Адаптивное управление транспортными потоками показывает намного более лучшие результаты по сравнению с жестким управлением, существенно уменьшает транспортные задержки, время в пути и выбросы вредных веществ в атмосферу, поэтому современные исследователи разрабатывают новые и усовершенствуют существующие подходы и алгоритмы адаптивного управления транспортом. Например, активно развиваются подходы к управлению трафиком, основанные на концепции IoT и использовании облачных вычислений. Так же разрабатываются концепции применения агентного подхода к адаптивному управлению. В работе предлагается способ управления транспортными потоками и автоматизации дорожной инфраструктуры с использованием агентного подхода. Предлагаемый подход включает распределенное управление различными элементами дорожной сети и их прямую взаимосвязь друг с другом. Для реализации этой концепции был использован открытый стандарт распределенных систем управления и автоматизации МЭК 61499, а для проверки возможности реализации использованы несколько моделей транспортных пересечений, одно из которых создано на основе реальных данных и SUMO - пакет микроскопического и непрерывного моделирования дорожного движения.

IoT; управление дорожным движением; интеллектуальные транспортные системы; ИТС; транспортные потоки; транспортные заторы.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90102.

D.M. Elkin, V.V. Vyatkin

APPROACH TO TRAFFIC MANAGEMENT BASED ON THE IEC 61499 STANDARD

The number of vehicles on public roads is constantly increasing, and the development of road infrastructure is proceeding at a slow pace, and not high-quality transport management entails an increase in transportation costs, an increase in accidents, noise levels, and environmental pollution. As a consequence, there is a need to apply advanced algorithms and approaches to transport management in order to maximize the use of the existing road network and increase road capacity. In the course of recent studies, it has been revealed that adaptive approaches to traffic management are most effective on sections of the road network with high traffic intensity and variability. The essence of the approaches to adaptive management used today is that they are based on the analysis of traffic congestion and change the phases of traffic light operation depending on the received data in real time .. Adaptive traffic management shows much better results compared to tight control , significantly reduces transport delays, travel time and emissions of harmful substances into the atmosphere, therefore, modern researchers are developing new and improving existing approaches and algorithms for adaptive transport control. For example, traffic management approaches based on the concept of IoT and the use of cloud computing are actively developing. The concepts of applying the agent-based approach to adaptive control are also being developed. The paper proposes a method for managing traffic flows and automating road infrastructure using an agent-based approach. The proposed approach includes distributed management of various elements of the road network and their direct interconnection with each other. To implement this concept, the open standard of distributed control and automation systems IEC 61499 was used, and to test the feasibility of implementation, several models of traffic intersections were used, one of which was created on the basis of real data and SUMO - a microscopic and continuous traffic simulation package.

IoT; traffic management; intelligent transportation system; ITS; traffic; traffic jam.

Введение. На сегодняшний день существует несколько различных подходов к управлению транспортными потоками в условиях высокой загруженности и для повышения безопасности дорожного движения. Например, для управления движением на перекрестках, наиболее часто применяется жесткое светофорное управление [1].

Чтобы увеличить эффективность такого управления, период сигналов светофора изменяют в зависимости от времени суток [2]. Так же, для увеличения пропускной способности дороги применяется подход «Зеленой волны», в этом подходе для различных перекрестков расположенных рядом рассчитывается фазовый сдвиг в работе светофоров [3]. Рассмотренные подходы эффективны, когда движение транспортных потоков предсказуемо и теряет свою эффективность, когда трафик резко изменяется [4]. На участках дорожной сети с высокой интенсивностью и изменчивостью трафика, наиболее эффективны адаптивные подходы к управлению движением [5–7]. Подходы к адаптивному управлению основаны на анализе транспортной загруженности и изменения фаз работы светофора в зависимости от неё. Адаптивное управление транспортными потоками показывает намного более лучшие результаты по сравнению с жестким управлением, существенно уменьшает транспортные задержки, время в пути и выбросы вредных веществ в атмосферу [8], поэтому современные исследователи разрабатывают новые и усовершенствуют существующие подходы и алгоритмы адаптивного управления дорожным движением.

Например, активно развиваются подходы к адаптивному управлению трафиком, основанные на концепции IoT [9–11] и использовании облачных вычислений [12]. Так же разрабатываются концепции применения агентного подхода к адаптивному управлению [13–15]. Согласно проведенному обзору разрабатываемых решений по адаптивному управлению транспортом основные проблемы заключаются в сложности разработки и внедрения новых подходов для существующей дорожной инфраструктуры. Эти факторы увеличивают стоимость внедрения новых подходов, а также период от публикации предлагаемого подхода до тестирования и непосредственного применения.

Для решения обозначенных проблем предлагается подход к адаптивному управлению дорожным движением с помощью автоматизации дорожной инфраструктуры. Предлагаемый подход основан на управлении интеллектуальными устройствами на перекрестках и участках дорожной сети (светофоры, сенсоры, детекторы, знаки и т.д.). Все эти устройства являются элементами дорожной инфраструктуры и объединены каналами связи, образуя единую распределенную систему для управления транспортными потоками.

Для разработки и реализации предлагаемого подхода распределенной оптимизации использован открытый стандарт распределенных систем управления и автоматизации МЭК 61499 [16]. Работа в рамках стандарта МЭК 61499 позволяет быстро создать прототип системы для проверки работоспособности предлагаемого подхода, а также быстро внедрить разработку при наличии необходимых контроллеров, например в светофоре.

Далее в работе описана суть предлагаемого подхода к адаптивному управлению дорожным движением. Затем рассмотрена реализация разработанного подхода в среде имитационного моделирования и проверка его работы на имитационной модели участка дорожной сети. Затем в работе представлены сравнительные результаты управления транспортными потоками с использованием различных подходов к организации движения транспорта.

Подход к адаптивному управлению дорожным движением на основе взаимосвязанных интеллектуальных агентов. Подходы к управлению дорожным движением обычно, имеют централизованную структуру, которая характеризуется зависимостью объектов дорожной инфраструктуры от «Центра управления дорожным движением».

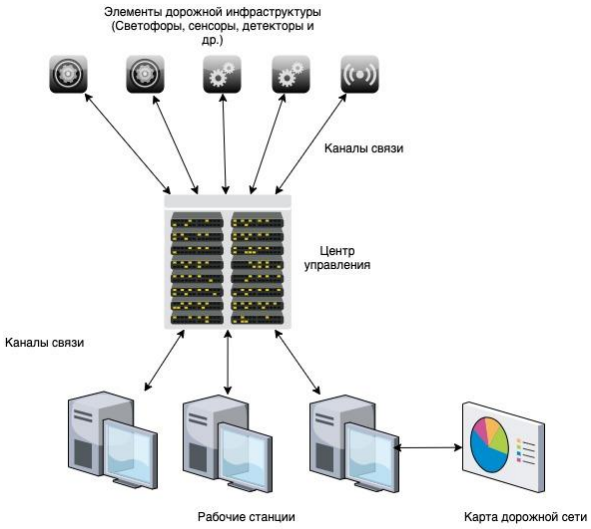

Рис. 1. Структура централизованной системы управления дорожным движением

Управляющие воздействия на транспортные потоки формируются в центре управления дорожным движением и данные о ситуации на дорожной сети так же обрабатываются централизованно. В результате система теряет гибкость и управляющие решения работают медленно. Однако, гибкость и скорость принятия решений важные свойства для управления динамическими средами.

Применение агентного подхода к управлению транспортными потоками позволяет сделать систему гибкой и интеллектуальной. Например, в работе [17] предлагается новая архитектура много-агентного подхода для управления движением на уча-

стке дорожной сети. Но существенным минусом предлагаемых решений является то, что нужно создавать новую инфраструктуру для реализации и разрабатывать специализированное оборудование, а этот процесс очень часто дорогой и долгий.

В то же время применение IoT устройств на базе современных микроконтроллеров [18, 19] позволяет частично решить проблему с оборудованием для новой дорожной инфраструктуры, но остаются острыми вопросы надежности такого оборудования и интеграции с существующими системами управления дорожным движением.

В связи с этим, предлагается концепция управления транспортными потоками с помощью взаимосвязанных интеллектуальных агентов. Каждый из агентов обладает полномочиями для применения управляющих воздействий на транспорт внутри перекрестка с помощью изменения циклов работы светофора или его отключения. Так же агенты передают данные о загруженности дорожной сети в зоне своей ответственности агентам управляющим соседними перекрестками для обеспечения более эффективного управления движением.

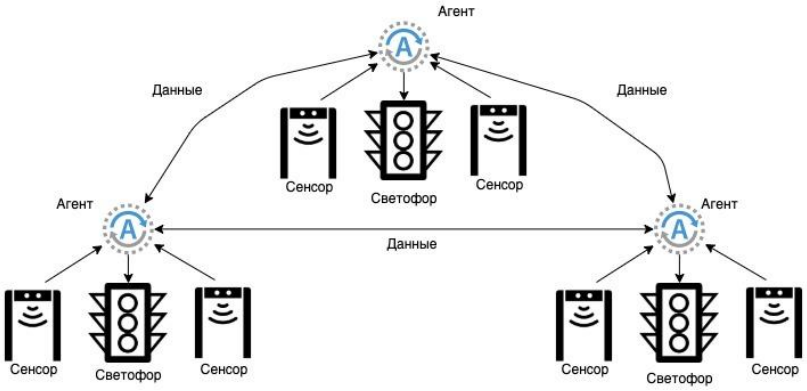

Рис. 2. Структура предлагаемого подхода

На данном этапе, рассматривается следующий принцип работы агента на перекрестке:

1. Получение данных с датчиков и сенсоров, расположенных на дорожной сети.
2. Анализ транспортной загруженности согласно логике, заложенной в агента.
3. Передача информации о загруженности соседним агентам.
4. Получение информации от соседних агентов.
5. Принятие решения о управляющем воздействии на участок дорожной сети.
6. Применение управляющего воздействия (изменение цвета сигнализации светофора).

Для проверки выдвигаемой гипотезы, была использована среда для работы с открытым стандартом по проектированию распределенных систем «NxtStudio» [20] и комплекс для проведения имитационного моделирования транспортных потоков SUMO [21].

Реализация концепции агентного управления. На данный момент в начале разработки концепции, предлагается реализация интеллектуального управления одним перекрестком на дорожной сети с помощью интеллектуального агента – регулировщика логика работы которого заключается в следующем:

Регулировщик, с помощью датчиков, установленных на дорожной сети, определяет количество автомобилей, движущихся по каждому направлению. Если количество автомобилей на дороге не превышает, допустимое значение для нерегулируемого перекрестка, агент не активен. Как только количество транспортных

средств превысило допустимое, регулировщик проверяет по какому направлению больше автомобилей движется и нужно начать их пропускать, анализируя каждую полосу движения. После определения, на выбранных полосах включается разрешающий сигнал светофора. Регулировщик постоянно фиксирует количество транспортных средств на каждой полосе, как только количество автомобилей по движущемуся направлению стало в половину меньше автомобилей ожидающих проезда, светофорная сигнализация изменяется на разрешающий сигнал для ожидающих автомобилей. Регулировщик работает пока количество транспорта на перекрестке не уменьшится до допустимого для отключения светофорной сигнализации.

Предложенную простую логику регулировщика при включении светофора для различных направлений на перекрестке, можно представить следующим образом:

$$\frac{100 * \sum_{l=1}^{n} l}{\sum_{r=1}^{k} r} > 50. \quad (1)$$

где n – общее количество полос для движения в движущемся направлении; l – количество полос в движущемся направлении; k – общее количество полос для движения в ожидающем направлении; r – количество полос в ожидающем направлении.

Агент регулировщик был реализован в виде функционального блока, выполненного по стандарту МЭК 61499.

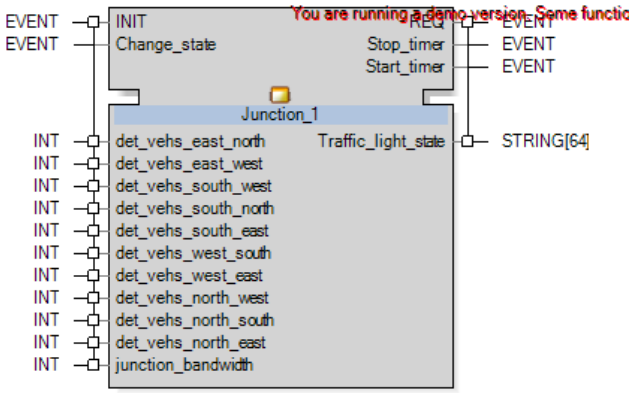

Рис. 3. Функциональный блок регулировщик

Входящее событие INIT – инициализирует работу функционального блока и позволяет считать данные о текущей загруженности перекрестка с транспортных детекторов, передающих данные на входные переменные: «det_vehs_east_north…det_vehs_north_east». Входная переменная «junction_bandwidth» определяет максимальную загруженность для перекрестка без светофорного регулирования.

Входящее событие «Change_state» – инициализирует изменение сброс светофорной сигнализации, когда количество автомобилей на перекрестке уменьшилось до допустимого.

Исходящее событие REQ – инициализирует выходную переменную «Traffic_light_state» в которой находится сформированный регулировщиком цикл работы светофора.

Исходящие события «Start_timer» и «Stop_timer» используются для контроля включения и выключения режима светофорного регулирования на перекрестке.

Логика работы регулировщика на перекрестке реализована в функциональном блоке с помощью ECC диаграммы и на языке программирования Structured text.

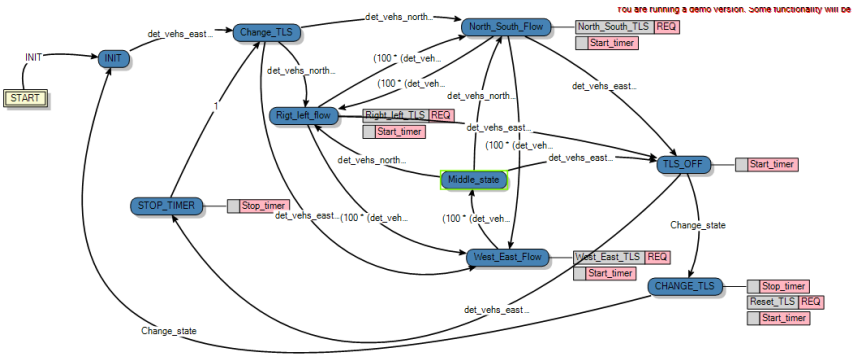

Рис. 4. ECC диаграмма

Для проверки гипотезы были созданы две модели х-образных перекрестков:

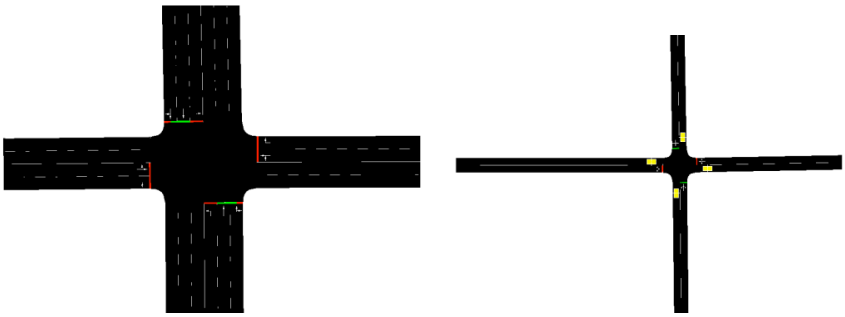

Рис. 5. Перекрёстки A и B

Перекресток B создавался без учета реальных транспортных и геометрических характеристик для дорожной сети. Перекресток имеет по одной полосе движения в каждом направлении и случайный объем транспортных потоков и стандартный цикл работы светофора.

Перекресток A создан на основе данных о транспортных и геометрических характеристиках из специализированного пособия для транспортных инженеров [22]. На перекрёстке расположены по 3 полосы для движения в каждом направлении с севера на юг и по 2 с запада на восток. Так же для него специализированно рассчитан цикл работы светофора исходя из транспортной загруженности.

Далее было разработано средство для коммуникации регулировщика с имитационной моделью участка дорожной сети.

В стандарте по проектированию распределенных систем, для коммуникации между устройствами и внешней средой по протоколу TCP разработан функциональный блок NETIO. Который был использован для коммуникации разработанного регулировщика со средой имитационного моделирования SUMO с использованием языка программирования Python и стандартного средства SUMO – TraCi. На языке Python был реализован асинхронный сервер для приема и обработки данных от функционального блока регулировщика к имитационной модели перекрестка реализованной в SUMO.

После объединения компонентов в среду для тестирования, была проведена серия экспериментов по управлению движением на перекрестках A и B различными способами.

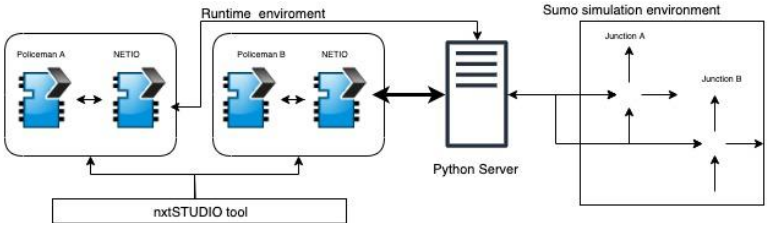

Рис. 6. Схема средства коммуникации

Серия экспериментов. Эксперименты по управлению движением были проведены на двух перекрестках A и B. В ходе экспериментов была запущена имитация длительностью 3600 секунд с тремя типами управления движением на перекрестке:

1) Управление агентом-регулировщиком;
2) Жесткое управление с помощью светофорного цикла;
3) Без регулирования (свободный проезд).

Во время имитационного моделирования фиксировались следующие параметры:

Таблица 1

Параметры

Задержка перед отправлением	Секунды (симуляции)	Время ожидания для автомобилей перед стартом
Скорость прибытия	м/с	Скорость автомобилей, завершающих движение
Время ожидания	секунды	Время, в течение которого скорость автомобиля была менее 0.1 м/с
Потерянное время	секунды	Время, потерянное в сравнении с оптимальным временем движения
Количество автомобилей	штуки	Количество автомобилей, проехавших через перекрёсток

В результате проведенного имитационного моделирования были получены следующие результаты: Параметр «Задержка перед отправлением» при использовании агента-регулировщика примерно на 25 процентов ниже чем без регулирования движения на перекрестке и на 80 процентов ниже, чем при использовании жесткого цикла светофорного регулирования.

Рис. 7. Задержка перед стартом

Параметр «Скорость прибытия» для управления с помощью регулировщика и без какого-либо управления практически одинаковы. При использовании стандартного светофорного регулирования скорость больше.

Рис. 8. Скорость прибытия

Самое минимальное время ожидания транспортных средств характерно для перекрестка без управления, но это актуально только в идеальных условиях моделирования, где не происходят ДТП. На регулируемом перекрестке управляющий агент снижает время ожидания на 14 процентов по сравнению с обычным светофорным циклом.

Рис. 9. Время ожидания

Параметр «Время ожидания» так же принимает наименьшее значение при управлении регулировщиком с преимуществом в 31 процент.

Рис. 10. Потерянное время

При агентном управлении пропускная способность перекрестка увеличивается на 25 процентов по сравнению со стандартным управлением движением.

Рис. 11. Количество автомобилей

На перекрестке А, также была проведена серия имитаций с мониторингом по аналогичным параметрам.

Рис. 12. Задержка перед стартом

В этом случае параметр «Задержка перед стартом» без светофорного регулирования значительно ниже, чем на регулируемом перекрестке, но у агентного подхода так же остается преимущество в 19 процентов.

Рис. 13. Скорость прибытия

Конечная скорость транспортных средств, также, как и на предыдущем перекрестке, остается примерно одинаковой.

Рис. 14. Потерянное время

Как можно увидеть, на более сложном перекрестке, агент-регулировщик обеспечивает наименьшие потери времени для транспортных средств, на 7 % по сравнению со стандартным светофорным регулированием.

Рис. 15. Время ожидания

Время ожидания при проезде пересечения, которое управляется регулировщиком на 22 процента ниже, чем на перекрестке без регулирования, и на 13 процентов ниже, чем на перекрестке с жестким светофорным циклом.

Рис. 16. Количество автомобилей

И как следствие, пропускная способность перекрестка, управляемого агентом-регулировщиком выше на 10 процентов чем с обычным светофором и на 20 % выше, чем без светофора, так как без светофора на данном типе пересечения возник большой затор со стороны второстепенной дороги.

Заключение. В работе был описан подход к управлению движением на различных перекрестках, основанный на простой логике регулировщика, который переключает сигналы светофора в зависимости от загруженности направлений движения.

В результате проведенного экспериментального исследования были выявлены очевидные преимущества адаптивного управления пересечением с помощью интеллектуального регулировщика, в сравнении с классическим светофорным регулированием, а также отсутствием управления на перекрестке. По большинству исследуемых параметров, управление с помощью агента превосходит конкурентные типы управления, а по некоторым в несколько раз. При этом, для реализации агента, был использован открытый стандарт МЭК 61499 и среда NXTStudio, что позволяет быстро создать прототип разработанного решения для поддерживаемого контроллера и внедрить его на экспериментальный участок дорожной сети. Такой подход позволяет с высокой скоростью переходить от этапа идеи и исследовательской работы к этапу реализации на реальном оборудовании. Это повышает экономическую и практическую эффективность проводимых исследований.

В развитие концепции управления транспортными потоками с помощью взаимосвязанных интеллектуальных агентов, дальнейшие исследования будут направлены на реализацию управления движением одновременно на нескольких перекрестках, агенты на которых, будут влиять на принятие решения о воздействии на транспортный поток обмениваясь данными о загруженности подконтрольной дорожной сети друг с другом.

Так же в будущих работах будет рассмотрен подход к управлению движением, где на каждом перекрестке работает множество агентов, которые коллективно принимают решение при формировании следующей фазы движения транспортных средств. Решение агентов основано на загруженности подконтрольной полосы и влиянии принятого решения на транспортную ситуацию в целом и мнения соседних агентов о необходимых фазах движения автомобилей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Roess R.P., Prassas E.S., McShane W.R.* Traffic engineering. Pearson/Prentice Hall, 2004.
2. *Heung, Tsin Hing, Tin Kin Ho, and Yu Fai Fung*. Coordinated road-junction traffic control by dynamic programming, *IEEE Transactions on Intelligent Transportation Systems*, 2005, 6.3, pp. 341-350.
3. *Nagatani Takashi*. Vehicular traffic through a sequence of green-wave lights, *Physica A: Statistical Mechanics and its Applications*, 2007, 380, pp. 503-511.

4. *Gershenson Carlos, and David A. Rosenblueth.* Self-organizing traffic lights at multiple-street intersections, *Complexity*, 2012, 17.4, pp. 23-39.
5. *Smith Stephen F., et al.* Smart urban signal networks: Initial application of the surtrac adaptive traffic signal control system, *Twenty-Third International Conference on Automated Planning and Scheduling*, 2013.
6. *Hunter Michael P., et al.* A probe-vehicle-based evaluation of adaptive traffic signal control, *IEEE Transactions on Intelligent Transportation Systems*, 2012, 13.2, pp. 704-713.
7. *Pandit Kartik, et al*. Adaptive traffic signal control with vehicular ad hoc networks, *IEEE Transactions on Vehicular Technology*, 2013, Vol. 62.4, pp. 1459-1471.
8. *Tielert Tessa, et al.* The impact of traffic-light-to-vehicle communication on fuel consumption and emissions, *2010 Internet of Things (IOT). IEEE, 2010.*
9. *Khanna Abhirup, and Rishi Anand.* IoT based smart parking system, *2016 International Conference on Internet of Things and Applications (IOTA). IEEE, 2016.*
10. *Bui Khac-Hoai Nam, Jai E. Jung, and David Camacho*. Game theoretic approach on Real-time decision making for IoT-based traffic light control, *Concurrency and Computation: Practice and Experience*, 2017, 29.11, e4077.
11. *Phan, Cao Tho, et al*. Applying the IoT platform and green wave theory to control intelligent traffic lights system for urban areas in Vietnam, *TIIS*, 2019, 13.1, pp. 34-51.
12. *He Wu, Gongjun Yan, and Li Da Xu.* Developing vehicular data cloud services in the IoT environment, *IEEE Transactions on Industrial Informatics*, 2014, 10.2, pp. 1587-1595.
13. *Mzahm Anas M., Mohd Sharifuddin Ahmad, and Alicia YC Tang.* Agents of Things (AoT): An intelligent operational concept of the Internet of Things (IoT), *2013 13th International Conference on Intellient Systems Design and Applications. IEEE, 2013*.
14. *Liu Ying, Lei Liu, and Wei-Peng Chen.* Intelligent traffic light control using distributed multi-agent Q learning, *2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2017*.
15. *Bui Khac-Hoai Nam, and Jason J. Jung*. Internet of agents framework for connected vehicles: A case study on distributed traffic control system, *Journal of Parallel and Distributed Computing*, 2018, pp. 116 89-95.
16. IEC61499-1, Function Blocks - Part 1 Architecture, International Electrotechnical Commission, Geneva, International standard, 2005.
17. *Kaminski Nicholas J., Maria Murphy, and Nicola Marchetti*. Agent-based modeling of an IoT network, *2016 IEEE international symposium on systems engineering (ISSE). IEEE, 2016*.
18. *Misbahuddin Syed, et al*. IoT based dynamic road traffic management for smart cities, *2015 12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET). IEEE, 2015*.
19. *Chong Hon Fong, and Danny Wee Kiat Ng.* Development of IoT device for traffic management system, *2016 IEEE Student Conference on Research and Development (SCOReD). IEEE, 2016.*
20. The tool for engineering of distributed systems [Online]. Available: https://www.nxtcontrol.com/en/engineering/.
21. The vehicular traffic simulator. [Online]. Available: http://sumo. sourceforge.net/.
22. *Stolyarov V., et al*. Guidelines to practical work and diploma design for students of the specialty 190700, *Substantiation of duration of the lighting cycle. 2012*.

Статью рекомендовал к опубликованию д.т.н., профессор А.Б. Чернышев.

Елькин Дмитрий Максимович – Южный федеральный университет; e-mail: delkin@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: +78634360839; кафедра синергетики и процессов управления; аспирант.

Вяткин Валерий Владимирович – e-mail: vvyatkin@sfedu.ru; Институт компьютерных технологий и информационной безопасности; профессор.

Elkin Dmitriy Maksimovich – Southern Federal University; e-mail: delkin@sfedu.ru; 2, Chehova street, Taganrog, 347928, Russia, phone: +78634360839; the department of synergetics and management processes; postgraduate student.

Vyatkin Valeriy Vladimirovich – e-mail: vvyatkin@sfedu.ru; the Institute of computer technologies and information security; professor.

УДК 621.373.132 DOI 10.18522/2311-3103-2020-5-111-123

П.А. Землянухин, А.В. Кондратьев, С.С. Свидельский

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ФОРМИРОВАТЕЛЯ ШУМОВОГО СИГНАЛА, КАК ИСТОЧНИКА ШУМА В МНОГОКАНАЛЬНОМ ГЕНЕРАТОРЕ ШУМА

Целью работы является исследование принципа работы и характеристик формирователя шумового сигнала модуляционного типа, в котором в качестве несущего колебания и модулирующего сигнала используются квазигармонические шумовые сигналы, и в котором обеспечивается управление шириной спектра шумового сигнала в заданном диапазоне частот. Выполнено исследование структуры построения и характеристик формирователя шумового сигнала, который может быть использован при создании адаптивных многоканальных генераторов шума для маскирования информативных компонент побочных электромагнитных излучений и наводок (ПЭМИН). По источникам отечественной и зарубежной литературы, а также патентной документации проведен анализ технических решений по исполнению генераторов шума, предназначенных для маскирования ПЭМИН. Этот анализ подтвердил актуальность проблемы по созданию адаптивных генераторов шума. Отмечено, что для улучшения характеристик генераторов шума, придания им более широкого применения с целью качественного противодействия несанкционированному съему злоумышленниками информации по каналам излучения ПЭМИН, необходимо создавать многоканальные адаптивные генераторы шума. В этих генераторах в каждом канале зашумления можно обеспечить регулировку мощности, формируемого шумового сигнала и управление шириной полосы частот зашумления, что позволит повысить электромагнитную совместимость подобных устройств. Для обеспечения этого предлагается использовать в формирователях шумового сигнала два аналоговых перемножителя сигналов, с выходов которых шумовые сигналы суммируются и поступают на выход формирователя шумового сигнала, что позволяет получить равномерный по амплитуде шумовой сигнал. При этом обеспечивается управление шириной спектра шумового сигнала не менее, чем в два раза в сравнении с традиционными методами формирования шумового сигнала модуляционными методами.

Генератор шума; формирователь шумового сигнала; шумовой сигнал; перемножитель аналоговых сигналов; ПЭМИН; квазигармонический шумовой сигнал.

P.A. Zemlyanukhin, A.V. Kondratiev, C.C. Svidelskiy

RESEARCH OF THE CHARACTERISTICS OF THE NOISE SIGNAL CONDITIONER AS A NOISE SOURCE IN MULTI-CHANNEL NOISE GENERATORS

The purpose of this work is to study the principle of operation and characteristics of a modulation-type noise signal conditioner in which quasi-harmonic noise signals are used as a carrier oscillation and modulating signal and in which the spectrum width of the noise signal is controlled in a given frequency range. A study of the structure of the construction characteristics of the noise signal generator that can be used to create adaptive multichannel noise generators to provide active protection of informative components of side electromagnetic radiation and interference (SERaI). According to the sources of domestic and foreign literature, as well as patent documentation, the analysis of technical solutions for the implementation of noise generators intended for masking SERaI were analyzed. The analysis confirmed the relevance of the problem of creating adaptive noise generators. It is noted that it is necessary to create multichannel adaptive noise generators to improve the characteristics of noise generators and make them more widely used in order to effectively counteract unauthorized leakage of information by hackers through the SERaI radiation channels. In these generators, each noise channel can be adjusted for power, generated noise signal and control of the noise masking frequency bandwidth, which will increase the electromagnetic compatibility of such devices. To ensure this, it is proposed to use two analog signal

multipliers in the noise signal conditioner, from the outputs of which the noise signals are summed and sent to the output of the noise signal conditioner which allows to obtain a uniform noise signal in amplitude. It provides control over the spectral width of the noise signal at least twice as compared to traditional methods of generating a noise signal using modulation methods.

Noise generator; noise signal conditioner; noise signal; analog signal multiplier; SERaI; quasi-harmonic noise signal.

Введение. Впервые в начале прошлого века было осуществлено считывание злоумышленниками информации, которая излучается по каналам побочных электромагнитных излучений и наводок (ПЭМИН). В 1985 году ученый Вим ван Эйк опубликовал статью [1], где показал, что «подслушивание» цифровых устройств может быть осуществлено с помощью бытовых приборов, например, телевизионного приемника. Эта публикация послужила мощным толчком для более широких исследований по съему информации, излучаемой по каналам ПЭМИН и по противодействию этому. Так в [2] показано, что на изолированном компьютере, который использовал протокол Диффи-Хеллмана на эллиптических кривых [3], путем анализа ПЭМИН в течение 3,3 секунд удалось извлечь ключ дешифрования. В [4] описан эксперимент по перехвату текстов с монитора на расстоянии 10 м через три стены из гипсокартона (через два офисных помещения) с использованием супергетеродинного приемника. Это говорит о том, что методы борьбы с ПЭМИН являются актуальными.

Одними из технических методов борьбы со считыванием информации по каналам ПЭМИН [5–7] являются активные методы защиты информации. К этим методам и относят использование генераторов шума (ГШ) для обеспечения маскирования ПЭМИН на объекте телекоммуникаций.

К числу технических устройств, например, средств вычислительной техники, обеспечивающих формирование ПЭМИН, относят: монитор, системный блок, накопители информации, сканер, принтер, «мышь» и др. Все эти устройства при передаче информационных сигналов в последовательном коде, способны обеспечить возникновение канала ПЭМИН, по которому распространяется информация в диапазоне частот от очень низких до 8 ГГц и выше [8–11]. Из-за широкого частотного диапазона формирования ПЭМИН, в каком-то частотном диапазоне спектральные составляющие ПЭМИН будут иметь низкую интенсивность, а в другом высокую. В этом случае часть спектральных составляющих ПЭМИН будет маскирована, уровень же других спектральных составляющих ПЭМИН будет превышать уровень шума, либо при достаточно высоком уровне шума будет наблюдаться снижение электромагнитной совместимости генератора шума относительно других радиотехнических устройств. Так, в [12] отмечается, что исторически ПЭМИН относится к специфическим задачам электромагнитной совместимости.

По мере совершенствования средств обработки, хранения и передачи информации по каналам связи, представляется **актуальным** создание высокоэффективных ГШ для маскирования ПЭМИН. Такие ГШ должны быть способны обеспечить, с одной стороны, сохранность информации, излучаемой по каналам ПЭМИН [13], а, с другой стороны, обеспечить электромагнитную совместимость технических средств активной защиты информации с другими радиотехническими устройствами и телекоммуникационными системами.

В настоящее время на рынке имеется большое количество сертифицированных ГШ для маскирования ПЭМИН. В тоже время подобные устройства по своей структуре являются одноканальными с максимальной частотой работы от 1ГГц до 2,5 ГГц [14–16]. Этого явно недостаточно, поскольку тактовые частоты тех же компьютеров постоянно возрастают. Это приводит и к расширению частотного диапазона излучения ПЭМИН. Известен генератор шума МИК-ГШ-3000 [17],

имеющий пять каналов зашумления. Он обеспечивает формирование шумового сигнала на частотах от 0,09 МГц до 3000 МГц. В нем предусмотрена регулировка уровня излучения шума в каждом из частотных диапазонов. Однако, в нем отсутствует оценка защищенности по ПЭМИН. В результате этого интенсивность излучения ГШ может значительно превышать минимальную мощность шумового сигнала, требуемую для применения.

Имеются работы, в которых для адаптации спектра шумового сигнала к ПЭМИН предлагается использовать многоканальную схему построения ГШ. Так, в [17] рассматривается построение девятиканальных ГШ. В данном случае в каждом канале используется независимый ГШ, и предусмотрена регулировка интенсивности излучения с помощью программы. При этом обеспечивается привязка шума к уровню излучения ПЭМИН. Однако, данный подход к построению ГШ приводит к существенному удорожанию стоимости этих устройств при том, что этот ГШ не обеспечивает существенного снижения уровня электромагнитной засоренности эфира, т.к. устройство не позволяет проводить управление шириной спектра шума в заданных каналах формирования шумового сигнала. Кроме того, отсутствует привязка шумового сигнала к спектру ПЭМИН конкретного технического средства.

Имеются патенты, в которых предлагаются способы реализации ГШ с улучшенными характеристиками [18]. В патентах [19, 20] оговаривается улучшение шумовых характеристик ГШ и снижение их влияния на электромагнитную обстановку в зоне расположения ГШ. Функционирование этих ГШ основано на одновременном использовании ГШ и сигнала с тактовой частотой работы устройства обработки информации. Эти сигналы поступают на преобразователь частоты [19] или на нелинейный усилитель [20]. Однако, в описаниях к патентам не оговаривается энергетическая равномерность спектра шумового сигнала в диапазоне частот до 10 ГГц.

Применительно к генераторам шума серии ГШ указывается [10], что в них выполняется плавное или дискретное управление интенсивностью выходного сигнала. Например, генератор шумового сигнала ГШ-1000У имеет пять независимых ГШ. Выход одного канала соединен непосредственно с антенной. К выходам 4-х других каналов могут быть подключены дополнительные внешние устройства: антенны, направленные ответвители и т.д. Подобные функции имеются и в ряде других ГШ. В то же время они не обеспечивают эффективной электромагнитной совместимости с другими электронными устройствами.

Многие проблемы, свойственные ГШ (электромагнитная совместимость и высокая выходная мощность; расширенный диапазон рабочих частот, вплоть до 10 ГГц), можно решить строя ГШ по принципу многоканальных систем [21]. Такие системы позволили бы:

- ♦ отключать от зашумления диапазоны частот, в рамках которых не наблюдается работа технических средств обработки информации;
- ♦ обеспечить регулировку выходной мощности шумового сигнала в требуемом частотном диапазоне (канале зашумления);
- ♦ обеспечить регулировку ширины спектра шумового сигнала в требуемом частотном диапазоне (канале зашумления).

Проведенный анализ показывает, что разработка многоканального адаптивного ГШ с максимальной частотой работы до 5–10 ГГц является **актуальной**. В тоже время практически отсутствуют теоретические исследования по построению подобных ГШ. Здесь можно отметить работу [22], где предлагается, используя организационные мероприятия, но не изменяя уровня электромагнитных шумов, путем изменения расположения технических средств снизить уровень возможного перехвата информации. Подобный подход видится малоэффективным, либо потребует повышения уровня шумов для маскирования ПЭМИН.

В [23] проведены теоретические исследования по построению модульных (разнесенных в пространстве) систем защиты информации от утечки по техническим каналам. Однако, подобный подход может вызвать существенное удорожание средств защиты от утечки информации по каналам ПЭМИН.

Для построения высокоэффективных ГШ для маскирования ПЭМИН, позволяющих предотвратить утечку информации по техническим каналам, необходимо использовать многоканальную структуру. Это позволит обеспечить качественное приближение амплитудно-частотной характеристики ГШ к уровням спектральных составляющих ПЭМИН в широком частотном диапазоне. Для построения подобных ГШ необходимо создать формирователь шумового сигнала, который обеспечит формирование шумового сигнала в заданном диапазоне частот и при этом обеспечит с одной стороны управление шириной спектра шумового сигнала, а с другой стороны – управление интенсивностью амплитуд спектральных составляющих шумового сигнала.

Целью работы является исследование принципа работы и характеристик формирователя шумового сигнала модуляционного типа, в котором в качестве несущего колебания и модулирующего сигнала используются квазигармонические шумовые сигналы, и в котором обеспечивается управление шириной спектра шумового сигнала в заданном диапазоне частот.

Структура формирователя шумового сигнала. В [24] рассмотрен возможный подход к формированию шумового сигнала модуляционным методом. Этот подход отличается от того, который широко используется при формировании шумового сигнала модуляционными методами [25], где в качестве несущего колебания используется сигнал, изменяющийся по гармоническому закону, а в качестве модулирующего сигнала – шумовой сигнал. В рассматриваемом формирователе шумового сигнала в качестве несущего колебания и модулирующего сигнала используется квазигармонический шум, сформированный с использованием частотно-избирательных цепей (например, колебательных контуров) из «белого шума». Далее эти квазигармонические шумы, разнесенные по оси частот на несколько порядков, подаются на перемножитель сигналов. На выходе перемножителя сигналов формируется шумовой сигнал, спектральная плотность которого включает спектральные составляющие, полученные в процессе перемножения каждой спектральной составляющей несущего колебания с каждой спектральной составляющей модулирующего сигнала:

$$S_{\text{ш}}(j\omega) = \int_{-\infty}^{\infty} \left[\sum_{i=1}^{n} s_{i.\text{н}}(t) \cdot \sum_{k=1}^{m} s_{k.\text{м}}(t) \right] e^{-j\omega t} dt,$$

где $s_{i.\text{н}}(t)$ и $s_{k.\text{м}}(t)$ – i-я и k-я спектральные составляющие несущего колебания и модулирующего сигнала, соответственно.

Здесь $\sum_{i=1}^{n} s_{i.\text{н}}(t)$ и $\sum_{k=1}^{m} s_{k.\text{м}}(t)$ представляют собой некоторые шумовые процессы $\xi_{\text{н}}(t)$ и $\xi_{\text{м}}(t)$ квазигармонического шумового сигнала.

Подобный подход к формированию шумового сигнала позволяет: обеспечить управление шириной спектра шума на выходе формирователя шумового сигнала за счет управления центральными частотами шумовых процессов $\xi_{\text{н}}(t)$ и $\xi_{\text{м}}(t)$; подключать (отключать) шумовой сигнал в заданных (требуемых) полосах частот при построении многоканальных ГШ; повысить электромагнитную совместимость ГШ.

Однако, формирователь шумового сигнала, рассмотренный в [24], имеет существенный недостаток. Этот недостаток выражается в том, что спектральная плотность шумового сигнала на выходе формирователя шумового сигнала в окрестности центральной частоты несущего колебания $\xi_{\text{н}1}(t)$, может иметь провал по наличию спектральных составляющих требуемой интенсивности. Эта проблема будет существенно усугубляться при увеличении центральной частоты модулирующего сигнала $\xi_{\text{м}1}(t)$.

В [26] сделана попытка решить эту проблему. Для этого обеспечивается суммирование шумового сигнала с выхода перемножителя сигналов и шумового процесса несущего колебания. Это может частично решить проблему с неравномерностью спектральной плотности амплитуд шумового сигнала на выходе формирователя шумового сигнала.

Однако, учитывая то, что квазигармонический шум несущего колебания является узкополосным шумовым сигналом, проблема неравномерности спектральной плотности амплитуд шумового сигнала на выходе формирователя шумового сигнала устраняется неполностью, что не позволяет обеспечить качественное маскирование ПЭМИН средств обработки, хранения и передачи информации.

Для преодоления препятствий по качественному маскированию ПЭМИН предлагается ввести в формирователь шумового сигнала еще один канал с перемножителем квазигармонических сигналов несущего колебания $\xi_{н2}(t)$ и модулирующего сигнала $\xi_{м2}(t)$ (рис. 1).

Формирователь шумового сигнала включает три цепи избирательных по частоте, где при этом первая цепь обеспечивает формирование шумового сигнала несущего колебания. Вторая цепь обеспечивает формирование шумового модулирующего сигнала. Третья цепь обеспечивает формирование шумового сигнала несущего колебания, центральная частота которого сдвинута по оси частот относительно центральной частоты несущего колебания, формируемого первой цепью избирательной по частоте. Все три цепи избирательные по частоте имеют входы управления для подстройки (задания) центральных частот, относительно которых обеспечивается формирование квазигармонического шума соответствующей цепью. Кроме того, все три цепи имеют входы, на которые подается шумовой сигнал по характеристикам близкий к белому шуму.

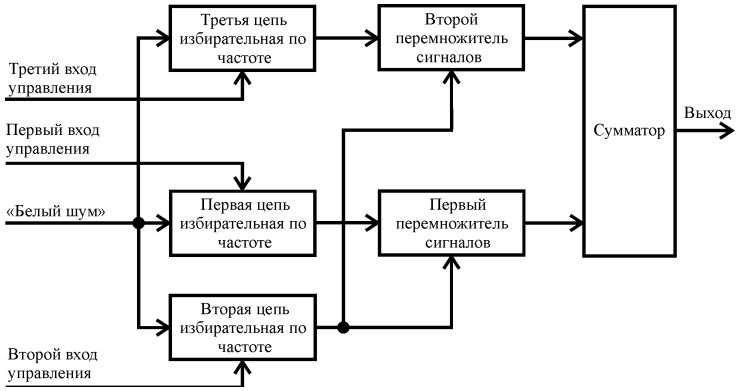

Рис. 1. Структурная схема формирователя шумового сигнала

В устройстве имеются первый и второй перемножители аналоговых сигналов, на первые входы которых подаются квазигармонические сигналы с выходов первой и третьей цепей избирательных по частоте, соответственно. На вторые входы перемножителей аналоговых сигналов подается квазигармонический сигнал с выхода второй цепи избирательной по частоте.

С выходов первого и второго перемножителей аналоговых сигналов шумовые сигналы поступают на сумматор, на выходе которого появляется шумовой сигнал, сформированный в заданной полосе частот.

Пусть центральные частоты квазигармонических сигналов, формируемых на выходах первой, второй и третьей цепей избирательных по частоте, соответственно, равны: f_{01}, f_{02} и f_{03}. Ширины спектров квазигармонических сигналов на выхо-

дах первой, второй и третьей цепей избирательных по частоте по уровню 0,707, в зависимости от добротности колебательных контуров, соответственно, равны: $2\Delta f_1 = f_{01}/Q_1$; $2\Delta f_2 = f_{02}/Q_2$ и $2\Delta f_3 = f_{03}/Q_3$, где Q_1, Q_2 и Q_3 – добротности колебательных контуров первой, второй и третьей цепей избирательных по частоте, соответственно.

Рассмотрим зависимость ширины спектра шумового сигнала на выходе первого аналогового перемножителя сигналов. На выходе этого перемножителя сигналов будет формироваться шумовой сигнал, полученный в процессе амплитудной модуляции. По уровню 0,707 границы нижней $f_{\text{АМ.н}}$ и верхней $f_{\text{АМ.в}}$ боковых полос этого шумового сигнала будут иметь вид:

$$f_{\text{АМ.н}} = f_{01} - \Delta f_1 - f_{02} - \Delta f_2; \quad f_{\text{АМ.в}} = f_{01} + \Delta f_1 + f_{02} + \Delta f_2.$$

Тогда, ширину спектра шумового сигнала можно описать в виде:

$$\Delta f_{\text{АМ}} = f_{\text{АМ.в}} - f_{\text{АМ.н}} = 2(f_{02} + \Delta f_1 + \Delta f_2). \quad (1)$$

Из выражения (1) можно видеть, что при постоянных значениях Δf_1 и Δf_2, ширина спектра шумового сигнала зависит от величины центральной частоты f_{02} модулирующего сигнала. При увеличении (уменьшении) величины f_{02} ширина спектра шумового сигнала увеличивается (уменьшается). Кроме того, при изменении частоты f_{02} будет изменяться и ширина спектра Δf_2 при постоянной добротности колебательного контура второй цепи избирательной по частоте.

Таким образом, обеспечивая управление центральной частотой второй цепи избирательной по частоте, можно организовать управление шириной спектра шумового сигнала на выходе первого аналогового перемножителя сигналов. Это может быть полезным при использовании подобного формирователя шумового сигнала в многоканальных ГШ, поскольку обеспечивается локальное маскирование ПЭМИН в заданном и управляемом по протяженности диапазоне частот. Кроме того, можно обеспечить повышение электромагнитной совместимости устройства.

Для нижней боковой полосы спектральные составляющие шумового сигнала, полученные в процессе амплитудной модуляции, будут располагаться в окрестности частоты $f_{01} - f_{02}$, а для верхней боковой полосы – в окрестности частоты $f_{01} + f_{02}$. Однако, при выполнении условия $f_{02} > \Delta f_1 - \Delta f_2$ от частоты $f_{01} - \Delta f_1 + f_{02}$ до частоты $f_{01} + \Delta f_1 - f_{02}$, можно наблюдать резкий спад амплитуд спектральных составляющих шумового сигнала, сформированного на выходе первого аналогового перемножителя сигналов.

Для преодоления этого недостатка в формирователе шумового сигнала использован второй аналоговый перемножитель сигналов. Резонансная частота f_{03} третьей цепи избирательной по частоте сдвинута относительно частоты f_{01} и выбрана в виде:

$$f_{03} = f_{01} + \frac{\Delta f_1 + f_{02}}{2}. \quad (2)$$

В этом случае нижняя боковая полоса спектра амплитудно-модулированного сигнала, формируемого на выходе второго аналогового перемножителя сигналов, будет закрывать диапазон частот от частоты $f_{01} - \Delta f_1 + f_{02}$ до частоты $f_{01} + \Delta f_1 - f_{02}$, где происходит спад амплитуд спектральных составляющих шумового сигнала, формируемого в процессе амплитудной модуляции на выходе первого аналогового перемножителя сигналов. Верхняя боковая полоса спектра амплитудно-модулированного сигнала обеспечит перекрытие шумовым сигналом дополнительного частотного диапазона при суммировании шумовых сигналов с выходов первого и второго аналоговых перемножителей сигналов.

В результате этого, рассматриваемый формирователь шумового сигнала, позволяет обеспечить равномерный спектр шумового сигнала в частотном диапазоне, определяемом резонансными частотами $f_{01},\ f_{02}$ и f_{03} и добротностями $Q_1,\ Q_2$ и Q_3 первого, второго и третьего колебательных контуров первой, второй и третьей цепей избирательных по частоте.

Модель формирователя шумового сигнала. На входы первой, второй и третьей цепей избирательных по частоте подается шумовой сигнал $\xi(t)$ по свойствам приближающийся к белому шуму. Цепи избирательные по частоте представляют собой параллельные колебательные контура, обладающие добротностями $Q_1,\ Q_2$ и Q_3 и имеющие резонансные частоты $f_{01},\ f_{02}$ и f_{03}, соответственно. С учетом этого алгоритм нахождения шумового сигнала будет иметь вид.

1. Нахождение комплексных частотных характеристик коэффициентов передачи напряжения первого $K_1(j\omega)$, второго $K_2(j\omega)$ и третьего $K_3(j\omega)$ колебательных контуров.

2. Вычисление спектральной плотности исходного шумового шума $\xi(t)$:

$$S_{\text{ш}}(j\omega) = \int_{-\infty}^{\infty} \xi(t) e^{-j\omega t}\, dt.$$

3. Вычисление откликов шумового сигнала на выходах колебательных контуров:

$$\xi_1(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} K_1(j\omega) \cdot S_{\text{ш}}(j\omega) e^{j\omega t} d\omega\,;$$

$$\xi_2(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} K_2(j\omega) \cdot S_{\text{ш}}(j\omega) e^{j\omega t} d\omega;$$

$$\xi_3(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} K_3(j\omega) \cdot S_{\text{ш}}(j\omega) e^{j\omega t} d\omega.$$

4. Вычисление спектральной плотности шумового сигнала на выходах первого и второго аналоговых перемножителей:

$$S_{\text{шс1}}(j\omega) = \int_{-\infty}^{\infty} \xi_1(t) \cdot \xi_2(t) e^{-j\omega t}\, dt;$$

$$S_{\text{шс2}}(j\omega) = \int_{-\infty}^{\infty} \xi_3(t) \cdot \xi_2(t) e^{-j\omega t}\, dt.$$

5. Вычисление спектральной плотности шумового сигнала на выходе формирователя шумового сигнала: $S_{\text{шс}}(j\omega) = S_{\text{шс1}}(j\omega) + S_{\text{шс2}}(j\omega)$.

В соответствии с этим алгоритмом в программе математического моделирования Mathcad был произведен расчет спектральной плотности шумового сигнала на выходе первого аналогового перемножителя. Результаты расчета приведены на рис. 2.

Из рис. 2 можно видеть, что при уменьшении протяженности диапазона частот между центральными частотами несущего колебания и модулирующего сигнала, увеличивается протяженность диапазона частот, где происходит спад амплитуд спектральных составляющих шумового сигнала на выходе первого, впрочем, и второго аналоговых перемножителей сигнала. Кроме того, при уменьшении протяженности диапазона частот между центральными частотами несущего колебания и модулирующего сигнала в провале спектра амплитуды спектральных составляющих уменьшаются существенно, стремясь к нулю.

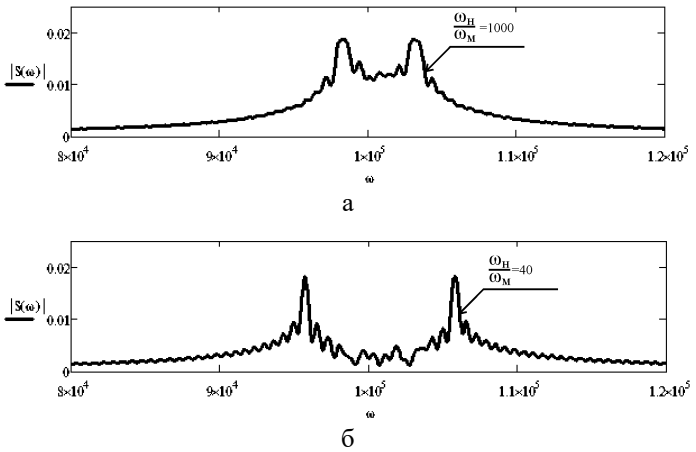

Рис. 2. Спектральная плотность шумового сигнала на выходе первого аналогового перемножителя сигналов при отличии центральных частот несущего колебания и модулирующего сигнала в 1000 раз (а) и в 40 раз (б)

На рис. 3 приведены графики отражающие зависимости ширины спектра шумового сигнала $\Delta f_{\text{АМ}}$ и ширины провала (спада) $\Delta f_{\text{С}}$ амплитуд спектральных составляющих шумового сигнала от центральной частоты модулирующего сигнала $f_{02} = f_{\text{м}} \cdot 10^2$ Гц.

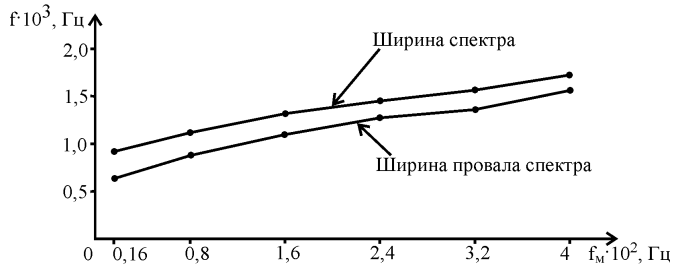

Рис. 3. Ширина спектра и ширина провала спектра шумового сигнала

Эти графики были получены в соответствии с алгоритмом, который приведен выше, и с использованием программы математического моделирования Mathcad, где выполнялся расчет спектральной плотности амплитуд шумового сигнала на выходе первого аналогового перемножителя.

Расчеты говорят о следующем. Значение центральной частоты несущего колебания близко к 10^5 рад/с ($f_{01} = 15924$ Гц) (рис. 2). Центральная частота модулирующего сигнала f_{02} изменяется от 16 Гц до 400 Гц. Добротности колебательных контуров первой и второй цепей избирательных по частоте равны $Q_1 = Q_2 = 20$. В этом случае ширина спектра шумового сигнала на выходе первого колебательного контура равна $2 \cdot \Delta f_1 = f_{01}/Q_1 = 796$ Гц. Ширины спектров модулирующего сигнала $2 \cdot \Delta f_2 = f_{02}/Q_2$ в зависимости от центральной частоты будут изменяться от 1,6 Гц ($f_{02} = 16$ Гц) до 40 Гц ($f_{02} = 400$ Гц). В данных случаях $\Delta f_1 = 388$ Гц, а Δf_2 изменяется от 0,8 Гц до 20 Гц.

Результаты моделирования для первого ($f_{02} = 16$ Гц) и второго случаев $f_{02} = 400$ Гц) ширины спектров $\Delta f_{\text{АМ}}$ шумового сигнала (рис. 3) по уровню 0,707 соответственно равны: 907 Гц и 1624 Гц. Для данных случаев выражение (1) дает

результаты: 809 Гц и 1616 Гц, соответственно. Можно видеть, что неточность результатов, полученных в соответствии с теоретическими исследованиями и путем математического моделирования в соответствии с использованным алгоритмом, для рассматриваемых двух крайних случаев составляет 12% и 0,49%. При этом, чем выше центральная частота модулирующего сигнала, тем более высокая точность расчетов достигается.

На рис. 4 представлены результаты схемотехнического моделирования спектральной плотности шумового сигнала на выходе рассматриваемого формирователя шумового сигнала.

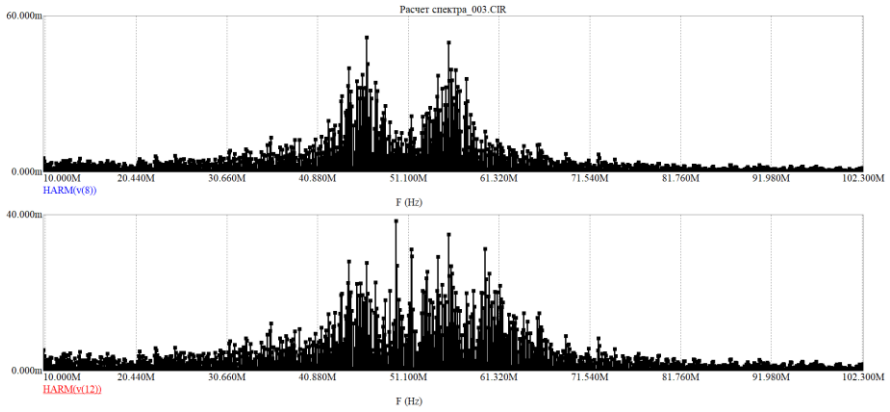

Рис. 4. Спектральная плотности шумового сигнала на выходе первого перемножителя сигналов (верхняя диаграмма) и на выходе формирователя шумового сигнала (нижняя диаграмма)

Моделирование выполнено в среде схемотехнического моделирования Micro-Cap. Центральная частота несущего колебания f_{01}, поступающего на первый аналоговый перемножитель сигналов, равна 50 МГц. Центральная частота несущего колебания f_{03}, поступающего на второй аналоговый перемножитель сигналов, согласно (2) равна 54,25 МГц. Центральная частота модулирующего сигнала f_{02} равна 6 МГц.

Результаты моделирования спектральной плотности шумового сигнала на выходе первого аналогового перемножителя сигналов и на выходе формирователя шумового сигнала говорят о следующем. Ширина спектра шумового сигнала по уровню 0,707 равна 16,2 МГц. В соответствии с (1) получено, что ширина спектра равна 17,5 МГц. Ширина частотного диапазона, где происходит спад амплитуд спектральных составляющих шумового сигнала, равна 6,9МГц, расчетные данные, согласно ранее проведенного анализа, дает цифру 7 МГц. Проведенный сравнительный анализ ширин спектра шумового сигнала говорит о том, что для оценки ширины спектра шумового сигнала и диапазона частот, где происходит провал амплитуд спектральных составляющих шумового сигнала, вполне можно использовать выражения, полученные в работе. Следует отметить, что формирование шумового сигнала на выходе устройства за счет использования двух аналоговых перемножителей сигналов, позволяет получить почти в два раза более широкий по частоте спектр шумового сигнала, в сравнении с тем, когда в качестве несущего колебания используется гармонический сигнал.

Заключение. Исследования, представленные в работе, говорят о следующем:

♦ теоретические результаты, отражающие процесс управления шириной спектра шумового сигнала на выходе формирователя шума, хорошо согласуются с экспериментальными данными, полученными в процессе моделирования, при этом, чем выше центральная частота модулирующего сигнала, тем более высокая точность расчетов может быть достигнута;

♦ рассмотренный в работе формирователь шумового сигнала, где формирование шумового сигнала осуществляется с использованием амплитудной модуляции, может быть использован в многоканальных генераторах шумового сигнала в качестве источника шумового сигнала с перестраиваемой по частоте шириной спектра в зависимости от центральной частоты модулирующего сигнала, в роли которого используется квазигармонический шум;

♦ использование в формирователе шумового сигнала двух аналоговых перемножителей сигналов позволяет исключить провал амплитуд спектральных составляющих шумового сигнала в широком диапазоне частот, что способствует получению равномерного по амплитуде спектра шумового сигнала на выходе устройства при выполнении операции изменении ширины спектра шумового сигнала;

♦ показано, что использование квазигармонических шумовых сигналов в качестве несущего колебания и модулирующего сигнала, позволяет достичь существенного увеличения ширины спектра шумового сигнала на выходе устройства, в сравнении с тем, когда в качестве несущего колебания используется гармонический сигнал.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Вим ван Эйк*. Электромагнитное излучение видеодисплейных модулей: риск перехвата информации. – 1985. – URL: https://revolution.allbest.ru/radio/00568869_0.html (дата обращения 24.11.2020).
2. *Daniel Genkin, Lev Pachmanov, Itamar Pipman.* Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation February 27, 2015. – URL: www.cs.tau.ac.il/~tromer/papers/radioexp.pdf (дата обращения 24.11.2020).
3. АНБ скомпрометировало протокол Диффи-Хеллмана? – URL: https://habr.com/ru/post/356870 (дата обращения: 24.11.2020).
4. *Хорев А.А.* Математическая модель обнаружения побочных электромагнитных излучений видеосистемы компьютера оптимальным приемником // Вопросы защиты информации. – 2014. – № 1 (104). – С. 65-71.
5. *Голиков А.М.* Защита информации от утечки по техническим каналам: учеб. пособие. – Томск: ТУСУР, 2015. – 256 с.
6. *Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.* Технические средства и методы защиты информации: учебник для вузов / под ред. А.П. Зайцева и А.А. Шелупанова. – М.: Изд-во «Машиностроение», 2009. – 508 с.
7. *Меньшаков Ю.К.* Защита объектов и информации от технических средств разведки: учеб. пособие. – М.: РГГУ, 2002. – 399 с.
8. *Маслов О.Н., Соломатин М.А., Василевский А.Д.* Тестовые сигналы для анализа ПЭМИН персональных ЭВМ // Инфокоммуникационные технологии. – 2007. – Т. 5, № 2. – С. 79-82.
9. *Маслов О.Н., Соломатин М.А., Егоренков В.Д.* Тестовые сигналы для анализа ПЭМИН периферийных устройств персональных ЭВМ // Инфокоммуникационные технологии. – 2007. – Т. 5, № 2. – С. 82-84.
10. *Иванов В.П.* Информационная безопасность, проблема ПЭМИН, генераторы радиошума // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 126-134.
11. *Бузов Г.А., Калинин С.В., Кондратьев А.В.* Защита от утечки информации по техническим каналам: учеб. пособие. – М.: Горячая линия, 2005. – 416 с.
12. *Газизов Т.Р.* Электромагнитная совместимость и безопасность радиоэлектронной аппаратуры: учеб. пособие. – Томск: «ТМЛ-Пресс», 2007. – 256 с.

13. *Барсуков В.С.* Безопасность: технологии, средства, услуги. – М.: КУДИЦ ОБРАЗ, 2001. – 496 с.
14. Патент RU №2170493 Российская Федерация, МПК H04K 3/00. Устройство радиомаскировки / Безруков В.А., Иванов В.П., Калашников В.С., Лебедев М.Н.; заявл. 15.05.2000; опубл. 10.07.2001, БИ № 19.
15. Система для защиты от утечки информации по каналам ПЭМИН "Гром-ЗИ-4Б". – URL: https://pro-spec.ru/catalog/generatory-shuma/sistema-dlya-zashchity-ot-utechki-informatsii-po-kanalam-pemin-grom-zi-4b (дата обращения: 24.11.2020).
16. SEL SP-21 "Баррикада" генератор пространственного зашумления. – URL: http://www.spectr-sks.ru/product/8535 (дата обращения: 24.11.2020).
17. *Акимов В.И., Барсуков А.Н., Данилов Н.С., Суворов П.А.* Предложения по созданию адаптивных генераторов шума системы зашумления информативных сигналов средств электронной вычислительной техники // Специальная техника. – 2012. – № 3. – 6 с. – URL: https://elibrary.ru/item.asp?id=17781926& (дата обращения 24.11.2020).
18. Патент RU №2114513 Российская Федерация, МПК H04K 3/00. Способ защиты информационного обмена в локальной системе радиосвязи / Павлов Ю.С.; заявл. 25.07.1995; опубл. 27.06.1998, БИ № 18.
19. Патент RU № 2421917 Российская Федерация, МПК H04K1/04, H03B29/00. Способ защиты системы обработки информации от побочных электромагнитных излучений, устройство для реализации способа и генератор шумового сигнала для реализации устройства / Демин В.М., Лепеха Ю.П., Поярков Л.А.; заявл. 15.04.10; опубл. 20.06.11, БИ № 17.
20. Патент RU № 2669065 Российская Федерация, МПК H03B 29/00. Устройство для защиты автоматизированных систем от утечки информации по каналам побочных электромагнитных излучений / Щербаков В.А., Хорев А.А.; заявл 13.12.17; опубл. 08.10.18, БИ № 28.
21. *Землянухин П.А.* Многоканальный адаптивный генератор шума для маскирования ПЭМИН // Известия ЮФУ. Технические науки. – 2016. – № 9. – С. 82-93.
22. *Бехтин М.А.* Система обнаружения побочных информационных электромагнитных излучений технических средств: автореф. дисс. … канд. техн. наук. – М., 2009. – 23 с.
23. *Вертилевский Н.В.* Разработка концепции модульного построения трансформируемой системы защиты информации от утечки по техническим каналам: автореф. дисс. … канд. техн. наук. – Владимир, 2008. – 24 с.
24. *Zemlyanuchin P., Suhoveev A.* Adaptive noise generator for masking side electromag-netic radiation and interference. Second International Conference on Futuristic Trends in Networks and Computing Technologies (FTCNT-2019). Jaypee University of Information Technology, Waknaghat, India and C-DAC, Mohali, India. 22-23 November 2019. – URL: https://www.springer.com/us/book/9789811544507.
25. *Куприянов А.И.* Радиоэлектронная борьба. – М.: Вузовская книга, 2013. – 360 с.
26. Патент на полезную модель RU № 193698 Российская Федерация, МПК H03B 29/00, H04K 3/00. Формирователь шумового сигнала / Землянухин П.А., Очиров Ц.В.; заявл 30.04.2019; опубл. 11.11.2019, БИ № 32.

REFERENCES

1. *Vim van Eyk*. Elektromagnitnoe izluchenie videodispleynykh moduley: risk perekhvata informatsii [Electromagnetic radiation of video display modules: risk of information interception], 1985. Available at: https://revolution.allbest.ru/radio/00568869_0.html (accessed 24 November 2020).
2. *Daniel Genkin, Lev Pachmanov, Itamar Pipman.* Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation February 27, 2015. Available at: www.cs.tau.ac.il/~tromer/papers/radioexp.pdf (accessed 24 November 2020).
3. ANB skomprometirovalo protokol Diffi-Khellmana? [The NSA compromised the Diffie-Hellman Protocol?]. Available at: https://habr.com/ru/post/356870 (accessed 24 November 2020).
4. *Khorev A.A.* Matematicheskaya model' obnaruzheniya pobochnykh elektromagnitnykh izlucheniy videosistemy komp'yutera optimal'nym priemnikom [Mathematical model of detection of side electromagnetic radiation of a computer video system by an optimal receiver], *Voprosy zashchity informatsii* [Information security issues], 2014, No. 1 (104), pp. 65-71.
5. *Golikov A.M.* Zashchita informatsii ot utechki po tekhnicheskim kanalam: ucheb. posobie [The Protection of information from leakage via technical channels: the manual]. Tomsk: TUSUR, 2015, 256 p.

6. *Zaytsev A.P., SHelupanov A.A., Meshcheryakov R.V. i dr. T*ekhnicheskie sredstva i metody zashchity informatsii: uchebnik dlya vuzov [Technical means and methods of information protection: textbook for universities], ed. by A.P. Zaytseva and A.A. Shelupanova. Moscow: Izdvo «Mashinostroenie», 2009, 508 p.
7. *Men'shakov Yu.K.* Zashchita ob"ektov i informatsii ot tekhnicheskikh sredstv razvedki: ucheb. posobie [Protection of objects and information from technical means of intelligence: textbook]. Moscow: RGGU, 2002, 399 p.
8. *Maslov O.N., Solomatin M.A., Vasilevskiy A.D.* Testovye signaly dlya analiza PEMIN personal'nykh EVM [Test signals for analyzing SERaI of personal computers], *Infokommunikatsionnye tekhnologii* [Infocommunication technologies], 2007, Vol. 5, No. 2, pp. 79-82.
9. *Maslov O.N., Solomatin M.A., Egorenkov V.D.* Testovye signaly dlya analiza PEMIN periferiynykh ustroystv personal'nykh EVM [Test signals for the analysis of SERaI of peripherals of personal computers], *Infokommunikatsionnye tekhnologii* [Infocommunication technologies], 2007, Vol. 5, No. 2, pp. 82-84.
10. *Ivanov V.P.* Informatsionnaya bezopasnost', problema PEMIN, generatory radioshuma [Information security, the problem of SERaI, radionoise generators], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counteraction to threats of terrorism], 2009, No. 13, pp. 126-134.
11. *Buzov G.A., Kalinin S.V., Kondrat'ev A.V.* Zashchita ot utechki informatsii po tekhnicheskim kanalam: ucheb. posobie [Protection from information leakage through technical channels: textbook]. Moscow: Goryachaya liniya, 2005, 416 p.
12. *Gazizov T.R.* Elektromagnitnaya sovmestimost' i bezopasnost' radioelektronnoy apparatury: ucheb. posobie [Electromagnetic compatibility and safety of radio electronic equipment: textbook]. Tomsk: «TML-Press», 2007, 256 p.
13. *Barsukov V.S.* Bezopasnost': tekhnologii, sredstva, uslugi [Security: technologies, tools, services]. Moscow: KUDITS OBRAZ, 2001, 496 p.
14. *Bezrukov V.A., Ivanov V.P., Kalashnikov B.C., Lebedev M.N.* Ustroystvo radiomaskirovki [Device of radio deception]. Patent RU No. 2170493 Russian Federation, IPC H04K 3/00; declared 15.05.2000; publ. 10.07.2001, BI No. 19.
15. Sistema dlya zashchity ot utechki informatsii po kanalam PEMIN "Grom-ZI-4B" [System for protection against information leakage through SERaI channels "Grom-ZI-4B"]. Available at: https://pro-spec.ru/catalog/generatory-shuma/sistema-dlya-zashchity-ot-utechki-informatsii-po-kanalam-pemin-grom-zi-4b (accessed 24 November 2020).
16. SEL SP-21 "Barrikada" generator prostranstvennogo zashumleniya [SEL SP-21 "Barricada" spatial noise generator]. Available at: http://www.spectr-sks.ru/product/8535 (accessed 24 November 2020).
17. *Akimov V.I., Barsukov A.N., Danilov N.S., Suvorov P.A.* Predlozheniya po sozdaniyu adaptivnykh generatorov shuma sistemy zashumleniya informativnykh signalov sredstv elektronnoy vychislitel'noy tekhniki [Proposals for the creation of adaptive noise generators for the noise reduction system of informative signals of electronic computer equipment], *Spetsial'naya tekhnika* [Special equipment], 2012, No. 3, 6 p. Available at: https://elibrary.ru/item.asp?id=17781926& (accessed 24 November 2020).
18. *Pavlov Yu.S.* Sposob zashchity informatsionnogo obmena v lokal'noy sisteme radiosvyazi [Method of protection of information exchange in the local radio system]. Patent RU No. 2114513 Russian Federation, IPC H04K 3/00; declared 25.07.1995; publ. 27.06.1998, BI No. 18.
19. *Demin V.M., Lepekha Yu.P., Poyarkov L.A.* Sposob zashchity sistemy obrabotki informatsii ot pobochnykh elektromagnitnykh izlucheniy, ustroystvo dlya realizatsii sposoba i generator shumovogo signala dlya realizatsii ustroystva [The protection method of an information processing system from side electromagnetic radiation, the device for implementing the method and the generator of the noise signal for the implementation of devices], Patent RU No. 2421917 Russian Federation, IPC H04K1/04, H03B29/00; declared 15.04.10; publ. 20.06.11, BI No. 17.
20. *Shcherbakov V.A., Khorev A.A.* Ustroystvo dlya zashchity avtomatizirovannykh sistem ot utechki informatsii po kanalam pobochnykh elektromagnitnykh izlucheniy [Device for protection of automated systems from information leakage through channels of side electromagnetic radiation]. Patent RU No. 2669065 Russian Federation, IPC 29/00 H03B; declared 13.12.17; publ. 08.10.18, BI No. 28.

21. *Zemlyanukhin P.A.* Mnogokanal'nyy adaptivnyy generator shuma dlya maskirovaniya PEMIN [Multichannel noise generator to mask SERaI], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2016, No. 9, pp. 82-93.
22. *Bekhtin M.A.* Sistema obnaruzheniya pobochnykh informatsionnykh elektromagnitnykh izlucheniy tekhnicheskikh sredstv: avtoref. diss. … kand. tekhn. nauk [System for detecting side information electromagnetic radiation of technical means: autoabstract cand. of eng. sc. diss.]. Moscow, 2009, 23 p.
23. *Vertilevskiy N.V.* Razrabotka kontseptsii modul'nogo postroeniya transformiruemoy sistemy zashchity informatsii ot utechki po tekhnicheskim kanalam: avtoref. diss. … kand. tekhn. nauk [Development of the concept of modular construction of a transformable information protection system against leakage through technical channels: autoabstract cand. of eng. sc. diss.]. Vladimir, 2008, 24 p.
24. *Zemlyanuchin P., Suhoveev A.* Adaptive noise generator for masking side electromag-netic radiation and interference. Second International Conference on Futuristic Trends in Networks and Computing Technologies (FTCNT-2019). Jaypee University of Information Technology, Waknaghat, India and C-DAC, Mohali, India. 22-23 November 2019. Available at: https://www.springer.com/us/book/9789811544507.
25. *Kupriyanov A.I.* Radioelektronnaya bor'ba [Radio-electronic struggle]. Moscow: Vuzovskaya kniga, 2013, 360 p.
26. *Zemlyanukhin P.A., Ochirov Ts.V.* Formirovatel' shumovogo signala [A noise signal conditioner]. Patent for utility model RU No. 193698 Russian Federation, IPC 29/00 H03B, H04K 3/00; declared 30.04.2019; publ. 11.11.2019, BI No. 32.

Статью рекомендовал к опубликованию д.т.н., профессор С.Г. Капустян.

Землянухин Петр Андреевич – Южный федеральный университет, e-mail: pazemlyanuchin@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89185061318; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; доцент.

Кондратьев Александр Владиславович – e-mail: alkondratev@sfedu.ru; тел.: 89888979234; кафедра информационной безопасности телекоммуникационных систем; студент.

Свидельский Сергей Сергеевич – e-mail: svidelskiy@sfedu.ru; тел.: 89281410341; кафедра высшей математики; аспирант.

Zemlyanukhin Petr Andreevich – Southern Federal University; e-mail: pazemlyanuchin@sfedu.ru; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +79185061318. the department of information security of telecommunication systems; associate professor, cand. of eng. sc.

Kondratiev Alexandr Vladislavovich – e-mail: alkondratev@sfedu.ru; phone: +79888979234; the department of information security of telecommunication systems; student.

Svidelsky Sergey Sergeevich – e-mail: svidelskiy@sfedu.ru; phone: +79281410341; the department of higher mathematics; postgraduate student.

УДК 004.4'42 DOI 10.18522/2311-3103-2020-5-123-130

М.Ю. Поленов, А.О. Курмалеев

ИСПОЛЬЗОВАНИЕ ИНЖИНИРИНГА ЗНАНИЙ ДЛЯ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ТРАНСЛЯЦИИ МОДЕЛЕЙ*

Рассмотрена проблема повторного использования ранее разработанных программных моделей сложных систем и их компонентов, возникающая перед исследователями при необходимости перехода к новым средствам моделирования. В качестве решения поставленной задачи была разработана программная среда –Мультитранслятор, которая позво-

* Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 19-07-00936.

лила реализовать многоязыковую трансляцию исходных кодов моделей в требуемый формат целевой среды моделирования при помощи создаваемых трансляционных модулей. Далее на основе Мультитранслятора было разработано клиент-серверное приложение – Распределенная библиотека моделей, которая наряду с функцией трансляции моделей выполняла функцию их сетевого хранения и доступа, обеспечивая распределенную реализацию подхода. Развитие подхода и Распределенной библиотеки моделей выполнялось в направлении автоматизации трансляции и разрешения исключительных случаев, возникающих при трансляции моделей, вызванных недостаточностью входных данных или неопределенностью решений по конвертации моделей, возникающей при наличии слишком большого числа исходов при разборе. Для решения данной задачи было предложено использовать экспертную систему с базой знаний. В качестве основного процесса синтеза необходимых знаний для базы знаний в работе рассмотрен инжиниринг знаний. Предложены следующие источники получения знаний в ходе разработки экспертной системы: трансляционный модуль Мультитранслятора; техническая документация входного/выходного языков описания моделей для трансляции; расширенные и дополнительные публикации по описанию данных языков; эксперты по языкам описания моделей для трансляции. Далее рассмотрены основные этапы инжиниринга знаний: определение стратегии приобретения знаний; идентификация элементов знаний; создание системы классификации знаний; разработка подробной функциональной компоновки; предварительное планирование процессов передачи управления; определение требований к системе. Полученные результаты позволят расширить функциональные возможности распределенной библиотеки моделей при трансляции моделей при помощи экспертной системы и эффективной обработки неопределенностей, возникающих в процессе трансляции.

Трансляция моделей; трансляционный модуль; экспертная система; инжиниринг знаний; источники знаний.

M.Yu. Polenov, A.O. Kurmaleev

KNOWLEDGE ENGINEERING USE FOR THE INTELLECTUAL SUPPORT OF MODELS' TRANSLATION

In the work the problem of reuse of earlier developed software models in complex systems and their components, arising before researchers in case of necessity of transition to new modeling tools, is considered. As a solution to this problem, a Multitranslator software environment was developed, which made it possible to implement multilanguage translation of models' source codes into the required format of the target modeling environment using the created translation modules. Then, based on the Multitranslator, a client-server application was developed – a Distributed models library, which, along with the models translation function, performed the function of their network storage and access, providing a distributed implementation of the approach. The development of the approach and the Distributed models library was carried out in the direction of translation automation and resolving exceptional cases that occur during model translation caused by insufficient input data or uncertainty in model conversion decisions that occur when there are too many outcomes during parsing. To solve this problem, it was proposed to use an expert system with a knowledge base. Knowledge engineering is considered as the main process of synthesis of necessary knowledge for the knowledge base. The following sources of knowledge acquisition during the development of the expert system are proposed: the translation module of Multitranslator; technical documentation of input/output languages for describing models for translation; extended and additional publications on describing these languages; experts on languages for describing models for translation. The main stages of knowledge engineering are considered next: defining a knowledge acquisition strategy; identifying knowledge elements; creating a knowledge classification system; developing a detailed functional layout; pre-planning of control transfer processes; and defining system requirements. The results obtained will allow expanding the functionality of the Distributed models library when translating models using an expert system and efficient processing of uncertainties that arise during translation.

Models' translation; translation module; expert system; knowledge engineering; knowledge sources.

Введение. В области моделирования сложных систем наблюдается постоянное совершенствование используемых инструментальных программных средств моделирования, а также разработка новых средств для различных доменов [1]. Многообразие существующих пакетов моделирования, их развитие и появление новых средств приводит к задаче конвертации (трансляции) существующих моделей для их дальнейшего использования исследователями в новых средствах в силу необходимости сохранения и повторного использования ранее разработанных и отлаженных моделей сложных систем и их компонент. Однако, данный процесс приводит к значительным дополнительным временным затратам для каждой такой конвертации, как на изучение нового средства моделирования, языка и формата представления моделей, так и для собственно трансляции существующих моделей в требуемый формат.

Для решения данной проблемы была поставлена задача разработки средств для конвертации моделей между исходной и целевой средами моделирования. В результате решения этой задачи была разработана программная среда многоязыковой трансляции, названная Мультитранслятором (МТ) [2]. Основой процесса конвертации моделей является трансляционный модуль (ТМ) Мультитранслятора, представляющий собой набор правил описания грамматик исходного языка моделирования на языке описания грамматик и генерации выходного кода моделей действий преобразования на языке описания действий. Мультитранслятор реализован как среда разработки трансляционных модулей, а также как среда конвертации моделей, использующая уже разработанные трансляционные модули. Очевидно, что для большинства исследователей в основном востребована функция конвертации моделей, поскольку при разработке ТМ необходимы как знания самой среды, входного и выходного языков описания моделей, так и языков описания трансляционного модуля Мультитранслятора [3, 4]. В процессе работы и использования МТ также было решено создать версию Мультитранслятора в виде клиент-серверного приложения на основе архитектуры распределенных систем [5], где сам МТ находился бы на стороне сервера и проводил бы трансляцию моделей для удаленных исследователей-клиентов, выполняя тем самым распределенную реализацию подхода к повторному использованию моделей [6]. Также было решено дополнительно реализовать в данном клиент-серверном приложении функцию распределенного хранилища (репозитария) моделей, что значительно упрощало совместный доступ исследователей к исходным и оттранслированным моделям.

На основе использования перечисленных подходов и объединения функций трансляции и хранения исходных и конвертированных моделей была создана Распределенная библиотека моделей [7]. В данной библиотеке на стороне исследователя-клиента используется упрощенный пользовательский интерфейс по подключению к серверу, выбору трансляционного модуля для конвертации, выбору исходных моделей из локального или серверного хранилища, и по завершению процедуры трансляции, доступу к коду конвертированной модели на выходном языке для целевой среды моделирования.

Развитие подхода и Распределенной библиотеки моделей выполнялось в направлении автоматизации трансляции и разрешения исключительных случаев, возникающих при трансляции моделей, вызванных недостаточностью входных данных или неопределенностью решений по конвертации моделей, возникающей при наличии слишком большого числа исходов при разборе.

Для решения данной задачи было предложено использовать экспертную систему (ЭС) [8]. Основным элементом при построении экспертной системы [9] является база знаний [10], наполнение которой является многоэтапным процессом, сопряженным с разработкой самой ЭС [11, 12]. Основой базы являются знания, ко-

торые будут формировать правила в виде обработчиков-объектов или простых правил-фактов для начальных версий экспертной системы. Основным процессом синтеза необходимых знаний для базы знаний является инжиниринг знаний, который и рассматривается в данной работе.

Знания для инжиниринга. Рассмотрим основные этапы сбора знаний для реализации предлагаемого подхода.

Прежде всего необходимо вынести требования к получаемым знаниям [13] по многоязыковой трансляции для экспертной системы, в этот этап входит определение источника знаний, оценка важности источников, оценка их доступности и, как итог, выбор источников для их использования в ходе разработки.

В ходе разработки и создания средств многоязыковой трансляции в качестве основы конвертации исходных кодов моделей использовались трансляционные модули Мультитранслятора. Трансляционный модуль агрегирует все знания, которые использует МТ в ходе процесса трансляции моделей, и декомпозировав его, можно заложить фундамент базы знаний. Этот источник является наиболее достоверным и доступным, поскольку он неоднократно проверялся при разработке различных трансляционных модулей. У этого источника знаний можно установить самый высокий приоритет и использовать в качестве основы предлагаемого подхода.

На следующем этапе должна быть рассмотрена официальная техническая документация исходного языка описания моделей и выходного языка, на котором генерируется результат трансляции, поскольку такой источник является столь же достоверным, как и трансляционный модуль МТ последней версии. По важности этот источник следует за трансляционным модулем и не уступает ему по доступности и достоверности.

После официальной технической документации необходимо рассмотреть основные публикации по расширенному описанию этой документации с практическими примерами, которые менее важны и достоверны по сравнению с технической документацией, в случае с последними редакциями книг, и средне доступны в связи в необходимостью их поиска в электронных библиотеках или покупки электронных или печатных версий, в случае недоступности электронных версий последних редакций.

И завершающим этапом идет получение знаний от экспертов. Этот источник является менее важным, чем предыдущие, но после завершения предыдущих этапов может оказаться наиболее значительным для случаев, когда техническая документация совместно с книгами по описанию языков, необходимых для трансляционного модуля, окажутся недостаточными для разрешения всех найденных исключительных случаев трансляции. Здесь необходимо отметить, что знания трансляционного модуля являются базовыми и они недостаточны для разрешения исключительных случаев трансляции моделей. Этот источник является наименее доступным и потребует приглашения специалистов со стороны и применения подхода менеджмента знаний по отношению к сбору информации от экспертов для большей достоверности информации.

Таким образом, можно перечислить этапы и источники получения знаний в ходе разработки экспертной системы:

1) трансляционный модуль МТ;
2) техническая документация входного/выходного языков трансляции;
3) расширенные и дополнительные публикации по описанию языков;
4) эксперты по языкам описания моделей для трансляции.

В итоге, резюмируя приведенную информацию, можно отобразить ее в виде структуры, отображающей взаимодействие между компонентами Распределенной библиотеки моделей и экспертной системой, используемой в процессе трансляции моделей, представленной на рис. 1.

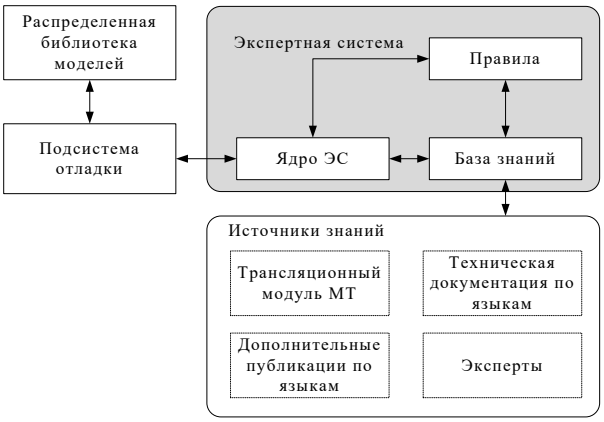

Рис. 1. Структура системы трансляции и организации наполнения базы знаний экспертной системы

Использование инжиниринга знаний для многоязыковой трансляции. В начале описания предлагаемого подхода необходимо уточнить, что представляет собой инжиниринг знаний. В качестве определения можно рассматривать следующее: инжиниринг знаний – это процесс разработки систем, основанных на знаниях любой отрасли [14]. Он в общем виде состоит из определения и выбора источника знаний с последующим их приобретением, анализом и извлечением [15]. Вопросы определения и выбора источников были рассмотрены в предыдущем разделе.

С учетом специфики решения поставленной задачи, приобретение знаний состоит из следующих базовых этапов [16]:

- определение стратегии приобретения знаний;
- идентификация элементов знаний;
- создание системы классификации знаний;
- разработка подробной функциональной компоновки;
- предварительное планирование процессов передачи управления;
- определение требований к системе.

Рассмотрим подробнее суть предлагаемого подхода и реализацию данных этапов с учетом специфики поставленной задачи автоматизации трансляции моделей при использовании экспертной системы.

Определение стратегии приобретения знаний и идентификация элементов знаний

Поскольку в случае нашей задачи, основывающейся на формализованных языках [17, 18], все достоверные источники знаний известны заранее, то этап идентификации уже был пройден до момента определения стратегии получения знаний. Следовательно, на данном этапе выполняется описание процедур получения знаний и используемых методов для каждого из источников:

1. Источник – трансляционный модуль Мультитранслятора. Выполняется анализ и индукция правил трансляции, заложенных в трансляционном модуле в знания общего вида для последующего синтеза базовых правил экспертной системы.

2. Источник – техническая документация входного/выходного языков описания моделей для трансляции. Выполняется анализ и дедукция языков, начиная с их возможностей (таких как реализация подходов к разработке в рамках языковых структур, например, таких как объекты и функции) для подтверждения и синтеза новых правил и расширения существующих (например, добавления новых языковых конструкций, не приведенных в определенном контексте в документации), на основе уже полученных из предыдущего источника.

3. Источник – расширенные и дополнительные публикации по языковой документации. Выполняется более глубокий анализ структур языка и существующих правил, сгенерированных ранее, для превентивного синтеза правил, включающих в себя обработку возможных исключительных ситуаций нарушения процесса трансляции моделей.

4. Источник – эксперты по языкам описания моделей для трансляции. После запуска финального тестирования выполняется анализ результатов и на основе полученных исключительных случаев принимается решение о привлечении экспертов. Для каждого возникшего исключительного случая необходимо проводить структурированное интервью с составлением карты знания [19] для исключительного случая трансляции, где эксперту будет предоставлен полный исходный код модели или его фрагмент, не прошедший трансляцию.

Создание системы классификации знаний

Перед дополнением правилами базы знаний экспертной системы все полученные знания должны быть классифицированы и упорядочены с помощью иерархических групп [20]. При выполнении каждого этапа, описанного в предыдущем разделе, знания сразу же записываются в техническую документацию проекта экспертной системы и базы знаний, и лишь после этого происходит переход к этапу наполнения базы знаний необходимыми правилами.

Разработка подробной функциональной компоновки

На основе созданных классификаций составляется программная документация и происходит реализация базовой структуры ЭС и правил согласно принятым стандартам по проекту и соответствующей задачи технической реализации.

Предварительное планирование процессов передачи управления

Процессы передачи управления представляют собой функциональную архитектуру базы знаний, алгоритмы активизации групп правил. Данный этап является связывающей основой для базы знаний, управленческой структурой ЭС.

Определение требований к системе

После создания базы знаний и экспертной системы на каждом из четырех описанных выше этапов, в нашем случае будет составлена карта покрытия исключительных случаев. На основе этой карты описываются соответствующие правила и подбираются исходные коды моделей с различными вариациями таких исключительных случаев.

Заключение. В результате проведенных исследований был предложен и реализован подход к интеллектуальной поддержке трансляции моделей с целью обеспечения возможности их повторного использования. Подход основан на применении разработанной распределенной библиотеки моделей в качестве хранилища и средства трансляции внешних моделей для различных сред моделирования. Конвертация моделей реализована на основе использования модулей перевода моделей разработанной ранее среды трансляции – Мультитранслятора с поддержкой экспертной системы. Формирование необходимых знаний для базы знаний экспертной системы производится на основе инжиниринга знаний, рассмотренного в данной работе.

Полученные результаты позволят расширить функциональные возможности распределенной библиотеки моделей при трансляции внешних моделей за счет использования экспертной системы и эффективной обработки неопределенностей, возникающих в процессе трансляции, что в итоге приведет к сокращению временных затрат на конвертацию внешних моделей при моделировании сложных систем.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Колесов Ю.Б., Сениченков Ю.Б.* Моделирование систем. Объектно-ориентированный подход. – СПб.: БХВ-Петербург, 2017. – 186 с.
2. *Чернухин Ю.В., Гузик В.Ф., Поленов М.Ю.* Подход к формированию внешних библиотек сред виртуального моделирования на базе мультиязыковой трансляции // Вестник компьютерных и информационных технологий. – 2008. – № 10. – С. 2-12.
3. *Чернухин Ю.В., Гузик В.Ф., Поленов М.Ю.* Многоязыковая трансляция средств виртуального моделирования. – Ростов-на-Дону: Изд-во ЮНЦ РАН, 2009. – 368 с.
4. *Chernukhin Yu., Guzik V., Polenov M.* Multilanguage Translation Usage in Toolkit of Modeling Systems // WIT Transactions on Information and Communication Technologies. – 2014. – Vol. 58. – P. 397-404.
5. *Coulouris G., Dollimore J., Kindberg T., Blair G.* Distributed systems. Concepts and Design. Fifth Ed. – Addison-Wesley, 2012. – 1048 p.
6. *Robinson S., Nance R.E., Paul R.J., et al.* Simulation model reuse: definitions, benefits and obstacle // Simulation Modelling Practice and Theory. – 2004. – Vol. 12. – P. 479-494.
7. *Polenov M., Guzik V., Gushanskiy S., Kurmaleev A.* Development of the Translation Tools for Distributed Storage of Models // Proceedings of 9th International Conference on Application of Information and Communication Technologies (AICT 2015). – IEEE Press, 2015. – P. 30-34.
8. *Polenov M., Gushanskiy S., Kurmaleev A.* Synthesis of Expert System for Distributed Storage of Models // Advances in Intelligent Systems and Computing. – 2017. – Vol. 575. – P. 220-228.
9. *Waterman D.A.* A Guide to Expert Systems. – Addison-Wesley, 1986.
10. *Frost R.* Introduction to Knowledge Base Systems. – Macmillan Pub. Co., 1986. – 677 p.
11. *Buchanan B.G., Duda R.D.* Principles of rule-based expert system // Advances in Computers. – 1983. – Vol.22. – P.163-216.
12. *Джексон П.* Введение в экспертные системы. – 3-е изд. – Вильямс, 2001. – 624 с.
13. *Durkin J.* Expert Systems: Design and Development. – Macmillan Coll Div, 1994. – 800 p.
14. *Kendal S., Creen M.* An introduction to knowledge engineering. – Springer, 2007. – 300 p.
15. *Gonzalez A.J., Dankel D.D.* The Engineering of Knowledge-based Systems: Theory and Practice. – Prentice-Hall, 2000. – 523 p.
16. *Giarratano J.C., Riley G.D.* Expert Systems: Principles and Programming. 4th ed. – Course Technology, 2004. – 856 p.
17. *Rozenberg G., Salomaa A.* Handbook of Formal Languages. Vol. 1. – Springer, 1997. – 328 p.
18. *Scott M.L.* Programming Language Pragmatics. 4th ed. – Morgan Kaufmann, 2015. – 992 p.
19. *Boose J.H.* A survey of knowledge acquisition techniques and tools // Knowledge Acquisition. – 1989. – Vol.1. – P. 3-37.
20. *McGraw K.L., Harbison-Briggs K.* Knowledge Acquisition: Principles and Guidelines. – Prentice Hall, 1989. – 250 p.

REFERENCES

1. *Kolesov Yu.B., Senichenkov Yu.B.* Modelirovaniye sistem. Ob"yektno-oriyentirovannyy podkhod [System modeling. Object oriented approach]. Saint Petersburg: BHV-Petersburg, 2017, 186 p.
2. *Chernukhin Yu., Guzik V., Polenov M.* Podkhod k formirovaniyu vneshnikh bibliotek sred virtual'nogo modelirovaniya na baze mul'tiyazykovoy translyatsii [An approach to the development of external libraries of virtual modeling environments based on multilanguage translation], *Vestnik komp'iuternykh i informatsionnykh tekhnologii* [Herald of computer and information technologies], 2008, No. 10, pp. 2-12.
3. *Chernukhin Yu., Guzik V., Polenov M.* Mnogoyazykovaya translyatsiya sredstv virtual'nogo modelirovaniya [Multilanguage Translation for Virtual Modeling Environments]. Rostov-on-Don: Publishing house of Southern Scientific Center of Russian Academy of Sciences, 2009, 368 p.
4. *Chernukhin Yu., Guzik V., Polenov M.* Multilanguage Translation Usage in Toolkit of Modeling Systems, *WIT Transactions on Information and Communication Technologies*, 2014, Vol. 58, pp. 397-404.
5. *Coulouris G., Dollimore J., Kindberg T., Blair G.* Distributed systems. Concepts and Design, Fifth Ed., Addison-Wesley, 2012, 1048 p.

6. *Robinson S., Nance R.E., Paul R.J., et al.* Simulation model reuse: definitions, benefits and obstacle, *Simulation Modelling Practice and Theory*, 2004, Vol. 12, pp. 479-494.
7. *Polenov M., Guzik V., Gushanskiy S., Kurmaleev A.* Development of the Translation Tools for Distributed Storage of Models, *Proc. of 9th International Conference on Application of Information and Communication Technologies (AICT 2015)*, IEEE Press, 2015, pp. 30-34.
8. *Polenov M., Gushanskiy S., Kurmaleev A.* Synthesis of Expert System for Distributed Storage of Models, *Advances in Intelligent Systems and Computing*, Springer, 2017, Vol. 575, pp. 220-228.
9. *Waterman D.A.* A Guide to Expert Systems. Addison-Wesley, 1986.
10. *Frost R.* Introduction to Knowledge Base Systems. Macmillan Pub. Co., 1986, 677 p.
11. *Buchanan B.G., Duda R.D.* Principles of rule-based expert system. *Advances in Computers*, 1983, Vol. 22, pp.163-216.
12. *Dzhekson P.* Vvedenie v ekspertnye sistemyи [Introduction to Expert Systems]. 3rd ed. Vil'yams, 2001, 624 p.
13. *Durkin J.* Expert Systems: Design and Development. Macmillan Coll Div, 1994, 800 p.
14. *Kendal S., Creen M.* An introduction to knowledge engineering. Springer, 2007, 300 p.
15. *Gonzalez A.J., Dankel D.D.* The Engineering of Knowledge-based Systems: Theory and Practice. Prentice-Hall, 2000, 523 p.
16. *Giarratano J.C., Riley G.D.* Expert Systems: Principles and Programming. 4th ed. Course Technology, 2004, 856 p.
17. *Rozenberg G., Salomaa A.* Handbook of Formal Languages. Vol. 1. Springer, 1997, 328 p.
18. *Scott M.L.* Programming Language Pragmatics. 4th ed. Morgan Kaufmann, 2015, 992 p.
19. *Boose J.H.* A survey of knowledge acquisition techniques and tools. *Knowledge Acquisition*, 1989, Vol.1, pp. 3-37.
20. *McGraw K.L., Harbison-Briggs K.* Knowledge Acquisition: Principles and Guidelines. Prentice Hall, 1989, 250 p.

Статью рекомендовал к опубликованию д.т.н., профессор В.И. Божич.

Поленов Максим Юрьевич – Южный федеральный университет, e-mail: mypolenov@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 88634371550; кафедра вычислительной техники; к.т.н.; доцент.

Курмалеев Артём Олегович – e-mail: kurmaleev@sfedu.ru; тел.: 88634371656; кафедра вычислительной техники; соискатель.

Polenov Maxim Yuryevich – Southern Federal University; e-mail: mypolenov@sfedu.ru; 44, Nekrasovskiy, Taganrog, 347928, Russia; phone: +78634371550; the department of computer engineering; cand. of eng. sc,; associate professor.

Kurmaleev Artem Olegovich – e-mail: kurmaleev@sfedu.ru; phone: +78634371656; the department of computer engineering; researcher.

УДК 551.594 DOI 10.18522/2311-3103-2020-5-130-141

С.С. Свидельский, В.С. Литвинова, Г.В. Куповых, А.Г. Клово

ФОРМИРОВАНИЕ СТРУКТУРЫ АТМОСФЕРНОГО ЭЛЕКТРОДНОГО СЛОЯ

Рассматривается проблема формирования электрического состояния нижнего слоя атмосферы вблизи поверхности земли. Исследуется электродинамическая модель нестационарного турбулентно-конвективного призменного слоя в приближении электродного эффекта (ЭЭ). Исходная система состоит уравнений, описывающих ионизационные и рекомбинационные процессы для аэроионов, и уравнения Пуассона для электрического поля. В зависимости от метеорологических условий в атмосфере отдельно рассмотрены модели электродного слоя (ЭС) в приближениях классического и турбулентного ЭЭ, а также в приближении сильного турбулентного перемешивания. В качестве факторов, влияющих на

пространственно-временную структуру ЭС, выступают турбулентный и конвективный перенос аэроионов, уровень ионизации воздуха и присутствие в нем субмикронного аэрозоля. Выявлены безразмерные параметры (критерии подобия) для электродинамических уравнений, позволяющие осуществлять выбор соответствующего приближения для моделирования структуры электродного слоя в зависимости от атмосферных условий. В свободной от аэрозоля атмосфере время установления стационарного состояния в электродном слое составляет примерно 5 мин., для классического слоя (характерная высота около 4-5 м), а в турбулентном - примерно 15 мин. (высота порядка 10 м). В случае сильного турбулентного перемешивания масштаб распределения электрических величин возрастает до сотен метров. Соотношение характерных скоростей турбулентного и конвективного процессов указывает на преобладающий физический механизм переноса ионов и формирования структуры ЭС. Увеличение скорости конвективного переноса, направленного вниз, приводит к ослаблению механизма турбулентного перемешивания, а при переносе вверх, имеет место обратный эффект. Присутствие в атмосфере субмикронного аэрозоля приводит к образованию тяжелых ионов, подвижность которых много меньше, чем у аэроионов. Однократно заряженные аэрозольные частицы с концентрацией, не превышающей число аэроионов, незначительно меняют пространственно-временные характеристик ЭС. Тогда как наличие в приземном воздухе многократно заряженных аэрозольных частиц, увеличивает время электрической релаксации и уменьшает высоту ЭС. При достаточно больших концентрациях аэрозоля (больше числа аэроионов на порядок и более) необходимо учитывать его перенос турбулентно-конвективными потоками, а структура ЭС определяется только тяжелыми ионами.

Атмосфера; приземный слой; электродный эффект; электродный слой; электрическое поле; проводимость; ток; турбулентность; конвекция; аэрозоль.

S.S. Svidelsky, V.S. Litvinova, G.V. Kupovykh, A.G. Klovo

FORMATION OF THE ATMOSPHERIC ELECTRODE LAYER STRUCTURE

The problem of the formation of the electric state in the lower layer of the atmosphere near the Earth's surface is considered in the article. An electrodynamic model of a non-stationary turbulent-convective surface layer is investigated in the approximation of the electrode effect. The initial system consists of the ionization-recombination equations for aeroions and the Poisson equation. Depending on the meteorological conditions in the atmosphere, the cases of classical and turbulent electrode effects, as well as the approximation of strong turbulent mixing, are considered separately. Turbulent and convective transport, the degree of air ionization, and the presence of submicron aerosol particles in the air are factors that affect the space-time structure of the electrode layer. Dimensionless parameters (similarity criteria) for electrodynamic equations are revealed, which allow choosing the appropriate approximation for modeling the structure of the electrode layer depending on atmospheric conditions. In an aerosol-free atmosphere, the time to establish a stationary state in the electrode layer is about 5 minutes, for the classical layer (the typical height is about 4-5 m), and in the turbulent layer-about 15 minutes. (the typical height is about 10 m). In the case of strong turbulent mixing, the distribution scale of electrical quantities increases to hundreds of meters. The ratio of the characteristic velocities of turbulent and convective processes indicates the predominant physical mechanism of ion transport and the formation of the electrode layer structure. An increase in the rate of convective transport directed downwards leads to a weakening of the turbulent mixing mechanism, and when moving up, the opposite effect occurs. The presence of a submicron aerosol in the atmosphere leads to the formation of heavy ions, the mobility of which is much less than that of aeroions. Single-charged aerosol particles with a concentration not exceeding the number of aeroions slightly change the spatiotemporal characteristics of the electrode layer. While the presence of repeatedly charged aerosol particles in the surface air increases the time of electrical relaxation and reduces the height of the electrode layer. At sufficiently high concentrations of aerosol (more than the number of aeroions by an order of magnitude or more), it is necessary to take into account its transport by turbulent-convective flows, and the structure of the electrode layer is determined only by heavy ions.

Atmosphere; surface layer; electrode effect; electrode layer; electric field; conductivity; current; turbulence; convection; aerosol.

Введение. Глобальная электрическая цепь атмосферы характеризуется ее общим сопротивлением $R \approx 230$ Ом, потенциалом ионосферы $\varphi_\infty \approx 250\text{-}300$ кВ, полным электрическим током $I \sim 10^3$ A, полным (эффективным) зарядом $Q \sim 10^5$ Кл, а также электроемкостью $C \approx 2{,}9$ Ф [1–5]. Время исчезновения электрического поля в атмосфере, при отсутствии в ней токовых генераторов, можно оценить как $\tau = RC \approx 10$ мин. Локальными характеристиками электричества приземного слоя атмосферы являются напряженность электрического поля $E \sim 10^2$ В/м, плотность вертикального электрического тока $j \sim 10^{-12}$ А/м^2, проводимость воздуха $\lambda \sim 10^{-14}\text{-}10^{-15}$ См/м (в условиях хорошей погоды), а также плотность объемного электрического заряда ρ и потенциал электрического поля φ [1–5]. Эти характеристики не являются независимыми, например, первые три из них связывает дифференциальная форма закона Ома, но, именно они используются при проведении атмосферно-электрических измерений [6].

Приземный слой атмосферы представляет собой ионизированную среду за счет действия постоянного космического излучения, а также радиоактивности воздуха и почвы. Электрическое поле и ток направлены вертикально вниз. Поверхность земли является отрицательно заряженной, вблизи которой возникает совокупность процессов, называемых электродным эффектом (ЭЭ) [7, 8]. В результате вблизи поверхности образуется электродный слой (ЭС), где величины локальных электрических характеристик атмосферы зависят от его характерного пространственного масштаба [7, 8].

В теории атмосферного электричества проблема ЭЭ формулируется в виде стационарной задачи о нахождении распределения положительных и отрицательных легких ионов (аэроионов), электрического поля и плотности электрического тока вблизи поверхности земли. Постановка математической задачи включает два предельных случая: классический и турбулентный ЭЭ. Классический ЭЭ имеет место, когда приземная атмосфера считается неподвижной, а структура ЭС формируется под воздействием только электрического поля. Турбулентный ЭЭ предполагает, что структура ЭС определяется, наряду с электрическими силами, турбулентными потоками воздуха, причем последний фактор может быть определяющим (приближение сильного турбулентного перемешивания) [6–8].

Наличие субмикронного аэрозоля в атмосфере, приводит к появлению тяжелых ионов за счет его взаимодействия с аэроионами, что оказывает влияние на характеристики ЭС. При достаточно больших концентрациях аэрозоля необходимо учитывать его перенос турбулентными потоками, а структура ЭС определяется только тяжелыми ионами. Подробная теория ЭЭ в атмосфере приведена в работах [6–8].

Цель настоящей работы исследовать процессы формирования пространственно-временной структуры ЭС в зависимости от метеорологических и физических условий в атмосфере.

Модель турбулентно-конвективного электродного слоя. Проведем анализ уравнений электродинамической модели нестационарного турбулентно-конвективного ЭС в чистой атмосфере [9]:

$$\begin{cases} \dfrac{\partial n_{1,2}}{\partial t} \pm \dfrac{\partial}{\partial z}\left(b_{1,2} \cdot n_{1,2} \cdot E\right) - \dfrac{\partial}{\partial z}\left(D_T(z,t) \cdot \dfrac{\partial n_{1,2}}{\partial z}\right) + \dfrac{\partial}{\partial z}\left(\upsilon(z,t) \cdot n_{1,2}\right) = q - \alpha n_1 n_2 \\ \dfrac{\partial E}{\partial z} = \dfrac{e}{\varepsilon_0}\left(n_1 - n_2\right) \end{cases} \quad (1)$$

с начальными:

$$\begin{cases} n_1(z)\big|_{t=0} = n_2(z)\big|_{t=0} = n_0, \\ E(z)\big|_{t=0} = E_0, \end{cases} \tag{2}$$

и граничным условиям:

$$\begin{cases} n_1(z)\big|_{z=z_0} = n_2(z)\big|_{z=z_0} = 0, n_1(z)\big|_{z=l} = n_2(z)\big|_{z=l} = \sqrt{\dfrac{q}{\alpha}}, \\ E(z)\big|_{z=z_0} = E_0 \end{cases} \tag{3}$$

где $n_{1,2}$ – концентрация полярных аэроионов; $b_{1,2}$ – их подвижности; E – напряженность электрического поля; υ – параметр конвективного переноса; $D_T(z) = D_1 z$ – параметр турбулентного переноса; q – скорость ионизации воздуха; α – параметр рекомбинации; E_0 – электрическое поле у поверхности; z_0 – параметр шероховатости поверхности; l – верхняя граница ЭС; e – заряд электрона; ε_0 – электрическая постоянная.

Для определения характерного пространственного масштаба ЭС введем обозначения:

$$n_{1,2}\big|_{z\to\infty} = n_\infty = \sqrt{\frac{q}{\alpha}},\ E\big|_{z\to\infty} = E_\infty,\ n'_{1,2} = \frac{n_{1,2}}{n_\infty},\ E' = \frac{E}{E_\infty}. \tag{4}$$

Подставляя (4) в ионизационно-рекомбинационные уравнения системы (1), получаем:

$$\begin{aligned} &\tau\frac{\partial n'_1}{\partial t} + \tau b_1 E_\infty \frac{\partial(n'_1 E')}{\partial z} - D_m\tau\frac{\partial}{\partial z}\left(z\frac{\partial n'_1}{\partial z}\right) + \upsilon\tau\frac{\partial n'_1}{\partial z} = 1 - n'_1 n'_2, \\ &\tau\frac{\partial n'_2}{\partial t} - \tau b_2 E_\infty \frac{\partial(n'_2 E')}{\partial z} - D_m\tau\frac{\partial}{\partial z}\left(z\frac{\partial n'_2}{\partial z}\right) + \upsilon\tau\frac{\partial n'_2}{\partial z} = 1 - n'_1 n'_2. \end{aligned} \tag{5}$$

Параметр $\tau = (q\cdot\alpha)^{-1/2}$ представляет собой характерное время процесса установления стационарного состояния. В уравнениях (5) можно выделить четыре характерных пространственных масштаба для электродного слоя: $L_{nE_1} = b_1\cdot E_\infty\cdot\tau$, $L_{nE_2} = b_2\cdot E_\infty\cdot\tau$, $L_D = D_1\cdot\tau$, $L_\upsilon = \upsilon\cdot\tau$.

Для значений параметров: D_1 = 0,1 м/с, υ = 0,01 м/с, $q = 7\cdot10^6$ м$^{-3}$с$^{-1}$, E = 100 В/м, $b_1 = 1{,}2\cdot10^{-4}\ м^2B^{-1}c^{-1}$, $b_2 = 1{,}4\cdot10^{-4}\ м^2B^{-1}c^{-1}$, $\alpha = 1{,}6\cdot10^{-12}\ м^3c^{-1}$ получаем значения масштабов: $\tau \approx 300c$, $L_D = 30$ м, $L_\upsilon = 3$ м, $L_{nE_1} = 3{,}6$ м, $L_{nE_2} = 4{,}2$ м. Характерные пространственные масштабы распределения по вертикали ЭС соответствуют разным моделям ЭЭ в зависимости от условий в приземном слое.

Для анализа системы (1) введем следующие безразмерные параметры:

$$n_{1,2}\big|_{z\to\infty} = n_\infty,\ E\big|_{z\to\infty} = E_\infty,\ l_1 = D_1\cdot\tau,$$
$$t' = t/T,\ z' = z/l_1,\ n'_{1,2} = n_{1,2}/n_\infty,\ E' = E/E_\infty.$$

Подставляя их в систему (1), после некоторых преобразований получаем:

$$\begin{cases} \dfrac{\tau}{T}\dfrac{\partial n'_{1,2}}{\partial t'} \pm \dfrac{b_{1,2}E_\infty}{D_1}\dfrac{\partial}{\partial z'}(n'_{1,2}\cdot E') - \dfrac{\partial}{\partial z'}\left(z'\cdot\dfrac{\partial n'_{1,2}}{\partial z'}\right) + \\ + \dfrac{\upsilon}{D_1}\dfrac{\partial n'_{1,2}}{\partial z'} = \dfrac{q}{q_\infty} - n_1\cdot n_2, \\ \dfrac{\partial E'}{\partial z'} = \dfrac{e\cdot n_\infty l_1}{\varepsilon_0 E_\infty}\left(n'_1 - n'_{2'}\right), \end{cases} \quad (6)$$

В уравнениях системы (6) появляются безразмерные параметры, являющиеся критериями подобия для электродинамической модели (1):

$$\xi_{1,2} = \frac{|b_{1,2}|\cdot E_\infty\cdot\tau}{l_1} = \frac{|b_{1,2}|E_\infty}{D_1},\ \chi = \frac{\upsilon}{D_1},\ \gamma = \frac{en_\infty l_1}{\varepsilon_0 E_\infty} = \frac{en_\infty D_1\tau}{\varepsilon_0 E_\infty}. \quad (7)$$

Тогда, получаем окончательную запись безразмерной системы (1):

$$\begin{cases} \dfrac{\tau}{T}\dfrac{\partial n'_{1,2}}{\partial t'} \pm \xi_{1,2}\dfrac{\partial}{\partial z'}(n'_{1,2}\cdot E') - \dfrac{\partial}{\partial z'}\left(z'\cdot\dfrac{\partial n'_{1,2}}{\partial z'}\right) + \chi\dfrac{\partial n'_{1,2}}{\partial z'} = \dfrac{q}{q_\infty} - n_1\cdot n_2, \\ \dfrac{\partial E'}{\partial z'} = \gamma\left(n'_1 - n'_2\right). \end{cases} \quad (8)$$

Используя параметры подобия (7), проанализируем систему (8) при различных условиях в атмосфере. Время протекания T гидрометеорологических процессов в атмосфере обычно имеет порядок нескольких часов, тогда как время электрической релаксации составляет $\tau = 250$ с ($q = 10^7$ м$^{-3}$с$^{-1}$ и $\alpha = 1{,}6\cdot10^{-12}$ м^{3}с$^{-1}$), т.е. на порядок меньше. Поэтому в теории ЭЭ используется стационарное приближение уравнений атмосферной электродинамики.

Когда параметр $|\gamma| \ll 1$, то электрическим полем объемного заряда в ЭС, можно пренебречь, т.е., фактически, явление ЭЭ отсутствует.

При выполнении условия $\xi_{1,2} \geq 1$ имеет место приближение классического ЭЭ [5, 7]. Образуется ЭС с характерной высотой $L_{nE_2} = 4{,}2$ м. Если $\xi_{1,2} < 1$, то имеет место приближение турбулентного ЭЭ [2,4,6,10-13], а характерная высота ЭС равна $L_D = 30$м. Когда $\xi_{1,2} \ll 1$ перенос аэроионов осуществляется только турбулентными потоками, а распределения электрического поля и плотности заряда, также, зависит от параметров турбулентности, но при сформировавшемся профилем электрической проводимости (приближение сильного турбулентного перемешивания) [5, 7]. Характерный масштаб ЭС в чистой атмосфере зависит от типа турбулентного перемешивания и может достигать сотен метров [5, 7].

При значении $\chi \ll 1$, конвективным переносом аэроионов можно пренебречь. Если значения параметра D_1 сопоставимо или меньше υ ($D_1 \leq \upsilon$), то конвекция является основным фактором в формировании турбулентно-конвективного ЭС [3–6, 11], а его высота составляет около $L_\upsilon = 3$ м и может расти с усилением конвективного переноса [6, 11].

Моделирование структуры ЭС с учётом аэрозольного загрязнения. С точки зрения математического моделирования, классический и турбулентный случаи ЭЭ отличаются условиями на нижней границе поверхности земли для аэроионов. В первом случае концентрация отрицательных аэроионов равна нулю, а положительных – нет. Во втором случае значения положительной и отрицательной

концентраций аэроионов равны нулю, а граничные условия задаются на некоторой высоте, которая определяется масштабом шероховатости z_0, зависящим от аэродинамических свойств воздушного потока и поверхности, в частности, от числа Рейнольдса.

Присутствие в атмосфере субмикронного аэрозоля приводит к образованию тяжелых ионов, подвижность которых много меньше, чем у аэроионов. В предположении, что количество аэрозольных частиц в атмосфере не превышает числа аэроионов, условия равновесия между ними можно считать выполненными, а ток заряженных тяжелых ионов пренебрежимо мал. В противном случае предположение о стационарности тяжелых ионов не выполняется.

Уравнения электродинамической модели для случая однократно заряженных аэрозоля при условии $\mathrm{N} \le \mathrm{n}_{1,2}$ представляются как [10–14, 17]:

$$\frac{\partial \mathrm{n}_{1,2}}{\partial \mathrm{t}} \pm \frac{\partial}{\partial \mathrm{z}}\left(\mathrm{b}_{1,2}\mathrm{En}_{1,2}\right) - \frac{\partial}{\partial \mathrm{z}}\left(\mathrm{D}_{\mathrm{T}}(\mathrm{z}) \cdot \frac{\partial \mathrm{n}_{1,2}}{\partial \mathrm{z}}\right) + \frac{\partial}{\partial \mathrm{z}}\left(\upsilon(\mathrm{z}) \cdot \mathrm{n}_{1,2}\right) =$$

$$= \mathrm{q}\text{-}\alpha\ \mathrm{n}_1\mathrm{n}_2 - \mathrm{n}_{1,2}\eta_2\mathrm{N}_0 - n_{1,2}\eta_1\mathrm{N}_{2,1},$$

$$\frac{\partial \mathrm{N}_{1,2}}{\partial \mathrm{t}} - \frac{\partial}{\partial \mathrm{z}}\left(\chi\ (\mathrm{z}) \cdot \frac{\partial \mathrm{N}_{1,2}}{\partial \mathrm{z}}\right) + \frac{\partial}{\partial \mathrm{z}}\left(\upsilon(\mathrm{z}) \cdot \mathrm{N}_{1,2}\right) = \mathrm{n}_{1,2}\eta_2\mathrm{N}_0 - \mathrm{n}_{2,1}\eta_1\mathrm{N}_{1,2},$$

$$\mathrm{N}_1 + \mathrm{N}_2 + \mathrm{N}_0 = \mathrm{N}=\mathrm{const},$$

$$\frac{\partial \mathrm{E}}{\partial \mathrm{z}} = \frac{e}{\varepsilon_0} \cdot \left(\mathrm{n}_1 - \mathrm{n}_2 + \mathrm{N}_1 - \mathrm{N}_2\right). \qquad (9)$$

Обозначения для аэрозольной составляющей системы: N_0, $N_{1,2}$, N – концентрации нейтральных, однократно заряженных положительных и отрицательных тяжелых ионов и общая концентрация субмикронных аэрозольных частиц, соответственно, η_1 и η_2 – параметры воссоединения, χ – параметр турбулентной диффузии тяжелых ионов.

Начальные и граничные условия имеют вид: для легких ионов и электрического поля (2)–(3), а для тяжелых ионов:

$$N_{1,2}(t=0) = \frac{\eta_2 N}{2\eta_2 + \eta_1}, \left(\frac{\partial N_{1,2}}{\partial z}\right)_{z=z_0} = 0,\ N_{1,2}(z=l) = \frac{\eta_2 N}{2\eta_2 + \eta_1}. \qquad (10)$$

Многократную заряженность тяжелых ионов рассмотрим ниже.

Для исследования влияния источников ионизации на структуру ЭС обычно используется стационарный профиль ионизации, в виде: $q(z) = q + Q_0 \cdot \mathrm{e}^{\left(-z/l\right)}$, где q – ионизация за счет космических лучей, второе слагаемое - отражает вклад, создаваемой радиоактивностью воздуха с характерным масштабом распределения l [7, 15–19].

Основные характеристики ЭС в различных условиях. ***Установление стационарного состояния в ЭС.*** В свободной от аэрозоля атмосфере время установления стационарного режима в классическом ЭС составляет примерно 5 мин. Время установления в турбулентном ЭС в несколько раз больше, чем в классическом, и равно примерно 15 мин. [8]. Влияние однократно заряженных аэрозольных частиц с концентрацией, не превышающей концентрацию аэроионов, на время установления незначительно [18–20].

Результаты исследования влияния аэрозольных частиц в диапазоне размеров 0,01 мкм – 0,4 мкм показывают [10–14, 17], что с увеличением радиуса частиц *r*, увеличивается число зарядов *k* на них (при $r < 0,04$ мкм $k = 1$; при $0,04 \le r < 0,07$ мкм $k = 2$; при $0,07 \le r < 0,1$ мкм $k = 3$; при $0,1 \le r \le 0,2$ мкм $k = 4$; при $0,2 < r \le 0,4$ мкм $k = 5$). Возрастание концентрации аэрозоля приводит к увеличению времени установления τ электрической структуры ЭС. При этом τ растет пропорционально размеру аэрозольных частиц (при $N = 10^9$ м$^{-3}$ в случае $r = 0,04$ мкм и $\tau = 800$ с, а в случае $r = 0,4$ мкм и $\tau = 1200$ с).

В работах [9, 11] рассмотрен вопрос о влиянии конвективного переноса на структуру ЭС. Увеличение скорости конвективного переноса, направленного вниз, приводит к ослаблению механизма турбулентного перемешивания, а при переносе вверх, происходит его усиление.

Приближение классического ЭЭ. В классическом ЭС при усилении электрического поля у поверхности земли, отношение E_0/E_∞ практически не меняется, а высота ЭС увеличивается [1, 7, 15]. Вследствие чего, изменяются параметры ЭС: $E(z)/E_\infty$, $z \le l$ с увеличивается, $n_1(z)/n_\infty$ – практически постоянно, а $n_2(z)/n_\infty$ – уменьшается.

Появление в атмосфере аэрозоля концентрациями N~(10^8-10^9) м$^{-3}$ уменьшает высоту ЭС, параметр E_0/E_∞ при этом остается неизменным. При значениях $N \ge 5 \cdot 10^9$ м$^{-3}$, структура ЭС определяется, в основном, тяжелыми ионами.

Усиление электрического поля увеличивает значения параметра $E(z)/E_\infty$, $z \le l$, но в меньшей степени, чем в чистой атмосфере. Другие характеристики ЭС меняются следующим образом: $n_2(z)/n_\infty$ и $N_2(z)/N_\infty$ уменьшаются, $N_1(z)/N_\infty$ увеличивается, а $n_1(z)/n_\infty$ остается неизменым.

В условиях невысокой степени ионизации воздуха объемный электрический заряд в классическом ЭС положителен, а его величина определяются мощностью источника ионизации, и зависит от электрического поля. При наличии тонкого (l несколько десятков сантиметров) слоя повышенной ионизации $Q_0 \ge 80$ $см^{-3}с^{-1}$ вблизи поверхности земли появляется отрицательный объемный заряд. Он возникает и при невысокой степени ионизации воздуха, но слабом электрическом поле (порядка нескольких десятков вольт на метр). При увеличении электрического поля или масштаба распределения повышенной ионизации воздуха объемный заряд опять становится положительным.

Приближение турбулентного ЭЭ. Высота турбулентного ЭС зависит от скорости приземного ветра [1, 7, 16]. При небольших скоростях (~ 1 м/с) параметр $n_1(z)/n_\infty$ быстро растет и достигает значения равного единице на высоте около одного метра. Плотность положительного объемного заряда максимальна, а на высоте 5 м и выше разница в значениях $n_1(z)/n_\infty$ и $n_1(z)/n_\infty$ не превышает нескольких процентов, как и классическом ЭС. При увеличении скорости ветра до 5 – 6 м/с разница значений $n_1(z)/n_\infty$ и $n_1(z)/n_\infty$ на высоте один метр не более 10 %. Высота турбулентного ЭС увеличивается и достигает нескольких десятков метров. Параметр $E(z)/E_\infty$, $z \le l$ увеличиваются при усилении ветра, но параметр E_0/E_∞ остается постоянным.

При высокой степени ионизации воздуха (Q_0 = 80 см$^{-3}$с$^{-1}$) и небольшой скорости ветра (менее 1 м/с) в турбулентном ЭС объемный заряд – отрицательный, как и в классическом случае. Масштаб его распределения возрастает до 10–15 м, а плотность за-

ряда уменьшается. При усилении турбулентности или электрического поля знак объемного заряда меняется на положительный. В сильном электрическом поле влияние турбулентности ослабевает: плотность объёмного заряда возрастает, параметр $E(z)/E_\infty$ увеличивается, и структура турбулентного ЭС становится похожей на классический.

Аэрозоль концентрацией менее $10^9 м^{-3}$, как и в классическом случае, незначительно влияет на характеристики турбулентного ЭС. При высоких концентрациях аэрозоля ($N \sim 10^{10} м^{-3}$ и более) также появляется отрицательный объемного заряда, обусловленный тяжелыми ионами.

В случае присутствия многократно заряженных аэрозольных частиц в воздухе с характерными размерами от $r = 0{,}02 мкм$ до $r = 0{,}1 мкм$ показывают, что влияние на параметры ЭС тяжелых ионов с зарядом от 3 до $5e$ почти на порядок меньше, чем для ионов с 1–2e. При высоких концентрациях аэрозоля ($N \sim 10^{10} м^{-3}$ и более) в слое высотой до 5 м наблюдается также реверс ЭЭ, что свидетельствует о преобладании отрицательного объемного заряда тяжелых ионов, а вкладом заряда аэроионов можно пренебречь. В этом случае необходимо дополнять электродинамическую модель уравнениями переноса тяжелых ионов. В условиях повышенной ионизации воздуха учет аэрозольных частиц большего размера увеличивает плотность отрицательного объемного заряда и смещает его к поверхности.

Приближение сильного турбулентного перемешивания. При условиях в приземном слое, когда параметр $\xi_{1,2} << 1$, стационарный вариант системы (1) расщепляется на систему линейных относительно электрического поля уравнений [5, 7]. В нулевом приближении распределение аэроионов определяется только турбулентным переносом и не зависит от электрического поля [5, 7]. Электродинамическая модель преобразуется к виду:

$$-\frac{d}{dz}\left(D_T(z)\frac{dn_{1,2}}{dz}\right) = q - \alpha n_{1,2}^2; \qquad (11)$$

$$-\frac{D_T(z)}{\varepsilon_0}\frac{d^2E}{dz^2} + \lambda(z)E = j_0.$$

$$n_1(z = z_0) = n_2(z = z_0) = 0,\ \left.\frac{dE}{dz}\right|_{z=z_0} = 0,\ n_1(\infty) = n_2(\infty) = \left(q(\infty)/\alpha\right)^{1/2},\ E_\infty = \frac{j_0}{\lambda_\infty}.$$

Профили электрической проводимости воздуха $\lambda(z)$ и плотности объемного заряда $\rho(z)$ по формулам:

$$\lambda(z) = e\left(b_1 n_1(z) + b_2 n_2(z)\right),\quad \rho(z) = e\left(n_1(z) - n_2(z)\right). \qquad (12)$$

Характерный масштаб распределение аэроионов (электрической проводимости) определяется как $l_m = \left(D_m \tau\right)^{\frac{1}{2-m}}$, $\tau = \left(q_\infty \alpha\right)^{-\frac{1}{2}}$, т.е. расстояние, проходимое аэроионом вследствие турбулентного переноса за время релаксации. Характерный масштаб распределение для профиля электрического поля определяется профилем электрической проводимости и турбулентным переносом. Характерный масштаб распределения для электрического поля, определяющий высоту турбулентного ЭС равен $L_m = \left(D_m \tau_{\lambda\infty}\right)^{\frac{1}{2-m}}$, $\tau_{\lambda\infty} = \left(4\pi\lambda_\infty\right)^{-1}$, m = 0;1;4/3 – параметр стратификации соответственно устойчивой, нейтральной и неустойчивой атмосферы [1].

Расчеты показывают [5, 7], что при увеличении степени неустойчивости атмосферы высота ЭС и масштаб распределения его характеристик растет. Плотность электрического заряда резко возрастает в тонком слое у поверхности, а за-

тем монотонно уменьшается. Наиболее сильным этот максимум проявляется при термически неустойчивой стратификации (m =4/3) атмосферы. В случае нейтральной стратификации атмосферы профиль электрической проводимости носит логарифмический характер [5, 7].

С помощью оценки масштаба L_m, который играет роль критерия подобия, можно сделать вывод, что увеличение аэрозольного загрязнение атмосферы и, одновременно, понижение степени ионизации воздуха, уменьшает высоту ЭС и характерный масштаб распределения его характеристик [5, 7].

Заключение. Проведенный анализ электродинамической модели атмосферного приземного слоя в приближении ЭЭ выявил, что в результате ионизационно-рекомбинационных процессов образуется ЭС, в котором пространственно-временные распределения электрических характеристик зависят от его характерного масштаба. Высота ЭС, прежде всего, зависит от степени метеорологической устойчивости приземной атмосферы. Существенную роль в формировании структуры ЭС играют турбулентный и конвективный переносы, а также ионизация атмосферы и степень ее аэрозольного загрязнения. Применение той или другой модели ЭЭ для решения научно-прикладных задач можно обосновывать с помощью критериев подобия, полученных при исследовании уравнений электродинамической модели.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Атмосфера. Справочник (справочные данные, модели). – Л.: Гидрометеоиздат, 1991. – 506 с.
2. *Анисимов С.В., Мареев Е.А.* Геофизические исследования глобальной электрической цепи // Физика Земли. – 2008. – № 10. – С. 8-18.
3. Williams E.R. The global electrical circuit: A Review // Atm. Res. – 2009. – Vol. 91. – P. 140-152.
4. *Мареев Е.А.* Достижения и перспективы исследований глобальной электрической цепи // УФН. – 2010. – Т. 180, № 5. – С. 527-534.
5. *Морозов В. Н., Куповых Г.В.* Математическое моделирование глобальной атмосферной электрической цепи и электричества приземного слоя: монография. – СПб.: Астерион, 2017. – 307 с.
6. *Афиногенов Л.П., Грушин С.И., Романов Е.В.* Аппаратура для исследований приземного слоя атмосферы. – Л.: Гидрометеоиздат, 1977. – 319 с.
7. *Куповых Г.В., Морозов В.Н., Шварц Я.М.* Теория электродного эффекта в атмосфере. – Таганрог. Изд-во ТРТУ, 1998. – 123 с.
8. *Куповых Г.В.* Электродинамические процессы в приземном слое атмосферы. – Таганрог. Изд-во ТТИ ЮФУ, 2009. – 114 с.
9. *Редин А.А., Куповых Г.В., Болдырев А.С.* Электродинамическая модель конвективно-турбулентного приземного слоя атмосферы // Известия вузов. Радиофизика. – 2013. – № 11-12, Т. 56. – С. 820-828.
10. *Редин А.А., Куповых Г.В., Клово А.Г., Болдырев А.С.* Математическое моделирование электродинамических процессов в приземном слое в условиях аэрозольного загрязнения атмосферы // Известия ЮФУ. Технические науки. – 2011. – № 8 (121). – С. 111-121.
11. *Болдырев А.С., Редин А.А., Куповых Г.В., Морозов В.Н.* Электродинамическая модель конвективно-неустойчивого атмосферного приземного слоя // Известия высших учебных заведений. Сев.-Кав. регион. Естественные науки. Спецвыпуск. Физика атмосферы. – 2010. – С. 23-28.
12. *Редин А.А., Клово А.Г., Куповых Г.В., Морозов В.Н.* Генерация объемного заряда вблизи поверхности земли с учетом взаимодействия аэрозольных частиц с аэроионами // Известия высших учебных заведений. Сев.-Кав. регион. Естественные науки. Спецвыпуск. Физика атмосферы. – 2010. – С. 81-85.
13. *Kupovykh G., Redin A., Boldyreff A.* Modeling of ionization-recombination processes in the atmospheric surface layer // Journal of Electrostatics. – 71. Elsevier B.V. – 2013. – P. 305-311.

14. *Морозов В.Н., Куповых Г.В., Редин А.А., Кудринская Т.В.* Нестационарное физико-математическое моделирование электрических процессов в приземном слое атмосферы с учетом субмикронных аэрозольных частиц // Тр. ГГО им. А.И. Воейкова. – СПб., 2017. – Вып. 584. – С. 36-57.
15. *Клово А.Г., Куповых Г.В., Свидельский С.С., Скляров Н.Е.* Исследования структуры электродного слоя в приземной атмосфере // Известия высших учебных заведений. Сев.-Кав. регион. Естественные науки. – 2018. – № 1. – С. 77-89.
16. *Куповых Г.В., Клово А.Г., Тимошенко Д.В., Свидельский С.С.* Приближенное аналитическое решение задачи об электродинамическом состоянии приземной атмосферы в условиях аэрозольного загрязнения // Известия высших учебных заведений. Сев.-Кав. регион. Естественные науки. – 2018. – № 2. – С.84-89.
17. *Клово А.Г., Куповых Г.В., Тимошенко Д.В., Свидельский С.С.* Моделирование структуры турбулентного электродного слоя в условиях аэрозольного загрязнения приземной атмосферы // Известия высших учебных заведений. Сев.-Кав. регион. Естественные науки. – 2018. – № 3. – С. 82-88.
18. *Кудринская Т.В., Куповых Г.В., Редин А.А.* Исследования ионизационного состояния приземного слоя атмосферы в разных геофизических условиях // Метеорология и гидрология. – 2018. – № 4. – С. 77-85.
19. *Kupovykh G.V., Timoshenko D.V., Klovo A. G., Kudrinskaya T.V.* Electrodynamic processes models in atmospheric surface layer // CATPID-2019. IOP Conf. Series: Materials Science and Engineering. – Vol. 698. – 2019 044034. – 8 p.
20. *Куповых Г.В., Кудринская Т.В., Тимошенко Д.В., Клово А.Г., Свидельский С.С., Литвинова В.С.* Математическое моделирование электрических процессов в приземном слое атмосферы // VIII Всероссийская конференция по атмосферному электричеству с международным участием (Нальчик, 23-27 сентября 2019 г.). – СПб.: Изд-во ВКА им. А.Ф. Можайского, 2019. – С. 191-193.

REFERENCES

1. Atmosfera. Spravochnik (spravochnye dannye, modeli) [Atmosphere. Handbook (reference data, models)]. Leningrad: Gidrometeoizdat, 1991, 506 p.
2. *Anisimov S.V., Mareev E.A.* Geofizicheskie issledovaniya global'noy elektricheskoy tsepi [Geophysical studies of the global electric circuit], *Fizika Zemli* [Physics of the Earth], 2008, No. 10, pp. 8-18.
3. *Williams E.R.* The global electrical circuit: A Review, *Atm. Res*., 2009, Vol. 91, pp. 140-152.
4. *Mareev E.A.* Dostizheniya i perspektivy issledovaniy global'noy elektricheskoy tsepi [Achievements and prospects of research of the global electric circuit], *UFN* [Advances in Physical Sciences], 2010, Vol. 180, No. 5, pp. 527-534.
5. *Morozov V. N., Kupovykh G.V.* Matematicheskoe modelirovanie global'noy atmosfernoy elektricheskoy tsepi i elektrichestva prizemnogo sloya: monografiya [Mathematical modeling of the global atmospheric electric circuit and surface layer electricity: a monograph]. Saint Petersburg: Asterion, 2017, 307 p.
6. *Afinogenov L.P., Grushin S.I., Romanov E.V.* Apparatura dlya issledovaniy prizemnogo sloya atmosfery [Equipment for studies of the surface layer of the atmosphere]. Leningrad: Gidrometeoizdat, 1977, 319 p.
7. *Kupovykh G.V., Morozov V.N., Shvarts Ya.M.* Teoriya elektrodnogo effekta v atmosphere [Theory of the electrode effect in the atmosphere]. Taganrog. Izd-vo TRTU, 1998, 123 p.
8. *Kupovykh G.V.* Elektrodinamicheskie protsessy v prizemnom sloe atmosfery [Electrodynamic processes in the surface layer of the atmosphere]. Taganrog. Izd-vo TTI YuFU, 2009, 114 p.
9. *Redin A.A., Kupovykh G.V., Boldyrev A.S.* Elektrodinamicheskaya model' konvektivno-turbulentnogo prizemnogo sloya atmosfery [Electrodynamic model of convective-turbulent surface layer of the atmosphere], *Izvestiya vuzov. Radiofizika* [Izvestiya vuzov. Radio], 2013, No. 11-12, Vol. 56, pp. 820-828.
10. *Redin A.A., Kupovykh G.V., Klovo A.G., Boldyrev A.S.* Matematicheskoe modelirovanie elektrodinamicheskikh protsessov v prizemnom sloe v usloviyakh aerozol'nogo zagryazneniya atmosfery [Mathematical modeling of electrodynamic processes in the surface layer under conditions of aerosol pollution of the atmosphere], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2011, No. 8 (121), pp. 111-121.

11. *Boldyrev A.S., Redin A.A., Kupovykh G.V., Morozov V.N.* Elektrodinamicheskaya model' konvektivno-neustoychivogo atmosfernogo prizemnogo sloya [Electrodynamic model of convective-unstable atmospheric surface layer], *Izvestiya vysshikh uchebnykh zavedeniy. Sev.-Kav. region. Estestvennye nauki. Spetsvypusk. Fizika atmosfery* [News of higher educational institutions. North Caucasus region. Natural sciences. Special issue. Physics of the atmosphere], 2010, pp. 23-28.
12. *Redin A.A., Klovo A.G., Kupovykh G.V., Morozov V.N.* Generatsiya ob"emnogo zaryada vblizi poverkhnosti zemli s uchetom vzaimodeystviya aerozol'nykh chastits s aeroionami [The generation of space charge near the earth's surface, accounting for the interaction of aerosol particles with air ions], *Izvestiya vysshikh uchebnykh zavedeniy. Sev.-Kav. region. Estestvennye nauki. Spetsvypusk. Fizika atmosfery* [News of higher educational institutions. North Caucasus region. Natural sciences. Special issue. Physics of the atmosphere], 2010, pp. 81-85.
13. *Kupovykh G., Redin A., Boldyreff A.* Modeling of ionization-recombination processes in the atmospheric surface layer, *Journal of Electrostatics*, 71, Elsevier B.V., 2013, pp. 305-311.
14. *Morozov V.N., Kupovykh G.V., Redin A.A., Kudrinskaya T.V.* Nestatsionarnoe fiziko-matematicheskoe modelirovanie elektricheskikh protsessov v prizemnom sloe atmosfery s uchetom submikronnykh aerozol'nykh chastits [Nonstationary physical and mathematical modeling of electrical processes in the surface layer of the atmosphere taking into account submicron aerosol particles], *Tr. GGO im. A.I. Voeykova* [Proceedings of the Voeikov State Educational Institution]. Saint Petersburg, 2017, Issue 584, pp. 36-57.
15. *Klovo A.G., Kupovykh G.V., Svidel'skiy S.S., Sklyarov N.E.* Issledovaniya struktury elektrodnogo sloya v prizemnoy atmosfere [Studies of the structure of the electrode layer in the surface atmosphere], *Izvestiya vysshikh uchebnykh zavedeniy. Sev.-Kav. region. Estestvennye nauki* [News of higher educational institutions. North Caucasus region. Natural sciences], 2018, No. 1, pp. 77-89.
16. *Kupovykh G.V., Klovo A.G., Timoshenko D.V., Svidel'skiy S.S.* Priblizhennoe analiticheskoe reshenie zadachi ob elektrodinamicheskom sostoyanii prizemnoy atmosfery v usloviyakh aerozol'nogo zagryazneniya [Approximate analytical solution of the problem of the electrodynamic state of the surface atmosphere under conditions of aerosol pollution], *Izvestiya vysshikh uchebnykh zavedeniy. Sev.-Kav. region. Estestvennye nauki* [News of higher educational institutions. North Caucasus region. Natural sciences], 2018, No. 2, pp.84-89.
17. *Klovo A.G., Kupovykh G.V., Timoshenko D.V., Svidel'skiy S.S.* Modelirovanie struktury turbulentnogo elektrodnogo sloya v usloviyakh aerozol'nogo zagryazneniya prizemnoy atmosfery [Modeling of the structure of a turbulent electrode layer in the conditions of aerosol pollution of the surface atmosphere], *Izvestiya vysshikh uchebnykh zavedeniy. Sev.-Kav. region. Estestvennye nauki* [News of higher educational institutions. North Caucasus region. Natural sciences], 2018, No. 3, pp. 82-88.
18. *Kudrinskaya T.V., Kupovykh G.V., Redin A.A.* Issledovaniya ionizatsionnogo sostoyaniya prizemnogo sloya atmosfery v raznykh geofizicheskikh usloviyakh [Studies of the ionization state of the surface layer of the atmosphere in different geophysical conditions], *Meteorologiya i gidrologiya* [Meteorology and hydrology], 2018, No. 4, pp. 77-85.
19. *Kupovykh G.V., Timoshenko D.V., Klovo A. G., Kudrinskaya T.V.* Electrodynamic processes models in atmospheric surface layer, *CATPID-2019. IOP Conf. Series: Materials Science and Engineering*, Vol. 698, 2019 044034, 8 p.
20. *Kupovykh G.V., Kudrinskaya T.V., Timoshenko D.V., Klovo A.G., Svidel'skiy S.S., Litvinova V.S.* Matematicheskoe modelirovanie elektricheskikh protsessov v prizemnom sloe atmosfery [Mathematical modeling of electrical processes in the surface layer of the atmosphere], *VIII Vserossiyskaya konferentsiya po atmosfernomu elektrichestvu s mezhdu-narodnym uchastiem (Nal'chik, 23-27 sentyabrya 2019 g.)* [VIII All-Russian Conference on Atmospheric Electricity with international participation (Nalchik, September 23-27, 2019)]. Saint Petersburg: Izd-vo VKA im. A.F. Mozhayskogo, 2019, pp. 191-193.

Статью рекомендовал к опубликованию д.ф.-м.н. А.Н. Каркищенко.

Свидельский Сергей Сергеевич – Южный федеральный университет; e-mail: svidelskiy@sfedu.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: 89281410341; аспирант.

Литвинова Валерия Сергеевна – e-mail: litvvalery@mail.ru; тел.: 89185884396; аспирант.

Куповых Геннадий Владимирович – e-mail: kupovykh@sfedu.ru; тел.: 89289543642; д.ф.-м.н.; профессор.

Клово Александр Георгиевич – e-mail: klovo_ag@mail.ru; тел.: 89281221064; к.ф.-м.н.; доцент.

Svidelsky Sergey Sergeevich – Southern Federal University; e-mail: svidelskiy@sfedu.ru; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +79281410341; postgraduate student.

Litvinova Valeria Sergeevna – e-mail: litvvalery@mail.ru; phone: +79185884396; postgraduate student.

Kupovykh Gennady Vladimirovich – e-mail: kupovykh@sfedu.ru; phone: +79289543642; dr. of phys. and math. sc.; professor.

Klovo Alexander Georgievich – e-mail: klovo_ag@mail.ru; phone: +79281221064; cand. of phys. and math. sc.; associate professor.

УДК 621.396.94:621.376 DOI 10.18522/2311-3103-2020-5-141-149

Hussein Ahmed Mahmood, К.Е. Румянцев, Al-Karawi Hussein Shookor

ЭВОЛЮЦИЯ РАДИОСВЯЗИ ПО ОПТИЧЕСКОМУ КАНАЛУ СВЯЗИ В СВОБОДНОМ ПРОСТРАНСТВЕ С ИСПОЛЬЗОВАНИЕМ МУЛЬТИПЛЕКСИРОВАНИЯ ПОДНЕСУЩИХ С АМПЛИТУДНОЙ МАНИПУЛЯЦИЕЙ

В беспроводных системах и сетях отмечается высокий спрос на радиосвязь по оптическому каналу связи в свободном пространстве (RoFSO) с широкой полосой пропускания и высокой скоростью передачи данных. Такая связь обеспечивает такую же скорость передачи данных, как в волоконно-оптических системах, но при меньшей стоимости на её развёртывание. Системы RoFSO реализуются комбинированием радиосигнала (RF) с оптическим сигналом для беспроводных каналов в свободном пространстве (FSO). Предлагается моделирование системы с мультиплексированием поднесущих с амплитудной манипуляцией (SCM/ASK) для оптической связи в свободном пространстве. В системе Скорость передачи данных принята равной 1 Гбит/с. Электронный амплитудный модулятор настроен на радиосигнал 10 ГГц. К нему добавляются 100 каналов с частотным разнесением поднесущих частот на 10 МГц при рабочей частоте первого канала 60 МГц. Эти каналы поднесущих смешиваются с гармоническим радиосигналом с несущей частотой 10 ГГц в гибридном ответвителе со сдвигом фазы в 90º. Непрерывное лазерное излучение с входной мощностью 10 дБм и длиной волны 1550 нм модулируется сформированным радиосигналом в оптическом LiNb модуляторе Маха-Цендера на LiNb-кристалле. Выходной сигнал модулятора передаётся по разным оптическим линиям связи в свободном пространстве протяжённостью 300 ... 1000 м под воздействием атмосферной турбулентности, определяемой структурной характеристикой флуктуаций показателя преломления. Система оценивается с точки зрения Q-добротности и частоты ошибок бит (BER) с использованием программного обеспечения Optisystem. Показано, что максимальная протяжённость связи при слабой турбулентности ($C_n^2 = 5 \times 10^{-15}$ м$^{-2/3}$) и BER=10^{-9} составляет 950 м, а при сильной турбулентности ($C_n^2 = 5 \times 10^{-13}$ м$^{-2/3}$) – 850 м.

Радиосвязь; оптический канал; свободное пространство; поднесущие составляющие; мультиплексирование; амплитудная манипуляция; оптический модулятор Маха-Цендера; частоты ошибок бит; добротность.

Hussein Ahmed Mahmood, K.Y. Rumyantsev, Al-Karawi Hussein Shookor

EVOLUTION OF RADIO OVER FREE SPACE OPTICAL COMMUNICATION UTILIZING SUBCARRIER MULTIPLEXING / AMPLITUDE SHIFT KEYING

The high demand for increased bandwidth, data rate and quality in optical communication systems in modern applications. Radio over free space optics (RoFSO) is deemed a new design methodology over wireless systems and networks. This technique has to ensure data rates like ones presented by means optical fiber communication techniques in keeping with a portion of its arrangement cost. Such systems are implemented by combined radio signal (RF) with optical signal, which containing various wireless administrations and Free Space Optics (FSO) link. In this paper, the simulation and evaluation system of Subcarrier Multiplexing/Amplitude Shift Keying (SCM/ASK) transmitter for Free Space Optical Communication is proposed. 1Gb/s data Rate given to the system. Whilst 10 GHz radio frequency signal setting in electrical amplitude modulator. Thereafter, radio signal is added with 100 subcarrier channels of 10 MHz spacing channel at operated first channel frequency of 60 MHz. These subcarrier channels with 90^0 combined with 10 GHz sin wave signal (radio frequency) at hybrid coupler, the combination of each subcarriers and radio signal are modulated by LiNb Mach-Zehnder optical modulator with 1550 nm wavelength continues wave laser signal at 10 dBm input power. The optical modulated signal (after optical modulator) is transmitted over a various free space optical link from 300m to 1km under the Atmospheric turbulence effect (the structure feature of the refractive index). The system is evaluated utilizing Opti system software with Q-factor and BER terminology. It is shown that the maximum optical distance for weak turbulence ($C_n^2 = 5 \times 10^{-15}\ m^{-2/3}$) at BER equal to 10^{-9} is 950m, while the maximum optical distance for strong turbulence $C_n^2 = 5 \times 10^{-13}\ m^{-2/3}$) is 850m.

Subcarrier Multiplexing; Radio Over Free Space Optics; Amplitude Shift Keying (ASK); Mach-Zehnder optical modulator; Radio Signal (RF); Q-factor, Bit Error Rate (BER).

Introduction. There have been many advantages of free space optical communication (FSO) systems or wireless optical communication, for instance large capacity, unlicensed system, excellent protection and minimal cost-efficiency of transmitting high data rates besides radio frequency (RF) signals with the identical size as optical fiber [1–6]. Though, it's a feasible technology that corresponding with point-to-point communication. FSO communication systems effectiveness is highly vulnerable to adverse atmospheric situations caused by fluctuations in the deflective index due to temperature inhomogeneities and changes in pressure.[4]. Due to variations in the refractive index via transmission signal along the path link, atmospheric turbulence affects variations (scintillation) in both the intensity and phase of the received signal [2].

Many different mathematical models have recently been suggested to explain this variation based on atmospheric turbulence in both weak and strong fading regimes in the optical channel, such as:

1) log-normal distribution;
2) gamma-gamma distribution;
3) negative exponential dissemination [4–7].

In addition, In addition, the analysis of the malfunction probability and the median capacity of free – space channels is evaluated, derived from the closed form expression for the malfunction probability and the regular capacity of communication systems over atmospheric turbulence-induced fading channels modelled by the distribution of log-normal and gamma-gamma with regard to turbulence influences [2]. It is proposed to simulate and compare the hybrid modulation technique namely PPM-MSK-SIM based on PPM and MSK subcarrier strength modulation. Additionally, theoretical analysis of the BER performance under lognormal turbulence model for an avalanche photodetector system [8].

In Conjunction with using the SIM-DPSK modulation method over the lognormal turbulence channel, the performance review of the free space optical communication system is proposed with regard to the misalignment effects. Likewise, the formulas for the average of BER and probability have been derived [9]. For the FSO framework with avalanche photodetector receiver, it is proposed to derive theoretical representation for the average BER of the SIM-BPSK modulation format.

In addition, under the influence of the gamma-gamma atmospheric turbulence model, the magnitude fluctuation of the optical signal is regarded [10]. The simulation studies of optical communications utilized subcarrier phase shift keying intensity modulation over atmospheric turbulence conditions. The bit error rate is derived for optical system using either on/off key or subcarrier PSK intensity modulation format [11].

In relation to our knowledge, a study of the optical communication method of radio over free space using subcarrier multiplexing / Amplitude Shift Keying was not carried out in previous papers. Therefore, the assessment of radio over free space optical (FSO) transmission at different free space links from 300 m to 1 km with 10 GHz radio signal is fulfilled in this paper. It is proposed to handle all this under atmospheric turbulences conditions (weak and strong) utilizing subcarrier multiplexer/Amplitude Shift Keying (SCM/ASK) is suggested. In addition, the method of estimation is explained in terms of the BER Q-factor and value.

Theoretical analysis. This section presents a brief overview of the Amplitude Shift Keying (ASK), optical subcarrier multiplexing (SCM), optical modulation and gamma-gamma distribution model turbulence.

A. Amplitude Shift Keying (ASK)

Amplitude shift keying is a type of amplitude modulation which characterizes the binary data (0 or 1) for differences within the amplitude of a carrier wave. Fig. 1. is represented the waveform of the amplitude shift keying (ASK) signal, the transmitted ASK signal for symbol *i* is defined by [12].

$$S_i(t) = \sqrt{\frac{2E_i(t)}{T}}\cos(\omega_o t + \emptyset) \qquad \begin{Bmatrix} 0 \le t \le T \\ i = 1, \dots, M \end{Bmatrix}. \tag{1}$$

Where the amplitude phrase $\sqrt{2E_i(t)/T}$ will utilize M values, besides the phase term ϕ is a constant value.

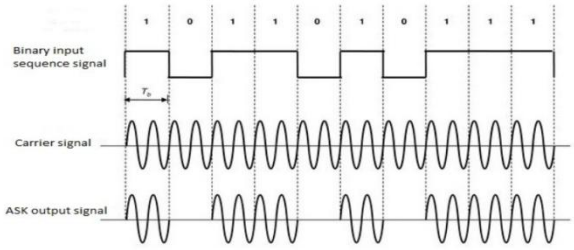

Fig. 1. Binary Amplitude Shift Keying (ASK)

B. Optical subcarrier multiplexing (SCM)

Optical subcarrier multiplexing (SCM) [13] is a system through it numerous signals are multiplexed in the radio frequencies domain as well as used to modulate with the light signal to be transferred through a single wavelength [14]. Furthermore, this system considers a more sensitive to noise effect and more flexible for superior data rate diffusion in the field of optical communication to increase the efficiency of the bandwidth [15]. The basic scheme of SCM is demonstrated in fig. 2.

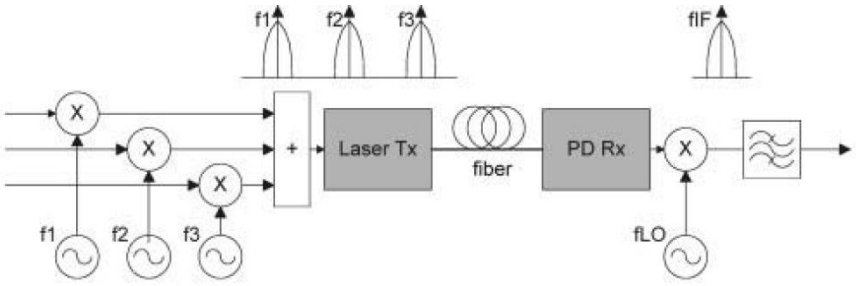

Fig. 2. The basic scheme of Subcarrier Multiplexing (SCM) within optical system [20]

C. Optical modulation

In optical communication systems, the electrical signal is modulated onto a light source (carrier) by an optical modulator. The configuration of Dual-Arm LiNb Mach-Zehnder optical Modulator is shown in fig. 3. The electric signal is divided into two signals V_1 and V_2 with 90^0 phase shifts between them, mathematical expression for each signal as given in Eq. (1).

$$V_1(t) = V_{RF}\cos(\omega_{RF}(t) + \emptyset(t)). \quad (2)$$

Where V_{RF}, $\omega_{RF}(t)$ and $\emptyset(t)$ correspond to the amplitude, frequency and phase of electrical signal component correspondingly, Whereas, the yield signal of dual-arm MZM which is define in Eq. (2) [16].

$$E_o = \frac{E_i}{2}\left[exp\left(j\pi\frac{V_1}{V_\pi}\right) + exp\left(j\pi\frac{V_2}{V_\pi}\right)\right]. \quad (3)$$

Where E_i is the light signal, V_1 and V_2 are the modulated electrical signals, V_π is the voltage to offer a phase shift to each phase modulator.

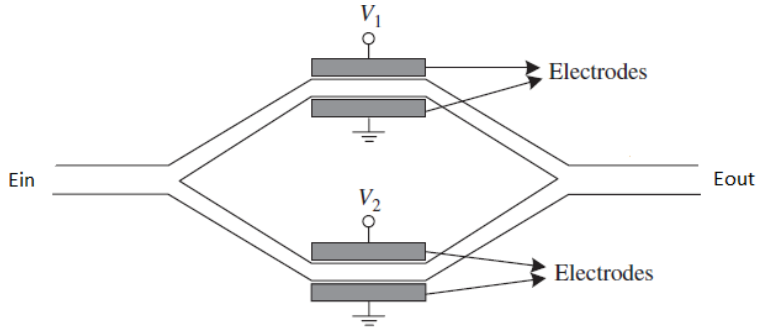

Fig. 3. The basic scheme Dual-Arm MZM [21]

D. Gamma-Gamma dissemination model turbulence

The gamma–gamma prototype is represent mutually small-scale in addition large-scale atmospheric fluctuations besides factor the irradiance such as the result of two separate random procedures, every getting a gamma PDF, as the expression following [4, 6, 17]:

$$f_I(I) = \frac{2(ab)^{(a+b)/2}}{\Gamma_{(a)}\Gamma_{(b)}} I^{\{(a+b)/2\}-1} K_{a-b}\left(2\sqrt{abI}\right). \quad (4)$$

Where $\Gamma(.)$ is the Gamma function, $K_n(.)$ is the modified Bessel function of the second kind of order n, a and b are the active numbers of small scale what is more large scale eddies of the scattering situation and characterized for spherical wave through aperture-averaged scintillation as following [4, 18, 19]

$$a = \left[exp\left(\frac{0.49\delta^2}{(1 + 0.18d^2 + 0.56\delta^{12/5})^{7/6}} \right) - 1 \right]^{-1} \quad (5)$$

and

$$b = \left[exp\left(\frac{0.51\delta^2}{(1 + 0.9d^2 + 0.62\delta^{12/5})^{5/6}} \right) - 1 \right]^{-1} \quad (6)$$

Where: $d = \sqrt{kD^2/4L}$, $k = 2\pi/\lambda$ is the optical wave number, L is the length of the optical link and D is the receiver's aperture diameter. The parameter δ^2 is the Rytov variance given by

$$\delta^2 = 1.23 C_n^2 k^{7/6} L^{11/6}. \quad (7)$$

Through C_n^2 being the altitude-dependent turbulence strength and changing from 10^{-17} to 10^{-13} $m^{-2/3}$ matching to the atmospheric turbulence terms.

Simulation setup. The proposed system of radio over free space optical communication utilizing subcarrier multiplexing/Amplitude Shift Keying transmitter is illustrated in fig..4. This system is simulated using optisystem software. The design simulation as well as system factors are inserted in table 1 and table 2 respectively.

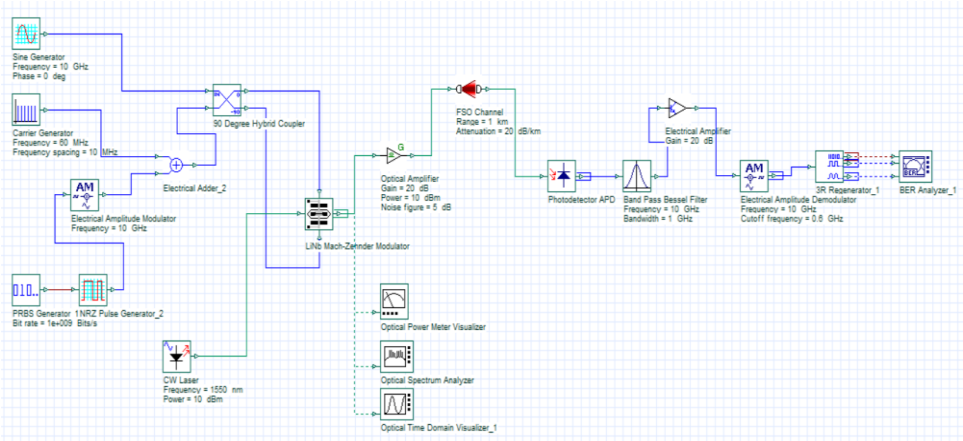

Fig. 4. Block diagram of proposed SCM/ASK free space optical communication system

Table 1

Layout simulation parameters

Parameters	Value
Bit rate G bit/s	1
Sequence length	64
Samples / bit	256
Central frequency (nm)	1550

Table 2

System parameters

Parameters	Value
ASK frequency GHz	10
Carrier generator frequency MHz	60
Sinewave generator frequency GHz	10
Optical amplifier gain dB	20
Optical amplifier power dBm	10
Optical amplifier noise figure dB	5
Free space channel attenuation dB/Km	20
APD photodiode responsivity A/W	0.9
APD photodiode dark current nA	10
Band pass Bessel filter frequency GHz	10
Bandwidth Bessel filter GHz	1
ASK demodulated frequency GHz	10
Low pass filter cutoff frequency GHz	0.6

A pseudo-random bit sequence (PRBS) initiator involves the transmitter and generates the modulation signal. The NRZ pulse generator has been utilized as low speed electrical coded. When setting the 10 GHz radio signal in the electric amplitude modulator as a baseband radio frequency converter. In this case, the frequency domain is given by the modulation format for amplitude shift keying (ASK). On the other hand, the radio frequency signal is modulated with subcarrier multiplexing, involving the setting of the carrier generator at 100 channels of the 10 MHz spacing channel at the 60 MHz first channel operated and the 10 GHz frequency of the sinewave signal generator. The 90^0 hybrid coupler is provided with these combined signals. A 90^0 hybrid coupler breaches the input signal into two output with 90^0 phase shift in the middle of each other. After that, the subcarrier radio signals of the hybrid coupler are came to the tow arm of LiNb Mach-Zehnder optical Modulator which modulate and adjust electrical signal to optical domain with continuous wave laser source has the yield power 10 dBm, linewidth of 10 MHz and 1550nm wavelength. In free space link, the transmitted signals are propagated over various lengths from 300m to 1km under different atmospheric turbulence conditions (gamma-gamma distribution model), weak ($C_n^2 = 5 \times 10^{-15}\ m^{-2/3}$) and strong $C_n^2 = 5 \times 10^{-13}\ m^{-2/3}$). Signals are processed on the receiver side of the APD photodiode used to transform optical signal to electrical signal with a 5-degree receiver gain, 0.9 A / W responsivity and 10 nA dark current. Subsequently, the subcarrier radio signal is transmitted at 10 GHz frequency and 1 GHz bandwidth through the electric band pass Bessel filter configuration. Radio signal demodulated by AM electric demodulator set to 10 GHz frequency and 0.6 GHz cut-off frequency after filter.

Results. Effects are simulated using version 10 of Opti system software. The transmission optical spectrum after the LiNb Mach-Zehnder optical modulator is shown in fig. 5. The Q-factor values vs. transmission distance are shown in fig. 6 (free space link from 300m to 1km) according to various atmospheric turbulence conditions (feeble

turbulence at $C_n^2 = 5 \times 10^{-15}\ m^{-2/3}$ and strong turbulence at $C_n^2 = 5 \times 10^{-13}\ m^{-2/3}$). At the same conditions, fig. 7 shown the values of bit error rate (BER) vs transmission distance. The evaluation system is depending of the special value of BER equal to 10^{-9}.

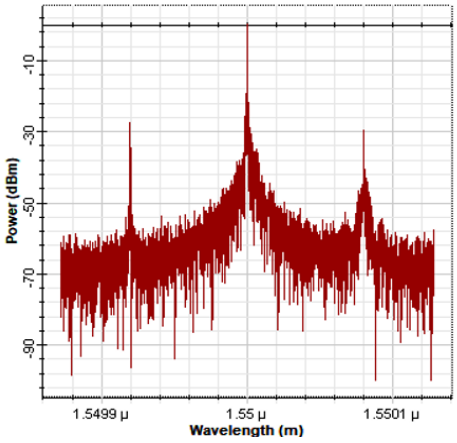

Fig. 5. optical spectrum at 1550nm wavelength after LiNb Mach-Zehnder optical Modulator

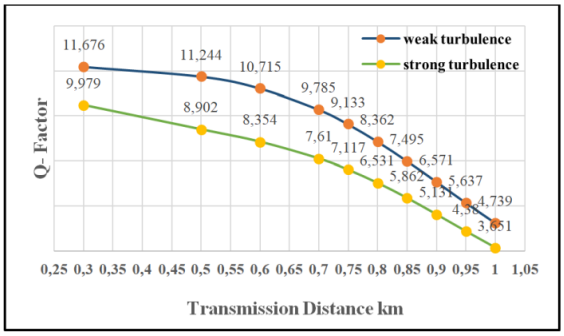

Fig. 6. Q-factor vs transmission distance for ($C_n^2 = 5 \times 10^{-15}\ m^{-2/3}$) frail turbulence (Blue line) and $C_n^2 = 5 \times 10^{-13}\ m^{-2/3}$) sturdy turbulence (Green line).

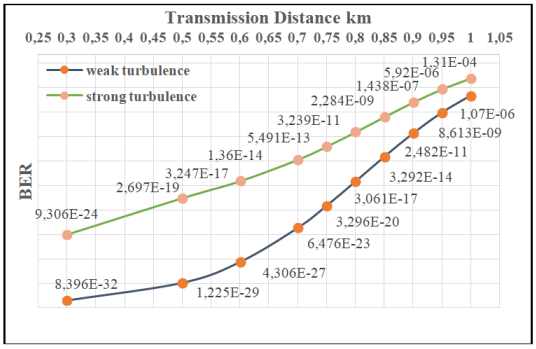

Fig. 7. BER vs transmission distance for ($C_n^2 = 5 \times 10^{-15}\ m^{-2/3}$) frail turbulence (Blue line) and $C_n^2 = 5 \times 10^{-13}\ m^{-2/3}$) sturdy turbulence (Green line)

Conclusion. We have proposed the subcarrier multiplexing/Amplitude Shift Keying transmitter system for radio over free space optical communication. Radio frequency, 10 GHz is modulated with the multiplexing portion of the subcarrier including the transporter generator and the sine wave signal. Free space optical channel under deferent atmospheric turbulence conditions weak and strong. The simulation system is reported that the maximum transmission distance for weak atmospheric turbulence is 950m at BER equal to 8.613×10^{-9} and Q-factor is 5.637. While the maximum transmission distance for strong atmospheric turbulence is 850m at BER equal to 2.284×10^{-9} and Q-factor is 5.862.

REFERENCES

1. *Kedar D. and Arnon S.* Urban optical wireless communication networks: the main challenges and possible solutions, *IEEE Commun. Mag.*, 2004, Vol. 42, No. 5, pp. S2-S7.
2. *Farid A.A. and Hranilovic S.* Outage capacity optimization for free-space optical links with pointing errors, *J. Light. Technol.*, 2007, Vol. 25, No. 7, pp. 1702-1710. Doi: 10.1109/JLT.2007.899174.
3. *Lim W., Yun C., and Kim K.* BER performance analysis of radio over free-space optical systems considering laser phase noise under Gamma-Gamma turbulence channels, *Opt. Express*, 2009, Vol. 17, No. 6, pp. 4479. Doi: 10.1364/oe.17.004479.
4. *Nistazakis H.E., Tsiftsis T.A., and Tombras G.S.* Performance analysis of free-space optical communication systems over atmospheric turbulence channels, *IET Commun.*, 2009, Vol. 3, No. 8, pp. 1402-1409. Doi: 10.1049/iet-com.2008.0212.
5. *Heatley D.J.T., Wisely D.R., Neild I., and Cochrane P.* Optical wireless: The story so far, *IEEE Commun. Mag.*, 1998, Vol. 36, No. 12, pp. 72-82. Doi: 10.1109/35.735881.
6. *Bekkali A., Ben Naila C., Kazaura K., Wakamori K., and Matsumoto M.* Transmission analysis of OFDM-based wireless services over turbulent radio-on-FSO links modeled by gamma–gamma distribution, *IEEE Photonics J.*, 2010, Vol. 2, No. 3, pp. 510-520.
7. *Andrews L.C., Phillips R.L., Hopen C.Y., and Al-Habash M.A.* Theory of optical scintillation, *J. Opt. Soc. Am. A*, 1999, Vol. 16, No. 6, p. 1417. Doi: 10.1364/josaa.16.001417.
8. *Liu H., Liao R., Wei Z., Hou Z., and Qiao Y.* BER Analysis of a Hybrid Modulation Scheme Based on PPM and MSK Subcarrier Intensity Modulation, *IEEE Photonics J.*, 2015, Vol. 7, No. 4, pp. 1-10. Doi: 10.1109/JPHOT.2015.2449265.
9. *Ismail T. and Leitgeb E.* Performance analysis of SIM-DPSK FSO system over lognormal fading with pointing errors, *Int. Conf. Transparent Opt. Networks*, 2016, Vol. 2016-Augus, No. 2, pp. 1-4. Doi: 10.1109/ICTON.2016.7550350.
10. *Petkovic M.I., Milic D.N., and Djordjevic G.T.* Optimisation of subcarrier intensity modulation binary phase-shift keying free space optical link with avalanche photodiode receiver influenced by gamma-gamma atmospheric turbulence and pointing errors, *IET Commun.*, 2016, Vol. 10, No. 12, pp. 1473-1479. Doi: 10.1049/iet-com.2015.0333.
11. *Li J., Liu J.Q., and Taylor D.P.* Intensity Modulation Through Atmospheric Turbulence Channels, *IEEE Trans. Commun.*, 2007, Vol. 55, No. 8, pp. 1598-1606,.
12. Sklar B. *Digital communications: fundamentals and applications*. 2001.
13. *Singh H., Singh M.L., and Singh R.* A novel full duplex 16 Gbps SCM/ASK radio over fiber WDM-PON sharing wavelength for up- and down-link using bidirectional reflective filter, *Optik (Stuttg).*, 2014, Vol. 125, No. 14, pp. 3473-3475. Doi: 10.1016/j.ijleo.2014.01.064.
14. *Mahmood H.A. and Rumyantsev K.Y.* Effect of FBG Compensated Dispersion on SCM/ASK Radio over Fiber System, *Proc. - 2019 12th Int. Congr. Image Signal Process. Biomed. Eng. Informatics, CISP-BMEI 2019*, 2019, pp. 3-7. Doi: 10.1109/CISP-BMEI48845.2019.8966032.
15. *Hui R., Zhu B., Huang R., Allen C.T., Demarest K.R., and Richards D.* Subcarrier multiplexing for high-speed optical transmission, *J. Light. Technol.*, 2002, Vol. 20, No. 3, pp. 417-427. Doi: 10.1109/50.988990.
16. *Ho K.P. and Cuei H.W.* Generation of arbitrary quadrature signals using one dual-drive modulator, *J. Light. Technol.*, 2005, Vol. 23, No. 2, pp. 764-770. Doi: 10.1109/JLT.2004.838855.
17. *Majumdar A.K.* Free-space laser communication performance in the atmospheric channel, *J. Opt. Fiber Commun. Reports*, 2005, Vol. 2, No. 4, pp. 345-396. Doi: 10.1007/s10297-005-0054-0.

18. *Uysal M., Li J., and Yu M.* Error rate performance analysis of coded free-space optical links over gamma-gamma atmospheric turbulence channels, *IEEE Trans. Wirel. Commun.*, 2006, Vol. 5, No. 6, pp. 1229-1233. Doi: 10.1109/TWC.2006.1638639.
19. *Vu B.T., Dang N.T., Thang T.C., and Pham A.T*. Bit error rate analysis of rectangular QAM/FSO systems using an APD receiver over atmospheric turbulence channels, *J. Opt. Commun. Netw.*, 2013, Vol. 5, No. 5, pp. 437-446. Doi: 10.1364/JOCN.5.000437.
20. *Gomes N.J., Monteiro P.P., and Gameiro A. Next generation wireless communications using radio over fiber*. John Wiley & Sons, 2012.
21. *Kumar S. and Deen M.J*. Fiber optic communications: Fundamentals and applications, *Fiber Optic Communications: Fundamentals and Applications*, 2014, Vol. 9780470518. pp. 1-553. Doi: 10.1002/9781118684207.

Статью рекомендовал к опубликованию д.т.н., профессор О.И. Шелухин.

Hussein Ahmed Mahmood – Диялайский университет; e-mail: hussein.ahmed8282@gmail.com; Дияла, Ирак; кафедра инженерных коммуникаций.

Al-Karawi Hussein Shookor – e-mail: alkarawi80@gmail.com; кафедра инженерных коммуникаций.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; г. Таганог, Россия; тел.: 89281827209; д.т.н.; профессор.

Hussein Ahmed Mahmood – College of Engineering, University of Diyala; e-mail: hussein.ahmed8282@gmail.com; Diyala, Iraq; the department of communications engineering.

Al-Karawi Hussein Shookor – e-mail: alkarawi80@gmail.com; the department of communications engineering.

Rumyantsev Konstantin Yvgen'evich – Southern Federal University; e-mail: rke2004@mail.ru; Taganrog, Russia; phone: +79281827209; dr. of eng. sc.; professor.

Раздел III. Информационный анализ

УДК 004.056.52 DOI 10.18522/2311-3103-2020-5-150-158

В.В. Лапшичёв, О.Б. Макаревич

НАБОР ПРИЗНАКОВ УСТАНОВЛЕНИЯ HTTPS-СОЕДИНЕНИЯ TLS V1.3 ПРОГРАММНЫМ КОМПЛЕКСОМ «TOR»

Пресечение незаконной деятельности пользователей сети Интернет является одной из актуальных проблем обеспечения информационной безопасности в Российской Федерации. Пресечение деятельности лиц, совершающих противоправные действия с использованием цифровых технологий, в частности, при помощи анонимной сети «Tor», является одной из задач федеральных правоохранительных органов, обеспечивающих информационную безопасность. Сложность выявления и идентификации использования программного комплекса «Tor» в сетях передачи данных обусловлена целым рядом мер, предпринятых его разработчиками, направленными на маскирование потока данных комплекса, среди которых использование современных алгоритмов шифрования пакетов данных. Целью работы является создание и описание набора признаков установления https-соединения программным комплексом «Tor» в условиях применения TLS-шифрования данных протоколом версии v1.3. Задачами работы являются подготовка и анализ материалов трафика программного комплекса «Tor», а также создание на основе полученных данных набора признаков установления соединения между клиентом и сервером анонимной сети. В ходе анализа потока данных анонимной сети исследовался этап установления соединения между клиентом и входным сервером цепи узлов сети «Tor», так называемое «TLS-рукопожатие». Следует отметить, что данная работа дополняет предыдущие исследования по тематике анализа TLS-шифрования в части, касающейся применяемого с 2018 года протокола шифрования TLS v1.3, описывая его особенности как часть механизма реализации анонимизации программным комплексом «Tor». Авторы предлагают использовать размер пакетов «TLS-рукопожатия» в качестве основных признаков, несущих идентифицирующую информацию об установлении анонимного соединения между клиентом и узлом сети «Tor». Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) в рамках научного проекта №23/2020.

Программный комплекс «Tor»; обфускация данных; TLS-рукопожатие; протокол шифрования версии TLS v1.3; законное блокирование доступа.

V.V. Lapshichyov, O.B. Makarevich

SET OF DISTINCTIVE FEATURES OF TLS V1.3 HTTPS-CONNECTION ESTABLISHING BY TOR SOFTWARE COMPLEX

The suppression of illegal activities of Internet users is one of the urgent problems of information security in the Russian Federation. The suppression of the activities of persons committing illegal actions using digital technologies, in particular, using the Tor anonymous network, is one of the tasks of federal law enforcement agencies that ensure information security. The difficulty of detecting and identifying the use of the Tor software package in data transmission networks is due to a number of measures taken by its developers aimed at masking the data flow of the complex, including the use of modern algorithms for encryption of data packets. The aim of the work is to create and describe a set of attributes for establishing an https-connection by the Tor software

package in the context of using TLS data encryption using the version 1.3 protocol. The tasks of the work are the preparation and analysis of traffic materials of the Tor software package, as well as the creation, based on the data obtained, of a set of signs of establishing a connection between the client and the server of the anonymous network. In the course of analyzing the data flow of the anonymous network, the stage of establishing a connection between the client and the input server of the chain of nodes of the Tor network, the so-called "TLS handshake", was investigated. It should be noted that this work complements previous studies on the analysis of TLS encryption in terms of the TLS v1.3 encryption protocol used since 2018, describing its features as part of the mechanism for implementing anonymization by the Tor software package. The authors propose to use the size of the "TLS handshake" packets as the main features that carry identifying information about the establishment of an anonymous connection between the client and the Tor network node. The reported study was funded by Russian Ministry of Science (information security), project number 23/2020.

«Tor» software complex; obfuscation of data; TLS handshake; encryption protocol TLS v1.3; legal blocking of access.

Введение. В ряде работ, посвященных тематике выявления и идентификации использования программного комплекса «Tor», деанонимизации его пользователей, предлагается реализация анализа потока данных различными формами и методами: анализ действий злоумышленника с использованием открытых баз анонимизирующих ресурсов, в том числе, выходных узлов сети «Tor» [1], использованием гравитационной кластеризации [2], пассивного долгосрочного анализа трафика сети «Tor» [3], классической атаки «человек посередине», MITM (man-in-the-middle) [4–5], применением наиболее эффективного на сегодняшний момент «глубокого анализа пакетов», DPI (deep packet inspection) [6–7]. Благодаря утечке документов ограниченного распространения специальных служб Великобритании и США, ответственных за информационную безопасность, стало известно, что ими ведутся разработки собственных технологий выявления трафика сети «Tor» и деанонимизации её пользователей, а также содержание этих разработок и их принципы [8–15]. При этом в своих исследованиях они также используют вышеперечисленные приемы и методы. В отдельных работах внимание исследователей помимо всего прочего обращено на анализ свойств самоподписываемых сертификатов X.509, используемых сетью «Tor» в ходе установления соединения с клиентом, изучение которых и стало основной задачей исследований авторов статьи.

Авторами в ходе проведенных исследований, направленных на разработку метода обнаружения и идентификации использования программного комплекса «Tor», подготовлен ряд статей [16–20], в которых рассматриваются как отдельные характеризующие признаки соединений (размер сертификатов X.509, имена субъекта и объекта сертификации, используемые для подключения порты), устанавливаемых сетью «Tor», так и предлагается алгоритм, использующий эти признаки, для осуществления законного блокирования доступа клиента данной сети к входному узлу. В последние несколько лет в ходе подключения к сети Tor стали использоваться сервисы подключаемых транспортных протоколов (Pluggable Transports, PT) (обфускаторов), которые маскируют поток данных с целью предотвращения его анализа снифферами. В качестве дополнительной меры защиты данных от идентификации применяется TLS-шифрование версии v1.3, которое позволяет сократить процесс рукопожатия между клиентом и сервером сети «Tor» и шифрует пакеты данных, в том числе сертификат, при установлении соединения.

Учитывая, что авторами уже проведены исследования рукопожатия TLS-шифрования версии v1.2 и приведены наборы признаков и алгоритм блокирования подключения к сети [16-18, 20], предлагаемая статья содержит результаты исследования данных начального этапа реализации TLS-шифрования версии v1.3 в ходе установления соединения, а также признаков такого соединения.

Несмотря не то, что в Российской Федерации в настоящее время, вслед за Китаем, рассматривается вопрос законодательного ограничения использования протокола TLS-шифрования версии v1.3, выявление и идентификация протоколов обоих версий для законного блокирования установления соединения с сетью «Tor» не теряет своей актуальности.

Анализ соединения с сетью «Tor». В ходе анализа соединения с сетью «Tor» исследовалась стадия установления зашифрованного соединения т.н. «TLS-рукопожатия», которое в версии TLS v1.3 оказалось не менее информативным, чем в TLS v1.2, несмотря на практически изначальное шифрование передаваемых данных.

Для проведения исследования потока данных сети «Tor», а также процессов установления и осуществления соединения, в том числе рукопожатия между клиентом и сервером, через сервис сайта bridges.torproject.org был получен набор пар данных для подключения вида [`IP-адрес:порт`], заведомо не использующие обфускацию передаваемой информации:

```
[92.206.11.41:993; 45.155.157.193:9001;
81.202.93.10:9001; 95.217.197.205:11900;
144.76.185.37:9001; 185.220.101.77:5989].
```

Каждая из пар была добавлена в поле «Вставьте узлы из доверенных источников» на странице настроек браузера «Tor» `about:preferences#tor` в качестве адреса входного узла сети для подключения клиента. После чего было произведено соединение с сетью «Tor». Захват данных, передаваемых онлайн между клиентом и сервером «Tor», осуществлялся при помощи сниффера «Wireshark», которые затем сохранялись в дампы с расширением «.pcap» для дальнейшего анализа офлайн.

Для ограничения постороннего трафика данных исследование проводилось в программной среде «Kali Linux», установленной на виртуальной машине Oracle VM VirtualBox.

Следует отметить, что классическая схема рукопожатия версии протокола TLS v1.2 (полученная путем анализа этих же дампов, т.к. эта версия тоже используется в отдельных случаях) упрощенно состоит из следующих друг за другом пакетов: запрос на подключение клиента `client_hello`, ответ о возможности подключении к серверу `server_hello`, передача сертификата сервера клиенту `certificate`, передача ключей сервера для шифрования `server_key_exchange`, окончание процесса рукопожатия `server_hello_done`.

В ходе исследования выявлена схема рукопожатия версии TLS v1.3, применяемая в установлении соединения «Tor», которая характеризуется набором признаков, позволяющих отличить это соединение от других подобных. Следует отметить, что только фрейм `server_hello` передается незашифрованным, тогда как `change_cipher_spec` и фреймы `application_data` передаются в зашифрованном виде. Весь поток данных протокола TLS v1.3 содержит 5 описаний фреймов: `client_hello` (запрос на установление соединения клиентом), `server_hello` (ответ сервера об установлении соединения), `change_cipher_spec` (изменение наборов шифров, используемых при установлении соединения), `application_data` (зашифрованные данные приложения) и `continuation_data` (данные для продолжения соединения), при этом фреймы `application_data` занимают приблизительно 90% от всего количества передаваемых данных.

В табл. 1 представлены результаты анализа пакетов и фреймов соединений между клиентом и сетью «Tor», особенностью которых является прямой обмен между локальным IP-адресом 10.0.2.15 и IP-адресами сети «Tor».

Таблица 1

Результаты анализа пакетов рукопожатия «Tor»

Вид пакета	Размер пакета (размер TLS фрей-мов), байт	Размер TLS фреймов v1.3, байт					
		Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
Соединение 10.0.2.15:443↔92.206.11.41:993							
Client Hello	385	-	-	-	-	-	-
Server Hello	1229 (1143)	155	1	23	614	281	69
Соединение 10.0.2.15:443↔ 45.155.157.193:9001							
Client Hello	378	-	-	-	-	-	-
Server Hello	1233 (1147)	155	1	23	618	281	69
Соединение 10.0.2.15:443↔ 81.202.93.10:9001							
Client Hello	376	-	-	-	-	-	-
Server Hello	1226 (1140)	155	1	23	611	281	69
Соединение 10.0.2.15:443↔ 95.217.197.205:11900							
Client Hello	377	-	-	-	-	-	-
Server Hello	1234 (1148)	155	1	23	619	281	69
Соединение 10.0.2.15:443↔ 144.76.185.37:9001							
Client Hello	379	-	-	-	-	-	-
Server Hello	1063 (987)	не учитываются из-за подключения по версии TLSv1.2					
Соединение 10.0.2.15:443↔ 185.220.101.77:5989							
Client Hello	375	-	-	-	-	-	-
Server Hello	1221 (1135)	155	1	23	606	281	69

Следует отметить, что одно из соединений использовало протокол TLS v1.2, в котором пакет `server_hello` меньше почти на 200 байт типичного для версии v1.3 размера пакета, хотя клиентский пакет был передан в версии v1.3. При этом было реализовано характерное для версии 1.2 рукопожатие, в ходе которого был передан в незашифрованном виде сертификат (593 байта).

Для верификации результатов анализа контрольной группы адресов из списка узлов сети «Tor» был взят случайный адрес `193.106.166.105`, не использующий обфускацию, который был добавлен в качестве входного узла. При этом сначала подключение велось путем запуска браузера «Tor» и его последующего закрытия, а затем производилась смена цепочки узлов нажатием на соответствующую команду меню. Таким образом были применены различные способы воздействия на программный комплекс для реализации иных вариантов соединения с анонимной сетью и достижения большего количества рукопожатий. Результаты представлены в табл. 2.

Таблица 2

Результаты анализа дополнительного набора пакетов «Tor»

Вид пакета	Размер пакета (размер TLS фрей-мов), байт	Размер TLS фреймов v1.3, байт					
		Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
Запуск/закрытие браузера «Tor»							
Client Hello	371	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69
Client Hello	389	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69

Client Hello	390	-	-	-	-	-	-
Server Hello	1225 (1141)	155	1	23	612	281	69
Client Hello	387	-	-	-	-	-	-
Server Hello	1221 (1137)	155	1	23	608	281	69
Смена цепочки узлов сети «Tor»							
Client Hello	385	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	382	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	369	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	389	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	370	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	380	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	374	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	381	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69
Client Hello	379	-	-	-	-	-	-
Server Hello	1226 (1142)	155	1	23	613	281	69

В итоге размер пакета `client_hello` находится в пределах от 369 до 385 байт, а `server_hello` – в пределах от 1221 до 1234 байт. При этом часть `server_hello`, относящаяся непосредственно к TLS-шифрованию имеет постоянные размеры фреймов, за исключением 4-го фрейма, который предположительно, содержит зашифрованный файл сертификата, размер которого приближается к установленному размеру сертификата в TLS v1.2 [16–18]. Порядок расположения величин фреймов в пакете `server_hello` указан на рис. 1. Данный порядок размеров фреймов может служить частью набора признаков для осуществления блокирования путем сравнения размеров, где 619 байт ≥ n ≥ 606 байт.

Server Hello	Change Cipher Spec	Application Data	Application Data	Application Data	Application Data
155	1	23	n	281	69

Рис. 1. Структура пакета `server_hello` «Tor» с размерами фреймов

Сравнительный анализ https-соединения «vk.com». В целях сравнительного анализа свойств и данных отличного от «Tor» https-соединения, использующего версию протокола шифрования TLS v1.3, было проведено практическое рассмотрение https-соединений в сети «Интернет», которое указало на тот факт, что большинство сайтов на момент проведения исследования используют старую версию установления зашифрованного соединения по протоколу TLS v1.2. Тем не менее, такие сайты, как facebook.com, instagram.com, twitter.com, vk.com, используют всё

же новую версию – TLS v1.3. Поскольку исследование ориентировано на российский сегмент сети «Интернет», для изучения передачи данных был выбран сайт социальной сети «ВКонтакте» (vk.com). Для сравнения данных соединения сервера «Tor» после успешного подключения производился переход на заглавную страницу социальной сети «ВКонтакте» (vk.com).

Исследуя обмен данными браузера «Tor» с сайтом соцсети «ВКонтакте», использующей сертификаты X.509 для установления зашифрованного соединения по протоколу TLS v1.3, выявлено следующее. Пакет `client_hello`, передаваемый во время осуществления всех 6 указанных выше подключений между браузером «Tor» и соцсетью «ВКонтакте», имел размер 585 байт, а `server_hello` передавался также 6 фреймами, но они были разбиты на два пакета (3554 и 662 байта) по 3 фрейма каждый и имели другой размер. Структура пакета `server_hello` социальной сети «ВКонтакте» по результатам анализа представлена на рис. 2. Соединение с сервером vk.com осуществляется зеркалированием на виртуальный интерфейс – IP-адрес локального хоста 127.0.0.1, а не прямым соединением с IP-адресом соцсети.

1-й пакет	Server Hello	Change Cipher Spec	Application Data
	122	1	36
2-й пакет	Application Data	Application Data	Application Data
	3726	96	69

Рис. 2. Структура пакета `server_hello` соцсети «ВКонтакте»

Сравнение структуры пакетов сети «Tor» и соцсети «ВКонтакте» позволяет отметить схожесть пакетов `server_hello` обоих ресурсов, отличающихся наличием 6-ти фреймовой структурой, определенным порядком фреймов `server_hello-change_cipher_spec-application_data-application_data-application_data-application_data` и постоянством их величин. Однако есть и отличия, заключающиеся в разбиении `server_hello` социальной сети «ВКонтакте» на два пакета (в противоположность единому пакету у «Tor»), а также в переменном размере 4-го фрейма пакета сети «Tor», который по размерам соотносится с сертификатом «Tor», используемом в протоколе TLS v1.2 [16–18].

Таким образом набором признаков соединения сети «Tor» при шифровании данных с помощью алгоритма TLS v1.3 будут являться:

- размер пакета `client_hello` (369-385 байт);
- размер пакета `server_hello` (1221-1234 байт);
- структура фреймов пакета `server_hello` (`server_hello-change_cipher_spec-application_data-application_data-application _data-application_data`);
- величины фреймов пакета `server_hello` (155-1-23-n-281-69 байт) и их расположение в установленном порядке;
- величина 4-го фрейма (n, где 619 байт ≥ n ≥ 606 байт).

Заключение. В работе представлены результаты подготовки и анализа снифферером Wireshark материалов трафика программного комплекса «Tor», а также созданный на основе полученных данных набор признаков установления соединения между клиентом и сервером анонимной сети.

Исследован этап установления соединения (TLS-рукопожатие) между клиентом и входным сервером цепи узлов сети «Tor», проведено описание структуры пакетов и сравнение их со структурой пакетов другого сервиса, использующего протокол TLS v1.3.

Проведена верификация результатов анализа различными способами воздействия на программный комплекс для реализации иных вариантов соединения с анонимной сетью.

В ходе верификации было установлено, что порядок фреймов в пакете, передаваемом сетью «Tor», и их размер остался неизменным, за исключением переменного значения n 4-го фрейма, которое соотносится с размером сертификата сети «Tor», шифруемого протоколом TLS v1.2.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Басыня Е.А., Хиценко В.Е., Рудковский А.А.* Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, № 2. – С. 45-51. – DOI: 10.21293/1818-0442-2019-22-2-45-51.
2. *Rao Z., Niu W., Zhang X.S., Li H.* Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Networking and Applications: Vol. 11, Issue 3. – New York: Springer Science+Business Media, 2017. – P. 592-601.
3. *Amann J., Sommer R*. Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement. Paper presented at the Passive and Active Measurement Conference (PAM), Heraklion, Crete, Greece, 2016.
4. *Makrushin D., Garnaeva M.* Uncovering Tor users: where anonymity ends in the Darknet. Kaspersky Lab SecureList. 18.06.2015. – URL https://securelist.com/uncovering-Tor-users-where-anonymity-ends-in-the-darknet/70673 (дата обращения: 03.11.2020).
5. *Лазаренко А.В.* Технологии деанонимизации пользователей «Tor» // Новые информационные технологии в автоматизированных системах. – 2016. – С. 19. – URL: https://cyberleninka.ru/article/v/tehnologii-deanonimizatsii-polzovateley-Tor (дата обращения: 01.11.2020).
6. *Sommer R., Amann J., Hall S*. Spicy: A Unified Deep Packet Inspection Framework Dissecting All Your Data (ICSI Technical Report), Berkeley, CA, USA, University of California, International Computer Science Institute, 2015.
7. *Ferry A.S., Isbat U.N., Balighani F.B.* Detecting and blocking onion router traffic using deep packet inspection. Paper presented at International Electronics Symposium (IES), Denpasar, Indonesia, 2017.
8. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0d08.dir/doc.pdf (дата обращения: 01.11.2020).
9. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network – Slides. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HA SHf400.dir/doc.pdf (дата обращения: 02.11.2020).
10. Government Communications Headquarters. Tor Hidden Services How Hidden is 'Hidden'? Applied Research. Snowden Surveillance Archive, 2011. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH3ae6.dir/doc.pdf (дата обращения: 02.11.2020).
11. National Security Agency. Tor - 2006 CES Summer Program. Snowden Surveillance Archive, 2006. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/ snowden1/index/ assoc/HASHbefc.dir/doc.pdf (дата обращения: 03.11.2020).
12. National Security Agency. TLS trends at GCHQ, Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2236.dir/doc.pdf (дата обращения: 04.11.2020).
13. National Security Agency. Tor Stinks. Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH7920.dir/doc.pdf (дата обращения: 03.11.2020).

14. National Security Agency. Types of IAT - Advanced Open Source Multi-Hop. Snowden Surveillance Archive, 2012. – URL: https://snowdenarchive.cjfe.org/ greenstone/collect/snowden1/index/assoc/HASH01ad/bb7e08bf.dir/doc.pdf (дата обращения: 01.11.2020).
15. National Security Agency (2013). Peeling Back the Layers of Tor with EGOTISTICAL GIRAFFE. Snowden Surveillance Archive, 2013. – URL: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.
16. *Лапшичёв В.В. Макаревич О.Б.* Метод обнаружения и идентификации использования программного комплекса «Тор» // Информатизация и связь. – 2020. – № 3. – С. 17-20. – DOI: 10.34219/2078-8320-2020-11-3-17-20.
17. *Lapshichyov V.V., Makarevich O.B.* TLS Certificate As A Sign Of Establishing A Connection With The Network Tor // The 12th International Conference on Security of Information and Networks (SIN 2019): Proceedings of the 12th International Conference on Security of Information and Networks. – 2019. – P. 92-97. – DOI: 10.1145/3357613.3357628.
18. *Lapshichev V.V.* TLS Certificates of the Tor Network And Their Distinctive Features // International Journal of Systems and Software Security and Protection. – 2019. – Vol. 10, No. 2. – P. 20-43. – DOI: 10.4018/IJSSSP.2019070102.
19. *Lapshichyov V., Makarevich O.* Technology of Deep Packet Inspection For Recognition And Blocking Traffic of the Tor Network // Безопасность информации и компьютерных сетей (SIN 2019): Матер. 12-й Международной научной конференции. – 2019. – С. 24-27.
20. *Lapshichyov V., Makarevich O.* Algorithm for Analyzing And Blocking Access to the Tor Network // Безопасность информации и компьютерных сетей (SIN 2019): Матер.12-й Международной научной конференции. – 2019. – С. 27-30.

REFERENCES

1. *Basynya E.A., Khitsenko V.E., Rudkovskiy A.A.* Metod identifikatsii kiberprestupnikov, ispol'zuyushchikh instrumenty setevogo analiza informatsionnykh sistem s primeneniem tekhnologiy anonimizatsii [Method of identification of cybercriminals using tools of network analysis of information systems using anonymization technologies], *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Reports of Tomsk State University of Control Systems and Radioelectronics], 2019, Vol. 22, No. 2, pp. 45-51. DOI: 10.21293/1818-0442-2019-22-2-45-51.
2. *Rao Z., Niu W., Zhang X.S., Li H.* Tor anonymous traffic identification based on gravitational clustering. Peer-to-Peer Networking and Applications: Vol. 11, Issue 3. New York: Springer Science+Business Media, 2017, pp. 592-601.
3. *Amann J., Sommer R*. Exploring Tor's Activity Through Long-term Passive TLS Traffic Measurement. Paper presented at the Passive and Active Measurement Conference (PAM), Heraklion, Crete, Greece, 2016.
4. *Makrushin D., Garnaeva M.* Uncovering Tor users: where anonymity ends in the Darknet. Kaspersky Lab SecureList. 18.06.2015. Available at: https://securelist.com/uncovering-Tor-users-where-anonymity-ends-in-the-darknet/70673 (accessed 03 November 2020).
5. *Lazarenko A.V.* Tekhnologii deanonimizatsii pol'zovateley «Tor» [Technologies of deanonymization of users "Tor"], *Novye informatsionnye tekhnologii v avtomatizirovannykh sistemakh* [New information technologies in automated systems], 2016, pp. 19. Available at: https://cyberleninka.ru/article/v/tehnologii-deanonimizatsii-polzovateley-Tor (accessed 01 November 2020).
6. *Sommer R., Amann J., Hall S*. Spicy: A Unified Deep Packet Inspection Framework Dissecting All Your Data (ICSI Technical Report), Berkeley, CA, USA, University of California, International Computer Science Institute, 2015.
7. *Ferry A.S., Isbat U.N., Balighani F.B.* Detecting and blocking onion router traffic using deep packet inspection. Paper presented at International Electronics Symposium (IES), Denpasar, Indonesia, 2017.
8. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0d08.dir/doc.pdf (accessed 01 November 2020).

9. Government Communications Headquarters. A potential technique to deanonymise users of the Tor network – Slides. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASHf400.dir/doc.pdf (accessed 02 November 2020).
10. Government Communications Headquarters. Tor Hidden Services How Hidden is 'Hidden'? Applied Research. Snowden Surveillance Archive, 2011. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH3ae6.dir/doc.pdf (accessed 02 November 2020).
11. National Security Agency. Tor - 2006 CES Summer Program. Snowden Surveillance Archive, 2006. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/ snowden1/index/assoc/HASHbefc.dir/doc.pdf (accessed 03 November 2020).
12. National Security Agency. TLS trends at GCHQ, Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH2236.dir/doc.pdf (accessed 04 November 2020).
13. National Security Agency. Tor Stinks. Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH7920.dir/doc.pdf (accessed 03 November 2020).
14. National Security Agency. Types of IAT - Advanced Open Source Multi-Hop. Snowden Surveillance Archive, 2012. Available at: https://snowdenarchive.cjfe.org/greenstone/ collect/snowden1/index/assoc/HASH01ad/bb7e08bf.dir/doc.pdf (accessed 01 November 2020).
15. National Security Agency (2013). Peeling Back the Layers of Tor with EGOTISTICAL GIRAFFE. Snowden Surveillance Archive, 2013. Available at: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.
16. *Lapshichev V.V. Makarevich O.B.* Metod obnaruzheniya i identifikatsii ispol'zovaniya programmnogo kompleksa «Tor» [Method of detection and identification of the use of the software complex "Tor"], *Informatizatsiya i svyaz'* [Informatization and Communication], 2020, No. 3, pp. 17-20. DOI: 10.34219/2078-8320-2020-11-3-17-20.
17. *Lapshichyov V.V., Makarevich O.B.* TLS Certificate as a Sign of Establishing A Connection With the Network Tor, *The 12th International Conference on Security of Information and Networks (SIN 2019): Proceedings of the 12th International Conference on Security of Information and Networks*, 2019, pp. 92-97. DOI: 10.1145/3357613.3357628.
18. *Lapshichev V.V.* TLS Certificates of the Tor Network and Their Distinctive Features, *International Journal of Systems and Software Security and Protection*, 2019, Vol. 10, No. 2, pp. 20-43. DOI: 10.4018/IJSSSP.2019070102.
19. *Lapshichyov V., Makarevich O.* Technology of Deep Packet Inspection For Recognition And Blocking Traffic of the Tor Network, *Bezopasnost' informatsii i komp'yuternykh setey (SIN 2019): Mater. 12-y Mezhdunarodnoy nauchnoy konferentsii* [Information Security and Computer Networks (SIN 2019): Proceedings of the 12th International Scientific Conference], 2019, pp. 24-27.
20. *Lapshichyov V., Makarevich O.* Algorithm for Analyzing And Blocking Access to the Tor Network, *Bezopasnost' informatsii i komp'yuternykh setey (SIN 2019): Mater. 12-y Mezhdunarodnoy nauchnoy konferentsii* [Information Security and Computer Networks (SIN 2019): Proceedings of the 12th International Scientific Conference], 2019, pp. 27-30.

Статью рекомендовала к опубликованию д.т.н., профессор Н.И. Червякова.

Лапшичёв Виталий Витальевич – Южный федеральный университет; e-mail: lapshichyov@sfedu.ru; г. Таганрог, ул. Чехова, 2; тел.: +79043467763; кафедра безопасности информационных технологий; аспирант.

Макаревич Олег Борисович – e-mail: obmakarevich@sfedu.ru; кафедра безопасности информационных технологий; д.т.н.; профессор.

Lapshichyov Vitaly Vitalyevich – South Federal University; e-mail: lapshichyov@sfedu.ru; 2, Chekhov street, Taganrog, Russia; phone: +79043467763; the department of IT Security; postgraduate student.

Makarevich Oleg Borisovich – e-mail: obmakarevich@sfedu.ru; the department of IT Security; dr. of eng. sc.; professor.

УДК 519.688 DOI 10.18522/2311-3103-2020-5-159-171

С.Л. Беляков, М.Л. Белякова, С.А. Зубков, Н.А. Голова, К.С. Яворчук

ТРАНСФОРМИРОВАНИЕ ОПЫТА ПРИНЯТИЯ РЕШЕНИЙ В ПРОСТРАНСТВЕННЫХ СИТУАЦИЯХ*

Рассматривается задача переноса опыта принятия решений в ситуационном анализе, использующим геоинформационные системы. Необходимость интеллектуальной поддержки со стороны геоинформационной системы обусловлена тем, что пространственные объекты и связи реального мира чрезвычайно динамичны. Применять в этих условиях аналитические модели процессов и явлений не удается из-за неполноты и противоречивости описывающей их информации. Статистические модели зависят от большого числа факторов, которое варьируется при изменении географического положения ситуации. Альтернативой может стать использование опыта экспертов, способных принимать эффективные решения в локальных пространственных ситуациях. Неконтролируемость повторного использования опыта является проблемой. Знания, полученные при выработке решений в одной местности, могут привести к неадекватным решениям в другой местности. Опыт решения проблемы в одной и той же местности теряет свою значимость с течением времени. В работе предлагается представление знаний в виде образа, состоящего из центра и допустимых преобразований центра. Вводятся функции трансформирования образов, выполняющие перенос знаний. Анализируются свойства функций трансформирования, которые несут в себе процедурное знание об образах ситуаций. Рассматривается использование выявленных свойств для формирования плана тестирования программных процедур трансформирования. Изучаются критерии успешного трансформирования. Формулируется оптимизационная задача поиска наилучшей функции трансформирования в базе знаний ГИС. Предлагается обобщенная методика трансформирования опыта. Приводится пример синтеза методов трансформирования для выбора центра оперативного обслуживания вызовов. Образ ситуации принятия решения о выборе земельного участка для центра обслуживания, трансформируется в заданную область на карте ГИС.

Интеллектуальные геоинформационные системы; ситуационный анализ; перенос знаний; принятие решений.

S.L. Belyakov, M.L. Belyakova, S.A. Zubkov, N.A. Golova, K.S. Yavorchuk

TRANSFORMING THE DECISION-MAKING EXPERIENCE IN SPATIAL SITUATIONS*

The problem of transferring the experience of decision-making in situational analysis using geoinformation systems is considered. The need for intellectual support from the geoinformation system is due to the fact that spatial objects and connections of the real world are extremely dynamic. Under these conditions, it is not possible to apply analytical models of processes and phenomena due to the incompleteness and inconsistency of the information describing them. Statistical models depend on a large number of factors, which vary as the geographical location of the situation changes. An alternative is to use the experience of experts who are able to make effective decisions in local spatial situations. The lack of control over the reuse of experience is a problem. The knowledge gained in developing solutions in one locality can lead to inadequate solutions in another locality. The experience of solving a problem in the same area loses its significance over time. In this paper, we propose a representation of knowledge in the form of an image consisting of a center and acceptable transformations of the center. Image transformation functions that perform knowledge transfer are introduced. The properties of transformation functions that carry procedural knowledge about the images of situations are analyzed. The use of the identified properties for the formation of a test plan for software transformation procedures is considered. The

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-07-00074.

criteria for successful transformation are studied. The optimization problem of finding the best transformation function in the GIS knowledge base is formulated. A generalized method of transforming experience is proposed. An example of the synthesis of transformation methods for selecting an operational call center is given. The image of the situation of making a decision about choosing a land plot for a service center is transformed into the specified area on the GIS map.

Intelligent geographic information systems; situational analysis; knowledge transfer; decision-making.

Введение. Использование интеллектуальных систем для принятия решений основано на повторном применении знаний, полученных в результате наблюдения и анализа объектов, событий и явлений в определенной области реального мира. Возможность повторного применения и возникающий при этом эффект не гарантируются, так как свойства и поведение мира непрерывно меняются. Для пространственных ситуаций данная особенность играет существенно важную роль. Опыт разрешения проблемной ситуации, полученный в некоторой местности, с течением времени может оказаться совершенно бесполезным из-за необратимых изменений природной и техногенной среды. Попытка применить знания к ситуации в другой местности сразу ставит вопрос о том, насколько корректно такое действие и каковы его последствия. Таким образом, конкретного знания, ограниченного тесными пространственно-временными рамками, оказывается недостаточно и требуется привлечение знания обобщенного. Но известна проблема использования обобщений, полученных для больших пространственно-временных областей: эти обобщения оказываются малодостоверны в областях локальных. Поэтому задача рационального сочетания обобщения и конкретизации в знаниях, применяемых для принятия решений в пространственном ситуационном анализе, остается актуальной.

В данной работе рассматривается выработка решений в пространственных ситуациях, описываемых объектами и отношениями реального мира с помощью геоинформационных систем (ГИС). Картографическое отображение в сочетании с инструментами пространственного анализа широко используется в различных областях производства, бизнеса и транспорта. Это создает благоприятные условия для накопления и совместного использования знаний профессиональными сообществами. Целью настоящей работы является анализ формы представления знаний, обеспечивающей контролируемый перенос опыта на проблемные пространственные ситуации.

Трансформирование знаний в ситуационном анализе. В общем случае ситуационный анализ предполагает выявление элементов и связей, характеризующих суть ситуации либо с целью выработки действий, которые переведут ее в требуемое состояние, либо для прогнозирования будущих состояний. Сложность решения таких задач с использованием ГИС [1] связана с неопределенностью и неполнотой аналитических моделей реальных объектов и процессов [2], огромным количеством конкретных пространственных данных, которые невозможно достоверно обобщить [3], трудностями обнаружения и формализации знаний экспертов, которые успешно решают задачи рассматриваемого типа [4]. Данную проблему можно решать, отображая известные образы ситуаций в заданную пространственную область [5]. Суть отображения в том, что ситуация в указанной области пространства реконструируется с использованием картографических данных ГИС. Карта несет в себе обширную информацию о структуре и топологии области анализа. Знание о наблюдавшихся ранее ситуациях при определенных условиях позволяют оценить реализуемость события или явления и затем рационально оценить принимавшиеся в данной ситуации решения. Факт реализуемости гипотетической ситуации представляется чрезвычайно важным. Эксперты-аналитики всегда интуитивно выполняют это действие, приступая к изучению проблемной си-

туации. Об этом говорят исследования когнитивной психологии [6]. Мысленное сопоставление известных прецедентов с проблемной ситуацией выполняется для оценки их смысловой близости. Например, неразумно сопоставлять ситуацию борьбы с пожаром в тайге и лесопарке, который расположен вблизи мегаполиса. Существует опасность того, что формально вычисляемая близость не учтет некоторых деталей и приведет к бессмысленному решению. Опасность усиливается тем, что пространственные ситуации отличаются наличием большого числа разнородных параметров, влияние которых существенно зависит от географического положения. Это заставляет пользоваться необоснованной аналогией, которая правдоподобна, но не достоверна [7].

Рассмотрим представление ситуации образом как кортеж

$$I =< s, H(s) >, \quad (1)$$

первый элемент которого (s) является центром образа I, второй ($H(s)$) – набором допустимых преобразований центра, сохраняющих смысл образа. Центром считается реально наблюдавшаяся ситуация, допустимое преобразование – вариант прецедента, не меняющий сути ситуации в целом. Допустимые преобразования описываются экспертом. Выражение (1) формализует понятие смысла, что необходимо для обоснования операции трансформирования. Исследуемая модель образного представления ситуаций включает кроме прецедента (s) его интуитивные экспертные обобщения ($H(s)$), благодаря которым становятся возможными дедуктивные заключения вида

(i) если два любых образа имеют одинаковые допустимые преобразования, то они близки по смыслу;
(ii) два образа A и B имеют одинаковые допустимые преобразования;
(iii) следовательно, A и B близки по смыслу.

Совпадение отдельных допустимых преобразований двух различных ситуаций есть факт, который ведет к правдоподобному и достоверному выводу. Однако, трудность использования указанного правила вывода заключается в необходимости расположения допустимых преобразований в одной пространственной области, играющей роль базы дедукции. Это приводит к необходимости трансформирования образов.

Обобщенно операция трансформирования должна выполняться применением функции трансформирования

$$I_{new} = F_{TR}(I_{src}, w) =< s_{new}, H(s_{new}) >,$$

где I_{src} – исходный образ, W – целевая область карты для трансформирования. Построение функции трансформирования представляет собой сложную проблему с большим числом вариантов трудно проверяемых с точки зрения достоверности решений, поэтому следует декомпозировать задачу для формулировки частных подзадач, решение которых можно проверить. Анализ показал следующее.

Функция трансформирования F_{TR} является векторной, размерность которой составляет *(M+2)* и определяется числом допустимых преобразований конкретного образа:

$$F_{TR} = (f_{TR_S}, f_{TR_{h_0}}, f_{TR_{h1}}, ..., f_{TR_{h_M}}),$$

где f_{TR_S} – функция трансформирования центра образа, $f_{TR_{h_i}}$ – его *i*-го допустимого преобразования. Компоненты вектора независимы и должны определяться соответственно типу отражающего преобразование картографического объекта. Например, уличная парковка всегда ориентирована вдоль линии дороги, тогда как

внутриквартальная ограничена находящимися рядом зданиями, сооружениями и дорогами. Таким образом, парковки двух типов должны отображаться в заданную местность по-разному, а функции трансформирования должны соответствовать типам допустимых преобразований.

Следуя принципам объектного подхода, можно утверждать, что каждый экземпляр образа должен включать программно реализованный метод трансформирования. Для того, чтобы применить f_{TR_S} в области W, всякий прецедент должен быть параметризован, т.е. выделены сущности, пространственное размещение которых определяет смысл прецедента. Например, логистическая цепь поставки задается расположением производителя продукта, потребителя и списком логистических операций; площадь разлива нефтепродуктов – точкой расположения источника утечки, объемом нефтепродукта, его средней плотностью. Параметризация позволяет избежать изучения огромного числа вариантов «вписывания» прецедента в область W.

Критерием достоверности трансформирования следует считать получение нетривиальных (обладающих центром) образов, которые сохраняют заданный инвариант преобразования: либо площадь отображения на карте, либо размерности допустимых преобразований, либо распределения типов допустимых преобразований, и т.д. Различные инварианты порождают различные результаты трансформирования. Подбор инварианта, адекватного сути ситуационного анализа, может основываться на имеющихся описаниях образов, т.е. данная поисковая задача автоматизируется.

Анализ известных подходов к трансформированию образов. Трансформирование образов можно рассматривать как реализацию обучения и построении рассуждений, основанных на применении аналогии [8]. Аналогия, не являясь достоверным способом рассуждения, используется при прогнозировании в условиях неопределенности. Основная решаемая проблема в этом случае – определение базы аналогии, т.е. набора фактов и логических правил, которые предполагается использовать для формирования утверждений по аналогии. Достоверность результата может быть проверена лишь на наборе данных о реальных событиях или явлениях. Возникает, таким образом, итерационный процесс подбора базы аналогии, приводящий к удовлетворительным выводам на наборе экспериментальных данных. Эта процедура носит чрезвычайно обобщенный характер и требует конкретизации отдельных подзадач. Например, формы представления знаний об элементах базы аналогии.

Близким по сути к трансформированию ситуаций можно считать процедуры принятия решений, основанные на абдукции [7]. Абдукция рассматривается как важный компонент научного познания [9]. Получение заключений от частного к частному дает возможность интеллектуальной системе генерировать гипотезы, тем самым моделируя человеческое воображение, необходимое для прогнозирования. Реализация данной идеи применительно к образам ситуаций требует исследования.

Прецедентный анализ (Case Based Reasoning, CBR) можно рассматривать как исследованную реализацию метода принятия решений по аналогии [10]. Картографический и ситуационный анализ используют CBR и существует много работ, исследующих представление знаний, метрики близости прецедентов и визуальное представление результатов логического вывода. Нерешенной проблемой остается сохранение смысловых рамок сравнения прецедентов. Эффективность результата CBR связана как с близостью задач, так и с близостью данных, используемых для их решения. Предполагается, что все особенности задач и данных учтены метрикой, однако универсального способа построения такой метрики на сегодняшний день не существует. Кроме того, в CBR не учитывается реализуемость прецедентов: считается, что пространство прецедентов однородно и сравнение близости

любой пары прецедентов корректно. Однако, это не так в случае пространственных ситуаций. Поэтому продолжение исследований CBR должны идти в направлении поиска способов сохранения смысловых рамок анализа прецедентов.

В исследованиях по машинному обучению фигурирует задача передачи знаний (transfer learning). Как показал анализ, исследуемые проблемы группируются следующим образом:

1) оценка изменений пространства признаков обучения исходной модели X_S и пространства признаков целевой области принятия решений X_T. Идея решения заключатся во введении весовых коэффициентов для признаков исходной и целевой области анализа [11, 12] при обучении модели для целевой области. Вес коэффициентов подбирается экспериментально. Другим вариантом является выявление наиболее значимых признаков, включаемых обеими областями [13, 14]. Для этого используются знания о признаках и их значимости. Такой подход ограничен тем, что проблемная и целевая области могут не иметь общих признаков;

2) учет различия распределений признаков в исходной и целевой области $(P(X_S) \neq P(X_T))$. По сути, данное соотношение отражает неоднородность пространства признаков. Для решения этой проблемы применяют методы извлечения знаний из данных [12, 15];

3) оценка влияния изменения оценок $Y_S \neq Y_T$ на наборах признаков в исходной и целевой областях. Данная особенность отражает разницу в толковании ситуаций из разных областей наблюдения. В этом случае также организуют поиск знаний о критериях оценки прецедентов [16];

4) оценка различия условных распределений $P(Y_S / X_S) \neq P(Y_T / X_T)$, отражающих смысловой различие из-за несовпадения причинно-следственных связей между ситуациями разных областей. Как и в предыдущем случае, используются выявленные при анализе данных знания [17]. Соответственно, проблемы представления и использования этих знаний остаются до конца не решенными.

Для переноса знаний используется также визуализация, исследуемая в ряде работ [9, 18]. Визуальные представления необходимы для совместной работы эксперта и интеллектуальной системы над выработкой решений. Следует отметить, что рассматриваемые исследования направлены на поиск удобных форм и способов визуализации. С этой точки зрения ГИС имеют преимущества как универсальный инструмент визуализации пространственных объектов. Тем не менее, обращает на себя внимание задача подбора адекватных показателей, позволяющих доверять визуализации объектов предметной области. Чаще всего здесь предлагаются узкоспециализированные решения.

Исследование задач прогнозирования, реализуемых ГИС, концентрируются на разработке адекватных задаче структур данных. Например, в работе [19] исследована модель оценки относительного перемещения объектов и динамики изменения заданных отношений. Введены соответствующие структуры данных, классы запросов и операторов. Это позволило реализовать сценарный анализ множеств движущихся объектов. Подобные исследования показывают полезность введения концепции специальных пространств представления анализируемых сущностей.

Типичным подходом к разработке новых методов прогнозирования является комбинирование моделей машинного обучения и биоинспирированных алгоритмов. Например, в работе [20] комбинируется классификатор с роевым алгоритмом. Это позволило создать эффективную модель прогнозирования наводнений. Трудностью использования комбинирования является необходимость экспериментальной проверки любого сочетания поискового алгоритма и области данных.

В работе [21] исследована модель «осмысленности» (meaningfulness) операций статистического прогнозирования и обобщения, используемых в ГИС. Задача сведена к построению функций оценки «осмысленности», которые зависят от типов факторов, представляющих измерения. На основе такого подхода авторами предлагается онтология статистического анализа в ГИС. Недостатком такой постановки задачи является отсутствием конструктивного способа получения образа ситуации в заданной местности.

Метод трансформирования в классе допустимого преобразования. Функция трансформирования реализует отображение ситуации x класса T_j в ситуацию y класса T_j в заданной пространственной области w

$$y = f_{TR}^{(T_j)}(x, w)$$

являясь методом этого класса допустимого преобразования. Укажем свойства, которыми должна обладать функция трансформирования:

$$1)\quad x = f_{TR}^{(T_j)}(x, A(< s, H(s) >)), x \in < s, H(s) >, \tag{2}$$

где $A(z)$ – функция определения границ области на карте, которую занимает множество картографических объектов Z. Свойство говорит о том, что трансформирование экземпляра допустимого преобразования в область самого образа рефлексивно;

$$2)\quad x \subseteq y \Rightarrow f_{TR}^{(T_j)}(x, w) \subseteq f_{TR}^{(T_j)}(y, w), \tag{3}$$

что является дискретным аналогом монотонности функции;

$$3)\quad f_{TR}^{(T_j)}(x \cup y, w) = f_{TR}^{(T_j)}(x, w) \cup f_{TR}^{(T_j)}(y, w). \tag{4}$$

Данное свойство реализует смысловую независимость наборов однотипных допустимых преобразований: трансформирование для каждого элемента не должно влиять на любой другой элемент, при этом результаты допустимо объединять;

$$4)\quad f_{TR}^{(T_j)}(x \cap y, w) = f_{TR}^{(T_j)}(x, w) \cap f_{TR}^{(T_j)}(y, w). \tag{5}$$

Данное свойство отражает смысловую общность набора однотипных преобразований.

Перечисленные свойства порождают требования к программной реализации трансформирования. Программная процедура должна тестироваться на тестовых случаях, разработанных для оценки соответствия свойствам.

При поиске конкретной реализации функции трансформирования возникает необходимость оценки качества найденного решения. Качество определяется достоверностью результата, полученного применением функции к картографическим объектам допустимого преобразования в определенной области карты. Здесь могут быть предложены различные варианты критериев, например:

– объект-оригинал x и его трансформация $f_{TR}^{(T_j)}(x, w)$ близки по площади, занимаемой на карте

$$| A(x) - A(f_{TR}^{(T_j)}(x, w)) | > \delta_S,$$

где δ_S – порог близости. Данный критерий естественен для полигональных объектов карты. Например, если изучается явление разлива жидкости, то площадь разлива является основным параметром оценки явления;

– объект-оригинал x и его трансформация близки по протяженности:

$$| L(x) - L(f_{TR}^{(T_j)}(x,w)) | > \delta_L ,$$

где $| L(x)$ – функция оценки протяженности объекта, δ_L – порог близости по протяженности. Например, если исследуется транспортная сеть, то протяженность маршрутов достоверно оценивается данным критерием;

– объект-оригинал x и его трансформация близки по мощности множеств составляющих их точечных объектов:

$$\| x | - | f_{TR}^{(T_j)}(x,w) \| > \delta_N ,$$

где δ_N – порог близости. Например, при ситуационном анализе вызовов городских оперативных служб важная количественная оценка – число вызовов на заданной территории;

– объект-оригинал x и его трансформация $f_{TR}^{(T_j)}(x,w)$ имеют близкое распределение заданного показателя $M(z)$:

$$\| P(M(x)) - P(M(f_{TR}^{(T_j)}(x,w))) \| > \delta_P ,$$

где δ_P – порог близости распределений показателя, $\| \bullet \|$ – метрика близости распределений, например, Кульбака-Лейблера [22].

Наличие критерия оценки качества функции трансформирования позволяет сформулировать оптимизационную задачу ее поиска. Если в базе знаний ГИС имеется множество образов $I_B = \{I_1, I_2, ... I_a\}$, описано множество классов допустимых преобразований $T_B = \{T_1, T_2, ... T_b\}$ и множество функций трансформирования для каждого класса $f_{TR_k}^{(T_j)}(x,w), k = 1,2,... K_{T_j}$, то функция $f_{TR}^{I_m}(x,w)$, наилучшим образом трансформирующая объект x в область w для заданного образа $I_m \in I_B$, минимизирует функционал

$$\sum_{T_B} \sum_{k} \| f_{TR}^{I_m}(x,w) - f_{TR_k}^{T_j}(x,w) \| \to \min . \qquad (6)$$

Анализ (6) позволил сделать следующие выводы:

1) применение конкретной функции трансформирования при использовании некоторого образа $I_m \in I_B$ определяется опытом применения трансформирования в конкретные области карты. Эта особенность выражением (6) не учитывается;

2) накопление знаний о функциях трансформирования ГИС является независимым процессом пополнения базы знаний. Новая функция вводится как процедурное знание, расширяющее функциональность ГИС. область применимости явно не задается;

3) процесс получения знаний об образах является дорогостоящей работой, которую проделывают эксперты. Поэтому следует ожидать, что их число не будет велико настолько, чтобы считать его статистически достаточным. Необходима процедура синтеза знаний о функциях трансформирования, учитывающая трудоемкость извлечения знаний;

4) вычислительная сложность процедуры поиска оценивается как $o(|T_B|)$, что в ряде приложений может вызвать проблемы. Перебор всех зарегистрированных в ГИС функций потенциально может быть сокращен добавлением пространственного индекса.

Все перечисленное приводит к идее зонирования территории, применяемой в географии и картографии [21–23]. В данном случае каждой зоне не карте сопоставляется функция трансформирования. Зоны могут перекрываться.

Имея тематическую карту зонирования функций трансформирования, поиск экземпляра функции трансформирования можно свести к определению покрытия области анализа

$$w_A = \bigcup_q Z_q,$$

где Z_q – зона функции трансформирования. Если $w_A = \varnothing$, это означает, что ГИС не обладает необходимыми знаниями для трансформирования. Если $q > 1$, то трансформирование может быть выполнено несколькими способами.

Реализация алгоритмов трансформирования. Ввиду того, что функции трансформирования определены на множестве картографических объектов, рассмотрим методику их синтеза как разработку алгоритма трансформирования. Свойства (2)–(5) определяют наиболее общие требования к программе реализации трансформирования. Соответственно этим требованиям должен тестироваться конечный продукт. Однако, этих требований недостаточно по причине значительного разнообразя классов трансформируемых объектов. Трансформирование не может быть универсальным. Но некоторые этапы могут быть унифицированы. Рассмотрим реализацию метода трансформирования на примере задачи принятия решения о размещении центра оперативного обслуживания вызовов (ЦООВ). Задача состоит в том, чтобы в заданной области выбрать земельный участок, на котором должны быть размещены персонал, транспортные средства и вспомогательное оборудование для выезда группы реагирования в точку экстренного вызова. Выезд завершается либо возвращением группы в ЦООВ сразу, либо после перевозки пострадавших людей (или некоторых объектов) в сервисные центры (например, в клинические больницы) за пределами обслуживаемой территории. Сложность формального решения данной задачи в неоднозначности возможной постановки и критериев оценки решения. Более практичным подходом является сценарное планирование, предполагающее анализ возможных вариантов размещения ЦООВ. Варианты связываются с принимавшимися ранее решениями в близких по смыслу ситуациях.

Ранее реализованное решение о размещении ЦООВ послужило основой создания образа, описанного картами на рис. 1. На рис. 1,a показано положение земельного участка с ЦООВ. Штриховкой показаны участки, использование которых допустимо. На рис. 1,b изображен фрагмент схемы дорожной сети из автомагистралей и внутриквартальных проездов. Любой допустимый участок размещения ЦООВ должен прилегать к автомагистрали. На рис. 1,c показано пространственное распределение среднего числа вызовов за сутки, на рис. 1,d – распределение плотности населения, на рис. 1,e приведено расположение внешних сервисных центров, на рис. 1,f – уровень сезонной доступности территории для автотранспорта (более плотная штриховка означает худшую доступность).

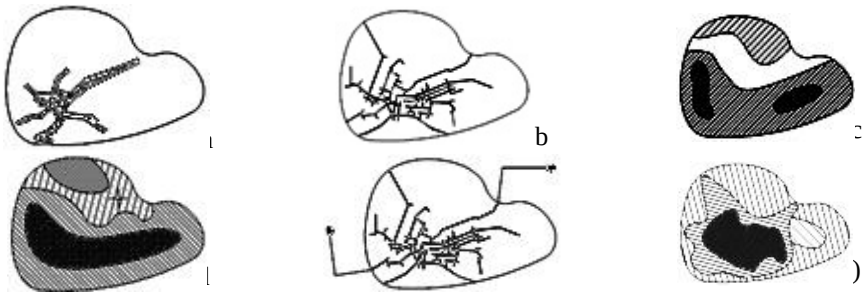

Рис. 1. Карты, использованные для трансформирования

Рис. 2. Трансформированная ситуация

На рис. 2 показана целевая область с трансформированным положением земельного участка. Алгоритм трансформирования реализован следующим образом:

1) выполняется геометрическое отображение полигона земельного участка на полигон целевой местности. Это возможно, поскольку форма участка позволяет его вписать в область, причем сделать это можно бесчисленным числом способов. Процедура трансформирования может быть продолжена;

2) реализуется алгоритм картографического отображения. Здесь должны быть проверены базовые ограничения на размещение картографического объекта «земельный участок» на карте. Ограничение состоит в том, что этот участок должен быть вписан в один из существующих участков на тематической карте земельных участков. Участок вписан, если геометрическая его форма позволяет расположить его внутри существующего участка, имеющего тип «Запланировано для индивидуального строительства» или «Запланировано для муниципальных нужд». Если таких вариантов не найдено, процесс трансформирования завершается без результата. В данном примере существовало несколько вариантов решения, поэтому процедура продолжается;

3) выполняется алгоритм оценки топологических ограничений, заданных прикладной задачей. К ним относятся следующие:

- ♦ земельный участок должен быть смежным с автомагистралью;
- ♦ расстояние до наиболее удаленного по транспортной сети жилого здания не должно превышать заданного значения. Это значение является параметром метода трансформирования;
- ♦ земельный участок должен располагаться в зоне наилучшей сезонной доступности;
- ♦ расстояние до внешних сервисных центров не должно превышать заданного (через входной параметр) значения.

Работа алгоритма в данном примере завершилась нахождением нескольких вариантов отображения. Этого, однако, недостаточно для завершения трансформирования. Смысловая целостность образа не нарушена, если учтены допустимые преобразования частот вызова экстренных служб, распределение населения и уровня се-

зонной доступности. Существенное отличие этих показателей от зафиксированных в образе делает результат трансформирования недостоверным. Перечислим особенности применения алгоритмов для трансформирования распределений.

Алгоритм геометрического трансформирования распределения некоторого показателя состоит в построении в целевой области полигонов распределения. Это означает, что аналитиком должен быть найден источник информации, позволяющий построить распределение показателя в целевой области.

Алгоритм картографического отображения распределения показателя основан на кригинге [24]. Соответствующие программные процедуры имеют многие современные ГИС. Процедура кригинга строит поле распределения показателя по заданному набору пространственных данных [25].

Алгоритм прикладного уровня реализует сравнение распределений образа и целевой области для определения того, не является ли аномальным их совпадение. Методов обнаружения аномалий существует достаточно много, как и их программных реализаций.

Окончательно трансформирование считается выполненным достоверно, если имеется непустое множество земельных участков возможного размещения и отсутствуют аномалии распределения среднего числа вызовов, распределения населения и сезонной доступности.

Заключение. Интеллектуальные ГИС для ситуационного анализа должны использовать формы представления знаний, позволяющих контролировать повторное применение знаний к проблемным ситуациям. В данной работе предложен способ использования образов ситуаций для выполнения трансформирования образа в заданную область пространства. Показано место функций трансформирования в объектной модели образа, сформулированы свойства, которым должна удовлетворять программная реализация метода трансформирования. Ввиду того, что методы трансформирования отражают процедурное знание, с целью повышения эффективности использования базы знаний ГИС предложено использовать зонирование территорий, принятое в географии. Сформулирована оптимизационная задача, позволяющая находить наилучшую функцию трансформирования в базе знаний ГИС. Рассмотренный пример показал реализуемость предложенного способа трансформирования образов. Дальнейшие исследования проблемы переноса знаний и опыта авторы видят в поиске новых формализмов описания топологии пространства образов, методов поиска достоверных отображений ситуаций.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Де Мерс М.* Географические информационные системы. Основы. – М.: Дата+, 1999.
2. *Мотовилов Ю.Г., Гельфан А.Н*. Модели формирования стока в задачах гидрологии речных бассейнов. – М.: Изд-во РАН, 2018.
3. *Yue P., Jiang L*. BigGIS: How big data can shape next-generation GIS // 2014 The Third International Conference on Agro-Geoinformatics, Beijing. – 2014. – P. 1-6.
4. *Shashi S., Hui, X*. Encyclopedia of GIS. – Springer, New York, 2017.
5. *Belyakov S., Bozhenyuk A., Rozenberg I.* The intuitive cartographic representation in decision-making // World Scientific Proceeding Series on Computer Engineering and Information Science. – 2016. – Vol. 10. – P. 13-18.
6. *Фаликман М.* Когнитивная наука: основоположения и перспективы // Логос. – 2014. – № 1. – С. 316-330.
7. *Вагин В.Н., Головина Е.Ю., Загорянская А.А., Фомина М.В.* Достоверный и правдоподобный вывод в интеллектуальных системах. – М.: Физматлит, 2001.
8. *Timperley M., Mokhtar M., Bellaby G., Howe J.* Explanation-based learning with analogy for impasse resolution // Expert Systems with Applications. – 2016. – Vol. 61. – P. 181-191.
9. *Cao N., Gotz D., Sun J., Qu H.* DICON: interactive visual analysis of multidimensional clusters // IEEE Trans. Vis. Comput. Graph. – 2011. – Vol. 17 (12). – P. 2581-2590.

10. *Aamodt A., Plaza, E.* Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches // AI Communications. – 1994. – Vol. 7 (1). – P. 39-59.
11. *Gentner D., Holyoak K.J.* Reasoning and learning by analogy: introduction // Am. Psychol. – 1997. – Vol. 52 (1). – P. 32-34.
12. *Chattopadhyay R., Ye J., Panchanathan S., Fan W., Davidson I.* Multi-source domain adaptation and its application to early detection of fatigue // ACM Trans. Knowl. Discov. Data. – 2012. – Vol. 6 (4). – P. 18-22.
13. *Han J., Kamber M*. Data Mining: Concepts and Techniques. – Morgan Kaufmann Publishers, 2000.
14. *Duan L., Tsang I.W., Xu D.* Domain transfer multiple kernel learning // IEEE Trans. Pattern Anal. Mach. Intell. – 2012. – Vol. 34 (3). – P. 465-479.
15. *Wen Y.-M., Lu B.-L.* Incremental learning of support vector machines by classifier combining // Proceedings of the 11th Pacific-Asia Conference on Knowledge Discovery and Data Mining, Nanjing. – 2007. – P. 904-911.
16. *Long M., Wang J., Ding G., Sun J., Yu P.S.* Transfer feature learning with joint distribution adaptation // IEEE 2013 Conference on Computer Vision, Sydney. – 2013. – P. 2200-2207.
17. *Fruchterman T.M., Reingold E.M.* Graph drawing by force-directed placement // Softw. Pract. Exp. – 1991. – Vol. 21 (11). – P. 1129-1164.
18. *Heimerl F., Koch S., Bosch H., Ertl T.* Visual classifier training for text document retrieval // IEEE Trans. Vis. Comput. Graph. – 2012. – Vol. 18 (12). – P. 2839-2848.
19. *Stasch C., Scheider S., Pebesma E., Kuhn W.* Meaningful spatial prediction and aggregation // Environmental Modelling & Software. – 2014. – Vol. 51. – P. 149-165.
20. *Верещака Т.В., Баканова М.Ю.* Особенности технологии создания (обновления) специализированных топографических карт нефтегазового назначения // Изв. вузов «Геодезия и аэрофотосъемка». – 2019. – Т. 63, № 6. – С. 678-688.
21. *Кресникова Н.И., Васильевых Н.А.* Применение данных дистанционного зондирования и геоинформационных технологий для обеспечения территориального планирования // Изв. вузов «Геодезия и аэрофотосъемка». – 2018. – Т. 62, № 2. – С. 212-217.
22. *Паламарчук Н.А.* Зонирование территорий города // Землеустройство, кадастр и мониторинг земель. – 2013. – № 7 (103). – С. 48-52.
23. *Александров А.А.* Моделирование взрывоопасности и зонирование территории при хранении жидкого углеводородного топлива по критериям риска / под ред. В.И. Ларионова. – Уфа: Изд-во: БЭСТС, 2004.
24. *Демьянов В.В., Савельева Е.А.* Геостатистика: теория и практика / под ред. Р.В. Арутюняна; Ин-т проблем безопасного развития атомной энергетики РАН. – М.: Наука, 2010.
25. Визуализация и анализ географических данных на языке R. – https://tsamsonov.github.io/r-geo-course/ (дата обращения: 29.11.2020).

REFERENCES

1. *De Mers M.* Geograficheskie informatsionnye sistemy. Osnovy [Geographic information systems]. Moscow: Data+, 1999.
2. *Motovilov Yu.G., Gel'fan A.N.* Modeli formirovaniya stoka v zadachakh gidrologii rechnykh basseynov [Models of runoff formation in the problems of river basin hydrology]. Moscow: Izd-vo RAN, 2018.
3. *Yue P., Jiang L*. BigGIS: How big data can shape next-generation GIS, *2014 The Third International Conference on Agro-Geoinformatics, Beijing*, 2014, pp. 1-6.
4. *Shashi S., Hui, X.* Encyclopedia of GIS. Springer, New York, 2017.
5. *Belyakov S., Bozhenyuk A., Rozenberg I.* The intuitive cartographic representation in decision-making, *World Scientific Proceeding Series on Computer Engineering and Information Science*, 2016, Vol. 10, pp. 13-18.
6. *Falikman M.* Kognitivnaya nauka: osnovopolozheniya i perspektivy [Cognitive science: fundamentals and prospects], *Logos* [Logos], 2014, No. 1, pp. 316-330.
7. *Vagin V.N., Golovina E.Yu., Zagoryanskaya A.A., Fomina M.V.* Dostovernyy i pravdopodobnyy vyvod v intellektual'nykh sistemakh [Reliable and plausible conclusion in intelligent systems]. Moscow: Fizmatlit, 2001.
8. *Timperley M., Mokhtar M., Bellaby G., Howe J.* Explanation-based learning with analogy for impasse resolution, *Expert Systems with Applications*, 2016, Vol. 61, pp. 181-191.

9. *Cao N., Gotz D., Sun J., Qu H.* DICON: interactive visual analysis of multidimensional clusters, *IEEE Trans. Vis. Comput. Graph*., 2011, Vol. 17 (12), pp. 2581-2590.
10. *Aamodt A., Plaza, E.* Case-Based Reasoning: Foundational Issues, Methodological Variations, and System Approaches, *AI Communications*, 1994, Vol. 7 (1), pp. 39-59.
11. *Gentner D., Holyoak K.J.* Reasoning and learning by analogy: introduction, *Am. Psychol*., 1997, Vol. 52 (1), pp. 32-34.
12. *Chattopadhyay R., Ye J., Panchanathan S., Fan W., Davidson I.* Multi-source domain adaptation and its application to early detection of fatigue, *ACM Trans. Knowl. Discov. Data*., 2012, Vol. 6 (4), pp. 18-22.
13. *Han J., Kamber M*. Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers, 2000.
14. *Duan L., Tsang I.W., Xu D.* Domain transfer multiple kernel learning, *IEEE Trans. Pattern Anal. Mach. Intell*., 2012, Vol. 34 (3), pp. 465-479.
15. *Wen Y.-M., Lu B.-L.* Incremental learning of support vector machines by classifier combining, *Proceedings of the 11th Pacific-Asia Conference on Knowledge Discovery and Data Mining, Nanjing*., 2007, pp. 904-911.
16. *Long M., Wang J., Ding G., Sun J., Yu P.S.* Transfer feature learning with joint distribution adaptation, *IEEE 2013 Conference on Computer Vision, Sydney*, 2013, pp. 2200-2207.
17. *Fruchterman T.M., Reingold E.M.* Graph drawing by force-directed placement, *Softw. Pract. Exp*., 1991, Vol. 21 (11), pp. 1129-1164.
18. *Heimerl F., Koch S., Bosch H., Ertl T.* Visual classifier training for text document retrieval, *IEEE Trans. Vis. Comput. Graph*., 2012, Vol. 18 (12), pp. 2839-2848.
19. *Stasch C., Scheider S., Pebesma E., Kuhn W.* Meaningful spatial prediction and aggregation, *Environmental Modelling & Software*, 2014, Vol. 51, pp. 149-165.
20. *Vereshchaka T.V., Bakanova M.Yu.* Osobennosti tekhnologii sozdaniya (obnovleniya) spetsializirovannykh topograficheskikh kart neftegazovogo naznacheniya [Features of technology for creating (updating) specialized topographic maps for oil and gas purposes], *Izv. vuzov «Geodeziya i aerofotos"emka»* [Izvestiya vuzov "Geodesy and aerial photography"], 2019, Vol. 63, No. 6, pp. 678-688.
21. *Kresnikova N.I., Vasil'evykh N.A.* Primenenie dannykh distantsionnogo zondirovaniya i geoinformatsionnykh tekhnologiy dlya obespecheniya territorial'nogo planirovaniya [Application of remote sensing data and geoinformation technologies to ensure territorial planning], *Izv. vuzov «Geodeziya i aerofotos"emka»* [Izvestiya vuzov "Geodesy and aerial photography"], 2018, Vol. 62, No. 2, pp. 212-217.
22. *Palamarchuk N.A.* Zonirovanie territoriy goroda [Zoning of city territories], *Zemleustroystvo, kadastr i monitoing zemel'* [Land management, cadastre and land monitoring], 2013, No. 7 (103), pp. 48-52.
23. *Aleksandrov A.A.* Modelirovanie vzryvoopasnosti i zonirovanie territorii pri khranenii zhidkogo uglevodorodnogo topliva po kriteriyam riska [Modeling of explosion hazard and zoning of the territory during storage of liquid hydrocarbon fuel according to risk criteria], ed. by V.I. Larionova. Ufa: Izd-vo: BESTS, 2004.
24. *Dem'yanov V.V., Savel'eva E.A.* Geostatistika: teoriya i praktika [Geostatistics: theory and practice], ed. by R.V. Arutyunyana; In-t problem bezopasnogo razvitiya atomnoy energetiki RAN. Moscow: Nauka, 2010.
25. Vizualizatsiya i analiz geograficheskikh dannykh na yazyke R. Available at: https://tsamsonov.github.io/r-geo-course/ (accessed 29 November 2020).

Статью рекомендовал к опубликованию д.т.н., профессор Л.К. Самойлов.

Беляков Станислав Леонидович – Южный федеральный университет; e-mail: beliacov@yandex.ru; 347922, г. Таганрог, пер. Некрасовский, 44; кафедра информационно-аналитических систем безопасности; профессор.

Белякова Марина Леонтьевна – e-mail: mlbeliacova@sfedu.ru; доцент.

Зубков Сергей Александрович – e-mail: szubkov@sfedu.ru; с.н.с.

Голова Никита Александрович – e-mail: ngolova@sfedu.ru; аспирант.

Яворчук Кирилл Сергеевич – e-mail: kyavorchuk@sfedu.ru; аспирант.

Belyakov Stanislav Leonidovich – Southern Federal University; e-mail: beliacov@yandex.ru; 44, Nekrasovsky, Taganrog, 347928, Russia; phone: +78634371695; the department of information and analytical security system; professor.

Belyakova Marina Leontievna – e-mail: mlbeliacova@sfedu.ru; associate professor.

Zubkov Sergey Alexandrovich – e-mail: szubkov@sfedu.ru; senior researcher.

Golova Nikita Alexandrovich – e-mail: ngolova@sfedu.ru; graduate student.

Yavorchuk Kirill Sergeevich – e-mail: kyavorchuk@sfedu.ru; graduate student.

УДК 004.932.2 DOI 10.18522/2311-3103-2020-5-171-184

А.Н. Каркищенко, В.Б. Мнухин

О ВЛИЯНИИ ЗАШУМЛЕНИЯ НА РАСПОЗНАВАНИЕ СИММЕТРИИ 3-ГО ПОРЯДКА В ГЕКСАГОНАЛЬНЫХ ИЗОБРАЖЕНИЯХ*

Излагается алгебраический подход к представлению и обработке цифровых изображений, заданных на гексагональных решетках. Описанный подход основан на представлении изображений как функций на конечных полях «целых Эйзенштейна». Как оказывается, элементы таких полей естественно соответствуют пикселям гексагональных изображений определенных размеров. Описаны экспоненциальное и логарифмическое преобразования в полях Эйзенштейна. Приведен метод обнаружения центров вращательной симметрии 3-го порядка на полутоновых изображениях и введена соответствующая нормированная мера симметрии. Основной целью работы является исследование влияния зашумления на изображении на качество оценки симметрии с помощью введенной меры. Фактор зашумленности необходимо принимать во внимание, поскольку уменьшение меры может быть вызвано не только неполной симметрией реального объекта, но и искажениями из-за шумов, что практически всегда имеет место. Очевидно, что это отличие будет пропорционально уровню шумовой составляющей. В работе получены аналитические оценки влияния шума на критерий обнаружения симметрии. Если изображения подвержены случайному зашумлению, то мера симметрии отдельных областей изображения будет случайной величиной, закон распределения которой определяется законами распределения шумовых составляющих. При этом в работе делается стандартное для обработки изображений предположение о модели нормальной и независимой зашумленности функции яркости. Особенность введенной меры симметрии третьего порядка не позволяет напрямую применить стандартные методы для получения вероятностных оценок. С этой целью была проведена оценка кумулятивной функции распределения вероятностей, на основании которой получено выражение для вероятностей уклонения меры симметрии от истинного значения на заданную величину. В силу сделанных априорных предположений полученную оценку следует рассматривать как достаточно «осторожную» и можно ожидать, что в реальности разброс меры, вызванный шумами на изображении, будет существенно меньше, чем теоретически установленные границы.

Симметрия 3-го порядка; гексагональное изображение; числа Эйзенштейна; конечные поля; полярно-логарифмические координаты; полярное представление; нормальное зашумление; распределение меры симметрии.

* Работа выполнена при финансовой поддержке РФФИ, проект № 19-07-00873.

A.N. Karkishchenko, V.B. Mnukhin

ON THE INFLUENCE OF NOISE ON THE RECOGNITION OF THREEFOLD ROTATIONAL SYMMETRY IN HEXAGONAL IMAGES

The article presents an algebraic approach to the representation and processing of digital images defined on hexagonal lattices. The described approach is based on the representation of images as functions on finite fields of "Eisenstein's integers". As it turns out, the elements of such fields naturally correspond to the pixels of hexagonal images of certain sizes. The exponential and logarithmic transformations in the Eisenstein fields are described. A method for detecting the centers of threefold rotational symmetry in grayscale images is presented and the corresponding normalized measure of symmetry is introduced. The main purpose of the work is to study the effect of noise on the image on the quality of the symmetry assessment using the introduced measure. The noise factor must be taken into account, since a decrease in the measure can be caused not only by the incomplete symmetry of the real object, but also by distortions due to noise, which is almost always the case. Obviously, this difference will be proportional to the level of the noise component. Analytical estimates of the effect of noise on the criterion for detecting symmetry are obtained in this work. If images are subject to random noise, then the measure of symmetry of local image areas will be a random variable, the distribution law of which is determined by the distribution laws of noise components. At the same time, the standard for image processing assumption is made in the work about the model of normal and independent noise level of the brightness function. The peculiarity of the introduced threefold rotational symmetry measure does not allow directly applying standard methods to obtain probabilistic estimates. For this purpose, an assessment of the cumulative probability distribution function was carried out, on the basis of which an expression was obtained for the probabilities of deviation of the symmetry measure from the true value by a given value. By virtue of the a priori assumptions made, the obtained estimate should be considered as rather "cautious" and it can be expected that in reality the spread of the measure caused by noise in the image will be significantly less than the theoretically established boundaries.

Threefold symmetry; hexagonal image; Eisenstein numbers; finite fields; log-polar coordinates; polar representation; normal noise; symmetry measure distribution.

Введение. Симметрия объектов играет решающую роль в визуальном восприятии, дизайне и проектировании. Поэтому обнаружение и анализ симметрии – важная задача в таких областях как машинное зрение, медицинская визуализация, классификация паттернов и др. [1, 2].

При исследовании симметрии на изображениях необходимо принимать во внимание различие между непрерывным и дискретным случаями. Действительно, непрерывный объект может характеризоваться группой симметрии, инвариантной к вращению, масштабированию и трансляционным преобразованиям. В то же время в отношении цифровых изображений можно говорить только о некоторой мере симметрии, которая зависит от поворотов и масштабирования. Для уменьшения искажений изображения при преобразованиях можно использовать гексагональную пиксельную решетку, которая имеет ряд преимуществ перед квадратной решеткой. Они заключаются в следующем [3]:

- *Изопериметрия*. Шестиугольник имеет наибольшую площадь среди всех правильных многоугольников равного периметра, заполняющих плоскость
- *Дополнительные равноудаленные соседи*. Каждый шестиугольный пиксель имеет шесть равноудаленных соседей с общим краем в отличие от квадратного пикселя, который имеет только четыре. Это означает, что кривые лучше представляются на гексагональной решетке.
- *Дополнительные оси симметрии*. Каждый шестиугольник в решетке имеет 6 осей симметрии, в то время как в квадрате их всего четыре. Это означает, что на гексагональных решетках будет меньше неоднозначности при обнаружении симметрии изображений.

В целом гексагональная структура обеспечивает более гибкий и эффективный способ выполнять преобразование и поворот изображения без потери информации об изображении [4].

Несмотря на отсутствие аппаратных средств для формирования и отображения гексагональных изображений, в настоящее время проводятся значительные исследования в области обработки изображений на таких структурах [3]. Для этого используется программное преобразование изображений на квадратной решетке в соответствующее изображение на гексагональной решетке. Более того, гибридные системы, включающие оба типа представления, полезны также для использования преимуществ каждого из них.

При разработке алгоритмов анализа изображения, как на квадратной, так и на гексагональной шестиугольной решетках часто исходят из предположения непрерывности изображений. Это позволяет эффективно применять инструменты непрерывной математики. Однако применение этих методов к цифровым изображениям часто приводят к систематическим ошибкам, связанным с невозможностью адекватно перенести некоторые понятия непрерывной математики на дискретную плоскость. В качестве примеров можно указать такие понятия, как вращение в плоскости и полярная система координат. Будучи естественными и элементарными в непрерывном случае они теряют эти качества, когда их пытаются точно определить на дискретной плоскости. В результате формальное применение непрерывных методов к цифровым изображениям может быть осложнено систематическими ошибками [5, 6]. Это обстоятельство приводит к необходимости разрабатывать методы, изначально ориентированные на дискретные изображения.

В работе [7] авторов данной статьи рассматривался один из таких методов, основанный на определении гексагональных изображений как функций на «полях целых Эйзенштейна». Значимость такого подхода основано на том, что конечные поля чисел Эйзенштейна наследуют некоторые свойства непрерывного комплексного поля. В частности, понятия комплексных логарифма и экспоненты может быть перенесено на поля чисел Эйзенштейна. Это позволяет ввести дискретные «полярно-логарифмические» координаты в гексагональных изображениях. Соответствующее представление гексагональных изображений можно использовать для анализа их симметрии подобно тому, как это было сделано для непрерывных изображений [2, 5, 6, 8] и для цифровых изображений на квадратных решетках [9–12].

Несмотря на многочисленные исследования в области обнаружения симметрии (например, [1, 2, 5]) и в области обработки гексагональных изображений, лишь немногие из них (если таковые вообще имеются) посвящены распознаванию симметрии гексагональных изображений. В частности, в [13] предложена 3-х координатная схема, которая использует неявную симметрию гексагональной решетки. В этой же работе представлена серия геометрических преобразований, таких как масштабирование, вращение и сдвиг в соответствующей 3-координатной системе ([3, с. 20]), но симметрия гексагональных изображений не исследована [4].

Следует отметить, что известен ряд работ по приложениям алгебраических структур и теоретико-числовых преобразований при обработке изображений; такие методы разрабатываются уже около 40 лет [14] и получили обширную теоретическую и экспериментальную проработку [15, 16]. В частности, в 1993 г. в работе [17] предложено кольцо гауссовских целых чисел для обработки изображений на квадратных решетках; позже активно применяли «конечные комплексные поля» [10–12, 18, 19]. Тем не менее, применение «конечных полей целых Эйзенштейна» к анализу изображений на гексагональных решетках представляется новым.

В упомянутой выше работе [7] был рассмотрен случай обнаружения вращательной симметрии третьего порядка, который имеет важные практические приложения. Как оказывается, распознавание симметрии 3-го порядка в настоящее время востребовано в различных областях кристаллографии [20, 21], вирусологии [22], анализе изображений, полученных с электронного микроскопа [23], и т.п. Предложенный алгоритм оптимизирован для работы с гексагональными изображениями, но может быть использован и для обычных изображений на квадратных решетках после ресэмплинга (передискретизации). Однако, несмотря на наличие явной формулы, позволяющей установить наличие или отсутствие симметрии на изображении, в указанной работе, как и во многих аналогичных публикациях, предполагается, что функция изображения задана точно, что почти никогда не имеет место при анализе реальных изображений. Это обстоятельство, безусловно, влияет на получаемые результаты. Поэтому возникает вопрос о качестве определения симметрии при наличии шума. В тех случаях, когда анализ погрешностей проводится, обычно прибегают к статистическим оценкам на основе экспериментальных исследований. Понятно, что данный подход не позволяет получить обоснованные теоретические оценки при всевозможных значениях параметров, описывающих как изображение, так и саму процедуру распознавания.

В данной статье, которую можно рассматривать как продолжение работы [7], для удобства чтения дается краткое описание изложенного в ней подхода к описанию гексагональных изображений. Затем проводится теоретический анализ, и даются соответствующие аналитические оценки влияния зашумления функции, задающей цифровое изображение, на критерий, определяющий наличие или отсутствие тройной вращательной симметрии.

Конечные поля целых чисел Эйзенштейна. Приведем вначале краткое описание подхода к формализации гексагональных изображений и его применение к обнаружению вращательной симметрии. Более подробное изложение можно найти в работе авторов [7].

Пусть $\mathbb{Z}$ – кольцо целых чисел, а $\mathbb{C}$ – комплексное поле. Обозначим $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ — кольцо классов вычетов по модулю целого $n \geq 2$, и пусть $\mathbb{GF}(p^m)$ – поле Галуа с p^m элементами, где p – простое число, а $m > 0$ – целое число.

В теории чисел [24, гл. 1.4] гауссовское целое число — это комплексное число $z = a + bi \in \mathbb{C}$, действительная и мнимая части которого являются целыми числами. Целые числа Эйзенштейна – это комплексные числа вида $z = a + b\omega$, где также $a,b \in \mathbb{Z}$ и $\omega = \exp(2\pi i/3) \in \mathbb{C}$ – примитивный кубический корень из единицы, так что $\omega^3 = 1$ и $\omega^2 + \omega + 1 = 0$. Заметим, что в комплексной плоскости целые числа Эйзенштейна образуют треугольную решетку, в отличие от целых чисел Гаусса, которые образуют квадратную решетку.

Целые числа Гаусса и Эйзенштейна с обычным сложением и умножением комплексных чисел, образуют, соответственно, подкольца $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ в поле $\mathbb{C}$. К сожалению, отсутствие деления в этих кольцах существенно ограничивает его применимость к задачам обработки изображений [17]. Поэтому естественно искать конечные поля, свойства которых были бы в некотором отношении аналогичны свойствам $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$. Известно, что если p – такое простое число, что $p \equiv 3 \bmod 4$, тогда факторкольцо $\mathbb{C}(p) = \mathbb{Z}_p[x]/(x^2+1) \cong \mathbb{GF}(p^2)$ является «конечным комплексным полем». Его приложения для анализа и обработки цифровых изображений на квадратной решетке рассмотрено в [10–12, 18, 19].

Аналогичный подход использован для построения «конечных полей целых чисел Эйзенштейна». А именно, можно показать, что если число $p = 12k + 5$ является простым, то многочлен $x^2 + x + 1$ неприводим над $\mathbb{Z}_p$, но $x^2 + 1$ таковым не является. Из этого вытекает следующее определение.

Определение 1. *Пусть* $p \geq 5$ *такое простое число, что* $p \equiv 5 \bmod 12$. *Тогда конечное поле* $\mathbb{E}(p) = \mathbb{Z}_p[x]/(x^2 + x + 1) \cong \mathbb{GF}(p^2)$ *называется* полем чисел Эйзенштейна. *Элементы* $\mathbb{E}(p)$ *называются* дискретными числами Эйзенштейна.

Таким образом, поля Эйзенштейна имеют p^2 элементов, где p = 5, 17, 29, 41, 53, 89, 101, 113, 137, 149, 173, 197, 233, 257,… В частности, имеется 44 поля $\mathbb{E}(p)$ для $5 \leq p < 1000$. Элементы поля чисел Эйзенштейна имеют вид $z = a + b\omega$, где $a, b \in \mathbb{Z}_p$ и ω обозначает класс вычетов, так что $x^2 + x + 1 = 0$. Сложение определяется стандартно, а произведение задается выражением

$$(a + b\omega)(c + d\omega) = (ac - bd) + (bc + ad - bd)\omega,$$

В этом случае деление в $\mathbb{E}(p)$ корректно определено.

Полярные разложения полей Эйзенштейна. Аналогия между полями $\mathbb{C}$ и $\mathbb{E}(p)$ позволяет ввести представление элементов из $\mathbb{E}(p)$ в «экспоненциальной форме». Для этого напомним алгебраический метод введения полярно-логарифмической системы координат на непрерывной комплексной плоскости. Пусть $\mathbb{C}^*$ — мультипликативная группа комплексных чисел и $\mathbb{R} = \langle \mathbb{R}, + \rangle$ — аддитивная группа вещественных чисел. Соответствие

$$0 \neq z = re^{i\theta} = e^{\ln r + i\theta} \leftrightarrow (l, \theta), \text{ где } l = \ln r \in \mathbb{R} \text{ и } 0 \leq \theta < 2\pi,$$

между ненулевыми комплексными числами z и их полярно-логарифмическими координатами (l, θ) можно рассматривать как изоморфизм

$$\mathbb{C}^* \simeq \mathbb{R} \times (\mathbb{R} / 2\pi\mathbb{Z}). \quad (1)$$

Перенесем эту конструкцию на $\mathbb{E}(p)$. Для этого заметим, что поскольку $\mathbb{E}(p)$ — конечное поле, его мультипликативная группа $\mathbb{E}^*(p) = \mathbb{E}(p) \setminus \{0\}$ циклическая [25, п. 314] и порождается некоторым примитивным элементом g. Например, легко проверить, что $g = 1 + 3\omega$ является примитивным в $\mathbb{E}^*(p)$ при $p = 5, 17, 89, 101, 257$ и $g = 1 + 5\omega$ – примитивный при $p = 29, 53, 113, 233$ и т.д.

Справедлива следующая лемма.

Лемма 1. *Для любого* $p = 12k + 5$ *числа* $m = 2(p - 1) = 8(3k + 1)$ *и* $n = (p + 1)/2 = 3(2k + 1)$ *взаимно просты.*

Поскольку $mn = p^2 - 1 = |\mathbb{E}^*(p)|$, то для $\mathbb{E}^*(p)$ справедлив [25, с. 163] следующий аналог разложения (1).

Теорема 1. *Для любого конечного поля чисел Эйзенштейна* $\mathbb{E}(p)$ *его мультипликативная группа разлагается в прямое произведение циклических групп порядков* $m = 2(p - 1)$ *и* $n = (p + 1)/2$,

$$\mathbb{E}^*(p) = \langle g \rangle = \mathbb{Z}_m \times \mathbb{Z}_n.$$

Данное выражение называется *полярным разложением* $\mathbb{E}(p)$.

Полярное разложение позволяет перенести на $\mathbb{E}(p)$ понятие комплексного логарифма. Для этого зафиксируем произвольный примитивный элемент g и определим отображение $\mathrm{Exp}_g : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{E}^*(p)$ следующим образом:

$$\mathrm{Exp}_g(l,\theta) = g^{nl+m\theta} = z \in \mathbb{E}^*(p), \text{ где } (l,\theta) \in \mathbb{Z}_m \times \mathbb{Z}_n .$$

Exp_g является изоморфизмом между аддитивной группой кольца $\mathbb{Z}_m \times \mathbb{Z}_n$ и мультипликативной группой поля чисел Эйзенштейна $\mathbb{E}(p)$.

Определение 2. *Отображение* $\mathrm{Exp}_g : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{E}^*(p)$ *называется* модулярной экспонентой *по основанию* g, *а обратное к нему отображение* $\mathrm{Ln}_g : \mathbb{E}^*(p) \to \mathbb{Z}_m \times \mathbb{Z}_n$ – модулярный логарифм *по основанию* g. *Его область определения* $\mathbb{Z}_m \times \mathbb{Z}_n$ *называется* полярной областью.

Заметим, что значение $\mathrm{Ln}_g(0)$ не определено, а чтобы вычислить $(l,\theta) = \mathrm{Ln}_g(z)$ для любого $z = g^s \in \mathbb{E}^*(p)$ необходимо решить диофантово уравнение $nx + my = s$ и положить

$$(l,\theta) = (x \bmod m,\ y \bmod n) \in \mathbb{Z}_m \times \mathbb{Z}_n .$$

Например, пусть $g = 1 + 3\omega \in \mathbb{E}^*(5)$ и $z = g^2 = 2 + 2\omega$. Тогда $s = 2$, $m = 8$, $n = 3$ и уравнение $3x + 8y = 2$ имеет очевидное решение $x = -2$, $y = 1$. Следовательно, $\mathrm{Ln}_g(2 + 2\omega) = (-2 \bmod 8, 1 \bmod 3) = (6,1) \in \mathbb{Z}_8 \times \mathbb{Z}_3$. Заметим, что в зависимости от g либо $\mathrm{Ln}_g(\omega) = (0, n/3)$, либо $\mathrm{Ln}_g(\omega) = (0, 2n/3)$.

Пару $(l,\theta) \in \mathbb{Z}_m \times \mathbb{Z}_n$ можно рассматривать как «полярно-логарифмические координаты» соответствующего дискретного числа Эйзенштейна z.

Гексагональные изображения как функции на полях Эйзенштейна. Пусть $\mathbb{E}(p)$ – произвольное поле целых Эйзенштейна характеристики $p = 12k + 5$, и пусть $f(z) : \mathbb{E}(p) \to \mathbb{R}$ – любая вещественнозначная функция на $\mathbb{E}(p)$. Функцию $f(z)$ будем называть *гексагональным полутоновым изображением размера* $p \times p$, или просто *гексагональным изображением*.

Другой способ описания гексагональных изображений основан на введенном полярном разложении. А именно, $p \times p$ — гексагональному изображению $f(z)$ можно сопоставить изображение на квадратной решетке размера $m \times n$. Для этого зафиксируем произвольный примитивный элемент $g \in \mathbb{E}^*(p)$ и определим функцию $\psi : Z_m \times \mathbb{Z}_n \to \mathbb{R}$ такую, что

$$\psi\left(\mathrm{Ln}_g(z)\right) = f(z),\ 0 \neq z \in \mathbb{E}^*(p).$$

Определение 3. *Преобразование* $\mathcal{P}_g[f] = \psi$ *называется* полярно-логарифмическим преобразованием по основанию g *гексагонального изображения* f *или просто его* полярным преобразованием $\mathcal{P}$. *Изображение* ψ *называется* полярной формой f.

Полярную форму f можно рассматривать как расположение всех ее пикселей, кроме $f(0,0)$, в виде $(m\times n)$-матрицы. Таким образом, изображение f «почти» восстанавливается своей полярной формой ψ. Чтобы достичь полной восстанавливаемости, необходимо формально расширить полярную область с помощью дополнительного элемента ∞, полагая, что $\psi(\infty)=f(0,0)$. Заметим, что в такой расширенной полярной области $Z_m\times\mathbb{Z}_n\cup\{\infty\}$ полярное преобразование $\mathcal{P}$ становится обратимым. Линейность $\mathcal{P}$ очевидна.

Следующее утверждение показывает, что преобразование $\mathcal{P}$ можно рассматривать как дискретный аналог перехода к полярно-логарифмической системе координат.

Утверждение 1. *Если* $\mathcal{P}_g[f(z)]=\psi(l,\theta)$, *то* $\mathcal{P}[f(wz)]=\psi(l-l_0,\theta-\theta_0)$, *где* $0\neq z\in\mathbb{E}(p)$ *и* $\mathrm{Ln}(w)=(l_0,\theta_0)$.

Данное соотношение можно применить к анализу симметрии в гексагональном изображении. Как известно, непрерывный объект обладает r-кратной вращательной симметрией относительно точки C, если поворот вокруг C на угол $2\pi/r$ не меняет объект. К сожалению, это определение не работает для цифровых изображений, поскольку цифровое вращение определить значительно труднее (см., например, [26, стр. 377] для квадратных изображений и [4, 13], [3, с. 97] для гексагональных изображений). В результате для цифровых изображений можно говорить лишь о некоторой *степени симметрии*, которая зависит от поворотов и масштабирования. Вместе с тем для гексагональных изображений на полях Эйзенштейна понятие симметрии 3-го порядка вводится следующим образом.

Определение 4. *Гексагональное изображение* f *имеет центральную симметрию третьего порядка в том и только том случае, если* $f(\omega z)=f(z)$.

Пусть $\psi=\mathcal{P}[f]$ – полярная форма гексагонального $p\times p$ изображения f. Её можно рассматривать как $(m\times n)$-матрицу, где $n=3(2k+1)$, $m=8(3k+1)$ и $k=(p-5)/12\in\mathbb{Z}$. Поскольку n кратно 3, разложим ψ на три блока ψ_1, ψ_2 и ψ_3 равного размера $m\times n/3$. Тогда из предыдущего определения вытекает

Утверждение 2. *Изображение* f *обладает центральной симметрией 3-го порядка тогда и только тогда, когда его полярную форму* ψ *можно разложить на три равных блока* $\psi_1=\psi_2=\psi_3$.

Доказательство этого утверждения можно найти в [7].

Очевидно, что на реальных изображениях можно ожидать только приблизительных равенств $\psi_1\simeq\psi_2\simeq\psi_3$, так что возникает задача выбора подходящей меры симметрии $\mu(f)$ для изображения f. Один из возможных способов введения такой меры состоит в следующем. Для любой нормированной матрицы полярных форм $\tilde{\psi}=\psi/\max\{\psi\}$ изображения f положим

$$\kappa(f)=\exp\left(-\alpha x^{\beta}\right),\ \text{где}\ x=\max\left\{\|\tilde{\psi}_1-\tilde{\psi}_2\|,\|\tilde{\psi}_2-\tilde{\psi}_3\|,\|\tilde{\psi}_3-\tilde{\psi}_1\|\right\}. \qquad (2)$$

Здесь $\|\bullet\|$ обозначает любую матричную норму, под которой можно понимать, в частности, норму Фробениуса, а α, β – неотрицательные действительные числа, точные значения которых могут варьироваться в зависимости от решаемой практической проблемы. Таким образом, $\kappa(f)$ «оценивает» степень симметричности 3-го порядка изображения f в предположении, что центр симметрии совпадает с центром изображения.

Вместе с любым из методов скользящего окна представленный подход может использоваться для обнаружения центров локальной тройной симметрии на изображениях. Следует заметить, что для фиксированного p полярное преобразование основано на предварительных вычислениях и не требует дополнительных текущих вычислительных затрат.

Оценка влияния шума на меру симметрии. Как было отмечено выше, точное значение меры симметрии может быть получено по формуле (2) лишь в идеальном случае, когда на изображении отсутствуют шумы. Фактор зашумленности необходимо принимать во внимание, поскольку отличие от единицы меры симметрии $\kappa(f)$ может быть вызвано не только неполной симметрией реального объекта, но и искажениями из-за шумов на изображении. Очевидно, что это отличие будет пропорционально уровню шумовой составляющей. Для аналитической характеристики уклонения меры симметрии от истинного значения, обусловленного зашумлениями, необходимо задаться моделью шума и получить оценку распределения вероятностей величины $x = \max\left\{\|\tilde{\psi}_1 - \tilde{\psi}_2\|, \|\tilde{\psi}_2 - \tilde{\psi}_3\|, \|\tilde{\psi}_3 - \tilde{\psi}_1\|\right\}$.

Далее для определенности под нормой матрицы будем понимать норму Фробениуса, поэтому нормы матриц в формуле (2) можно рассматривать как эвклидовы нормы соответствующих векторов, составленных из столбцов этих матриц. Будем считать, что матрице ψ_i соответствует построенный указанным образом вектор ε_i. Поскольку каждая матрица ψ_i имеет размер $m \times n/3$, то соответствующий ей вектор ε_i будет иметь размер $N = mn/3$.

В дальнейшем потребуется следующее простое утверждение.

Утверждение 3. *Пусть* $a, b, c \in R^n$, *причем* $a + b + c = 0$. *Тогда*

$$\max\left(\|a\|, \|b\|, \|c\|\right) \le \max\left(\|a - b\|, \|c\|\right),$$

где $\|\bullet\|$ *– эвклидова норма.*

Доказательство. Применяя неравенство треугольника, запишем очевидные соотношения:

$$2\|a\| = \|(a+b)+(a-b)\| \le \|a+b\| + \|a-b\|, \quad 2\|b\| = \|(a+b)+(b-a)\| \le \|a+b\| + \|a-b\|.$$

Отсюда следует, что $\max\left\{\|a\|, \|b\|\right\} \le \max\left\{\|a+b\|, \|a-b\|\right\}$. Учитывая, что $a + b = -c$, получаем: $\max\left\{\|a\|, \|b\|\right\} \le \max\left\{\|c\|, \|a-b\|\right\}$. Остается только заметить, что добавление под знаком максимума в левой части неравенства величины $\|c\|$ не может нарушить полученное нестрогое неравенство. ■

В качестве наиболее естественного допущения примем предположение о нормальном характере зашумления. А именно, пусть в каждом пикселе z функция изображения $f(z)$ представляет собой результат независимого аддитивного нормально распределенного зашумления точного значения $f_0(z)$, т.е. $f(z) = f_0(z) + \xi$, где ξ – случайная величина, распределенная по нормальному закону $\mathcal{N}(0, \sigma^2)$. Единственной характеристикой, которую требуется оценить при описании зашумления, является среднеквадратическое отклонение. Этот вопрос здесь не обсуждается, поскольку этот параметр определяется используемым оборудованием, условиями и расстоянием до объекта съемки и пр.

В дальнейшем I_k будет обозначать единичную матрицу размера $k \times k$.

Утверждение 4. *Пусть* $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in R^N$ и $\varepsilon_i \sim \mathcal{N}\left(0, \sigma^2 I_N\right)$, $i = 1,2,3$. *Тогда, если* $x = \max\left(\|\varepsilon_1 - \varepsilon_2\|, \|\varepsilon_2 - \varepsilon_3\|, \|\varepsilon_3 - \varepsilon_1\|\right)$, *то для любого* $\delta > 0$

$$P\left(x < \delta\right) \geq \Phi\left(\frac{\delta^2 - 6N\sigma^2}{6\sqrt{2N}\sigma^2}\right)\Phi\left(\frac{\delta^2 - 2N\sigma^2}{2\sqrt{2N}\sigma^2}\right),$$

где $\Phi(u) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-\frac{t^2}{2}}dt$ – функция Лапласа.

Доказательство. Рассмотрим блочный вектор $\varepsilon = \begin{pmatrix}\varepsilon_1 \\ \varepsilon_2 \\ \varepsilon_3\end{pmatrix}$, составленный из векторов $\varepsilon_1, \varepsilon_2, \varepsilon_3$. Очевидно, что вектор ε имеет нормальное распределение с математическим ожиданием $M[\varepsilon] = 0$ и ковариационной матрицей $K_\varepsilon = \sigma^2 I_{3N}$.

Заметим, что векторы $\varepsilon_1 - \varepsilon_2$, $\varepsilon_2 - \varepsilon_3$, $\varepsilon_3 - \varepsilon_1$ линейно зависимы, поскольку их сумма равна нулевому вектору, поэтому вектор $\varepsilon_3 - \varepsilon_1 = -(\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3)$ является неслучайной функцией векторов $\varepsilon_1 - \varepsilon_2$ и $\varepsilon_2 - \varepsilon_3$, и его распределение полностью определяется распределением векторов $\varepsilon_1 - \varepsilon_2$ и $\varepsilon_2 - \varepsilon_3$.

Для определения распределения векторов $\varepsilon_1 - \varepsilon_2$ и $\varepsilon_2 - \varepsilon_3$ рассмотрим блочный вектор $\mu = \begin{pmatrix}\varepsilon_1 - \varepsilon_2 \\ \varepsilon_2 - \varepsilon_3\end{pmatrix}$ и заметим, что ε и μ связаны очевидной линейной зависимостью $\mu = \begin{pmatrix} I_N & -I_N & \mathbf{0} \\ \mathbf{0} & I_N & -I_N \end{pmatrix}\varepsilon = C\varepsilon$. Случайный вектор μ также имеет нормальное распределение с математическим ожиданием $M[\mu] = \mathbf{0}$ с ковариационной матрицей

$$K_\mu = M\left[\mu\mu^T\right] = M\left[C\varepsilon\varepsilon^T C^T\right] = CM\left[\varepsilon\varepsilon^T\right]C^T = CK_\varepsilon C^T = \sigma^2\begin{pmatrix} 2I_N & -I_N \\ -I_N & 2I_N \end{pmatrix}.$$

Математическое ожидание и ковариационная матрица полностью описывают распределение вектора μ в R^{2N}. Полученное выражение для ковариационной матрицы говорит о коррелированности компонент вектора μ. Наиболее простое описание этого распределения можно получить, если перейти к статистически независимым случайным величинам, т.е. перейти к ортонормированному базису в R^{2N}, в котором ковариационная матрица новых случайных величин будет единичной. В качестве такого преобразования можно взять преобразование $\nu = \left(T\sqrt{\Lambda}\right)^{-1}\mu$, где $\sqrt{\Lambda} = \mathrm{diag}\left(\sqrt{\lambda_1}, \sqrt{\lambda_2}, ..., \sqrt{\lambda_{2N}}\right)$, где $\lambda_1, \lambda_2, ..., \lambda_{2N}$ — собственные значения матрицы K_μ, а T — матрица, столбцами которой являются ортонормированные собственные векторы, отвечающие соответственно собственным значениям $\lambda_1, \lambda_2, ..., \lambda_{2N}$. Поскольку матрица K_μ является положительно определенной, то матрица $\sqrt{\Lambda}$ определена корректно. Действительно, учитывая, что $T^{-1} = T^T$ и $\left(\sqrt{\Lambda}\right)^{-1} = \sqrt{\Lambda^{-1}}$, получаем:

$$K_\nu = M\left[\nu\nu^T\right] = M\left[\sqrt{\Lambda^{-1}}T^T\mu\mu^T T\sqrt{\Lambda^{-1}}\right] = \sqrt{\Lambda^{-1}}T^T M\left[\mu\mu^T\right]T\sqrt{\Lambda^{-1}} = I_{2N}.$$

Для того чтобы найти собственные значения и собственные векторы матрицы K_μ воспользуемся ее представлением в виде кронекеровского произведения:

$$K_\mu = \sigma^2 \begin{pmatrix} 2I_N & -I_N \\ -I_N & 2I_N \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \otimes \left(\sigma^2 I_N\right).$$

Тогда в силу «спектральных» свойств кронекеровского произведения собственные значения матрицы K_μ будут равны всевозможным произведениям собственных значений матриц $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$ и $\sigma^2 I_N$, а соответствующие собственные векторы будут получаться как кронекеровские произведения собственных векторов, отвечающих соответствующим собственным значениям [27]. С учетом этого непосредственными вычислениями получаем:

$$\Lambda = \sigma^2 \begin{pmatrix} I_N & \mathbf{0} \\ \mathbf{0} & 3I_N \end{pmatrix}, \; T = \tfrac{1}{\sqrt{2}} \begin{pmatrix} I_N & -I_N \\ I_N & I_N \end{pmatrix}.$$

Тогда вектор $\nu = \sqrt{\Lambda^{-1}} T^T \mu = \tfrac{1}{\sigma} \begin{pmatrix} I_N & \mathbf{0} \\ \mathbf{0} & \tfrac{1}{\sqrt{3}} I_N \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} I_N & I_N \\ -I_N & I_N \end{pmatrix} \mu = \tfrac{1}{\sqrt{2}\sigma} \begin{pmatrix} I_N & I_N \\ -\tfrac{1}{\sqrt{3}} I_N & \tfrac{1}{\sqrt{3}} I_N \end{pmatrix} \mu$ будет иметь ковариационную матрицу $K_\nu = I_{2N}$. Выразим вектор ν через исходный случайный вектор ε:

$$\nu = \tfrac{1}{\sqrt{2}\sigma} \begin{pmatrix} I_N & I_N \\ -\tfrac{1}{\sqrt{3}} I_N & \tfrac{1}{\sqrt{3}} I_N \end{pmatrix} \mu = \tfrac{1}{\sqrt{2}\sigma} \begin{pmatrix} I_N & I_N \\ -\tfrac{1}{\sqrt{3}} I_N & \tfrac{1}{\sqrt{3}} I_N \end{pmatrix} \begin{pmatrix} I_N & -I_N & \mathbf{0} \\ \mathbf{0} & I_N & -I_N \end{pmatrix} \varepsilon =$$

$$= \tfrac{1}{\sqrt{2}\sigma} \begin{pmatrix} I_N & \mathbf{0} & -I_N \\ -\tfrac{1}{\sqrt{3}} I_N & \tfrac{2}{\sqrt{3}} I_N & -\tfrac{1}{\sqrt{3}} I_N \end{pmatrix} \varepsilon = \tfrac{1}{\sqrt{2}\sigma} \begin{pmatrix} -(\varepsilon_3 - \varepsilon_1) \\ -\tfrac{1}{\sqrt{3}} \left((\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3)\right) \end{pmatrix}.$$

Таким образом, все компоненты вектора ν статистически независимы, причем имеют распределение $\mathcal{N}(0,1)$.

Случайные величины $\left\| -\tfrac{1}{\sqrt{2}\sigma} (\varepsilon_3 - \varepsilon_1) \right\|^2$ и $\left\| -\tfrac{1}{\sqrt{6}\sigma} \left((\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3)\right) \right\|^2$ имеют χ^2-распределение с N степенями свободы. Как известно, χ^2-распределение с ростом N асимптотически сходится к нормальному распределению $\mathcal{N}(N, 2N)$. Поэтому при достаточно большом значении N (уже при $N > 30$) [28] можно считать, что $\left\| -\tfrac{1}{\sqrt{2}\sigma} (\varepsilon_3 - \varepsilon_1) \right\|^2 \sim \mathcal{N}(N, 2N)$ и $\left\| -\tfrac{1}{\sqrt{6}\sigma} \left((\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3)\right) \right\|^2 \sim \mathcal{N}(N, 2N)$ или $\left\| \varepsilon_3 - \varepsilon_1 \right\|^2 \sim \mathcal{N}\left(2N\sigma^2, 8N\sigma^4\right)$ и $\left\| (\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3) \right\|^2 \sim \mathcal{N}\left(6N\sigma^2, 72N\sigma^4\right)$.

Как известно, функция распределения максимума независимых случайных величин равна произведению функций распределения этих величин [29]. Поэтому

$$\max\left(\left\| (\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3) \right\|^2, \left\| \varepsilon_3 - \varepsilon_1 \right\|^2 \right) \sim \mathcal{N}\left(6N\sigma^2, 72N\sigma^4\right) \mathcal{N}\left(2N\sigma^2, 8N\sigma^4\right).$$

Обозначим $y = \max\left(\left\| (\varepsilon_1 - \varepsilon_2) - (\varepsilon_2 - \varepsilon_3) \right\|, \left\| \varepsilon_3 - \varepsilon_1 \right\| \right)$. В силу утверждения 3 имеет место неравенство $x \le y$, это значит, что для любого положительного δ выполняется $P\left(x < \delta\right) \ge P\left(y < \delta\right) = P\left(y^2 < \delta^2\right)$. Поэтому получаем окончательно:

$$P\left(x<\delta\right)\geq\Phi\left(\frac{\delta^2-6N\sigma^2}{6\sqrt{2N}\sigma^2}\right)\Phi\left(\frac{\delta^2-2N\sigma^2}{2\sqrt{2N}\sigma^2}\right).\ \blacksquare$$

Следствие 1. $P\left(x<\delta\right)\geq\Phi\left(\frac{\delta^2-6N\sigma^2}{6\sqrt{2N}\sigma^2}\right)$ при больших N.

Доказательство. Расстояние между математическим ожиданиями распределений равно $6N\sigma^2-2N\sigma^2=4N\sigma^2$ превышает сумму среднеквадратических отклонений $6\sqrt{2N}\sigma^2+2\sqrt{2N}\sigma^2=8\sqrt{2N}\sigma^2$ в $\sqrt{N}/2\sqrt{2}$ раз, и это отношение увеличивается с ростом N. Это означает, что при больших значениях N (фактически уже при $N>70$) практическим влиянием распределения $\Phi\left(\frac{\delta^2-2N\sigma^2}{2\sqrt{2N}\sigma^2}\right)$ можно пренебречь. ■

Пример. Рассчитаем с помощью данного следствия величину δ, которую x не превысит с вероятностью α не менее 99%, т.е. $\alpha=0.99$, при условии, что $\sigma=0.01$.

Очевидно, $\delta\geq\delta(\alpha)$ зависит от заданной вероятности α и может быть найдено из условия $\Phi\left(\frac{\delta^2-6N\sigma^2}{6\sqrt{2N}\sigma^2}\right)\geq\alpha$. Отсюда $\frac{\delta^2-6N\sigma^2}{6\sqrt{2N}\sigma^2}\geq\Phi^{-1}\left(\alpha\right)$ и, следовательно, $\delta\geq\sigma\sqrt{6N+6\sqrt{2N}\Phi^{-1}\left(\alpha\right)}$. При значении $\alpha=0.99$, пользуясь таблицами для функции Лапласа, получаем

$$\delta\geq\sigma\sqrt{6N+6\sqrt{2}\sqrt{N}\Phi^{-1}(0.99)}\approx\sigma\sqrt{6N+6\sqrt{2}\cdot2.34\sqrt{N}}=\sigma\sqrt{6N+19.86\sqrt{N}}\ .$$

Для значения $\sigma=0.01$ и $N=\frac{150\cdot150}{3}=7\,500$ находим окончательно $\delta\geq2.16$.

Заключение. В данной статье кратко излагается алгебраический метод обработки гексагональных изображений, основанный на их представлении как функций на «полях чисел Эйзенштейна». Однако основным новым результатом работы является получение аналитическиой оценки влияния шума на критерий обнаружения тройной вращательной симметрии на таком изображении. Учитывая сделанные при получении результата предположения, можно сделать вывод, что полученная оценка является достаточно «осторожной», т.е. можно ожидать, что в реальности разброс меры симметрии, вызванный шумами на изображении, будет существенно меньше, чем теоретически установленные границы.

Следует заметить также, что описанный подход к оценке влияния шума не ограничивается применением только к методу определения симметрии, изложенному в [7]. Проблема оценки точности выражений типа (2) возникает и в других задачах (например, [30]). Возможно, при этом потребуются некоторые обобщения приведенных в данной статье результатов (например, распространение оценивания на большее количество объектов при кратной вращательной симметрии и др.). Это может стать предметом отдельного исследования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Gool L., Moons T., Ungureanu D., Pauwels E.* Symmetry from Shape and Shape from Symmetry // Int. J. Robotics Res. – 1995. – 14 (5). – P. 407-424.
2. *Martinet A., Soler C., Holzschuch N., Sillion F.* Accurate Detection of Symmetries in 3D Shapes // ACM Trans. Graph. – 2006. – 25 (2). – P. 439-464.
3. *Middleton L., Sivaswamy J.* Hexagonal Image Processing: A Practical Approach. Springer, 2005.
4. *Xiangjian He,Wenjing Jia, Namho Hur, QiangWu, Jinwoong Kim.* Image Translation and Rotation on Hexagonal Structure // In: 6th IEEE Intern. Conf. on Computer and Information Technology (CIT'06). Seoul, 141. – 2006.
5. *Chertok M., Keller Y.* Spectral Symmetry Analysis // IEEE Trans. on Pattern Analysis and Machine Intelligence. – 2010. – 32 (7). – P. 1227-1238.
6. *Derrode S., Ghorbel F.* Shape Analysis and Symmetry Detection in Gray-level Objects Using the Analytical Fourier-Mellin Representation // Signal Processing. – 2004. – 84 (1). – P. 25-39.
7. *Karkishchenko A.N., Mnukhin V.B.* Threefold Symmetry Detection in Hexagonal Images Based on Finite Eisenstein Fields // Analysis of Images, Social Networks, and Texts. 5th International Conference, AIST'2016. Selected Papers. Communications in Computer and Information Science 661, Springer. – 2017. – P. 281-292.
8. *Каркищенко А.Н., Мнухин В.Б.* Распознавание симметрии изображений в частотной области // Тр. 9-й Международной конференции «Интеллектуализация обработки информации – 2012», TORUS Press, Moscow, 2012. – С. 426-429.
9. *Campello de Souza R.M., Farrell R.G.* Finite Field Transforms and Symmetry Groups // Discrete Mathematics. – 1985. – 56. – P. 111-116.
10. *Mnukhin V.B.* Transformations of Digital Images on Complex Discrete Tori // Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications. – 2014. – 24 (4). – P. 552-560.
11. *Каркищенко А.Н., Мнухин В.Б.* Применение модулярных логарифмов на комплексных дискретных торах в задачах обработки цифровых изображений // Вестник Ростовского государственного университета путей сообщения. Вып. 3. – Ростов-на-Дону: РГУПС, 2013. – С. 137-142.
12. *Mnukhin V.B.* Fourier-Mellin Transform on a Complex Discrete Torus // In: 11th Int. Conf. "Pattern Recognition and Image Analysis: New Information Technologies" (PRIA-11-2013), September 23-28 2013. Samara, Russia, 2013. – P. 102-105.
13. *Her I.* Geometric Transforms on the Hexagonal Grid // IEEE Transactions on Image Processing. – 1995. – 4 (9). – P. 1213-1222.
14. *Creutzburg R., Labunets V.G.* The Early Papers on Number-theoretic Transforms. – https://www.researchgate.net/publication/229043248.
15. *Лабунец В.Г.* Теоретико-числовые преобразования над квадратичными полями // Сложные системы управления. – Киев: Институт кибернетики УССР, 1982. – С. 30-37.
16. *Вариченко Л.В., Лабунец В.Г., Раков М.А.* Абстрактные алгебраические системы и цифровая обработка сигналов. – Kiev: Наукова Думка, 1986.
17. *Baker H.G.* Complex Gaussian Integers for Gaussian Graphics // ACM Sigplan Notices. – 1993. – 28 (11). – P. 22-27.
18. *Bandeira J., Campello de Souza R.M.* New Trigonometric Transforms Over Prime Finite Fields for Image Filtering // In: VI International Telecommunications Symposium (ITS2006), Fortaleza-Ce, Brazil. – 2006. – P. 628-633.
19. *Campello de Souza R.M., de Oliveira H.M., Silva D.* The *Z* Transform over Finite Fields // ArXiv preprint 1502.03371 published online February 11. – 2015.
20. *Hundt R., Schön J.C., Hannemann A., Jansen M.* Determination of Symmetries and Idealized Cell Parameters for Simulated Structures // Journal of Applied Crystallography. – 1999. – 32. – P. 413-416.
21. *Spek A.L.* Structure Validation in Chemical Crystallography // Acta Crystallographica. D65. – 2009. – P. 148-155.
22. *Zeyun Yu, Bajaj C.* Automatic Ultrastructure Segmentation of Reconstructed CryoEM Maps of Icosahedral Viruses // IEEE Transactions on Image Processing. – 2005. – 14 (9). – P. 1324-1337.

23. *Seiichi Kondo, Mark Lutwyche, Yasuo Wada* Observation of Threefold Symmetry Images due to a Point Defect on a Graphite Surface Using Scanning Tunneling Microscope (STM) // Japanese Journal of Applied Physics. – 1994. – 33 (9B). – P. 1342-1344.
24. *Ireland K., Rosen M.* A Classical Introduction to Modern Number Theory. – Springer-Verlag, 1982.
25. *Dummit D.S., Foote R.M.* Abstract Algebra. – John Wiley&Sons, 2004.
26. *Каркищенко А.Н., Мнухин В.Б.* Топологическая фильтрация для распознавания и анализа симметрии цифровых изображений // Машинное обучение и анализ данных. – 2014. – 1 (8). – С. 966-987.
27. *Маркус М., Минк Х.* Обзор по теории матриц и матричных неравенств. – М.: Наука, 1972. – 232 с.
28. *Кибзун А.И., Горяинова Е.Р., Наумов А.В.* Теория вероятностей и математическая статистика. Базовый курс с примерами и задачами. – М.: Физматлит, 2013. – 232 с.
29. *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей. – М.: Наука, 1969. – 368 с.
30. *Каркищенко А.Н., Горбань А.С.* К определению мер сходства полутоновых изображений // Известия ЮФУ. Технические науки. – 2008. – № 4 (81). – С. 98-103.

REFERENCES

1. *Gool L., Moons T., Ungureanu D., Pauwels E.* Symmetry from Shape and Shape from Symmetry, *Int. J. Robotics Res*., 1995, 14 (5), pp. 407-424.
2. *Martinet A., Soler C., Holzschuch N., Sillion F.* Accurate Detection of Symmetries in 3D Shapes, *ACM Trans. Graph*., 2006, 25 (2), pp. 439-464.
3. *Middleton L., Sivaswamy J.* Hexagonal Image Processing: A Practical Approach. Springer, 2005.
4. *Xiangjian He,Wenjing Jia, Namho Hur, QiangWu, Jinwoong Kim.* Image Translation and Rotation on Hexagonal Structure, *In: 6th IEEE Intern. Conf. on Computer and Information Technology (CIT'06).* Seoul, 141, 2006.
5. *Chertok M., Keller Y.* Spectral Symmetry Analysis, *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2010, 32 (7), pp. 1227-1238.
6. *Derrode S., Ghorbel F.* Shape Analysis and Symmetry Detection in Gray-level Objects Using the Analytical Fourier-Mellin Representation, *Signal Processing*, 2004, 84 (1), pp. 25-39.
7. *Karkishchenko A.N., Mnukhin V.B.* Threefold Symmetry Detection in Hexagonal Images Based on Finite Eisenstein Fields, *Analysis of Images, Social Networks, and Texts. 5th International Conference, AIST'2016. Selected Papers. Communications in Computer and Information Science 661, Springer, 2017*, pp. 281-292.
8. *Karkishchenko A.N., Mnukhin V.B.* Raspoznavanie simmetrii izobrazheniy v chastotnoy oblasti [Symmetry Recognition in the Frequency Domain], *Tr. 9-y Mezhdunarodnoy konferentsii «Intellektualizatsiya obrabotki informatsii – 2012», TORUS Press, Moscow, 2012* [In 9th International Conference on Intelligent Information Processing, TORUS Press, Moscow, 2012], pp. 426-429.
9. *Campello de Souza R.M., Farrell R.G.* Finite Field Transforms and Symmetry Groups, *Discrete Mathematics*, 1985, 56, pp. 111-116.
10. *Mnukhin V.B.* Transformations of Digital Images on Complex Discrete Tori, *Pattern Recognition and Image Analysis: Advances in Mathematical Theory and Applications*, 2014, 24 (4), pp. 552-560.
11. *Karkishchenko A.N., Mnukhin V.B.* Primenenie modulyarnykh logarifmov na kompleksnykh diskretnykh torakh v zadachakh obrabotki tsifrovykh izobrazheniy [Applications of Modular Logarithms on Complex Discrete Tori in Digital Image Processing], *Vestnik Rostovskogo gosudarstvennogo universiteta putey soobshcheniya* [Bulletin of the Rostov State University of Railway Transport]. Issue 3. Rostov-on-Don: RGUPS, 2013, pp. 137-142.
12. *Mnukhin V.B.* Fourier-Mellin Transform on a Complex Discrete Torus // In: 11th Int. Conf. "Pattern Recognition and Image Analysis: New Information Technologies" (PRIA-11-2013), September 23-28 2013. Samara, Russia, 2013. – P. 102-105.
13. *Her I.* Geometric Transforms on the Hexagonal Grid, *IEEE Transactions on Image Processing*, 1995, 4 (9), pp. 1213-1222.
14. *Creutzburg R., Labunets V.G.* The Early Papers on Number-theoretic Transforms. Available at: https://www.researchgate.net/publication/229043248.

15. *Labunets V.G.* Teoretiko-chislovye preobrazovaniya nad kvadratichnymi polyami [Number Theoretic Transforms over Quadratic Fields], *Slozhnye sistemy upravleniya* [Complex Control Systems]. Kiev: Institut kibernetiki USSR, 1982, pp. 30-37.
16. *Varichenko L.V., Labunets V.G., Rakov M.A.* Abstraktnye algebraicheskie sistemy i tsifrovaya obrabotka signalov [Abstract Algebraic Systems and Digital Signal Processing]. Kiev: Naukova Dumka, 1986.
17. *Baker H.G.* Complex Gaussian Integers for Gaussian Graphics, *ACM Sigplan Notices*, 1993, 28 (11), pp. 22-27.
18. *Bandeira J., Campello de Souza R.M.* New Trigonometric Transforms Over Prime Finite Fields for Image Filtering // *In: VI International Telecommunications Symposium (ITS2006), Fortaleza-Ce, Brazil, 2006*, pp. 628-633.
19. *Campello de Souza R.M., de Oliveira H.M., Silva D.* The *Z* Transform over Finite Fields, *ArXiv preprint 1502.03371 published online February 11*, 2015.
20. *Hundt R., Schön J.C., Hannemann A., Jansen M.* Determination of Symmetries and Idealized Cell Parameters for Simulated Structures, *Journal of Applied Crystallography*, 1999, 32, pp. 413-416.
21. *Spek A.L.* Structure Validation in Chemical Crystallography, *Acta Crystallographica. D65*, 2009, pp. 148-155.
22. *Zeyun Yu, Bajaj C.* Automatic Ultrastructure Segmentation of Reconstructed CryoEM Maps of Icosahedral Viruses, *IEEE Transactions on Image Processing*, 2005, 14 (9), pp. 1324-1337.
23. *Seiichi Kondo, Mark Lutwyche, Yasuo Wada* Observation of Threefold Symmetry Images due to a Point Defect on a Graphite Surface Using Scanning Tunneling Microscope (STM), *Japanese Journal of Applied Physics*, 1994, 33 (9B), pp. 1342-1344.
24. *Ireland K., Rosen M.* A Classical Introduction to Modern Number Theory. Springer-Verlag, 1982.
25. *Dummit D.S., Foote R.M.* Abstract Algebra. John Wiley&Sons, 2004.
26. *Karkishchenko A.N., Mnukhin V.B.* Topologicheskaya fil'tratsiya dlya raspoznavaniya i analiza simmetrii tsifrovykh izobrazheniy [Topological Filtration for Digital Images Recognition and Symmetry Analysis], *Mashinnoe obuchenie i analiz dannykh* [Journal of Machine Learning and Data Analysis], 2014, 1 (8), pp. 966-987.
27. *Markus M., Mink Kh.* Obzor po teorii matrits i matrichnykh neravenstv [Overview on the theory of matrices and matrix inequalities]. Moscow: Nauka, 1972, 232 p.
28. *Kibzun A.I., Goryainova E.R., Naumov A.V.* Teoriya veroyatnostey i matematicheskaya statistika. Bazovyy kurs s primerami i zadachami [Theory of Probability and Mathematical Statistics. Basic course with examples and tasks]. Moscow: Fizmatlit, 2013, 232 p.
29. *Venttsel' E.S., Ovcharov L.A.* Teoriya veroyatnostey [Theory of Probability]. Moscow: Nauka, 1969, 368 p.
30. *Karkishchenko A.N., Gorban' A.S.* K opredeleniyu mer skhodstva polutonovykh izobrazheniy [On the definition of measures of similarity of halftone images], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2008, No. 4 (81), pp. 98-103.

Статью рекомендовал к опубликованию д.ф.-м.н. Г.В. Куповых.

Каркищенко Александр Николаевич – Научно-исследовательский инсттут робототехники и процессов управления ЮФУ; e-mail: karkishalex@gmail.com; 347928, г. Таганрог, ул. Шевченко, 2; тел.: +78634371694; д.ф.-м.н.; профессор; в.н.с.

Мнухин Валерий Борисович – Южный федеральный университет; e-mail: mnukhin.valeriy@mail.ru; 347928, г. Таганрог, пер. Некрасовский, 44; тел.: +78634371606; к.ф.-м.н; доцент.

Karkishchenko Alexander Nikolaevich – Scientific Research Institute of Robotics and Control Processes of the Southern Federal University; e-mail: karkishalex@gmail.com; 2, Shevchenko street, Taganrog, 347928, Russia; phone: +78634371694, dr. of math. sc.; professor; leading researcher.

Mnukhin Valeriy Borisovich – Southern Federal University; e-mail: mnukhin.valeriy@mail.ru; 44, Nekrasovskiy lane, Taganrog, 347928, Russia; phone: +78634371606; cand. of phys. and math. sc.; associate professor.

УДК 004 DOI 10.18522/2311-3103-2020-5-185-193

Н.Е. Сергеев, А.В. Скринникова

ФОРМАЛИЗАЦИЯ НАБОРА ИНФОРМАТИВНЫХ ПРИЗНАКОВ ДИНАМИКИ МАНИПУЛЯЦИЙ УСТРОЙСТВАМИ УПРАВЛЕНИЯ КУРСОРОМ ПРИ РЕШЕНИИ ЗАДАЧИ ДИАГНОСТИКИ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ОПЕРАТОРОВ БТС

Информативные признаки динамики манипуляций устройствами управления типа стилус, палец, специальная ручка, мышь, трекбол, трекпоинт, сенсорная панель, ручка управления типа джойстик, игровой пульт, клавиатура, систем типа Microsoft Kinect, Leap Motion и т.п. играют важную роль при разработке программных комплексов идентификации операторов биотехнических систем по их индивидуальной динамике, при решении задач диагностики различных психоэмоциональных состояний и эффективности деятельности операторов в сферах технической и правоохранительной безопасности, медицинской и энергетической сферах, образовании и др. Система таких признаков однозначно не определена специалистами, поэтому решение этой задачи является актуальным. Цель работы – формализовать набор информативных признаков динамики манипуляции устройствами управления курсором при решении задачи диагностики эффективности деятельности операторов биотехнических систем. Поскольку вся сложность управления подобными устройствами переместилась с исполнительной части двигательных актов на центральные механизмы их регуляции в качестве конкретного примера, не нарушая общности, рассматриваются данные, полученные при манипуляциях с клавиатурой и мышью. Для достижения поставленной цели разработана схема взаимодействия оператора (биологического звена) с техническим звеном биотехнических систем, представлен краткий обзор наиболее часто используемых признаков динамики манипуляций устройствами управления, рассмотрен байесовский подход при статистической постановке задачи распознавания, на основе анализа ряда работ и собственных исследований произведена формализация набора информативных признаков динамики клавиатурного почерка и динамики манипуляций мышью, Также для диагностики эффективности деятельности операторов построены нечеткие правила на основе этого набора информативных признаков. Прогноз эффективности деятельности операторов, построенный на нечетких правилах по отобранным признакам, дал точность более 90 %. Для получения таких результатов был разработан программный комплекс. Преимуществом использования динамики манипуляций устройствами управления курсором операторов биотехнических систем при решении задачи диагностики эффективности деятельности операторов является отсутствие специального оборудования, требующего дополнительных затрат.

Устройства управления; задача распознавания; индивидуальная динамика.

N.E. Sergeev, A.V. Skrinnikova

FORMALIZATION OF A SET OF INFORMATIVE SIGNS THE DYNAMICS OF MANIPULATION BY CONTROL DEVICES TO SOLVING THE PROBLEM OF DIAGNOSING THE PRODUCTIVITY OF BTS OPERATORS

Informative signs of the dynamics of manipulation by control devices such as a mouse and keyboard play an important role in the development of software complexes for the identification of biotechnical systems (BTS) operators by their individual dynamics, in solving problems of diagnostics of various psycho emotional states and operator productivity. It finds application in the spheres of technical and law enforcement security, medical and energy spheres, etc. The purpose of this work is to formalize a set of informative signs of the dynamics of manipulation by control devices to solving the problem of diagnosing the productivity of BTS operators. To achieve this goal, an overview of the most frequently used features is presented, the Bayesian approach is considered in the statistical formulation of the recognition problem, a set of informative sings of the dynamics of keyboard handwriting and the dynamics of mouse manipulations is formalized based

on the results of a number of works. Operator productivity forecast based on fuzzy rules based on selected criteria gave an accuracy of more than 90%. The advantage of using the dynamics of manipulation of the control devices of the BTS operators is the absence of special equipment that requires additional costs.

Control devices; recognition task; individual dynamics.

Введение. Управление сложными техническими системами: энергоблоками, бортовыми системами корабля, беспилотными летающими аппаратами, рентгенографическими аппаратами и др. либо их разработка осуществляется человеком при помощи различных устройств управления: мышь, стилус, палец, специальная ручка, ручка управления типа джойстик, клавиатура, системы типа Microsoft Kinect, Leap 3D, ZeroN [1–4] и т.п. Современные БТС создают дружественными к человеку, однако, в них либо не предусматривается реагирование на существенные изменения состояний операторов и на их индивидуальные особенности либо реализации подобных решений дорого стоят. Существуют исследования [3, 5, 6], указывающие на то, что при помощи различных управляющих устройств, можно отследить, в частности, психоэмоциональные состояния (ПЭС), производительность оператора. Корректируя, в случае необходимости, например, состояния сниженного внимания, можно добиться повышения эффективности деятельности операторов БТС и, как следствие, повышения эффективности функционирования всей БТС.

На рис. 1 представлена схема взаимодействия оператора с техническим звеном БТС. Оператор в большинстве случаев работает либо с устройством типа мышь (выбирает указателем мыши цели) либо с устройством типа клавиатура (работа с текстом). Каждое устройство дает определенный набор информативных признаков динамики при манипуляции ним. Например, признаками клавиатурного почерка [3, 5, 11, 19, 20] служат длительность между удержанием соседних клавиш x_0, длительность удержания клавиши x_1, длительность между отжатием одной и нажатием следующей клавиши x_2 и т.п. Признаков динамики управления мышью гораздо больше (67 признаков обнаружено в работе [5]), например: x_3 – поправка на расстояние при достижении указателем мыши цели, x_4 – скорость движения, x_5 – ускорение указателя мыши, x_6 – кривизна кривой, которую описывает указатель при перемещении мыши, x_7 – общее время манипуляций мышью, x_8 – угловая скорость мыши, x_9 – длина кривой, которую описывает указатель при перемещении мыши [12–16]. Выбор информативных признаков является важнейшим этапом построения решающего правила, по которому будет надежно отличима, например, низкая эффективность деятельности оператора от высокой. Система таких признаков однозначно не определена специалистами, поэтому решение этой задачи является актуальным.

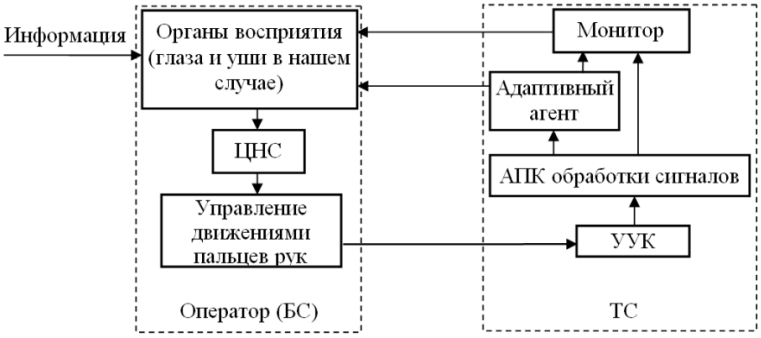

Рис. 1. Схема БТС«оператор-техническая система»

Изложение основного материала. Известно, что эффективность деятельности оператора зависит от его ПЭС и психомоторики [17, 18]. Разработаны методы и системы диагностики различных состояний операторов, использующие специальное оборудование. Например, изобретение [7] описывает систему контроля эмоционального состояния пользователя в процессе потребления мультимедийного содержания, в которой физиологические реакции: сердцебиение, давление, температуру, экспрессию лица, голос, жесты, – измеряют биосенсорами, инфракрасными камерами, микрофонами. Карточки учета рабочего времени, динамические и статические методы биометрии контролируют опоздания, нецелевое время, но не анализируют эффективность деятельности операторов. Применяют также и методы, не требующие дополнительных затрат: диагностика эффективности деятельности оператора на основе динамики манипуляций устройствами управления (ДМУУК). В работе [4] подобный метод отличается наименьшей средней квадратичной ошибкой по точности диагностики эффективности деятельности оператора среди аналогов [6, 8], фиксацией событий управляющих устройств и учетом пауз при манипуляциях ними, расчетом по фиксированным событиям признаков ДМУУК их числовых характеристик для дальнейшей диагностики путем сравнения текущей динамики с полученным заранее в нейтральном состоянии «эталонным» образцом динамики.

Произведем отбор информативных признаков ДМУУК при решении задачи диагностики эффективности деятельности операторов БТС.

Пусть эффективности деятельности оператора принадлежит одному из M возможных классов $E_1,\ldots,E_M$ множества $E = \{E_1,\ldots,E_M\}$. Есть совокупность признаков ДМУУК $X^{(N)} = (x_1,\ldots,x_N)$, которые могут быть использованы как признаки для диагностики одной из множества эмоций пользователя. Необходимо построить решающее правило $D(X^{(N,)})$: $X^{N)} \rightarrow$ M, которое отобразит множество $X^{(N)} = \{X^{N)}\}$ возможных значений признаков $x_1,\ldots,x_N$ на множество $M = \{1,\ldots,M\}$ номеров состояний $E_1,\ldots,E_M$, т.е., построить алгоритм определения значений индикаторной переменной $s = D(X^{(N)})$ в виде

$$s = \begin{cases} 1, \text{ если } X^{(N)} \in \Omega_1 \\ \ldots \\ M, \text{ если } X^{(N)} \in \Omega_M \end{cases},$$

где Ω_m, $m = 1,\ldots,M$ – непересекающиеся области пространства $X^{(N)}$, в которых принимаются решения в пользу класса E_m.

Здесь возникает статистическая постановка задачи распознавания [9], поскольку при различных уровнях эффективности деятельности $E_i \neq E_j$ могут совпадать значения каждого из имеющихся признаков X_n ($1 < n < N$). То есть допускается, что множества значений каждого признака, соответствующие различным классам, пересекаются.

При статистической постановке задачи распознавания часто используют байесовский подход, согласно которому классы эффективности деятельности $E_1,\ldots, E_M$ рассматриваются как случайные события с априорными вероятностями $P(E_m)$, $\sum_{m=1}^{M} P(E_M) = 1$, признаки – как случайные величины, для которых объективно существуют условные распределения $p_i(X^{(N)} \mid E_m)$, а множества $X_m^{(N)} = \{X^{(N)}: p(x^{(N)} \mid E_m) \neq 0\}$, $X_1^{(N)} \cup \ldots \cup X_M^{(N)} = X^{(N)}$ – собственные области классов в пространстве признаков.

Байесовский метод построения решающего правила $s = D(X^{(N,)})$ состоит в следующем. Пусть известны априорная вероятность $P(E_m)$ и условные распределения $p(X^{N)}|E_m)$, определены значения признаков $X_1 = \hat{X}_1, \ldots, X_N = \hat{X}_N$. Необходимо определить текущее состояние объекта $E_m \in E$. По формуле Байеса находим апостериорные вероятности:

$$X_m^{(N)} = \{X^{(N)}: p(x^{(N)} | E_m) \neq 0\},\ X_1^{(N)} \cup \ldots \cup X_M^{(N)} = X^{(N)}.$$

Соответствующее правило максимума апостериорной вероятности трех информативных признаков эквивалентно правилу вида

$$s = \begin{cases} 1,\ если\ \lambda_{12} > \lambda_{012}, \lambda_{13} > \lambda_{013} \\ 2,\ если\ \lambda_{12} < \lambda_{012}, \lambda_{23} > \lambda_{023} \\ 3,\ если\ \lambda_{13} < \lambda_{013}, \lambda_{23} < \lambda_{023}, \end{cases}$$

где

$$\lambda_{12} = \frac{P(\hat{X}^{(N)} | E_1)}{P(\hat{X}^{(N)} | E_2)}, \quad \lambda_{13} = \frac{P(\hat{X}^{(N)} | E_1)}{P(\hat{X}^{(N)} | E_3)}, \quad \lambda_{23} = \frac{P(\hat{X}^{(N)} | E_2)}{P(\hat{X}^{(N)} | E_3)}, \quad \lambda_{012} = \frac{P(E_1)}{P(E_2)},$$

$$\lambda_{013} = \frac{P(E_1)}{P(E_3)}, \quad \lambda_{023} = \frac{P(E_2)}{P(E_3)}.$$

Для оценки эффективности признаков при статистической постановке задачи распознавания используют информационный подход, согласно которому полезность признака связывают с уменьшением неопределенности (шенноновской энтропии) [10]. При этом следует различать информативность отдельного признака и информативность признака в совокупности с другими.

С точки зрения достоверности результатов диагностики эффективности деятельности более удачной оценкой полезности признака могут служить не изменение средней условной энтропии $H(E | X^{(N)})$, а изменение средней вероятности ошибки $P(e)$ или, в общем случае, среднего риска.

Очевидно, при числе классов M для любого фиксированного $X^{(M)} = \hat{X}^{(M)}$ условная вероятность ошибочных решений $P(e|\hat{X}^{(N)}) = 1 - \max\{P(E_1|\hat{X}^{(N)}),\ P(E_2|\hat{X}^{(N)})\}$ однозначно определяет и частную условную энтропию

$$H(E | \hat{X}^{(N)}) = -P(e | \hat{X}^{(N)}) \log_2 P(e | \hat{X}^{(N)}) - [1 - P(e | \hat{X}^{(N)})] \log_2 [1 - P(e | \hat{X}^{(N)})].$$

Однако признаков ДМУУК достаточно много и трудоемко рассчитать энтропии для всех возможных их сочетаний. Поэтому поступим иначе.

Отбор информативных признаков динамики манипуляций устройствами управления. Рассмотрим ДМУУК клавиатурного почерка по фиксированной фразе с учетом возможных перекрытий между клавишами. Составим массив межклавишных взаимодействий T из событий нажатия и отжатия и времени нажатия/отжатия клавиш. Пример данных представлен в табл. 1. Напротив каждой из набранных букв фразы «My dog is very big.» указан элемент массива

$$T = \begin{pmatrix} T_{11} & T_{12} & \ldots & T_{1n} \\ T_{21} & T_{22} & \ldots & T_{2n} \end{pmatrix},$$

где n – количество нажатий клавиш при наборе фиксированной фразы, T_{ji} – признак удержания/отжатия i-й клавиши (j=1 – клавиша нажата, j=2 – клавиша отжата), T_{1i} – длительность удержания (T_{2i} – отжатия) i-й клавиши, i=1,2,…,n. Знаками ↑ и ↓ условно обозначены отжатия и нажатия клавиш соответственно. Фраза набрана без ошибок с одним двойным перекрытием между буквами «е» и «г».

Таблица 1

Пример данных, извлеченных из клавиатурного почерка

Клавиша	Время в мс, прошедшее с момента запуска Windows		x_1	x_0	x_2
m	↓10322218	↑10322312	94	125	31
y	↓10322343	↑10322437	94	157	63
…	…	...	…	…	…
v	e↓10325609	r↓10325734	156	110	-46
e	e↑10326390	r↑10326500	125	234	109
r	↓10326734	↑10326812	78	312	234
y	↓10327046	↑10327109	63	1047	984
–	↓10328093	↑10328156	63	328	265
…	…	…	…	…	…

Анализ наиболее часто используемых признаков x_0, x_1 и x_2 показал, что $x_0[i] = x_1[i] + x_2[i]$. То есть, если у оператора под влиянием каких-то факторов увеличатся x_1 и уменьшатся x_2 или наоборот, то вероятность ошибочных решений будет выше при учете трех признаков x_0, x_1, x_2, чем при учете только x_1 и x_2. Поэтому целесообразно использовать только x_1 и x_2 без x_0. Хотя в процессе исследований по идентификации пользователей по клавиатурному почерку иногда используют триграммы и даже слова [11].

Данные динамики манипуляций мышью получают путем сбора событий мыши (будь то перемещение, перетаскивание или нажатия кнопки) и длительности этих событий *t* в миллисекундах, *XX* и *YY* координат курсора на экране монитора.

В табл. 2 дан анализ некоторых работ по точности диагностики эмоций при использовании различных признаков ДМУУК. Как видно признак x_7 дает хорошие результаты при распознавании. В работе [3] высокие результаты дал признак x_6. Поэтому имеем $X = (x_1, x_2, x_6, x_7)$ – совокупность информативных признаков ДМУУК.

Таблица 2

Сравнительный анализ зависимости между точностью диагностики эмоций и использованными признаками ДМУУК [11 - 14, 1]

Признак	Исследователи	Точность
x_3, x_8	S. Singh, Dr. K.V. Arya	Ошибки I, II рода до 6%
x_4,x_5,x_7, дрожание руки	Kaklauskas A., Zavadskas E.K., Seniut M.[at al]	Не указано
x_3,x_4, x_5	Maehr W.	Достоверности гипотез об однородности дисперсий до 45%, 100%
x_7, x_9	Weiss A.,Ramapanicker A., Shah P. [at al]	Точность распознавания до 80-92%
x_3, x_4, x_5,x_6, x_7	Скринникова А.В.	Точность распознавания до 90/90/90/95/99%

Построение нечетких правил на основе набора информативных признаков для диагностики эффективности деятельности **операторов.** Поскольку, сильное возбуждение: аффект, психоз и т.п. – вносят существенный разлад в деятельность человека; возбуждение: кураж, интенсивные эмоции – восторг, гнев,

ужас и т.д. – могут принести пользу в деятельности; депрессивное состояние может повлечь состояния сильно сниженной реакции («сон»), сниженной реакции, активности сознания, внимания («транс»), то поставим описанные ПЭС в соответствие одному из пяти классов производительности операторов P [в долях ед.]: p_5 – производительность в норме; p_4 – кураж, p_3 – транс, p_2 – аффект, p_1 – сон.

В случае диагностики эффективности деятельности по динамике манипуляций мышкой входные параметры X (x_6, x_7). Входные лингвистические переменные x_6 и x_7 описываются терм-множествами x_{61} – «минимальная кривизна кривой, которую описывает указатель при перемещении мыши», x_{62} – «средняя кривизна кривой», x_{63} – «максимальная кривизна кривой» и x_{71} – «минимальное время манипуляций мышью», x_{72} – «среднее время», x_{73} – «максимальное время» соответственно:

$$x_7 = \mu(x_{71})/x_{71} + \mu(x_{72})/x_{72} + \mu(x_{73})/x_{73}$$

и

$$x_6 = \mu(x_{61})/x_{61} + \mu(x_{62})/x_{62} + \mu(x_{63})/x_{63}\,.$$

Функции принадлежности получены при экспериментальном исследовании [4] в виде треугольных функций.

Выходная лингвистическая переменная P («эффективность деятельности оператора БТС») задана на терм-множествах p_5 – «эффективность деятельности в норме»; p_4 – «кураж», p_3 – «транс (снижена)»; p_2 – «аффект», p_1 – «сон (эффективность деятельности крайне низкая)»:

$$P = \mu(p_1)/p_1 + \mu(p_2)/p_2 + \mu(p_3)/p_3 + \mu(p_4)/p_4 + \mu(p_5)/p_5\,.$$

Представим базу нечетких правил вида «Если … То»:

ЕСЛИ $\mu(x_{61})/x_{61}$ И $\mu(x_{71})/x_{71}$, ТО $\mu(p_5)/p_5$,

ЕСЛИ $\mu(x_{61})/x_{61}$ И $\mu(x_{72})/x_{72}$ ИЛИ ЕСЛИ $\mu(x_{62})/x_{62}$ И $\mu(x_{71})/x_{71}$, ТО $\mu(p_4)/p_4$,

ЕСЛИ $\mu(x_{61})/x_{61}$ И $\mu(x_{73})/x_{73}$ ИЛИ ЕСЛИ $\mu(x_{62})/x_{62}$ И $\mu(x_{72})/x_{72}$ ИЛИ ЕСЛИ $\mu(x_{63})/x_{63}$ И $\mu(x_{71})/x_{71}$, ТО $\mu(p_3)/p_3$,

ЕСЛИ $\mu(x_{63})/x_{63}$ И $\mu(x_{72})/x_{72}$ ИЛИ ЕСЛИ $\mu(x_{62})/x_{62}$ И $\mu(x_{73})/x_{73}$, ТО $\mu(p_2)/p_2$,

ЕСЛИ $\mu(x_{63})/x_{63}$ И $\mu(x_{73})/x_{73}$, ТО $\mu(p_1)/p_1$.

В результате применения информативных признаков x_6 и x_7 и указанных нечетких правил при мониторинге ДМУУК в работе [4] получена точность прогноза эффективности деятельности операторов методом, основанным на нечеткой логике и мягких арифметических операциях, 90,14 %. Прогнозные значения сравнивались с данными, полученными из протоколов работы операторов по итогам отправки электронных писем участникам конференции результатов рецензирования присланных статей.

Заключение. В работе представлена формализация набора информативных признаков динамики манипуляций устройствами управления курсором. Разработанный программный комплекс, учитывающий описанный набор информативных признаков динамики манипуляций устройствами управления курсором, дал точность прогноза эффективности деятельности операторов более 90 %. Преимуществом предложенного комплекса является отсутствие специального оборудования, требующего дополнительных затрат.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Lee J., Post R., Ishii H.* ZeroN: Mid-Air Tangible Interaction Enabled by Computer Controlled Magnetic Levitation // UIST'11, Santa Barbara, CA, USA, October 16–19, 2011. – P. 10.
2. *Сатыбалдина Д.Ж., Калымова К.А.* Разработка приложения, управляемого жестами, с использованием Microsoft Kinect Sensor // Сб .тр. 21-й междунар. конф. «Цифровая обработка сигналов и её применение» – DSPA-2019, Москва, 27-29 марта 2019 г. – С. 525-529.
3. *Скринникова А.В.* Изменение индивидуальной динамики манипуляций устройствами управления курсором под влиянием эмоций страха и радости // Известия ЮФУ. Технические науки. – 2013. – № 5 (142). – С. 246-251.
4. *Бобырь М.В., Скринникова А.В., Милостная Н.А., Серегин С.П.* Нечеткая биотехническая система управления производительностью человека-оператора // Медицинская техника. – 2017. – № 4 (304). – С. 46-50.
5. *Zimmermann P.G.* Beyond Usability – Measuring Aspects of User Experience: dis. dr. sciences. Swiss federal institute of technology. – Zurich, 2008. – 112 p.
6. *Сержантова М.В., Ушаков А.В.* Конечные цепи Маркова в модельном представлении деятельности человека-оператора в квазистатической функциональной среде // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16, № 3. – С. 524-532.
7. Пат. 7698238 US, МПК G06F 17/00. Emotional controlled system for processing multimedia data / A. Barletta(DE), B. Moser(DE), M. Mayer(DE); assignee Sony Duetschland GmbH, Cologne (DE) – 13.04.2010. – 10 p.
8. *Евдокименков В.Н., Ким Р.В., Красильщиков М.Н., Себряков Г.Г.* Системы управления движущимися объектами // Известия РАН. Теория и системы управления. – 2015. – № 4. – С. 111-123.
9. *Шлезингер М.И., Главач В.* Десять лекций по статистическому и структурному распознаванию. – К : Наукова Думка, 2004. – 546 с.
10. *Файнзильберг Л.С.* Математические методы оценки полезности диагностических признаков: монография. – К.: Освита Украины, 2010. – 152 с.
11. *Dowland P., Furnell S.* A long-term trial of keystroke profiling using digraph, trigraph, and keyword latencies // Proc. of IFIP/SEC – 19th International Conf. on Information Security, Toulouse, France, 2004. – P. 275-289.
12. *Weiss A., Ramapanicker A., Shah P. [at al].* Mouse Movements Biometric Identification: A Feasibility Study // Proc. of CSIS, Pace Univ., May 2007. – P. 21-28.
13. *Singh S., Dr. K.V. Arya.* Mouse interaction based authentication system by classifying the distance travelled by the mouse // International Journal of Computer Applications. Vol. 17, No. 1, March 2011. – URL: http://www.ijcaon-line.org/volume17/number1/pxc3872752.pdf (дата обращения: 29.11.2011).
14. *Kaklauskas A., Zavadskas E.K., Seniut M.[at al].* Web-based biometric mouse decision support system for user's emotional and labour productivity analysis // The 25th Int. Symp. Automation and Robotics in Construction, 2008. – P. 69-75.
15. *Maehr W.* Estimation of the user's emotional state by mouse motions: diploma thesis for Fachhochschule Vorarlberg ; iTec – Information and Communication Engineering. – Dornbirn, Austria, August 2005. – P. 145.
16. *Nazar A., Traore I., Ahmed A.A.E.* Inverse biometrics for mouse dynamics // Int. Journ. of Pattern Recognition and Artificial Intelligence. – 2008. – Vol. 22, No. 3. – P. 461-495.
17. *Ахремчик О.Л., Базулев И.И.* Программный комплекс для измерения времени аудиомоторных реакций операторов систем управления химико-технологическими процессами // Программные продукты и системы. – 2017. – No. 2 (30). – С. 328-332.
18. *Цагарелли Ю.А. Труды Е.П.* Ильина как энциклопедия современной психологии // Психология человека в образовании. – 2019. – Т. 1, № 4. – С. 330-340. – DOI: 10.33910/2686-9527-2019-1-4-330-340.
19. *Hughes M., Aulck L., Johnson P.W.* Are there differences in typing performance and typing forces between short and long travel keyboards // Reviews of Human Factors and Ergonomics. – Sep. 2011. – Vol. 55. – P. 954-957.
20. *Giot R., El-Abed M., Rosenberger Ch.* Keystroke dynamics authentication // Biometrics. Pub: InTech, 2011. – P. 157-182.

REFERENCES

1. *Lee J., Post R., Ishii H.* ZeroN: Mid-Air Tangible Interaction Enabled by Computer Controlled Magnetic Levitation, *UIST'11, Santa Barbara, CA, USA, October 16–19, 2011*, pp. 10.
2. *Satybaldina D.Zh., Kalymova K.A.* Razrabotka prilozheniya, upravlyaemogo zhestami, s icpol'zovaniem Microsoft Kinect Sensor [The development of an application controlled by gestures using a Microsoft Kinect Sensor], *Sb .tr. 21-y mezhdunar. konf. «TSifrovaya obrabotka signalov i ee primenenie» – DSPA-2019, Moskva, 27-29 marta 2019 g.* [Collection of truls of the 21st International Conference "Digital signal processing and its application" – DSPA-2019, Moscow, March 27-29, 2019], pp. 525-529.
3. *Skrinnikova A.V.* Izmenenie individual'noy dinamiki manipulyatsiy ustroystvami upravleniya kursorom pod vliyaniem emotsiy strakha i radosti [Changing the individual dynamics of manipulations of cursor control devices under the influence of emotions of fear and joy], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 5 (142), pp. 246-251.
4. *Bobyr' M.V., Skrinnikova A.V., Milostnaya N.A., Seregin S.P.* Nechetkaya biotekhnicheskaya sistema upravleniya proizvoditel'nost'yu cheloveka-operatora [Bioengineering fuzzy control system performance of the human operator], *Meditsinskaya tekhnika* [Medical equipment], 2017, No. 4 (304), pp. 46-50.
5. *Zimmermann P.G.* Beyond Usability – Measuring Aspects of User Experience: dis. dr. sciences. Swiss federal institute of technology. Zurich, 2008, 112 p.
6. *Serzhantova M.V., Ushakov A.V.* Konechnye tsepi Markova v model'nom predstavlenii deyatel'nosti cheloveka-operatora v kvazistaticheskoy funktsional'noy srede [Finite Markov chains in the model representation of human operator activity in a quasi-static functional environment], *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics], 2016, Vol. 16, No. 3, pp. 524-532.
7. Partent 7698238 US, МПК G06F 17/00. Emotional controlled system for processing multimedia data, A. Barletta(DE), B. Moser(DE), M. Mayer(DE); assignee Sony Duetschland GmbH, Cologne (DE), 13.04.2010, 10 p.
8. *Evdokimenkov V.N., Kim R.V., Krasil'shchikov M.N., Sebryakov G.G.* Sistemy upravleniya dvizhushchimisya ob"ektami [Control systems for moving objects], *Izvestiya RAN. Teoriya i sistemy upravleniya* [Izvestiya RAS. Theory and control systems], 2015, No. 4, pp. 111-123.
9. *Shlezinger M.I., Glavach V.* Desyat' lektsiy po statisticheskomu i strukturnomu raspoznavaniyu [Ten lectures on statistical and structural recognition]. Kiev: Naukova Dumka, 2004, 546 p.
10. *Faynzil'berg L.S.* Matematicheskie metody otsenki poleznosti diagnosticheskikh priznakov: monografiya [Mathematical methods for evaluating the usefulness of diagnostic signs: monograph]. Kiev: Osvita Ukrainy, 2010, 152 p.
11. *Dowland P., Furnell S*. A long-term trial of keystroke profiling using digraph, trigraph, and keyword latencies, *Proc. of IFIP/SEC – 19th International Conf. on Information Security, Toulouse, France, 2004*, pp. 275-289.
12. *Weiss A., Ramapanicker A., Shah P. [at al]*. Mouse Movements Biometric Identification: A Feasibility Study, *Proc. of CSIS, Pace Univ., May 2007*, pp. 21-28.
13. *Singh S., Dr. K.V. Arya.* Mouse interaction based authentication system by classifying the distance travelled by the mouse, *International Journal of Computer Applications*, March 2011, Vol. 17, No. 1. Available at: http://www.ijcaon-line.org/volume17/number1/pxc3872752.pdf (accessed 29 November 2011).
14. *Kaklauskas A., Zavadskas E.K., Seniut M.[at al]*. Web-based biometric mouse decision support system for user's emotional and labour productivity analysis, *The 25th Int. Symp. Automation and Robotics in Construction, 2008*, pp. 69-75.
15. *Maehr W.* Estimation of the user's emotional state by mouse motions: diploma thesis for Fachhochschule Vorarlberg ; iTec – Information and Communication Engineering. Dornbirn, Austria, August 2005, pp. 145.
16. *Nazar A., Traore I., Ahmed A.A.E.* Inverse biometrics for mouse dynamics, *Int. Journ. of Pattern Recognition and Artificial Intelligence*, 2008, Vol. 22, No. 3, pp. 461-495.

17. *Akhremchik O.L., Bazulev I.I.* Programmnyy kompleks dlya izmereniya vremeni audio-motornykh reaktsiy operatorov sistem upravleniya khimiko-tekhnologicheskimi protsessami [Software package for measuring the time of audio-motor reactions of operators of control systems for chemical and technological processes], *Programmnye produkty i sistemy* [Software products and systems], 2017, No. 2 (30), pp. 328-332.
18. *Tsagarelli Yu.A. Trudy E.P.* Il'ina kak entsiklopediya sovremennoy psikhologii [Ilyin is like an encyclopedia of modern psychology], *Psikhologiya cheloveka v obrazovanii* [Human psychology in education], 2019, Vol. 1, No. 4, pp. 330-340. DOI: 10.33910/2686-9527-2019-1-4-330-340.
19. *Hughes M., Aulck L., Johnson P.W.* Are there differences in typing performance and typing forces between short and long travel keyboards, *Reviews of Human Factors and Ergonomics*, Sep. 2011, Vol. 55, pp. 954-957.
20. *Giot R., El-Abed M., Rosenberger Ch.* Keystroke dynamics authentication, *Biometrics. Pub: InTech, 2011*, pp. 157-182.

Статью рекомендовала к опубликованию к.т.н. С.В. Темникова.

Скринникова Анна Владимировна – Южный федеральный университет; e-mail: ann3005@rambler.ru; 347922, г. Таганрог, ул. Чехова, 2; тел.: 89185321859; специалист по учебно-методической работе Института компьютерных технологий и информационной безопасности.

Сергеев Николай Евгеньевич – e-mail: nesergeev@sfedu.ru; тел.: 89001278025; кафедра вычислительной техники; д.т.н.; профессор.

Skrinnikova Anna Vladimirovna – Southern Federal University; e-mail: ann3005@rambler.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone: +79001278025; specialist in educational and methodological work of the Institute of Computer Technologies and Information Security

Sergeev Nikolay Evgenyevich – e-mail: nesergeev@sfedu.ru; phone: +79001278025; the department of computer science; dr. of eng. sc.; professor.

ПРАВИЛА ОФОРМЛЕНИЯ РУКОПИСЕЙ

1. Объем статьи должен быть не менее 12 и не более 18 страниц. Формат (А 4). Редактор ***Word 7 for Windows***, шрифт Times New Roman, размер 14, интервал 1,5. Авторы представляют в редакцию 1 экз. статьи и идентичный электронный вариант.

2. Названию статьи предшествует индекс УДК, соответствующий заявленной теме.

3. Текст статьи начинается с названия статьи (на русском и английском языках), фамилии, имени и отчества автора (полностью) и снабжается аннотацией на русском и английском языках объёмом ***не менее 250-300 слов***. В тексте аннотации указывается цель, задачи исследования и краткие выводы. В аннотации ***не следует*** давать ссылки на номер публикации в списке литературы к статье. После аннотаций приводятся ключевые слова (словосочетания), несущие в тексте основную смысловую нагрузку (на русском и английском языках).

4. В тексте статьи следует использовать минимальное количество таблиц и иллюстраций. Рисунок должен иметь объяснения значений всех компонентов, порядковый номер, название, расположенное под рисунком. В тексте на рисунок дается ссылка. Таблица должна иметь порядковый номер, заголовок, расположенный над ней. Данные таблиц и рисунков не должны дублировать текст. Формулы должны быть набраны ***в редакторе формул Word 7 for Windows.***

5. Цитаты тщательно сверяются с первоисточником и визируются автором на обратной стороне последней страницы: "Цитаты и фактический материал сверены". Подпись, дата.

6. Наличие пристатейного библиографического списка на русском и английском языках обязательно. ***Ссылок должно быть не менее 20-ти,*** из них на зарубежные источники – не менее 35 %. В тексте ссылки должны быть в квадратных скобках.

Примеры оформления литературы: а) для книг: фамилия, инициалы автора(ов), полное название книги, место, год издания, страницы; б) для статей: фамилия и инициалы автора(ов), полное название сборника, книги, газеты, журнала, где опубликована статья, место и год издания (сборника, книги), номер (для журнала), год и дата (для газеты), выпуск, часть (для сборника), страницы, на которых опубликована статья. Иностранная литература оформляется по тем же правилам.

Ссылки на неопубликованные работы не допускаются.

7. Рукопись должна быть тщательно вычитана. Редакционная коллегия оставляет за собой право при необходимости сокращать статьи, редактировать и отсылать авторам на доработку.

8. Статьи сопровождаются сведениями об авторе(ах) (фамилия, имя, отчество, ученое звание, должность, место работы, адрес, электронный адрес и номер телефона) на русском и английском языках.

9. Плата с аспирантов за публикацию рукописей не взымается.

Адрес журнала в Интернете: http://izv-tn.tti.sfedu.ru/.