ISSN 2500-0403

ВЕСТНИК

БАЛТИЙСКОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА им. И. КАНТА

Серия

Физико-математические и технические науки

№ 4

Калининград
Издательство Балтийского федерального университета
им. Иммануила Канта
2020

Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. — 2020. — № 4. — 115 с.

Редакционная коллегия

А. В. Юров, д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта (главный редактор); *С. В. Мациевский,* канд. физ.-мат. наук, доц., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта (ответственный редактор); *Н. Л. Великанов,* д-р техн. наук, проф., Институт транспорта и технического сервиса, БФУ им. И. Канта; *В. Е. Захаров,* д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *А. И. Иванов,* д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *С. А. Ишанов,* д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *С. Б. Лебле,* д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *И. В. Карпов*, д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *С. И. Корягин,* д-р техн. наук, проф., Институт транспорта и технического сервиса, БФУ им. И. Канта; *С. П. Кшевецкий,* д-р физ.-мат. наук, проф., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта; *И. Б. Петров,* д-р физ.-мат. наук, проф., чл.-кор. РАН, факультет управления и прикладной математики, Московский физико-технический институт (государственный университет); *А. А. Шананин,* д-р физ.-мат. наук, проф., чл.-кор. РАН, факультет управления и прикладной математики, Московский физико-технический институт (государственный университет); *Б. Н. Четверушкин,* д-р физ.-мат. наук, проф., академик РАН, Институт прикладной математики им. М.В. Келдыша РАН; *А. А. Шпилевой,* канд. физ.-мат. наук, доц., Институт физико-математических наук и информационных технологий, БФУ им. И. Канта

Издание зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Свидетельство о регистрации СМИ ПИ № ФС 77-65005 от 04 марта 2016 г.

Адрес редакции:
236016, Россия, Калининград, ул. А. Невского, 14

© БФУ им. И. Канта, 2020

СОДЕРЖАНИЕ

Математика и информатика

Ткаченко С.Н., Куценко Е.А. Использование CRM-системы для анализа эффективности работы сотрудников банка 5

Мищенко М.П. Гибридная атака на задачу обучения с ошибками (LWE) с разряженным секретом 10

Каренин А.С. Нахождение оптимальных BKZ-параметров для редукции NTRU-решеток 16

Максимов-Наливайко Ф.Г. Защищенная отправка сообщений по меш-сети на основе Bluetooth 26

Демочкина П.Б. Масштабируемые zk-SNARK 34

Колесников Н.С. Эффективная реализация экспоненциальной части алгоритма подсчета точек в якобианах гиперэллиптических кривых рода 2 42

Теоретическая и экспериментальная физика

Румовская С.Б. Исследование коллективной деятельности по преодолению диагностической проблемы 49

Колесников А.В., Румовская С.Б., Ясинский Э.В., Солдатов С.А. Интеллектуализация оперативно-технологического управления региональной электроэнергетикой методами когнитивных гибридных интеллектуальных систем. Часть 1 57

Волхонская Е.В., Коротей Е.В., Власова К.В. Модельные исследования направленных свойств однозеркальной антенны с двухдиапазонным логопериодическим облучателем в среде MathCAD 88

Кадолич Ж.В., Зотов С.В. Расширение арсенала физических методов исследования жидких диэлектриков на примере экзотических видов растительных масел 96

Персичкин А.А., Шпилевая С.Г., Персичкина Н.В. Особенности стыковки измерительных приборов с программным пакетом Matlab 108

CONTENTS

Mathematics and computer science

Tkachenko S.N., Kutsenko E.A. Using CRM system to analyze the efficiency of bank employees 5

Mishchenko M.P. Hybrid attack on Learning with Errors (LWE) with sparse secret 10

Karenin A.S. Finding optimal BKZ parametrs for NTRU lattice reduction 16

Maksimov-Nalivaiko F.G. Secure sending of messages over the mesh network based on bluetooth 26

Demochkina P.B. Scalable zk-SNARK 34

Kolesnikov N.S. An efficient implementation of an exponential point-counting algorithm on Jacobians of genus 2 hyperelliptic curves 42

Theoretical and experimental physics

Rumovskaya S.B. The research of the collective activity to overcome a diagnostic problem 49

Kolesnikov A.V., Rumovskaya S.B., Yasinsky E.V., Soldatov S.A. Intellectualization of operational and technological control of regional electric power by cognitive hybrid intelligent systems. Part 1 57

Volkhonskaya E.V., Korotey E.V., Vlasova K.V. Model researches of a single-mirror antenna with a dual-band log-periodic irradiator directional properties in MathCAD 88

Kadolich Zh. V., Zotov S.V. Expansion of the arsenal of physical research methods of liquid dielectric examples exotic types of vegetable oils 96

Persichkin A.A., Shpilevaya S.G., Persichkina N.V. Features of connecting measuring devices with the software package Matlab 108

УДК 336.71: 519.23

С. Н. Ткаченко, Е. А. Куценко

ИСПОЛЬЗОВАНИЕ CRM-СИСТЕМЫ ДЛЯ АНАЛИЗА ЭФФЕКТИВНОСТИ РАБОТЫ СОТРУДНИКОВ БАНКА

Рассмотрена возможность использования данных, собираемых при помощи CRM-системы для работы с клиентами банка, в целях определения эффективности работы сотрудников банка. В результате анализа функций CRM-системы получено порядка 20 атрибутов для формирования профиля сотрудника, по которым можно рассчитать его интегральную эффективность.

The paper considers the possibility of using data collected by the CRM system for working with Bank clients to analyze the efficiency of Bank employees. An analysis of the CRM system functions was performed, from which about 20 attributes were obtained for forming the employee profile and by which it is possible to calculate its integral efficiency.

Ключевые слова: цифровой профиль, банк, CRM-система, эффективность.

Keywords: digital profile, bank, CRM system, efficiency.

Введение

В современных экономических условиях использование информационных систем для ведения коммерческой деятельности носит обязательный характер. Не составляет исключения и банковская сфера, которая зачастую выступает драйвером развития различных программных продуктов, автоматизирующих работу с клиентами, бизнес-процессами и т. д.

Одним из наиболее распространенных программных решений для автоматизации является CRM-система (Customer Relationship Management — управление взаимоотношениями с клиентами). Данный программный продукт встречается в большинстве компаний во всем мире.

Согласно определению Gartner Group, CRM — это бизнес-стратегия, разработанная для оптимизации прибыльности и рентабельности компании при одновременном повышении удовлетворенности и лояльности клиентов. Технологии CRM позволяют разрабатывать стратегию, а также выявлять текущие отношения с клиентами и управлять ими лично или виртуально. Программное обеспечение CRM предоставляет функциональные возможности компаниям в четырех сегментах: продажи, маркетинг, обслуживание клиентов и цифровая коммерция [1].

Применительно к банковской сфере CRM-система является «накопителем» данных по взаимодействию менеджеров банка с их клиентами — физическими и / или юридическими лицами — в самых разных аспектах оказания банковских услуг.

© Ткаченко С. Н., Куценко Е. А., 2020

Накопленная информация обо всех «касаниях» клиентов может служить средством для оценки эффективности сотрудников банка. В данной работе сделана попытка проанализировать, какие данные из CRM-системы могут послужить основой для подобной оценки.

Функции CRM-системы

Согласно классификации, предложенной Бартоном Голденбергом [2, p. 368], для CRM-системы характерны 11 функций, часть которых имеет сходный характер:

- управление контактами;
- управление продажами (сюда же можно отнести телемаркетинг, продажи при помощи мобильных приложений, сайта и т. д.);
- управление временем;
- поддержка клиентов (послепродажный сервис, Service Desk);
- управление маркетингом (от управления рекламными компаниями до сегментации клиентов и ведения отдельных каналов коммуникации);
- управление отчетностью, в первую очередь для руководства;
- интеграция с корпоративными системами более высокого уровня, в том числе ERP;
- синхронизация данных и т. д.

Как видно из этого списка, не все базовые функции могут дать информацию, подходящую для составления цифрового профиля сотрудника банка.

Далее мы выполним анализ функций CRM-системы, для того чтобы выделить список атрибутов, на основе которого можно судить об эффективности работы сотрудников.

В рамках данной работы не вводится определение эффективности, так как исследование сосредоточено на анализе CRM-системы банка и формировании списка данных, на основе которых может быть построена модель машинного обучения для того, чтобы судить об эффективности каждого сотрудника. Поэтому под эффективностью мы будем понимать общую полезность работника в рамках бизнес-процессов банка, которая обеспечивается такими качествами, как компетентность, умение четко планировать свои задачи в течение рабочего дня, стрессоустойчивость, высокий уровень коммуникабельности, стремление к решению проблем, ответственность и забота о клиентах. Для определения интегральной величины эффективности должны использоваться все влияющие на нее параметры.

Атрибуты данных, хранящихся в CRM-системе, применимые для оценки эффективности сотрудников

Функция управления контактами связана с хранением профиля клиента в системе. На первый взгляд, эффективность работы банковского сотрудника никак не обусловлена содержанием профиля клиента, однако это не так.

Очевидно, что CRM-система минимизирует ошибки при вводе данных клиента в систему при помощи использования разнообразных справочников и разработанных шаблонов. Однако ошибки все равно случаются, и их количество и частоту можно использовать как критерии, позволяющие судить об эффективности работника.

Помимо этого, сами данные клиента могут рассказать о том, с кем именно работает сотрудник. Согласно закону больших чисел, в течение длительного времени сотрудники контактируют со всеми категориями клиентов, тем не менее возможны определенные корреляции между возрастом, социальным положением, средним доходом и другими атрибутами клиента, с одной стороны, и месторасположением отделения банка — с другой. Все эти факторы будут влиять на продажи, время обслуживания и т.д. Поэтому некоторые усредненные характеристики клиентов (доход, возраст и т.д.), с которыми работает сотрудник, целесообразно включить в его цифровой профиль.

Общими характеристиками, связанными с клиентами, также являются региональная группа, тип населенного пункта, а для больших городов должно применяться районирование. Если не учитывать эти данные и не приводить значения к среднему в привязке к географическому месту в различных разрезах, то на величину эффективности сотрудника будет серьезно влиять такой фактор, как существенная разница значений средней заработной платы по регионам Российской Федерации.

Функция управления продажами наиболее тесно связана с эффективностью, поскольку здесь мы говорим о целевом действии сотрудника, которое и приносит прибыль компании. Поэтому вполне очевидно, что количество продаж, тип продаваемого продукта, сумма продаж в привязке к единице времени (это может быть один день, неделя, месяц и т.д.) должны быть основой для оценки эффективности сотрудника банка.

С продажами тесно связаны потери. Например, если клиент обратился за кредитом, но по каким-либо причинам не взял его, образуются потери от упущенного клиента. Также возможны финансовые потери, обусловленные ошибками в работе сотрудников. Поэтому целесообразно разделять потери на непосредственные и косвенные.

Атрибутом, связывающим потери и продажи, является конвертация потока клиентов в продажи. Данная характеристика измеряется в процентах и при значении выше среднего может говорить об эффективности сотрудника.

Использование CRM-системы должно приводить к сокращению временных издержек при работе с клиентами. Тем не менее проблема управления временем и корректного подсчета времени сотрудника попрежнему актуальна. При изменении норматива времени обслуживания, который сокращается при использовании CRM, возрастает нагрузка на самих работников. Поэтому в профиле сотрудника можно использовать различные атрибуты, связанные со временем: среднее время работы с клиентами определенной категории, соотнесенное с нормативом и средним по отделению банка. Также целесообразно отдельно от-

слеживать, сколько времени заняли вспомогательные операции, насколько вовремя были подготовлены дополнительные документы и т. д. Это влияет на операционные потери, о которых говорилось выше.

В качестве производного из управления временем параметра может быть взята частота отклонения от нормативного времени на обслуживание конкретного типа клиентов.

Управление поддержкой клиентов непосредственно связано с определенной категорией сотрудников, относящихся к Service Desk. Тем не менее каждый сотрудник банка имеет возможность оказать помощь клиенту в решении возникших вопросов. Зачастую многих проблем, в том числе потери клиента, удается избежать, если при первом обращении клиента к работнику банка ему был предложен корректный алгоритм действий. При этом необязательно, чтобы сотрудник, к которому обращался клиент, решил инцидент или проблему клиента. Данный параметр является трудно формализуемым, но очень желательным для включения в профиль работника банка. С этой целью выполняется сбор обратной связи с детализацией в виде специализированных вопросов.

Управление маркетингом влияет на продажи. Сама идея CRM-системы предполагает переход к индивидуализации продаж, кастомизации продукта в соответствии со специфическими запросами клиентов. Поэтому так важно, чтобы сотрудник, работающий с клиентом, не только ориентировался на его запрос, но и мог проконсультировать по линейке продуктов банка.

Нередко обращение клиента связано с тем, что его перестал устраивать ассортимент услуг (возможно, изменились его предпочтения, ожидания). В этой связи необходимо фиксировать информацию о том, какие банковские продукты были предложены клиенту в процессе обращения. Сам факт того, что подобные предложения были сделаны, положительно влияет на эффективность работника.

Еще одним доводом в поддержку учета данного фактора выступает сам факт существования маркетинговых потерь, когда клиенты уходят в другой банк, получив более выгодное маркетинговое предложение. Следовательно, если не делать предложений новых или обновленных банковских продуктов клиенту во время обращения (пусть и по другому вопросу), есть риск в итоге потерять его лояльность.

Управление отчетностью, как и другие функции, дает ряд признаков для оценки эффективности сотрудника. Базовыми параметрами могут служить количество ошибок (если только эти ошибки не сформированы самой CRM-системой) и своевременность сдачи отчетности. Важным фактором для оценки работы сотрудников будет не только вертикальная коммуникация, но и горизонтальная. Зачастую выполнение задач зависит от других работников, поэтому учет временных промежутков между операциями и выяснение причин, которые вызвали задержки, также является актуальным и подлежит фиксации в CRM.

Производным атрибутов в данном разделе могут выступать потери, которые возникли вследствие ошибок в отчетности.

Функции, связанные с техническими аспектами работы CRM-системы, не предоставляют каких-либо данных для характеристики работы сотрудников.

Предложенные характеристики, из которых можно составить достаточно полный цифровой профиль сотрудника, позволяют разработать модель для оценки эффективности различных категорий работников банка.

Выводы

Информация, содержащаяся в CRM-системе банка, многомерна и позволяет проанализировать не только клиентов организации, но и ее сотрудников. Помимо профиля работника и его социально-демографических признаков, в CRM-системе хранится множество «отражений» его профессиональной деятельности.

Разработанные атрибуты в количестве около 20 могут быть положены в основу модели машинного обучения, по которой можно судить об эффективности отдельного сотрудника банка и определять адекватность принимаемых мер по стимулированию работников.

Сама по себе оценка эффективности не должна быть «репрессивной» мерой по отношению к сотрудникам. Она призвана выделить лучших для их удержания на рабочих местах путем адекватного стимулирования. В случае низких значений эффективности необходимо обучение сотрудников в отношении продуктов и услуг банка, совершенствование навыков работы с информационными системами.

При наличии постоянной оценки эффективности работы персонала банка возрастает управляемость всей системой.

Список литературы

1. *Customer* Relationship Management (CRM) // Gartner : [сайт]. URL: https://www.gartner.com/en/information-technology/glossary/customer-relationship-management-crm (дата обращения: 26.04.2020).

2. *CRM:* Российская практика эффективного бизнеса / А. Кудинов, М. Сорокин, Е. Голышева [и др.] ; под ред. М. Сорокина. М., 2008.

Об авторах

Сергей Николаевич Ткаченко — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: tkasergey@yandex.ru

Елена Арсеньевна Куценко — магистрант, Балтийский федеральный университет им. И. Канта, Россия.
E-mail: alenka24.06@mail.ru

The authors

Dr Sergey N. Tkachenko, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: tkasergey@yandex.ru

Elena A. Kutsenko, Master's Student, Immanuel Kant Baltic Federal University, Russia.
E-mail: alenka24.06@mail.ru

УДК 004.056.5

М. П. Мищенко

ГИБРИДНАЯ АТАКА НА ЗАДАЧУ ОБУЧЕНИЯ С ОШИБКАМИ (LWE) С РАЗРЯЖЕННЫМ СЕКРЕТОМ

В 2007 г. Н. Хаугрейв-Грэм предложил атаку на криптосистему NTRU, которая заключается в совмещении техники редукции решеток и комбинаторного метода «встречи посередине» (атаки meet-in-the-middle, MiTM). В данной работе этот подход применяется к задаче Learning with Errors (LWE) с секретом малой длины. Задача LWE является одной из самых важных в теории криптографии на решетках. Безопасность большого количества криптографических схем, начиная от простых подписей и схем и заканчивая продвинутыми схемами, такими как групповые подписи и полностью гомоморфное шифрование, основывается на предположениях о сложности LWE. В статье представлен обзор гибридной атаки, а также используемых в ней алгоритмов. Это необходимо для дальнейшей практически значимой реализации атаки, главной целью которой является верификация корректности применения метода MiTM к гибридной атаке на LWE.

In 2007, Howgrave-Graham proposed attack against NTRU cryptosystem, which consists of two parts, combining lattice reduction technique and a combinatorial method called meet-in-the-middle (MiTM). In this article, we apply hybrid attack to the Learning with Errors Problem (LWE) with sparse secret. The LWE problem is considered to be one of the most important in lattice-based cryptography. Large number of cryprographic schemes ranging from basic signature and encryption schemes to advanced schemes like group signatures and fully homomorphic encryption, base their security on the hardness assumption of LWE. In this paper, we review the hybrid attack and the algorithms it is based on. It is required for further practical implementation of the attack, whose main objective is to verify correctness of MiTM to the hybrid attack against the LWE problem.

Ключевые слова: гибридная атака, криптография на решетках, обучение с ошибками, метод «встречи посередине».

Keywords: hybrid attack, lattice based cryptography, LWE, MiTM.

Решетки

В 1996 г. венгерский математик Миклош Айтаи опубликовал работу [2], в которой доказал, что можно построить случайную решетку с коротким вектором такую, что любой алгоритм нахождения этого вектора в данной решетке будет сводим к задаче нахождения приблизительно кратчайшего вектора в любой решетке. Этот факт положил начало направлению в современной криптографии, которое называют lattice based cryptography, или криптография на решетках.

Схемы, реализованные с помощью криптографии на решетках, имеют огромный потенциал и вызывают большой интерес к их изучению.

© Мищенко М.П., 2020
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 10 – 15.

В настоящее время происходит процесс стандартизации постквантовых криптографических протоколов (в частности, на решетках) в России и США. В 2018 г. Национальный институт стандартов и технологий опубликовал список из открытых вопросов, касающихся безопасности криптографических схем, основанных на решетках. Гибридная атака, изучаемая в данной работе, также релевантна для криптосистемы NTRU — кандидата к стандартизации. Таким образом, выбор параметров криптосистем, основанных на решетках, является открытым вопросом, требующим детального анализа.

Пусть $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}) \subset \mathbb{R}$ — множество линейно независимых векторов. Решеткой $\mathcal{L}$, порожденной векторами $\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}$, называют множество всех линейных комбинаций этих векторов с коэффициентами в $\mathbb{R}$:

$$\mathcal{L}(\mathbf{B}) = \{\alpha_0\mathbf{b}_0 + \cdots + \alpha_{n-1}\mathbf{b}_{n-1} | \alpha_0, \ldots, \alpha_{n-1} \in \mathbb{Z}\} \in \mathbb{R}^m.$$

Целочисленной называют решетку, все векторы которой имеют целочисленные координаты. Таким образом, целочисленная решетка является аддитивной подгруппой $\mathbb{Z}^m$ для некоторого $m \geq 1$. Базисом $\mathcal{L}$ называют любой набор независимых векторов, которые порождают $\mathcal{L}$, размерностью $\mathcal{L}$ — количество векторов в любом базисе $\mathcal{L}$.

Криптография на решетках основывается на вычислительной сложности решения определенных задач. Рассмотрим задачи, необходимые для описания атаки на LWE.

В задаче поиска ближайшего вектора (CVP) для $\mathbf{t} \notin \mathcal{L}$ требуется найти $\mathbf{v} \in \mathcal{L}$:

$$\|\mathbf{v} - \mathbf{t}\| \text{ минимально для всех } \mathbf{v} \in \mathcal{L}.$$

Пусть $dist(t, \mathcal{L}) \leq \frac{1}{\gamma}\lambda_1(\mathcal{L})$. Тогда получаем задачу о декодировании с ограниченным расстоянием (Bounded distance decoding, BDD): для базиса $\mathbf{B}$ решетки $\mathcal{L}$ и целевого вектора $\mathbf{t} \in \mathbb{R}^m$ найти вектор $\mathbf{e} \in \mathbb{R}^m$ такой, что выполняется $\|\mathbf{e}\| < \alpha\lambda_1(\mathcal{L}(\mathbf{B}))$ и $\mathbf{t} - \mathbf{e} \in \mathcal{L}(\mathbf{B})$.

Эвристики и алгоритмы

Теорема *(Теорема Эрмита). Для любой решетки $\mathcal{L}$ размерности n существует такой ненулевой вектор $\boldsymbol{b} \in LL$, что*

$$\|\mathbf{b}\| \leq \sqrt{n}\det(\mathcal{L})^{\frac{1}{n}}.$$

Гауссова эвристика предсказывает, что количество $|\mathcal{L} \cap \mathcal{B}|$ точек решетки, лежащих внутри измеримого объекта $\mathcal{B} \subset \mathbb{R}^n$, приблизительно равно $\mathcal{B}/Vol(\mathcal{L})$. Применяя эту эвристику для шара в n-мерном евклидовом пространстве, получим следующую оценку $\lambda_1(\mathcal{L})$ для заданной решетки $\mathcal{L}$.

Гауссова эвристика. Обозначим с помощью $gh(\mathcal{L})$ первый ожидаемый минимум решетки $\mathcal{L}$ согласно гауссовой эвристике. Для решетки $\mathcal{L}$ полного ранга в $\mathbb{R}^d$ имеем

$$gh(\mathcal{L}) = \sqrt{d/2e}Vol(\mathcal{L})^{\frac{1}{d}}.$$

Качество базиса после редукции можно измерить величиной, называемой корень-фактором Эрмита.

Корень-фактор Эрмита (эрмитова дельта) для базиса **B** решетки размерности d определяется как

$$\delta = (|\mathbf{b}_0/Vol(\mathbf{B})^{1/d})^{1/d}.$$

Замечание: рассмотрим версию теоремы, которая дает более точную (верхнюю) оценку для нормы кратчайшего вектора. Константой Эрмита δ_n называют такое наименьшее число, что для любой решетки $\mathcal{L}$ размерности n найдется вектор $\mathbf{w} \in \mathcal{L}$, который удовлетворяет

$$\| \mathbf{w} \|^2 \leq \delta_n \det(\mathcal{L})^{\frac{2}{n}}.$$

Алгоритм Бабая (Nearest Plane Algorithm). На вход принимается базис $\mathbf{B} \subset \mathbb{Z}^n$ решетки $\mathcal{L}$ и целевой вектор $\mathbf{t} \in \mathbb{R}^n$. Выходом алгоритма является вектор $\mathbf{e} \in \mathbb{R}^n$ такой, что $\mathbf{t} - \mathbf{e} \in \mathcal{L}(\mathbf{B})$.

Под редукцией базиса **B** решетки $\mathcal{L}$ понимают процесс нахождения последовательных базисов $\mathcal{L}$, векторы которых более короткие и ближе к тому, чтобы быть ортогональными. Важными понятиями редукции являются алгоритмы HKZ и БКЗ-β reduction. Алгоритм БКЗ принимает на вход базис решетки $\mathcal{L}$ и размер блока β, возвращая БКЗ-β редуцированный базис решетки $\mathcal{L}$.

Блочный алгоритм Эрмита — Коркина — Золотарёва, БКЗ (Block Korkine — Zolotarev Algorithm, BKZ). Базис $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{d-1})$ решетки $\mathcal{L}$ называется БКЗ-редуцированным (BKZ) с блоком размера β (БКЗ-β), если для его векторов справедливо

$$\mathbf{b}_i^* = \lambda_1(\mathcal{L}_{[i:\min(i+\beta,d)]}, \forall i < d.$$

Другими словами, БКЗ-редукция требует, чтобы конкретный вектор в базисе был наикратчайшим только при рассмотрении локальной спроектированной подрешетки таким образом, что локальность зависит от β. Трудность выполнения алгоритма БКЗ растет вместе с ростом β. В случае БКЗ-β-редукции дельта Эрмита является довольно предсказуемой величиной. Для блоков маленького размера дельта Эрмита вычисляется экспериментально, для блоков большого размера справедлива асимптотическая формула

$$\delta(\beta)^{2\beta-1} = (\beta/(2\pi e))(\beta\pi)^{\frac{1}{\beta}}.$$

LLL-алгоритм (Lenstra-Lenstra-Lovász, LLL) описывает нахождение оптимального ортогонального базиса для решеток любой размерности. Пусть $\mathbf{B} = (\mathbf{b}_0, \ldots, \mathbf{b}_{n-1})$ — базис решетки $\mathcal{L}$ и $\mathbf{B}^* = (\mathbf{b}_0^*, \ldots, \mathbf{b}_{n-1}^*)$ — соответствующий ортогональный базис. Говорят, что базис $\mathbf{B}^*$ LLL-редуцирован, если выполняются следующие два условия:

1) условие «размера»:

$$\| \mu_{i,j} \| = \frac{|\mathbf{b}_i \cdot \mathbf{b}_j^*|}{\|\mathbf{b}_j^*\|^2} \leq \frac{1}{2}, \text{для } 0 \leq j \leq n-1;$$

2) условие Ловаса:

$$\| \mathbf{b}_i^* \| \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \| \mathbf{b}_{i-1}^* \|^2, \text{для } 0 \leq j \leq n-1.$$

Задача обучения с ошибками (Learning with Errors, LWE)

Задача LWE [3]: Пусть n, q — положительные целые, χ — некоторое вероятностное распределение на $\mathbb{Z}$, $\mathbf{s}$ — некоторый (секретный) вектор в $\mathbb{Z}_q^n$. Обозначим с помощью $\Psi_{\mathbf{s},\chi,q}$ вероятностное распределение на $\mathbb{Z}_q^n \times \mathbb{Z}_q$, полученное путем выбора векторов $\mathbf{a} \in \mathbb{Z}_q^n$ случайно и равномерно и $\mathbf{e} \in \mathbb{Z}_q^m$ согласно χ. Требуется вернуть пару $(\mathbf{a}, \mathbf{c}) = (\mathbf{a}, \mathbf{as} + \mathbf{e}) \in$ $\in \mathbb{Z}^n \times \mathbb{Z}_q$.

В качестве вероятностного распределения $\chi \in \mathbb{Z}_q$ обычно берутся распределения, близкие к нормальному (распределение Гаусса N). Входными данными является пара $(\mathbf{A}, \mathbf{v})$, где $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ выбирается случайно согласно некоторому равномерному распределению, и вектор $\mathbf{As} + \mathbf{e}$ для равномерно выбранного $\mathbf{s} \in \mathbb{Z}_q^n$ и вектора $\mathbf{e} \in \mathbb{Z}_q^m$, выбранного с помощью распределения χ^m. Проблему составляет определение, каким путем был получен вектор, заданный $\mathbf{v}$. Эта задача может быть сведена к задаче BDD в q-арных решетках: для данной матрицы $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ и вектора $\mathbf{v} \in \mathbb{Z}_q^m$ определить, выбран вектор $\mathbf{v}$ равномерно из $\mathbb{Z}_q^m$ или же получен путем перебора всех координат случайной точки в решетке $\mathcal{L}_q(\mathbf{A}^T)$ согласно распределению χ.

Криптосистемы с разряженным секретом, то есть с секретом, коэффициенты которого принадлежат ограниченному интервалу, эффективны в прикладных задачах, так как позволяют быстрее производить вычисления. Рассмотрим общий вид атаки для случая, когда секрет является тринарным ($\mathbf{s} \in \{0, \pm 1\}^n$).

Гибридная атака на LWE

Для целых чисел $m, n, q \in \mathbb{Z}$, где $m > n$, положим

$$(\mathbf{A}, \mathbf{b}) = \mathbf{As} + \mathbf{e} \bmod q. \tag{1}$$

Это экземпляр LWE, где $\mathbf{A} \in \mathbb{Z}_q^{m \times n}, \mathbf{b} \in \mathbb{Z}_q^n$, секрет $\mathbf{s} \in \{0, \pm 1\}^n$ и вектор ошибки $\mathbf{e} \in \mathbb{Z}_q^m$.

Рассмотрим порожденную базисом решетку $\mathcal{L}(\mathbf{B})$ вида

$$\mathcal{L}(\mathbf{B}) = \begin{pmatrix} q\mathbf{I}_n & \mathbf{A} \\ \mathbf{0} & \mathbf{I}_n \end{pmatrix} \in \mathbb{Z}_q^{2n \times 2n}. \tag{2}$$

Вектор $(\mathbf{b}, \mathbf{0}) \in \mathbb{Z}_q^{2n}$ близок к решетке $\mathcal{L}(\mathbf{B})$ на $\|(\mathbf{e}, \mathbf{s})\|$. Разобьем матрицу $\mathbf{A}$ на две части: $\mathbf{A} = (\mathbf{A}_l | \mathbf{A}_g)$ так, что $\mathbf{A}_l \in \mathbb{Z}^{n \times l}$, $\mathbf{A}_g \in \mathbb{Z}^{n \times g}$ и $l + g = n$. Аналогичным образом разбиваем секрет $\mathbf{s}$ на две части: $\mathbf{s} = (\mathbf{s}_l | \mathbf{s}_g)$. Таким образом, получим новый экземпляр LWE:

$$\mathbf{b}' = \left(\mathbf{A}_l \middle| \mathbf{A}_g\right) \begin{pmatrix} \mathbf{s}_l \\ \mathbf{s}_g \end{pmatrix} + \mathbf{e} = \mathbf{A}_l \mathbf{s}_l + \mathbf{A}_g \mathbf{s}_g + \mathbf{e}' \bmod q.$$

Матрица $\mathbf{A}_l$ формирует подрешетку решетки $\mathcal{L}(\mathbf{B}')$, порожденную базисом:

$$\mathcal{L}(\mathbf{B}') = \begin{pmatrix} q\mathbf{I}_n & \mathbf{A}_l \\ \mathbf{0} & \mathbf{I}_l \end{pmatrix} \in \mathbb{Z}_q^{n+l \times n+l}. \quad (3)$$

Полученный таким образом новый экземпляр LWE решить гораздо проще, так как определитель $\det(L_q(A_g)) = q^m - n + g$ новой решетки существенно больше определителя $\det(L_q(A)) = q^m - n$ решетки $\mathbf{A}$. Для решения этой задачи можно свести проблему BDD к нахождению CVP.

Перед началом атаки вызывается процедура BDDPreprocess, которая редуцирует решетку $L_q(B')$ для поиска параметров атаки, в том числе размера блока β BKZ-редукции. Зная β, задачу BDD для решетки $\mathcal{L}(\mathbf{B}')$ можно свести к решению CVP в решетке $\mathcal{L}(\mathbf{B}')$.

Первую часть атаки (угадывание) можно ускорить с помощью метода «встречи посередине». Используя этот подход, возможно сократить количество попыток угадать вектор до квадратного корня от количества попыток при наивном подходе методом «грубой силы».

Алгоритм. Гибридная атака на LWE (MITM).

Input: $n, q \in \mathbb{Z}$ и $g \in \mathbf{N}$,

Output: $\mathbf{A} = (\mathbf{A}_l | \mathbf{A}_g)$, где $\mathbf{A}_l \in \mathbb{Z}^{n \times l}, \mathbf{A}_g \in \mathbb{Z}^{n \times g}, \mathbf{b} \in \mathbb{Z}_q^n$ вектор $\mathbf{s} \in \{0, \pm 1\}^n$ такой, что $\mathbf{b} = \mathbf{A}\mathbf{s} - \mathbf{e} \bmod q$.

1. Запустить алгоритм предобработки $BDDPreprocess(\mathcal{L}(\mathbf{B}'))$ для базиса $\mathbf{B}'$, заданного уравнением (3). Получим решетку $\mathbf{B}'_{red}$.

2. Сформируем два списка векторов L_1 и L_2:

$$L_1 = \{\mathbf{A}_l \mathbf{s}_1, \mathbf{s}_1)\} \in \mathbb{Z}_q^{n+l},$$

$$L_2 = \{\mathbf{b} - \mathbf{A}_l \mathbf{s}_2, \mathbf{s}_2)\} \in \mathbb{Z}_q^{n+l},$$

такие, что $\exists(\mathbf{s}_1, \mathbf{s}_2) \in L_1[2] \times L_2[2]$, в том числе $\mathbf{s}_g = \mathbf{s}_1 + \mathbf{s}_2$.

3. $V_1 = BDDQuery(\mathbf{B}'_{red}, L_1)$.

4. $V_2 = BDDQuery(\mathbf{B}'_{red}, L_2)$.

5. Вызвать $ClosestPairs(V_1, V_2, d)$ для целевого расстояния $d = \|(\mathbf{e}, \mathbf{s}_l)\|$.

Для того чтобы применить метод «встречи посередине», процедура BDDQuery должна быть аддитивно-гомоморфной. В качестве ее предлагается взять алгоритм Бабая, но его эвристика нуждается в проверке.

Также предполагается, что существует эффективная хеш-функция, которая решает проблему близких векторов ClosestPairs (V_1, V_2): для данных векторов V_1, V_2 и целевого расстояния (в евклидовой метрике) d найти все пары $(\mathbf{v}_1, \mathbf{v}_2) \in V_1 \times V_2$ такие, что $k\mathbf{v}_1 - \mathbf{v}_2$ для некоторого целого $k \leq d$. В качестве такой хеш-функции в данной реализации предлагается использовать алгоритм SimHash [4].

Работа над алгоритмом ведется на языке Python с использованием библиотек fpylll и G6k. На данный момент реализованы алгоритм SimHash, процедуры BDDPreprocess и ClosestPairs. Также предстоит реа-

лизовать процедуру BDDQuery, тем самым завершив предварительную реализацию атаки в общем виде. В дальнейшем предстоит проверить корректность применения MiTM к гибридной атаке, провести анализ времени выполнения алгоритма, определить вероятность успешного выполнения атаки, минимизировать время выполнения путем нахождения оптимальных параметров.

Список литературы

1. *Howgrave-Graham N.* A hybrid lattice-reduction and meet-in-the-middle attack against NTRU // Advances in Cryptology — CRYPTO 2007: Proceedings of 27th Annual International Cryptology Conference. Springer, 2007. Vol. 4622. P. 150—169. (Lecture Notes in Computer Science).

2. *Ajtai M.* Generating hard instances of lattice problems // Proceedings of the 28th annual ACM symposium on Theory of computing. Springer, 1996. P. 99—108.

3. *Regev O.* On lattices, learning with errors, random linear codes, and cryptography // Journal of the ACM. 2009. Vol. 56, iss. 6. P. 1—40.

4. *Fitzpatrick R., Bishof Ch. H., Buchmann J. et al.* Tuning GaussSieve for speed // International Conference on Cryptology and Information Security in Latin America. Springer, 2014. P. 288—305.

5. *Babai L.* On Lovász' lattice reduction and the nearest lattice point problem // Combinatorica. 1986. Vol. 6, iss. 1. P. 1—13.

6. *Buchmann J., Göpfert F., Player R., Wunderer Th.* On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack // International Conference on Cryptology in Africa. Springer, 2016. P. 24—43.

8. *Wunderer T.* Revisiting the Hybrid Attack: Improved Analysis and Refined Security Estimates // Cryptology ePrint Archive, Report 2016/733. URL: https://eprint.iacr.org/2016/733 (дата обращения: 15.10.2020).

9. *Micciancio D., Goldwasser S.* Complexity of lattice problems: a cryptographic perspective. Springer Science & Business Media, 2012. Vol. 671.

10. *Micciancio D.* Lattice-based cryptography // Encyclopedia of Cryptography and Security. Springer, 2011. P. 713—715.

11. *Conway J.H., Sloane N.J.A.* Sphere packings, lattices and groups. Springer Science & Business Media, 2013.

Об авторе

Максим Павлович Мищенко — студент, Балтийский федеральный университет им. И. Канта, Россия.

E-mail: mishchenkom_rel@bk.ru

The author

Maksim P. Mishchenko, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: mishchenkom_rel@bk.ru

УДК 512.5

А. С. Каренин

НАХОЖДЕНИЕ ОПТИМАЛЬНЫХ BKZ-ПАРАМЕТРОВ ДЛЯ РЕДУКЦИИ NTRU-РЕШЕТОК

Рассмотрен вопрос подбора оптимальных параметров для атаки методом редукции решетки с применением BKZ-алгоритма на решетчатые криптосистемы, использующие решетки с подрешетками малого ранга. Иллюстрируются проблемы некоторых подходов к организации таких решетчатых криптосистем. Описаны условия для существования полиномиальной атаки, представлен эффективный алгоритм, находящий параметры для данной атаки. Разработанный алгоритм является довольно быстрым и работает за время, оцениваемое как $O(\log^2 n)$*, где* n *– размерность решетки. Его корректность проверена численными эксперементами. Также приведены графики, связывающие параметры решетки и минимальные необходимые для ее успешной редукции параметры.*

This article is devoted to selection of optimal parameters for lattice reduction attack against lattice-based cryptosystems that use lattices with low rank sublattices. It illustrates design flaws caused by current approach to buiding these types of cryptosystems. Its relevance and novelty lies in the description of the conditions for the existence of a polynomial attack and in constructing an efficient algorithm that allows us to find optimal reduction attack parameters. The algorithm developed during the work on this article is quite fast and requires $O(\log^2 n)$ *of time to return results where* n *is the dimension of lattice. Its correctness has been verified by numerical experiments. As a result, graphs are shown connecting the parameters of the lattice and the minimum smallest parameters necessary for its successful reduction.*

Ключевые слова: криптография на открытом ключе, постквантовая криптография, решетки, BKZ-алгоритм.

Keywords: public key cryptography, post-quantum cryptography, lattice, BKZ algorithm.

Введение

Решеточные криптосистемы появились в 1990-е гг. как ответ на потребность в алгоритмах шифрования на открытом ключе, устойчивых к атакам с использованием квантовых алгоритмов. Их отличие состоит в том, что проблема редукции базиса решеток, мешающая злоумышленнику вскрыть зашифрованное сообщение, является предположительно устойчивой к атакам, выполняемым на квантовых компьютерах при использовании соответствующих алгоритмов [1].

В частности, неподдельный интерес в среде криптографов вызвала криптосистема NTRU, представленная Дж. Хоффштейном, Дж. Пайфер и Дж. Х. Сильверманом около 1996 г. Эта криптосистема среди прочих постквантовых обещала более короткие ключи и оптимальную

© Каренин А.С., 2020

производительность. Однако проблема однозначного расшифрования сообщения так и не была решена: сообщение с исчезающе малой, но все же ненулевой вероятностью могло не зашифроваться на данном ключе [1]. Также, несмотря на оптимальность производительности по сравнению с конкурирующими постквантовыми решениями, NTRU все же страдала неоптимизованностью. Именно поэтому в августе 2017 г. в статье [2] группа исследователей привела «готовый к практическому применению» вариант NTRU под названием NTRU Prime. Главными достижениями их подхода стали сокращенная длина ключа, оптимизированная производительность и гарантия возможности расшифровки сообщения. Однако ценой такого выигрыша является потенциально «растянутый» (англ. overstretched) параметр q, что может привести к возможной уязвимости к атакам с использованием подрешеток малого ранга, как это описано в [3].

Цель нашего исследования — реализация оптимизированного алгоритма поиска параметров BKZ-алгоритма β и размерности k подрешетки, к которой применяется BKZ-алгоритм, для дальнейшего использования при взломе криптосистем, в основу которых положена сложность проблемы нахождения кратчайшего вектора в так называемых NTRU-решетках [5].

Актуальность данной работы заключается в новизне предложенного алгоритма подбора оптимальных параметров (k, β) для редукции решетки с использованием BKZ-алгоритма (далее — BKZ-редукции), обеспечивающих наибольшую скорость ее выполнения.

Основные понятия

Пусть $v_1, ..., v_n \in R^m$ — множество линейно независимых векторов. Множество $\mathcal{L}$ их комбинаций с целочисленными коэффициентами называется решеткой, порожденной этими векторами. Иными словами,

$$\mathcal{L} = \{a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \mid a_i \in \mathbb{Z}\}.$$

Если все коэффициенты a_i являются целочисленными, такая решетка $\mathcal{L}$ тоже называется целочисленной.

Пусть $v_1, ..., v_n \in \mathbb{R}^m$ — базис решетки $\mathcal{L}$. Определим векторы $w_i = a_{i_1} v_1 + \ldots + a_{i_n} v_n, 1 \leqslant i \leqslant n,$ принадлежащие $\mathcal{L}$. Коэффициенты $a_{i,j}$, где $1 \leqslant i, j \leqslant n,$ целочисленны по определению решетки. Выразим v_i через w_i. В процессе нам понадобится матрица, обратная к матрице

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}.$$

Однако вспомним, что коэффициенты A^{-1} тоже должны быть целочисленными, поэтому можно сделать вывод о том, что все базисы решетки $\mathcal{L}$ связаны между собой целочисленными матрицами с определителем, равным ±1 [1].

Решетка $\mathcal{L}$, базисные векторы которой образуют строки или столбцы следующей матрицы:

$$B = \begin{pmatrix} q \cdot I_n & 0 \\ h & I_n \end{pmatrix},$$

где h — матрица размерности $n \times n$, называется NTRU-решеткой [4].

Криптостойкость решетчатых криптосистем, использующих NTRU-решетки, основывается на сложности задачи **SVP** (поиска кратчайшего вектора). Она заключается в отыскании такого вектора $w \in \mathcal{L}(v_1, \ldots, v_n) \setminus \{0\}$, что его норма минимальна.

Методы

В ходе работы расмотренно уравнение

$$\left(\frac{k}{2\pi e}\right)^{k/2} \cdot q^k < \delta_\beta^{k(3k-1)} (n/2)^n, \tag{1}$$

выведенное в статье [2], связывающее параметры n, q NTRU-решетки и необходимые для BKZ-редукции, описанной в той же статье, параметры k, β. Так как меньшие параметры k и β ведут к ускорению выполнения алгоритма, ставится задача нахождения наименьшего β и наименьшего k, удовлетворяющих (1) при выбранном β.

Данное уравнение проанализированно численными методами и решено методом бинарного поиска сначала по переменной β, а затем — по переменной k. Реализация алгоритма осуществлена в системе компьютерной алгебры Sage 9.1.

Ядро алгоритма состоит из двух циклов: по переменной β и вложенного цикла по переменной k. Внешний цикл работает по принципу бинарного поиска: множество поиска разбивается на две части, причем заведомо известно, что существует число β_0 такое, что для всех $\beta < \beta_0$ не существуют решения (1) такие, что $\beta \leqslant 2k \leqslant 2n$. Внутренний цикл тоже работает по принципу бинарного поиска, но ищется локальный максимум функции

$$\mathcal{D}(\beta, k) = \delta_\beta - \sqrt[k(3k-1)]{\left(\frac{k}{2\pi e}\right)^{k/2} \cdot q^k \cdot (n/2)^{-n}}$$

при помощи метода «ходьбы в гору»: множество поиска разбивается на две части (левую и правую) с пограничным элементом k_0. После этого высчитываются $\mathcal{D}(\beta, k_0 - 1)$ и $\mathcal{D}(\beta, k_0 + 1)$. Если первое значение больше, то выбирается левая часть, в противном случае — правая.

Исходный код программы размещен по ссылке: https://github.com/alexgit256/Diploma-NTRU-attack-params-BKZ-/blob/main/Optimal%20BKZ%20params%20finder.py.

Для иллюстрации зависимости параметров k, β от n и $\log q$ приведены соответствующие графики для случаев n = 128, 256, 384, 512, 640, 768, 896, 1024 (см. рис. 1—16). Все логарифмы берутся по основанию 2, если не указано иное.

Результаты

По итогам исследования был разработан алгоритм поиска параметров k, β, доступный по приведенной выше ссылке. Так как сложность бинарного поиска во множестве из n элементов оценивается как $O(\log n)$, сложность данного алгоритма равна $O(\log^2 n)$.

Ниже представлены графики зависимости β и k от $\log q$ для фиксированных значений n = 128, 256, 384, 512, 640, 768, 896, 1024 (рис. 1—16):

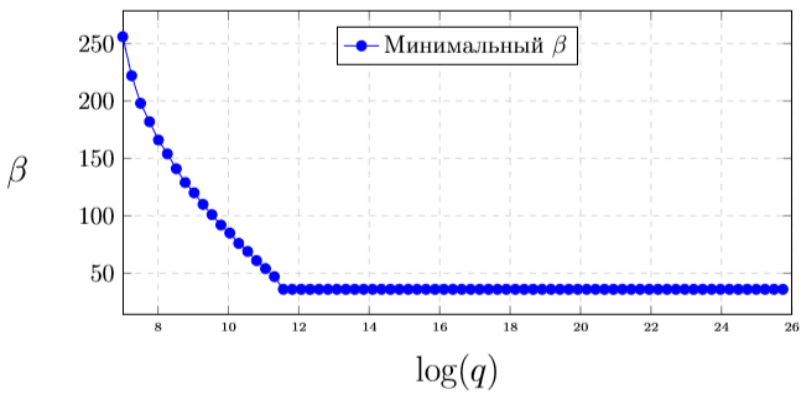


Рис. 1. График зависимости β от $\log q$ при n = 128

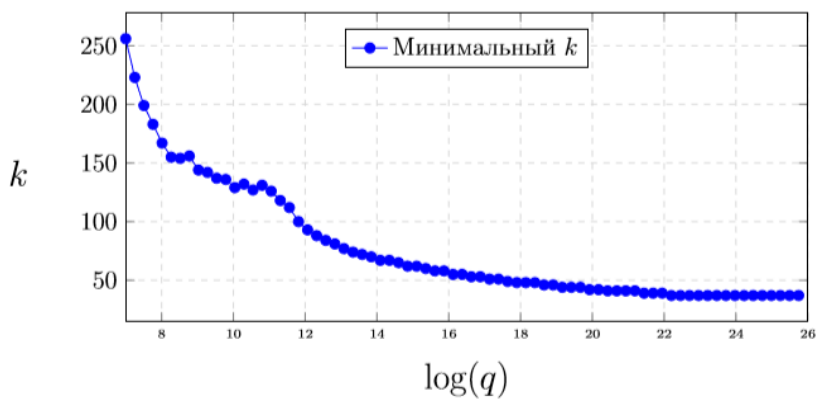


Рис. 2. График зависимости k от $\log q$ при n = 128

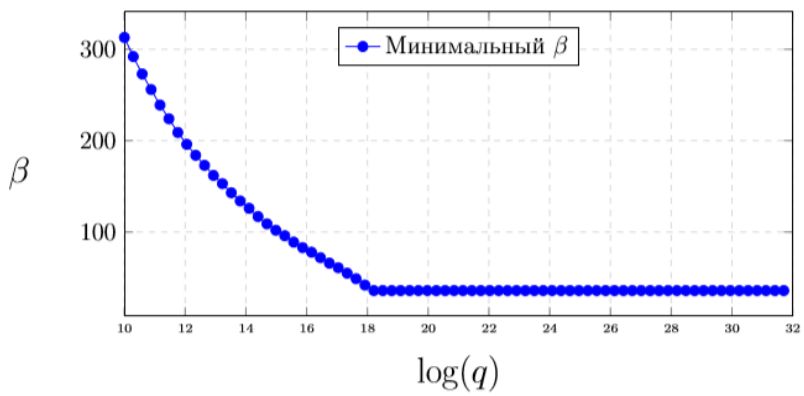


Рис. 3. График зависимости β от $\log q$ при $n = 256$

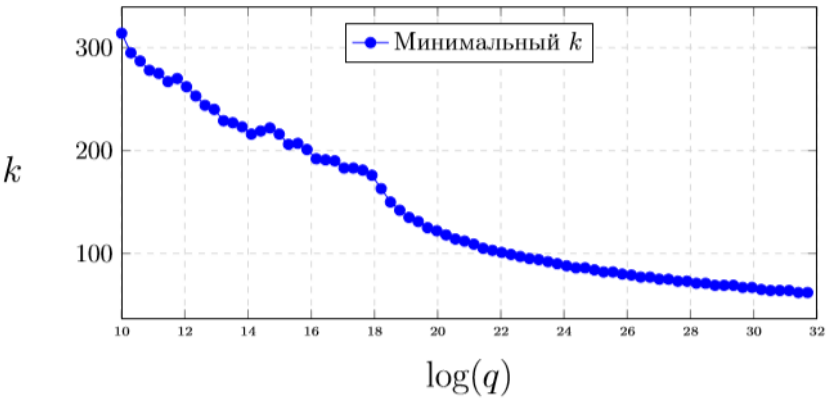


Рис. 4. График зависимости k от $\log q$ при $n = 256$

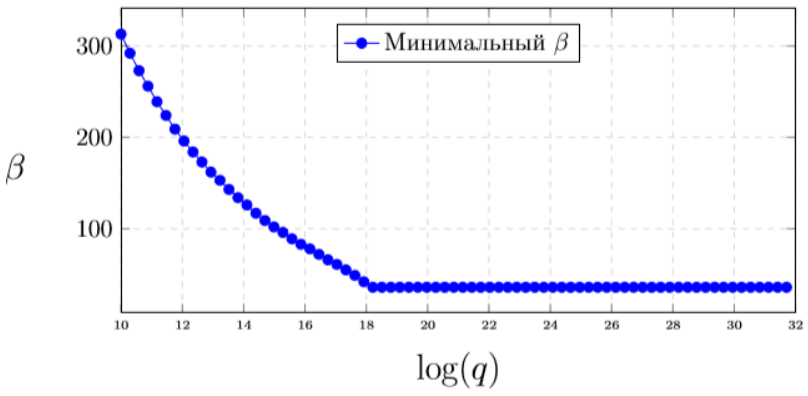


Рис. 5. График зависимости β от $\log q$ при $n = 384$

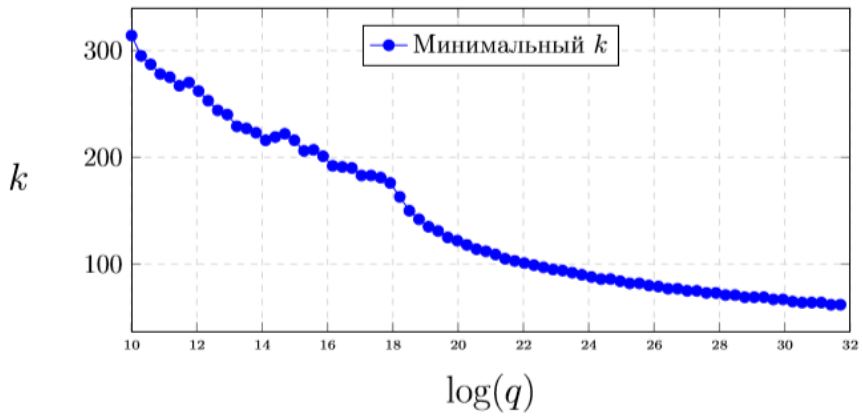


Рис. 6. График зависимости k от $\log q$ при $n = 384$

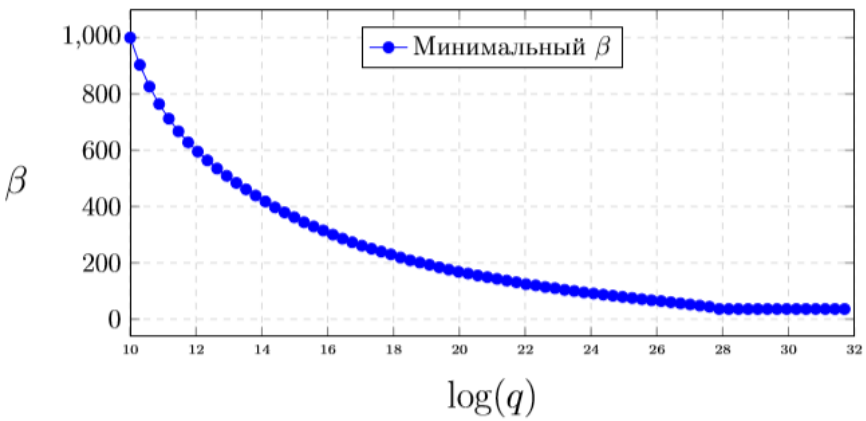


Рис. 7. График зависимости β от $\log q$ при $n = 512$

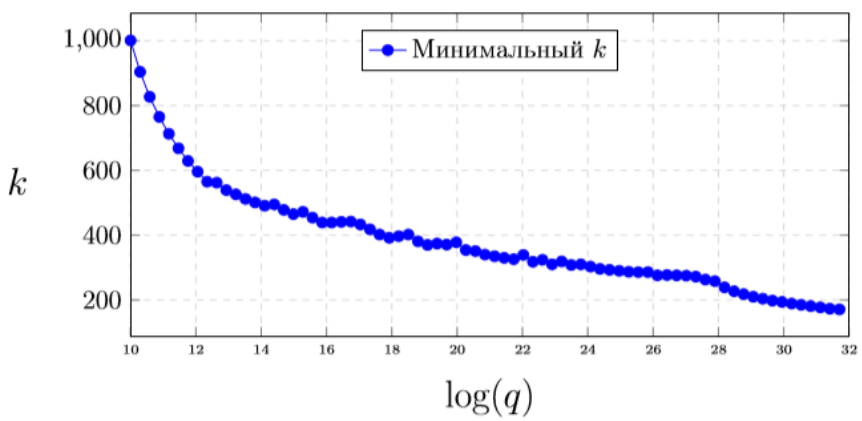


Рис. 8. График зависимости k от $\log q$ при $n = 512$

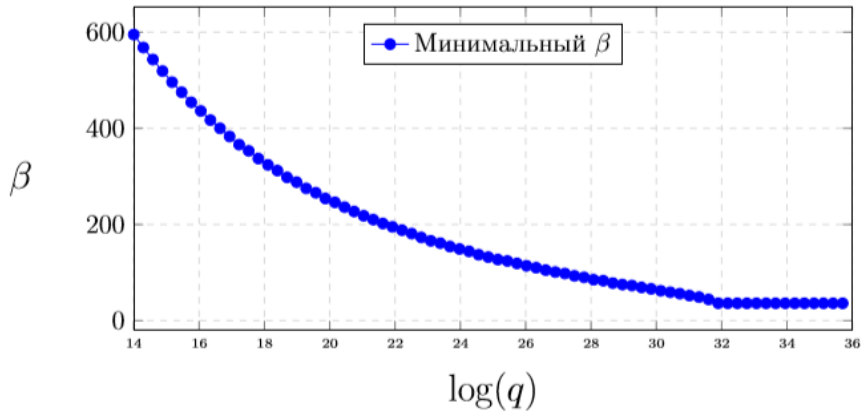


Рис. 9. График зависимости β от $\log q$ при $n = 640$

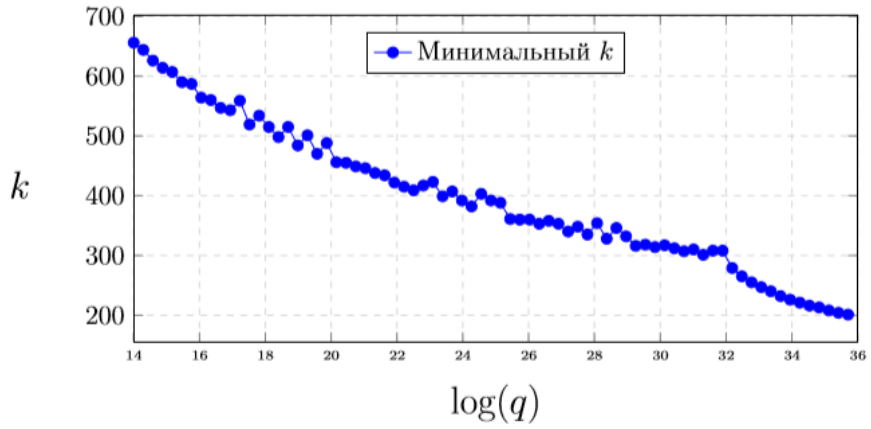


Рис. 10. График зависимости k от $\log q$ при $n = 640$

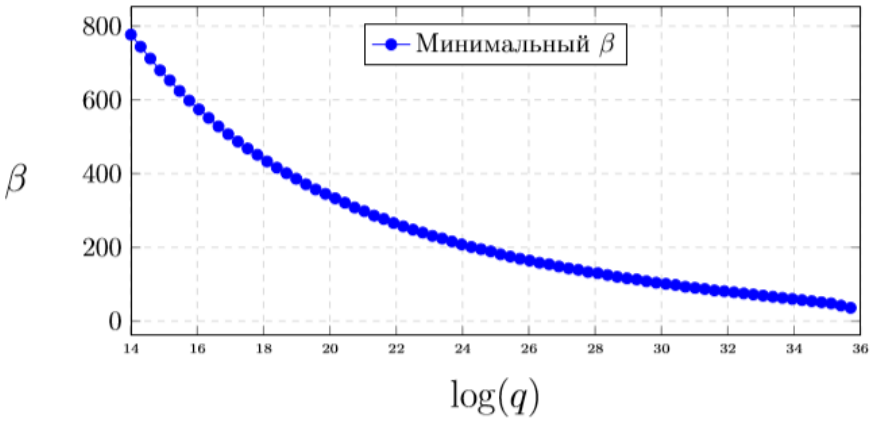


Рис. 11. График зависимости β от $\log q$ при $n = 768$

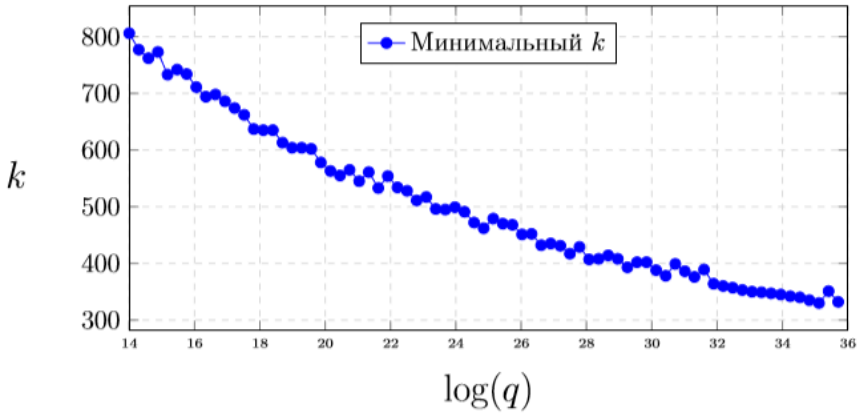


Рис. 12. График зависимости k от $\log q$ при $n = 768$

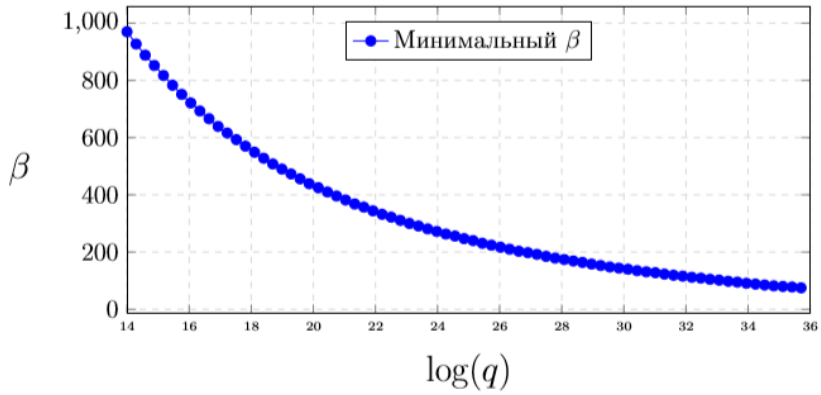


Рис. 13. График зависимости β от $\log q$ при $n = 896$

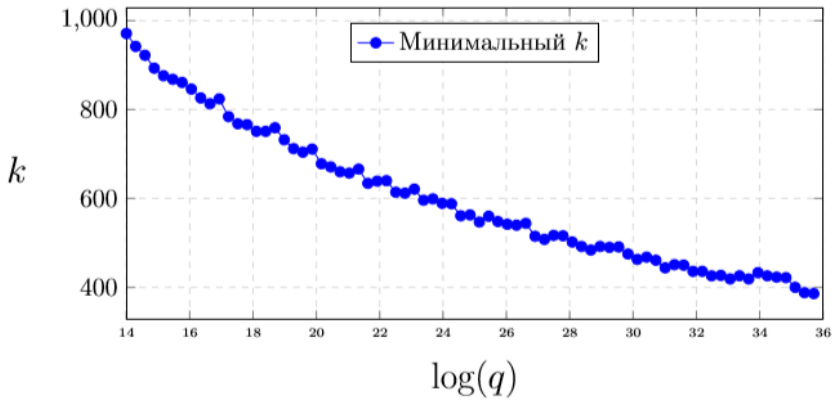


Рис. 14. График зависимости k от $\log q$ при $n = 896$

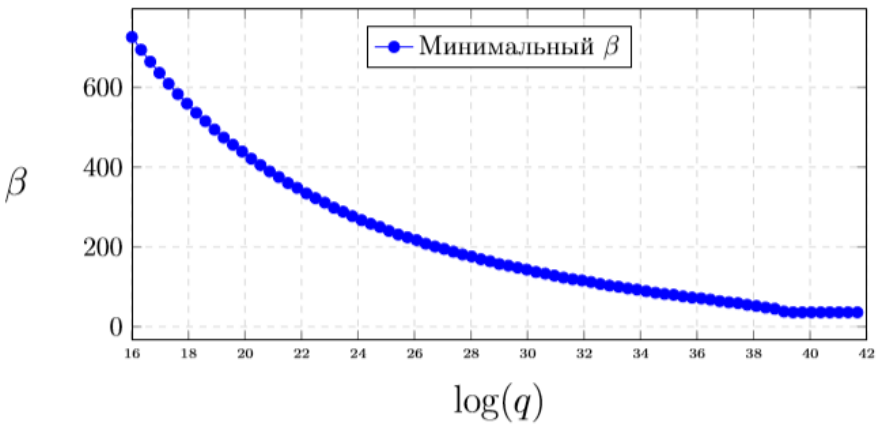


Рис. 15. График зависимости β от $\log q$ при $n = 1024$

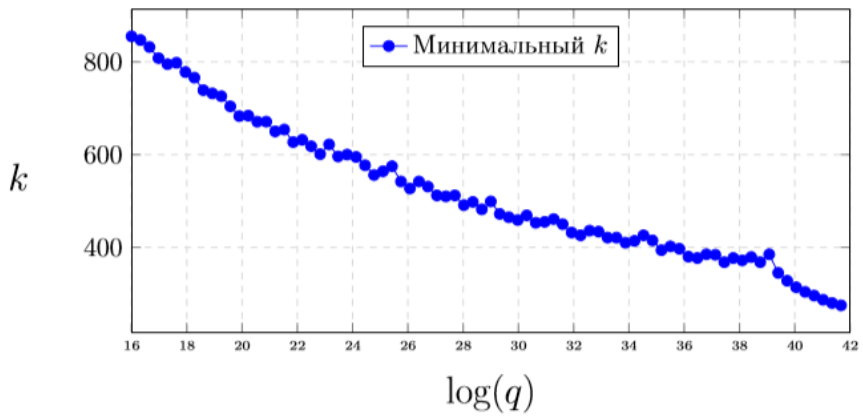


Рис. 16. График зависимости k от $\log q$ при $n = 1024$

Заключение

По итогам проведенного численного исследования был проверен результат [2], заключающийся в том, что модуль $q \approx 2^{\sqrt{n}}$ не является безопасным и ведет к возможности успешной атаки методом BKZ-редукции. Сложность проведения BKZ-редукции монотонно убывает с ростом $\log q$ что обусловленно убыванием параметра β, от которого зависит сложность атаки [2].

Интересным вопросом остается значение β, достаточное для успешной атаки на практике. Приведенное в [2] уравнение дает лишь верхнюю оценку для β, k, тогда как на деле атака может быть успешной и при немного меньших значениях этих параметров. Для этого следует провести численные эксперименты BKZ-редукции NTRU-решеток согласно методологии, описанной в [6], и сравнить их с результатами, выдаваемыми алгоритмом, предложенным в нашей статье.

Список литературы

1. *Hoffstein J., Pipher J., Silverman J.H.* An Introduction to Mathematical Cryptography. Springer, 2014.

2. *Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch.* NTRU Prime: reducing attack surface at low cost. URL: https://eprint.iacr.org/2016/461.pdf (дата обращения: 15.10.2020).

3. *Lee Ch., Wallet A.* Lattice analysis on MiNTRU problem. URL: https://www.semanticscholar.org/paper/Lattice-analysis-on-MiNTRU-problem-Lee-Wallet/d922d602c196bebb2057b734fd8012b1bbb3cb9a (дата обращения: 15.10.2020).

4. *Monteverde M.* NTRU software implementation for constrained devices. Leuven, 2007.

5. *Micciancio D., Voulgaris P.* Faster exponential time algorithms for the shortest vector problem // 21st Annual ACM-SIAM Symposium on Discrete Algorithms. Austin, 2010. P. 1468—1480.

6. *Chen Yu.* Réduction de réseau et sécurité concrete du chiffrement completement homomorphe : PhD Thesis. P., 2013.

Об авторе

Александр Сергеевич Каренин — студент, Балтийский федеральный университет им. И. Канта, Россия.

E-mail: tremeloesalex@gmail.com

The author

Alexander S. Karenin, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: tremeloesalex@gmail.com

УДК 004.056

Ф. Г. Максимов-Наливайко

ЗАЩИЩЕННАЯ ОТПРАВКА СООБЩЕНИЙ ПО МЕШ-СЕТИ НА ОСНОВЕ BLUETOOTH

Рассмотрены основные проблемы, решение которых необходимо для обеспечения безопасности конфиденциальности коммуникации между участниками мобильных меш-сетей на основе смартфонов. Представлены важные характеристики технологий Bluetooth и Bluetooth Low Energy, с помощью которых можно решить часть проблем. Кратко описана криптография на эллиптических кривых, выбрана конкретная кривая. На основе обмена ключами на эллиптических кривых и различных криптопримитивов построена гибридная модель шифрования, позволяющая обмениваться защищенной информацией с использованием симметричного шифрования. Показаны процессы зашифрования и расшифрования сообщений с использованием данной схемы. В результате описанные технологии и гибридная схема объединяются в базовый алгоритм защищенной передачи данных по меш-сети на основе Bluetooth, достаточный для программной реализации.

In the paper we discuss the main problems that have to be solved to ensure the confidentiality of communication between the nodes of mesh networks based on smartphones. We describe the important details of Bluetooth and Bluetooth Low Energy technologies, using which you can solve some of the problems described. Next, we briefly describe elliptic curve cryptography and choose a specific curve for it. We build an Elliptic Curve Integrated Encryption Scheme based on the elliptic curves key exchange and various crypto primitives that allows exchanging protected information using symmetric encryption. We also describe the processes of encryption and decryption of messages using this. As a result, the described technologies and the hybrid scheme are combined into the basic algorithm for secure data transmission over a mesh network based on Bluetooth, sufficient for software implementation.

Ключевые слова: меш-сеть, Bluetooth, BLE, эллиптические кривые, криптография, гибридная схема.

Keywords: mesh network, Bluetooth, BLE, elliptic curve, cryptography, ECIES.

Введение

В настоящее время активно развиваются альтернативные методы передачи данных, не связанные или только частично связанные с использованием централизованных коммерческих и государственных сетей. Подобно тому как криптовалюты позволяют людям совершать операции с деньгами без участия и контроля государства и банков, построенные на клиентских устройствах меш-сети дают пользователям возможность общения друг с другом без участия государственных органов и операторов связи. Помимо этого, развертка меш-сети помогает в тех ситуациях, когда обычные сети не покрывают данную область либо не справляются с нагрузкой: на природе, концертах и т. п.

© Максимов-Наливайко Ф.Г., 2020
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 26 – 33.

Одной из основных проблем в меш-сетях является обеспечение безопасности при передаче информации. Поскольку меш-сеть может покрывать большую площадь, а подключиться к ней есть возможность у любого человека, необходимо заботиться о защите сети от действий злоумышленников.

В данной работе рассматриваются технические основы меш-сетей, Bluetooth и Bluetooth Low Energy, а также описываются необходимые криптопримитивы. На основе этих технологий и алгоритмов строится прообраз сети, в которой можно обеспечить необходимую защиту при передаче сообщений.

Меш-сети

Беспроводная меш-сеть (wireless mesh network, WMN) — это сеть, которая включает в себя различные беспроводные устройства с точками доступа. Каждый клиент в сети также является сервером, передавая данные дальше по сети. Поскольку сеть децентрализована, передать данные узел может только своим соседям. Обычно в таких сетях используются технологии Wi-Fi, Wi-Fi Direct и Bluetooth.

Визуально архитектура WMN представляет собой связный граф, обычно со множеством циклов. Данные, направляясь от адресата к получателю, проходят через цепочку устройств посередине, совершая последовательность коротких «прыжков» (hops). Устройства посередине цепи могут передавать данные либо всем своим соседям, либо, зная маршрут до получателя, выбирать конкретные узлы для уменьшения нагрузки на сеть.

Необходимо решить основные проблемы безопасности меш-сетей.

1. *Доступность*, в частности:

а) *помехи*. Злоумышленник может атаковать доступность сети, создавая помехи и препятствуя коммуникации на физическом уровне. Эта проблема может возникать также вследствие естественных физических причин;

б) *отказ в обслуживании (DoS)*, обычно это лавинная передача запросов по сети, из-за которых сеть становится неспособной исполнять запросы обычных пользователей;

в) *истощение батареи*. В сетях, основанных на мобильных устройствах, атаки истощения батареи могут быть даже опаснее, чем DoS, так как они способны не только временно вывести из строя сеть, но и полностью вывести из строя устройства, на которых она основывается.

2. *Аутентификация*. Злоумышленник может замаскировать узел, получая неавторизованный доступ к ресурсам, чувствительной информации, а также возможность влиять на деятельность других узлов. Обычные способы аутентификации задействуют централизованную систему, которая администрирует ограничения согласно спискам доступа или сертификатам. В меш-сети наличие таких центров по большей части невозможно.

3. *Целостность*. Атаки на целостность сообщений обычно имеют своей причиной либо умышленное изменение данных злоумышленником, либо случайные ошибки в передаче, связанные с работой сети и отдельных устройств.

4. *Конфиденциальность* является ключевой проблемой в меш-сети, так как необходимо защитить коммуникацию с аутентифицированным пользователем в условиях, когда нет ни доверенных центров, ни единой структуры сети.

Bluetooth и Bluetooth Low Energy

Основная технология, на которой основана меш-сеть, — это семейство протоколов Bluetooth. **Bluetooth** представляет собой технологический стандарт беспроводного обмена данными на коротком расстоянии через радиосвязь. На сегодняшний день существует пять основных версий стандарта, последняя — Bluetooth 5.2.

Сосредоточимся на тех характеристиках Bluetooth, которые помогут нам решить некоторые из вышеописанных проблем меш-сетей.

В Bluetooth используется технология FHSS — псевдослучайная перестройка рабочей частоты. При передаче сигнала участники коммуникации 1600 раз в секунду меняют рабочую частоту внутри заданного диапазона. Для этого они используют секретную матрицу времени-частоты, доступную только двум участникам контакта. Благодаря FHSS сигнал, во-первых, устойчив к узкополосной интерференции, то есть, по сути, к *помехам*, а во-вторых, его становится сложнее перехватить, так как последовательность переключения частот неизвестна сторонним пользователям.

При передаче Bluetooth разделяет данные на пакеты, а затем передает каждый пакет по одному из доступных каналов. При передаче текстовой информации Bluetooth отвечает за целостность передаваемых и получаемых данных. Тем самым решена проблема *целостности* данных.

Для обеспечения *аутентификации* участников диалога в Bluetooth используется механизм сопряжения: перед началом обмена информацией устройства должны добавить друг друга в список связанных. В смартфонах это происходит с незначительным участием пользователя: он должен подтвердить соединение. Установив сопряжение, пользователи смогут иметь защищенный канал связи, однако он действует, только пока они находятся в непосредственной близости.

Bluetooth Low Energy (BLE) — спецификация ядра Bluetooth, которая значительно уменьшает энергопотребление при обмене данными ценой небольшого снижения скорости передачи данных. BLE программно несовместим с классическим Bluetooth, однако поддерживается в подавляющем большинстве современных смартфонов. Несмотря на то что передавать долгие сообщения по BLE бессмысленно, мы можем использовать BLE для передачи коротких и/или редких сообщений, например сообщений маршрутизации. Использование BLE помогает решить проблему *истощения батареи*.

Криптография на эллиптических кривых

В работе будут рассматриваться только несингулярные эллиптические кривые, так как в противном случае проблема дискретного логарифма, на которой основана криптографическая стойкость, будет легко решена.

Эллиптическая кривая E над полем K обозначается как E/K и определяется уравнением Вейерштрасса:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где коэффициенты $a_1, a_2, a_3, a_4, a_6 \in K$ таковы, что для каждой точки (x_1, y_1) с координатами в $\overline{K}$, удовлетворяющими уравнению кривой, частные производные $2y_1 + a_1x_1 + a_3$ и $3x_1^2 + 2a_2x_1 + a_4 - a_1y_1$ не равны нулю одновременно. Это условие равнозначно тому, что кривая будет несингулярной или гладкой.

Из всех точек кривой можно составить группу с операцией, которую обычно обозначают как «+». Многократное применение этой операции к одной и той же точке кривой P обозначают как $[n]P$ и называют умножением на скаляр:

$$[n]: E \to E,$$

$$P \mapsto [n]P = \underbrace{P + P + \ldots + P}_{n \text{ раз}}.$$

Отметим, что $[0]P = P_\infty$ и $[n]P = [-n](-P)$, $n < 0$. Подробные формулы и разъяснения приведены во многих учебниках и статьях, например в [1].

Выберем в качестве поля K конечное поле $\mathbb{F}_p$, где p — простое число $(p > 3)$. Точки кривой (вместе с «точкой на бесконечности») образуют конечную циклическую группу. Если сложить две точки кривой или умножить одну из точек на скаляр, результирующая точка будет находиться в той же циклической группе.

Введем понятие **проблемы нахождения дискретного логарифма на эллиптических кривых** (ECDLP): имея эллиптическую кривую, определенную над конечным полем $\mathbb{F}_p$, образующую точку G и выбранную произвольным образом точку P кривой, необходимо найти целое число k такое, что $P = [k]G$. Несмотря на то что в некоторых случаях эту проблему можно решить довольно быстро, в общем случае самый быстрый алгоритм требует $\sqrt{k}$ шагов для ключа размером в k бит.

На основе этой проблемы можно построить аналог **обмена ключами Диффи — Хеллмана** на эллиптических кривых: вместо возведения

в степень по модулю здесь используется умножение точек эллиптической кривой на элементы конечного поля. Алгоритм основывается на следующем свойстве в группе точек эллиптической кривой:

$$[b]([a]G) = [a]([b]G).$$

Назовем стороны обмена Алисой и Бобом. В общем алгоритм выглядит так:

1. Алиса генерирует случайную пару: закрытый ключ d_A — случайно выбранное число из интервала $[1\ldots n-1]$ и открытый ключ $Q_A = [d_A]G$.

2. Боб аналогично вычисляет пару d_B, Q_B.

3. Алиса и Боб обмениваются своими открытыми ключами Q_A, Q_B по публичному каналу.

4. Алиса вычисляет общий секрет $s = [d_A]Q_B$.

5. Боб вычисляет общий секрет $s = [d_B]Q_A$.

6. Теперь у обеих сторон есть одинаковый общий секрет s.

Кривая Curve25519

На практике при реализации криптографии на эллиптических кривых обычно выбирают конкретную кривую из числа рекомендованных стандартизирующими организациями. Для дальнейшей реализации выберем кривую Curve25519.

Эллиптическая кривая в форме Монтгомери

$$y^2 = x^3 + 486662x^2 + x,$$

определенная над полем $\mathbb{F}_{p^2}$, где $p = 2^{255} - 19$ — простое число, имеет название **Curve25519**.

В качестве первой координаты базовой точки используется $x = 9$. Эта точка генерирует циклическую подгруппу простого порядка, что предотвращает использование атаки с помощью алгоритма Полига — Хеллмана [2]. Данная кривая обеспечивает 128-битный уровень криптостойкости.

Благодаря форме Монтгомери можно эффективно применять групповые операции, используя только координаты X, Z. В качестве ключа в итоге используется только x-координата. В числе преимуществ при использовании этой кривой можно также отметить:

- постоянное время работы, что обеспечивает защиту от атак по времени;
- возможность использовать короткие открытые и закрытые ключи в 32 байта;
- нет необходимости валидировать публичный ключ — подойдет любая 32-байтная строка.

Благодаря своим преимуществам данная кривая была стандартизирована сообществом IETF и используется во многих популярных протоколах и приложениях: TLS 1.3, WhatsApp, Viber, Proton Mail, Tor, I2P.

Гибридная схема шифрования

Обычно данные не зашифровывают напрямую с помощью эллиптических кривых из-за проблем со скоростью. Вместо этого используют **гибридные схемы шифрования**, включающие обмен ключами на эллиптических кривых (ECIES).

Для реализации подобной схемы необходимо иметь:

- *функцию выработки ключа* (KA), которая генерирует общий секрет;
- *функцию формирования ключа* (KDF) — механизм, производящий набор ключей для симметричного шифрования на основании уже существующих асимметричных ключей;
- *симметричный алгоритм шифрования* (Enc);
- *имитовставку* (MAC) — данные аутентификации сообщения;
- *хеш-функцию* (Hash), которая используется в KDF и MAC.

Допустим, Алиса хочет отослать Бобу сообщение m.

1. Предварительно Алиса и Боб генерируют закрытые и открытые ключи. Обозначим через U, V их открытые ключи (точки кривой), u, v — закрытые (элементы поля).

2. Алиса использует KA: вычисляя $s = [u]V$, она получает общий секрет.

3. Алиса использует KDF, получая симметричный ключ и ключ имитовставки: $k_E \,||\, k_M := KDF(s, i)$, где i — необязательный параметр дополнительной информации.

4. Алиса шифрует сообщение m симметричным шифром Enc: $c = Enc(k_E, m)$.

5. Алиса вычисляет имитовставку $tag = MAC(k_M, c, i')$, где i' — необязательная дополнительная информация.

6. Наконец, Алиса отсылает криптограмму, состоящую из публичного ключа U, имитовставки tag и шифротекста c.

Чтобы получить исходное сообщение m из набора (U, tag, c), Боб должен сделать следующее:

1. Используя эфемерный открытый ключ U и собственный закрытый ключ v, получить общий секрет $s = [v]U$.

2. С помощью KDF получить ключи $k_E \,||\, k_M := KDF(s, i)$, i — необязательный параметр дополнительной информации.

3. Проверить правильность полученной криптограммы, вычислив имитовставку аналогичным образом: $tag' = MAC(k_M, c, i')$. Если $tag \neq tag'$, необходимо отклонить криптограмму как ошибочную.

4. Если имитовставки сошлись, можно расшифровать полученный шифротекст: $m = Enc^{-1}(k_E, c)$.

Единого набора конкретных алгоритмов, которые реализуют необходимые для данной схемы функции, не существует, однако, опираясь на стандарты ANSI X9.63, IEEE 1363a, ISO/IEC 18033-2 и SECG SEC 1, выберем следующие алгоритмы:

- KA: обмен ключами по Диффи — Хеллману, описанный выше на кривой;
- KDF: алгоритм KDF2, описанный в [3];
- симметричный шифр: AES в режиме сцепления блоков шифротекста (CBC-mode);
- MAC: HMAC-SHA-512;
- хеш-функция: SHA-512.

В связи с тем что обычно в среде разработки (в частности, для ОС Android) уже реализованы алгоритмы AES, SHA-512, KDF2 и HMAC, не будем останавливаться на их описании подробно. При необходимости их реализации можно обратиться к [3].

Защищенная передача сообщений по меш-сети

Итак, мы хотим получить меш-сеть, основанную на Bluetooth и BLE, с возможностью отправки защищенных сообщений участникам сети. У пользователей на устройстве установлено созданное нами ПО. В этом программном обеспечении реализованы криптографические примитивы, объединенные в гибридную схему шифрования на эллиптической кривой Curve25519, а также алгоритмы отправки данных по Bluetooth и BLE. Опишем теперь, как построить желаемую сеть.

Первый этап, который необходимо проделать, — **обмен ключами** между будущими сторонами коммуникации. Чтобы быть уверенными в том, что другой участник сети — тот, за кого себя выдает, для обмена потребуется находиться в зоне действия Bluetooth. Тогда мы можем открыть защищенный канал связи по Bluetooth вне основной сети. По этому каналу стороны должны установить общий секрет, а также, используя гибридную схему, описанную выше, произвести обмен пробными сообщениями, например подобный рукопожатию протокола TCP.

Если обе стороны успешно обменялись сообщениями, необходимо **сохранить** их **пары ключей** для дальнейшей коммуникации: теперь можно использовать общую сеть для обмена зашифрованными сообщениями через гибридную схему. При отправке в общую сеть в «заголовке» сообщения мы должны передавать открытые MAC-адрес адресата и имя отправителя, а в «теле» — шифртекст.

Работа сети будет поддерживаться следующим образом: каждый участник пересылает в незащищенном режиме сообщения своему окружению. Если один из участников обнаруживает рядом с собой адресата текущего сообщения, оно передается адресату с пометкой, что

предназначено именно ему. Получатель, зная отправителя, расшифровывает шифртекст по общему с отправителем ключу.

Для маршрутизации можно использовать оповещения через BLE, а для большей экономии батареи применять гибкий подход, например как описано в [4]. Для отражения атак отказа в обслуживании можно вести «черный список» узлов: если какое-то из устройств попытается отправлять значительно больше запросов, чем соседние точки, его можно временно игнорировать, с каждым разом увеличивая время ожидания.

Более гибкие подходы к маршрутизации включают в себя применение специальных алгоритмов для мобильных меш-сетей, например AODV, OLSR или DSR. Это позволит значительно уменьшить нагрузку на сеть в целом и на конкретные устройства-узлы в частности.

Общие результаты

Описанные выше технологии, криптопримитивы и общий алгоритм защищенной передачи закрывают большую часть проблем безопасности беспроводных меш-сетей. Полученного алгоритма достаточно для дальнейшей программной реализации защищенного обмена сообщениями на основе операционных систем Android и iOS.

Несмотря на то что каждая из частей алгоритма заслуживает детальной проработки и оптимизации, с помощью представленного подхода мы получим сеть, достаточную для реального применения.

Список литературы

1. *Avanzi R.M., Cohen H., Doche Ch. et al.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman & Hall/CRC, 2006.

2. *Bernstein D.J.* Curve25519: new Diffie-Hellman speed records // Public Key Cryptography — PKC 2006. Springer, 2006. URL: https://cr.yp.to/ecdh/curve25519-20060209.pdf (дата обращения: 11.10.2020).

3. *ISO/IEC* 18033-2:2006. Information technology — Security techniques — Encryption algorithms. Part 2 : Asymmetric ciphers. 2006. URL: https://www.iso.org/ru/standard/37971.html (дата обращения: 11.10.2020).

4. *Brandão A.S., Lima M.C., Abbas C.J.B. et al*. An Energy Balanced Flooding Algorithm for a BLE Mesh Network // IEEE Access. 2020. Vol. 8. URL: https://ieeexplore.ieee.org/document/9091162/ (дата обращения: 31.10.2020).

Об авторе

Филипп Геннадиевич Максимов-Наливайко — студент, Балтийский федеральный университет им. И. Канта, Россия.

E-mail: phmaksimov@gmail.com

The author

Filipp G. Maksimov-Nalivaiko, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: phmaksimov@gmail.com

УДК 004.056

П. Б. Демочкина

МАСШТАБИРУЕМЫЕ zk-SNARK

Описан общий принцип работы (этапы, используемые параметры) схемы доказательства с нулевым разглашением zk-SNARK, возможность и перспективы его улучшения. Реализации zk-SNARK, которые известны на данный момент, имеют ограничения масштабируемости, обусловленные величиной доказываемого вычисления. Во-первых, размер доказывающего ключа по крайней мере линейно зависит от верхней границы структуры, в которой мы работаем. Во-вторых, при доказательстве требуется запись всех предыдущих шагов. В статье описывается алгоритм достижения новой реализации zk-SNARK с использованием криптографии на эллиптических кривых, особенностей структуры поля и цельности доказательств. Практически такая реализация является рекурсивной композицией доказательства, при этом генерация ключей для любых размеров вычислений несет постоянные расходы по памяти. В дальнейшем в процессе доказательства осуществляются только постоянные мультипликативные по времени и аддитивные по памяти расходы. Таким образом, описанная реализация zk-SNARK наделяется двумя важными свойствами: емкость и инкрементальная вычислимость.

This article describes the General principle of operation (stages, parameters used) of the ZK-SNARK zero-knowledge proof scheme, the possibility and prospects for its improvement. Implementations of zk-SNARK that are currently known have scalability limitations that depend on the magnitude of the computation being proved. First, the size of the proving key depends at least linearly on the upper bound of the structure in which we work. Second, the proof requires a record of all previous steps. The article describes an algorithm for achieving a new implementation of zk-SNARK using elliptic curve cryptography, field structure features, and proof integrity. In practice, this implementation is a recursive composition of the proof, while generating keys for any size of calculations carries constant memory costs. Subsequently, the entire process of proof is solely multiplicative constant costs overtime and additivecosts in memory. Thus, the described implementation of zk-SNARK has two important properties: capacity and incremental computability.

Ключевые слова: zk-SNARK, Zcash, доказательство с нулевым разглашением, масштабируемость, инкрементально вычислимый.

Keywords: zk-SNARK, Zcash, zero-knowledge proof, scalability, incrementally computable.

Введение

С течением времени появляются все новые криптографические методы для обеспечения анонимности пользователей компьютерных систем. Однако, создавая новые, имеет смысл использовать и усовершенствовать

© Демочкина П. Б., 2020
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 34 – 41.

уже, казалось бы, хорошо изученные. Так, чтобы обеспечить доказательство с нулевым разглашением, возможно использовать zk-SNARK, который является механизмом работы криптовалюты Zcash. Насколько эффективна данная схема доказательств и как можно ее улучшить, мы рассмотрим в представленной статье.

Актуальность этого вопроса обусловлена тем, что в настоящее время криптовалюты активно внедряются в финансово-экономический спектр мира, и повышение их безопасности и скорости использования улучшит их характеристики и позволит расширить круг их пользователей.

Сущность и механизм работы zk-SNARK

Zk-SNARK — доказательство с нулевым разглашением, основанное на неинтерактивной аргументации, то есть доказательство о владении определенной информацией производится без раскрытия самой информации, при этом взаимодействие между проверяющим (verifier) и доказывающим (prover) минимально. Такое доказательство возможно проверить в течение нескольких миллисекунд, а само оно может иметь размер лишь несколько сотен байтов даже относительно очень большой программы.

Доказательство zk-SNARK используется в криптовалюте Zcash, платежной системе JP Morgan Chase, основанной на блокчейне, и в качестве средства безопасной аутентификации клиентов на серверах. Фокус нашего внимания направлен на zk-SNARK в Zcash. Строгая конфиденциальность, гарантированная Zcash, исходит из того факта, что экранированные транзакции (поддающиеся проверке, но не со стороны третьих лиц) в Zcash могут быть полностью зашифрованы с помощью блокчейна, но только если их можно проверить относительно правил согласования сети с помощью доказательств zk-SNARK [2].

В настоящее время доказательства zk-SNARK зависят от первоначальной доверенной установки открытых параметров. В Zcash эта начальная фаза настройки называется *церемонией генерации параметров* [3]. Предварительная настройка является важной процедурой, так как если злоумышленник получит доступ к механизму генерации параметров, то он сможет создать фальшивые доказательства. Для Zcash это означает, что злоумышленник может использовать поддельные монеты. Чтобы этого не случилось, Zcash генерирует публичные параметры посредством сложного многоуровневого процесса.

Протокол zk-SNARK состоит из трех алгоритмов: G, P и V.

G — генератор ключей, λ — параметр безопасности, C — функция от публичного значения x (например, факт совершения транзакции) и секретного значения w (то, что нужно доказать, например сумма транзакции). G получает на вход λ и C. Затем производится генерация общедоступных ключей: доказательного ключа pk и ключа проверки vk. То есть $(pk, vk) = G(\lambda, C)$.

P использует в качестве входных данных проверяющий ключ pk, случайный x (общедоступный) и значение w, которое требует доказательства без его раскрытия. Алгоритм P создает доказательство $prf = P(pk, x, w)$.

В качестве входных данных верификатор V принимает ключ доказательства, значение x и доказательство prf, а затем возвращает *True* или *False*.

В настоящее время в основе zk-SNARK лежит редуцированное эйтспаривание [4, с. 21] на кривой BLS12-381.

Ограничения масштабируемости zk-SNARK

Существующие реализации zk-SNARK имеют серьезные ограничения масштабируемости с точки зрения пространственной сложности, которые зависят от размера доказываемого вычисления. Во-первых, размер доказывающего ключа квазилинеен в верхней границе размера вычислений. Во-вторых, получение доказательства требует записи всех промежуточных значений на протяжении всего вычисления, а затем проведения глобальных операций, таких как быстрое преобразование Фурье.

Можно показать, что, используя новые криптографические методы, основанные на эллиптических кривых и конечных полях, и неопределенности систем доказательства, возможно получить реализацию zk-SNARK, которая практически достигает рекурсивной композиции доказательства. Для генерации ключей, поддерживающих все размеры вычислений, требуется постоянное время. Впоследствии процесс доказательства несет только постоянные мультипликативные расходы по сравнению с исходным временем вычисления и существенные постоянные аддитивные расходы по памяти.

Рассмотрим ограничения масштабируемости подробнее.

Дорогостоящая предварительная доверенная установка. Как упоминалось выше, zk-SNARK требует одноразовой доверенной настройки открытых параметров. В большинстве конструкций zk-SNARK эта настройка является дорогостоящей. Генератор ключей принимает в качестве входных данных верхнюю границу размера вычислений. В таком случае пространственная сложность генератора ключей и размер выходного ключа доказательства по крайней мере линейно зависят от этой верхней границы [1].

Чтобы снизить затраты на дорогостоящую предварительную генерацию параметров, можно сделать схему универсальной, чтобы она могла обрабатывать более одного входного значения. Известные реализации zk-SNARK ограничены пространством даже для скромных вычислений: например, имеющие доказывающий ключ более 4 Гб используются для схем всего с 16 миллионами входов.

Таким образом, дорогостоящая предварительная установка сильно ограничивает масштабируемость zk-SNARK.

Пространственно-интенсивная генерация доказательств. Это ограничение частично связано с первым. Генерация доказательств во всех опубликованных реализациях zk-SNARK имеет большую пространственную сложность. По существу, процесс доказательства требует записи всего вычисления сразу, а затем проведения на его основе глобальных вычислений (таких, как быстрые преобразования Фурье или возведения в степень). В частности, если схема показывает выполнение программы, то доказательство требует записи полного следа промежуточных состояний [1].

Решить данную проблему можно путем использования отдельных частей глобальных алгоритмов в качестве самостоятельных алгоритмов, что позволит повторять вычисления и не запоминать промежуточные состояния. Это значительно уменьшит пространственную сложность, но увеличит временную, поэтому такое решение нельзя считать оптимальным.

В идеале нужно реализовать zk-SNARK, который не страдает ни одним из вышеупомянутых ограничений масштабируемости, то есть удовлетворяющий следующим требованиям:

1. Генерация ключей является дешевой операцией (время зависит только от параметра безопасности) и подходит для всех вычислений (полиномиальной сложности). Такой zk-SNARK называется *полностью емким*.

2. Генерация доказательств производится за счет доказательств правильности вычислений в данный момент. Такой zk-SNARK называется *инкрементально вычислимым*.

Bootstrapping

Bootstrapping (рекурсивная композиция доказательств) zk-SNARK — это система с устойчивой к столкновениям хеш-функцией и предварительной обработкой zk-SNARK.

В описываемом методе каждый шаг требует доказательства утверждения, которое:

1) проверяет достоверность доказательств zk-SNARK на предыдущих шагах;

2) проверяет достоверность на текущем шаге.

Необходимо реализовать верификатор V в виде F-арифметической схемы C_V (представляющей собой подсхему C_{pcd}).

Основной подход: использование PCD-дружественных циклов эллиптических кривых. В предварительной обработке zk-SNARK верификатор V содержит в основном операции на эллиптической кривой над полем F_0, поэтому и выражается наиболее эффективно в виде арифметической схемы F_0. Конечно, если $F_0 = F$, то композиция может быть еще эффективнее, но это равенство математически невозможно.

«Запасной» метод: недетерминированная проверка спариваний. Верификатор zk-SNARK включает в себя, в частности, несколько проверок на

основе спаривания над заданной эллиптической кривой. Тем не менее каждая оценка спаривания является очень дорогой, если не выполняется тщательно.

PCD и PCD-дружественные циклы

Proof-carrying data (PCD) — это криптографический примитив, который сохраняет гарантии безопасности, предоставляемые рекурсивной композицией доказательств [1]. Построив систему PCD, можно использовать ее для получения нового zk-SNARK, который является масштабируемым (то есть полностью кратким и инкрементально вычислимым).

Пусть F — конечное поле, (G, P, V) — предварительная обработка zk-SNARK для F-арифметической схемы. Рекурсивная композиция доказательств проверяет выполнимость F-арифметической схемы C_{pcd}, которая, в свою очередь, проверяет достоверность предыдущих доказательств. Задача состоит в реализации верификатора V в виде F-арифметической схемы C_V — подсхемы C_{pcd}.

Способ записи C_V зависит от алгоритма V, обусловленного выбором эллиптической кривой в реализации zk-SNARK. Для доказательства утверждения о выполнимости FR-арифметической схемы для простого r, экземпляр (G, P, V) использует кривую E, которая определена над конечным полем F_q, где группа $E\left(\mathbb{F}_q\right)$ (группа $\mathbb{F}_q$-рациональных точек) имеет такой порядок r, что r делит $\#E(\mathbb{F}_q)$, в частности $r = \#E(\mathbb{F}_q)$. В таком случае все вычисления V выполняются над F_q или его расширениями до k-й степени, где k является степенью вложения E относительно r.

Для данного способа не подходят следующие случаи:

1. $q = r$. Это идеальный случай, ведь тогда арифметика V выполняется над тем же полем, для которого определен язык NP. Но данное условие невыполнимо, потому что если E имеет степень вложения k относительно r, то r должен делить $q^k - 1$, из чего следует, что $q \neq r$. Даже если $E(\mathbb{F}_q)$ имеет не простой порядок n, но простое r, которое делит n, условие также невыполнимо.

2. *«Длинная арифметика»*, то есть работа с битовыми фрагментами для целочисленных вычислений и взятие по модулю q. Но такой подход способствует увеличению порядка до $\log q$, что очень дорого.

Можно предложить использовать подход *цикл через несколько кривых*. Идея состоит в том, чтобы основывать рекурсивную композицию доказательств не на одном zk-SNARK, а на нескольких, при этом все экземпляры созданы на разных эллиптических кривых, которые совместно удовлетворяют специальному свойству.

Для примера рассмотрим простой случай. Пусть мы имеем два простых числа q_α и q_β, а также эллиптические кривые $E_\alpha / \mathbb{F}_{q_\alpha}$ и $E_\beta / \mathbb{F}_{q_\beta}$

такие, что $q_\alpha = \#E_\beta(\mathbb{F}_{q_\beta})$ и $q_\beta = \#E_\alpha(\mathbb{F}_{q_\alpha})$, то есть размер базового поля одной кривой равен порядку группы другой кривой и наоборот. Построим две предварительные обработки zk-SNARK $(G_\alpha, P_\alpha, V_\alpha)$ и $(G_\beta, P_\beta, V_\beta)$, созданные соответственно на кривых $E_\alpha / \mathbb{F}_{q_\alpha}$ и $E_\beta / \mathbb{F}_{q_\beta}$.

Отметим, что $(G_\alpha, P_\alpha, V_\alpha)$ работает для $\mathbb{F}_{q_\beta}$-арифметической выполнимости схем, но все арифметические вычисления V_α выполняются над $\mathbb{F}_{q_\alpha}$ (или над его расширением). По аналогии это верно и для $(G_\beta, P_\beta, V_\beta)$. Вместо того чтобы каждый zk-SNARK обрабатывал утверждения о своем верификаторе, он обрабатывает утверждения о верификаторе другого zk-SNARK. То есть V_α — $\mathbb{F}_{q_\beta}$-арифметическая схема C_{V_α}, а V_β — $\mathbb{F}_{q_\alpha}$-арифметическая схема C_{V_β}.

Затем можно выполнить рекурсивную композицию доказательств, чередуя две системы доказательств. Грубо говоря, можно использовать P_α, чтобы доказать успешную проверку доказательств по C_{V_β}, и, наоборот, P_β для успешной верификации доказательства по C_{V_α}. Выполнение этого чередования гарантирует, что поля «совпадают», и никакая длинная арифметика не требуется.

В случае когда две кривые E_α и E_β таким образом облегчают построение PCD, мы говорим, что (E_α, E_β) — PCD-дружественный 2-цикл (длины 2) эллиптических кривых. Таким образом, можно получить обобщенное определение.

Определение. Пусть $E_0, \ldots, E_{l-1}$ — эллиптические кривые, определенные над конечными полями $F_{q_0}, \ldots, F_{q_{l-1}}$ соответственно, где каждое q_i — простое число. Будем говорить, что $(E_0, \ldots, E_{l-1})$ — *PCD-дружественный цикл* длины *l*, если каждая E_i является дружественной к спариванию и, кроме того, для любого $i \in \{0, \ldots, l-1\}$ имеет место $q_i \neq \#E_{i+1 \bmod l}(\mathbb{F}_{q_{i+1 \bmod l}})$ [1].

Масштабируемые zk-SNARK

Теоретически построение можно описать следующим образом: нужно установить предварительную обработку zk-SNARK (G, P, V) и устойчивую к столкновениям хеш-функцию *H*. Цель состоит в том, чтобы построить полностью емкий вычислимый zk-SNARK (G^*, P^*, V^*) для доказательства / проверки правильности выполнения на данной машине произвольного доступа *M*. Преобразование можно описать в четыре этапа.

Шаг 1: от zk-SNARK до PCD. Первым шагом, не зависящим от *M*, является построение PCD $(\mathbb{G}, \mathbb{P}, \mathbb{V})$ с использованием zk-SNARK (G, P, V). Этот шаг включает в себя рекурсивную композицию доказательств zk-SNARK.

Шаг 2: делегирование памяти машины. Второй шаг предполагает уменьшение размера занимаемой памяти машины M путем делегирования ее оперативной памяти надежному хранилищу при помощи деревьев Меркла. Так M будет загружать значения из памяти как недетерминированные предположения вместе с их алгоритмами аутентификации, которые проверяются с помощью корня дерева Меркла и хеш-функции H. Таким образом, все состояния M включают только состояние процессора и корень дерева Меркла, который «суммирует» память.

Шаг 3: разработка предиката $\Pi_{M,H}$ *для пошаговой проверки*. Третий шаг заключается в разработке предиката соответствия $\Pi_{M,H}$, гарантирующего, что единственными $\Pi_{M,H}$-совместимыми сообщениями z будут те, которые представляют собой результат правильного выполнения (модифицированной) машиной M, по одному шагу за раз, что соответствует свойству инкрементальной вычислимости. Но поскольку $\Pi_{M,H}$ вызывается для проверки только одного шага за один раз, его можно использовать лишь в схемах постоянного размера.

Шаг 4: построение новой системы доказательств. (G^*, P^*, V^*) — это новая реализация zk-SNARK, построение которого заключается в следующем: G^* устанавливается на место G, вызываемого на $\Pi_{M,H}$; P^* использует PCD доказывающего P для пошагового доказательства правильного выполнения M, проводя инкрементальные распределенные вычисления. V^* использует V для установления $\Pi_{M,H}$-соответствия. В общем, поскольку $\Pi_{M,H}$ мал и достаточен для всех вычислений, новый zk-SNARK масштабируется: он полностью емок; более того, поскольку новый проверяющий вычисляет доказательство для каждого нового шага на основе предыдущего, он также является инкрементально вычислимым.

Таким образом zk-SNARK можно улучшить и использовать более эффективно.

Заключение

Мы описали способ избавления от проблем масштабируемости в zk-SNARK, что позволило сделать вывод: криптографические методы, в частности схема доказательств zk-SNARK, поддаются улучшениям эффективности их работы. Есть ли еще какие-либо возможности по повышению эффективности работы данной схемы?

Известно, что доказательства zk-SNARK осуществляются на основе спаривания на эллиптических кривых. Возникает вопрос: будет ли более эффективным применить к этой схеме гиперэллиптическую кривую, не уступающую по уровню безопасности? Таким образом, актуальной задачей является поиск нового математического объекта, использование которого в zk-SNARK будет более эффективным, чем применение эллиптической кривой.

Список литературы

1. *Sasson E., Chiesa A., Tromer E., Virza M.* Scalable Zero Knowledge via Cycles of Elliptic Curves // Algorithmica. 2017. №79 (4). P. 1102—1160.

2. *Что такое* zk-SNARK? // Z.CASH.RU : офиц. сайт криптовалюты Zcash. URL: https://z.cash/ru/technology/zksnarks (дата обращения: 07.11.2020).

3. *Что такое* zk-SNARKs и zk-STARKs? // Binance Academy : [сайт]. URL: https://academy.binance.com/ru/articles/zk-snarks-and-zk-starks-explained (дата обращения: 07.11.2020).

4. *Мельничук Е. М., Новоселов С. А.* Характеристические многочлены некоторых гиперэллиптических кривых родов 2, 3 и р-ранга // Прикладная дискретная математика. Приложение. 2019. №12. С. 21—24.

Об авторе

Полина Борисовна Демочкина — студ., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: polly.evseeva@gmail.com

The author

Polina B. Demochkina, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: polly.evseeva@gmail.com

УДК 512.772.7

Н. С. Колесников

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ ЭКСПОНЕНЦИАЛЬНОЙ ЧАСТИ АЛГОРИТМА ПОДСЧЕТА ТОЧЕК В ЯКОБИАНАХ ГИПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ РОДА 2

Задача вычисления порядка якобиана гиперэллиптической кривой является классической задачей теории чисел с приложениями в современной криптографии. Якобиан кривой используется для построения криптосистем, основанных на дискретном логарифме; как группа большого «неизвестного» порядка в конструкциях верифицируемых функций задержки (VDF) и других приложениях. В статье приводится обзор подходов к ускорению наиболее быстрого алгоритма подсчета точек в якобианах гиперэллиптических кривых – алгоритма Годри – Шоста. Данный алгоритм состоит из двух этапов: 1) нахождение числа точек (характеристического многочлена) по модулю малых простых чисел с объединением результата в один большой модуль по китайской теореме об остатках (полиномиальная часть алгоритма); 2) восстановление полного числа точек из информации по модулю с помощью алгоритмов, основанных на парадоксе дней рождения (экспоненциальная часть алгоритма). В теории алгоритм терминируется в первой части и имеет полиномиальную сложность $O(\log^8 q)$, где q – размер конечного поля. Однако на практике полиномиальная часть алгоритма останавливается на некотором простом числе ℓ из-за ограничений по использованию памяти, которая растет как $O(\ell^4)$, и полное число точек находят уже по экспоненциальному алгоритму. В данной работе выполнена многопоточная реализация экспоненциальной части алгоритма Годри – Шоста на языке программирования C++, дается оценка ее эффективности по затратам времени и памяти.

Computing the order of Jacobian of a hyperelliptic curve is a common number-theoretical problem that has lots of applications in modern cryptography. Namely, Jacobians are applicable to constructions of DLP-based cryptosystems, as well as constructions of verifiable delay functions (VDF's), since they can be viewed as large groups of unknown order. In this article, we present an overview of approaches to accelerate Gaudry-Schost point counting algorithm that is the fastest known algorithm for computing the order of Jacobians of hyperelliptic curves of genus 2. This algorithm consists of two stages: 1) computing the number of points (equivalently, the characteristic polynomial of the curve) modulo some small primes and combining the result into a large module using CRT (polynomial-time part); 2) restoring the number of points utilizing modular data using algorithms based on birthday paradox (exponential-time part). Theoretically, the algorithm terminates after the first stage with $O(\log^8 q)$ time-complexity, where q is a finite field modulus. However, in practice we terminate the polynomial-time part (due to high memory consumption), and we proceed to the second, memory-efficient, exponential-time part. This article presents a multithreaded C++ implementation of exponential part of Gaudry-Schost's point counting algorithm. We evaluate the efficiency of our multithreaded implementation.

© Колесников Н.С., 2020

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 42 – 48.

Ключевые слова: гиперэллиптическая кривая, якобиан, подсчет точек, алгоритм Годри — Шоста, кривые рода 2.

Keywords: hyperelliptic curve, Jacobian, point counting, Gaudry — Schost algorithm, genus 2 curves.

Введение

Пусть $C: y^2 = f(x)$ — гиперэллиптическая кривая рода $g = 2$ (то есть $\deg(f) = 2g + 1$), определенная над конечным полем $\mathbb{F}_q$. Введем следующие обозначения:

- Jac_C — якобиан кривой C. Элементами якобиана являются классы эквивалентности дивизоров кривой с представителями — редуцированными дивизорами;
- $D = \big(u(x), v(x)\big) \in Jac_C$ — представление редуцированного дивизора в координатах Мамфорда — Кантора, где $u(x)$ и $v(x)$ — многочлены с коэффициентами из поля $\mathbb{F}_q$. Для рассматриваемых в статье кривых рода 2 редуцированные дивизоры имеют вид $D = (x^2 + u_1 x + u_0,\ v_1 x + v_0)$. Таким образом, элемент якобиана может быть представлен четверкой $(u_0, u_1, v_0, v_1) \in \mathbb{F}_q^4$.
- $\chi(T) = T^4 - s_1 T^3 + s_2 T^2 - s_1 q T + q^2$ — характеристический многочлен эндоморфизма Фробениуса, индуцируемого в якобиане отображением $(x, y) \mapsto (x^q, y^q)$ на кривой. Имеем $\#Jac_C\big(\mathbb{F}_q\big) = \chi(1)$, поэтому вычисление числа точек эквивалентно нахождению $\chi(T)$. Кроме того, имеются границы (Хассе — Вейля и более точные для рода 2 [4, с. 3, (1)]) для коэффициентов $\chi(T)$ и числа точек:

$$|s_1| \le 4\sqrt{q},\ 2|s_1|\sqrt{q} - 2q \le s_2 \le \frac{s_1^2}{4} + 2q$$

$$\text{и } \big(\sqrt{q} - 1\big)^4 \le \#Jac_C\big(\mathbb{F}_q\big) \le \big(\sqrt{q} + 1\big)^4.$$

На множестве классов дивизоров Jac_C определена операция сложения дивизоров, что делает ее группой, однако порядок этой группы трудно вычислим — сложность нахождения порядка равна $O(log^8 q)$ при использовании алгоритма Годри — Шоста [2], что находится на грани практического применения. Такие группы традиционно используются в дизайне криптосистем с открытым ключом благодаря большой сложности дискретного логарифмирования, а с недавнего времени — также в конструкциях верифицируемых функций задержки (VDF) [3], криптографических аккумуляторов [6] и ненадежных CHAPKов (Trustless SNARKs) [7].

Подсчет числа точек в якобиане необходим для оценки безопасности построенных криптографических примитивов и генерации параметров для криптосистем на основе дискретного логарифма (как альтернатива генерации кривых методом комплексного умножения).

Подход, предложенный Годри и Шостом [2; 4], состоит из двух частей.

1. Полиномиальная часть: нахождение числа точек или характеристического многочлена по модулю как можно большего числа малых

простых ℓ и объединение данной информации в единый модуль m по китайской теореме об остатках. Соответствующий алгоритм представлен в [2].

2. Экспоненциальная часть: зная число точек $\#Jac_C(\mathbb{F}_q)$ по модулю m, восстановить полное число точек $\#Jac_C(\mathbb{F}_q)$, используя алгоритмы на основе парадокса дней рождения. Соответствующий алгоритм впервые был предложен в [5] и требовал большого (экспоненциального) количества памяти. Годри и Шост [4] улучшили его, снизив объем требуемой памяти до полиномиального.

Данная работа посвящена оптимизации и параллельной реализации экспоненциальной части алгоритма Годри — Шоста. Рассмотрим его более подробно.

Алгоритм поиска коллизий Годри — Шоста

Рассматриваемый алгоритм поиска коллизий является аналогом алгоритма Мацуо — Чао — Цудзии [5] с меньшими затратами памяти.

Вход: гиперэллиптическая кривая $C/\mathbb{F}_q$: $y^2 = f(x)$ рода 2; m (простое число) — модуль, для которого известны $\overline{s_1}, \overline{s_2}$ такие, что

$$\overline{s_1} \equiv s_1 \bmod m,$$
$$\overline{s_2} \equiv s_2 \bmod m$$

(элементы $\overline{s_1}, \overline{s_2} \in \mathbb{F}_m$ вычисляются в полиномиальной части алгоритма Годри — Шоста).

Выход: $N = \chi(1)$, где $\chi(T) = T^4 - s_1T^3 + s_2T^2 - s_1qT + q^2$,

$$s_1 = \overline{s_1} + m\widetilde{s_1},$$
$$s_2 = \overline{s_2} + m\widetilde{s_2}.$$

Алгоритм:

1. Выберем границы в соответствии с [4]:

$$B_{1,min} \le s_1 \le B_{1,max},$$
$$B_{2,min} \le s_2 \le B_{2,max}.$$

2. Введем обозначения:

$$R = \{(\sigma_1, \sigma_2), \sigma_1 \in [B_{1,min}, B_{1,max}], \sigma_2 \in [B_{2,min}, B_{2,max}]\},$$
$$K' \coloneqq K + m\left(-\frac{\lfloor B_{1,min}+B_{1,max} \rfloor}{2}(q+1) + \frac{\lfloor B_{2,min}+B_{2,max} \rfloor}{2}\right),$$
$$W \coloneqq \{K'D + (-\sigma_1(q+1) + \sigma_2)mD, (\sigma_1, \sigma_2) \in R\},$$
$$T \coloneqq \{(-\sigma_1(q+1) + \sigma_2)mD, (\sigma_1, \sigma_2) \in R\}.$$

При этом имеем $|W| = |T| = \#R$, $|W \cap T| \subseteq [0{,}25 \cdot \#R, \#R]$.

3. Зададим псевдослучайное (детерминированное) блуждание на множествах W, T:

3.1. Зафиксируем параметры $r \ge 0$, e_1, e_2 (определяются на практике), где e_1, e_2 — средняя (ожидаемая) длина одной цепочки случайного блуждания.

3.2. Вычисляем сдвиги:

$$O_{k,k',b} = (-1)^b \cdot \alpha_{k,k'}(q+1) \cdot m \cdot D + \beta_{k,k'} \cdot m \cdot D \in Jac_C,$$

$\forall k, k' \in [1, r]$, $\forall b \in [0,1]$. Множители $\alpha_{k,k'}$ и $\beta_{k,k'}$ здесь выбраны из равномерного распределения на отрезках $[0, 2l_1]$ и $[0, 2l_2]$ соответственно.

3.3. Задаем хеш-функцию $H: Jac_C \to [1, r]$.

3.4. Задаем «особые» точки множеств W и T, выбрав для них критерий, соответствующий некоторому значению хеш-функций. Например, будем считать «особыми» точки $P_W \in W$ и $P_T \in T$ такие, что $H_1(P_W) = 0$ и, соответственно, $H_2(P_T) = 0$.

3.5. Создаем два пустых списка — *listWild* и *listTame*.

4. Запускаем случайное блуждание по множеству W:

4.1. Выбираем случайным образом пару $(\sigma_1, \sigma_2) \in R$ и соответствующую ей точку $P_W \in W$. Полагаем $\alpha_1 \coloneqq \sigma_1$, $\beta_1 \coloneqq \sigma_2$.

4.2. Если $H_1(P_W) \neq 0$, то есть точка не является «особой»:

4.2.1. Вычисляем $\alpha_1 \coloneqq \alpha_{H_1(P_W),H_2(P_W)}$, $\beta_1 \coloneqq \beta_{H_1(P_W),H_2(P_W)}$.

4.2.2. $\sigma_1 \coloneqq \sigma_1 + \alpha_1$, $\sigma_2 \coloneqq \sigma_2 + \beta_1$, $P_W \coloneqq P_W + O_{H_1(P_W),H_2(P_W),1}$.

4.2.3. Возвращаемся к шагу 4.2.

4.3. Сохраняем найденную «особую» точку $(P_W, \alpha_1, \beta_1) \to listWild$.

5. Запускаем случайное блуждание по множеству T:

5.1. Выбираем случайным образом пару $(\sigma_1, \sigma_2) \in R$ и соответствующую ей точку $P_T \in T$. Полагаем $\alpha_2 \coloneqq \sigma_1$, $\beta_2 \coloneqq \sigma_2$.

5.2. Если $H_2(P_T) \neq 0$, то есть точка не является «особой»:

5.2.1. Вычисляем $\alpha_2 \coloneqq \alpha_{H_1(P_T),H_2(P_T)}$, $\beta_2 \coloneqq \beta_{H_1(P_T),H_2(P_T)}$.

5.2.2. $\sigma_1 \coloneqq \sigma_1 + \alpha_2$, $\sigma_2 \coloneqq \sigma_2 + \beta_2$, $P_T \coloneqq P_T + O_{H_1(P_T),H_2(P_T),0}$.

5.2.3. Возвращаемся к шагу 5.2.

5.3. Сохраняем найденную особую точку $P_T \to listTame$.

Замечание. Случайные блуждания по множествам W и T, то есть шаги алгоритма 4.1—4.2 и 5.1—5.2, выполняются параллельно и независимо. Алгоритм завершается после того, как будет найдена точка $P = P_T = P_W$ (коллизия между списками $listWild$ и $listTame$).

Вернуть $N = K - (\alpha_1 - \alpha_2)(q+1)m + (\beta_1 - \beta_2)m$.

С учетом того, что $\widetilde{s_1}$ и $\widetilde{s_2}$ равномерно распределены на отрезках $[B_{1,min}, B_{1,max}]$ и $[B_{2,min}, B_{2,max}]$ соответственно, ожидаемое время работы алгоритма составляет $T \approx 2{,}43\sqrt{\#R} = 19{,}5\frac{q^{3/4}}{m}$.

Оптимизации алгоритма поиска коллизий

Для дальнейших оптимизаций алгоритма могут использоваться следующие методы, которые предлагается добавить в программную реализацию и протестировать на практике.

1. Метод Гэлбрейта — Рупрая [8] предполагает разбиение интервалов случайных блужданий $[B_{1,min}, B_{1,max}]$ и $[B_{2,min}, B_{2,max}]$ на два класса эквивалентности. При этом на шаге 4.2.1 вычисляются сразу две точки — P_W и $P_W{}'$, соответствующие эквивалентным значениям $\alpha_1 \sim \alpha_1{}'$, $\beta_1 \sim \beta_1{}'$. Предложенный метод теоретически позволяет уменьшить ожидаемое время работы алгоритма до $1{,}478\sqrt{\#R} = 11{,}9\frac{q^{3/4}}{m}$.

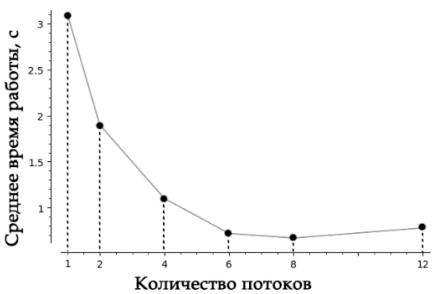
2. В анализе алгоритма Годри — Шоста предполагается, что распределение $\widetilde{s_1}$ и $\widetilde{s_2}$ равномерное. Этого достаточно для грубой оценки времени «в среднем». Но на самом деле распределение не является равномерным, и этот факт можно использовать для подсчета точек. Соответствующая оптимизация алгоритма была предложена в [10]. Распределение задается группой Сато — Тейта кривой, все возможные такие группы для рода 2 и соответствующие им распределения описаны в [11]. Заметим, что для кривой общего вида группа Сато — Тейта в большинстве случаев равна USp_4, и в алгоритме можно ограничиться данным случаем с соответствующим распределением ($\widetilde{s_1}$, $\widetilde{s_2}$). Другие группы Сато — Тейта соответствуют кривым с дополнительной структурой, например кривым с комплексным умножением, автоморфизмами, разложением якобиана на эллиптические кривые.

3. Метод Смита [9] для построения изогений между гиперэллиптическими и негиперэллиптическими кривыми рода 3. Данный метод использовался для вычисления дискретных логарифмов. Предполагается снижение сложности задачи с $O(q^{3/2})/m$ до $O(q/m)$.

Особенности реализации и результаты

За основу реализации взята экспериментальная программа Годри из пакета NTLJac2 [1], в которую было добавлено распараллеливание случайных блужданий на n потоков с помощью $std :: thread$. Реализация на C++ доступна под лицензией GNU GPL v2 и размещена на сервере GitHub. Представленные ниже результаты тестирования (рис. 1—3) были получены на машине с процессором XEON E-2146G (6 ядер/12 потоков) под управлением ОС Ubuntu 20.04.1 LTS, компилятор G++ из пакета GCC9.3.0.

В каждой из трех серий тестов была выбрана случайная кривая $y^2 = f(x)$ над конечными полями $\mathbb{F}_q$, где q — простое число, близкое к 2^{24}, 2^{30}, 2^{36} соответственно. Программа запускалась $N = 100$ раз с одинаковыми входными параметрами в каждом из режимов с числом потоков $\{1, 2, 4, 6, 8, 12\}$. Наибольшая эффективность реализации наблюдается при запуске в $n = 6$ потоков.

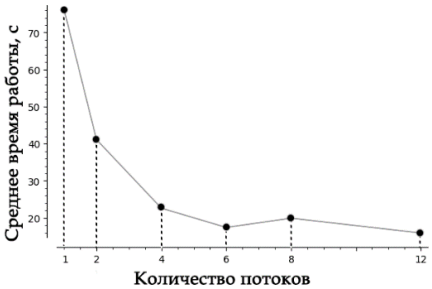


$$q = 16784711$$

$$f(x) = x^5 + 66737x^4 + 1073741x^3 + \\ +3827x^2 + 11537x + 374189$$

$$N = 100$$

Рис. 1. Время работы для $q \sim 24$ бит

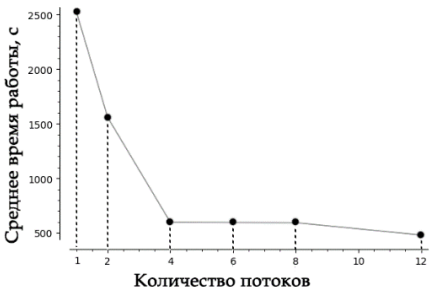


$$q = 107374127$$

$$f(x) = x^5 + 6673747x^4 + 10737411x^3 + \\ +73783827x^2 + 11537427x + 3741899$$

$$N = 100$$

Рис. 2. Время работы для $q \sim 30$ бит



$$q = 100000000003$$

$$f(x) = x^5 + 44951725753x^4 + \\ +35549991545x^3 + 14731848372x^2 + \\ +72263994727x + 67183483819$$

$$N = 100$$

Рис. 3. Время работы для $q \sim 36$ бит

Список литературы

1. *Gaudry P.* NTLJac2, Tools for genus 2 Jacobians in NTL. URL: http://www.lix.polytechnique.fr/Labo/Pierrick.Gaudry/NTLJac2/ (дата обращения: 13.10.2020).

2. *Gaudry P., Schost É.* Genus 2 point counting over prime fields // J. of Symbolic Computation. 2012. Vol. 47, №4. P. 368—400.

3. *Dobson S., Galbraith S.D., Smith B.* Trustless Groups of Unknown Order with Hyperelliptic Curves // Cryptology ePrint Archive, Report 2020/196. URL: https://eprint.iacr.org/2020/196 (дата обращения: 10.09.2020).

4. *Gaudry P., Schost É.*A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm // International Algorithmic Number Theory Symposium. Springer, 2004. P. 208—222.

5. *Matsuo K., Chao J., Tsujii S.* An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields // International Algorithmic Number Theory Symposium. Springer, 2002. P. 461—474.

6. *Boneh D., Bunz B., Fisch B.* Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains // Cryptology ePrint Archive, Report 2018/1188. URL: https://eprint.iacr.org/2018/1188.pdf (дата обращения: 10.09.2020).

7. *Bünz B., Fisch B., Szepieniec A.* Transparent SNARKs from DARK Compilers // Cryptology ePrint Archive, Report 2019/1229. URL: https://eprint.iacr.org/2019/1229.pdf (дата обращения: 10.09.2020).

8. *Galbraith S., Ruprai R.S.* Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval // International Workshop on Public Key Cryptography. Springer, 2010. P. 368—383.

9. *Smith B.* Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves // Advances in Cryptology — Eurocrypt. Springer, 2008. P. 163—180.

10. *Kedlaya K.S., Sutherland A.V.* Computing L-series of hyperelliptic curves // International Algorithmic Number Theory Symposium. Springer, 2008. P. 312—326.

11. *Fité F., Kedlaya K.S., Rotger, V., Sutherland, A.V.* Sato-Tate distributions and Galois endomorphism modules in genus 2 // Compositio Mathematica. 2012. T. 148, №5. P. 1390—1442.

Об авторе

Никита Сергеевич Колесников — мл. науч. сотр., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: NiKolesnikov1@kantiana.ru

The author

Nikita S. Kolesnikov, Research Fellow, Immanuel Kant Baltic Federal University, Russia.

E-mail: NiKolesnikov1@kantiana.ru

УДК 004.8

С. Б. Румовская

ИССЛЕДОВАНИЕ КОЛЛЕКТИВНОЙ ДЕЯТЕЛЬНОСТИ ПО ПРЕОДОЛЕНИЮ ДИАГНОСТИЧЕСКОЙ ПРОБЛЕМЫ

В настоящее время все больше диагностических ситуаций требуют своего рассмотрения с позиции не только лечащего врача, но и консилиума медиков одной или, как правило, разных специализаций. Созыв консилиума часто затруднен или предполагает длительное ожидание, поэтому моделирование механизмов решения и когнитивной визуализации диагностических проблем актуально. Последнее обусловлено также тем, что от оперативности реакции врача на возникающую проблемную диагностическую ситуацию зависит безопасность принимаемых решений. В статье представлено исследование особенностей созыва и коллективной деятельности членов консилиума, результаты которого в дальнейшем предполагается использовать в качестве основы функциональных гибридных интеллектуальных систем с когнитивным моделированием диагностической проблемы.

Currently, a number of diagnostic situations requiring consideration from the position of a council of physicians of the same (rarely) or different specialization is growing. Convening a council is often difficult or it is necessary to wait for a long time. Therefore, modeling mechanisms for solving of a diagnostic problems and its and cognitive visualization is relevant. The latter is also due to the fact that the safety of the made decisions depends on the speed of the doctor's response to the emerging problematic diagnostic situation. The paper is dedicated to the research of the convening and group activity of specialists within the council. Results of it would provide the basis of hybrid functional intellectual systems with cognitive modeling of a diagnostic problem.

Ключевые слова: коллектив экспертов, консилиум, диагностическая проблема, рак поджелудочной железы.

Keywords: collectives of experts, council, diagnostic problems, pancreatic cancer.

Введение

В данной работе излагается один из результатов большого исследования, направленного на моделирование представлений специалистов-медиков о реальных диагностических проблемах и их механизмов рассуждения, направляющих и упорядочивающих процесс их решения по принципу консилиума. В условиях растущей гетерогенности решаемых диагностических проблем только коллективы специалистов могут преодолеть возникшую перед ними неопределенность диагностической ситуации. В связи с этим исследование механизмов и особенно-

© Румовская С. Б., 2020

стей созыва и работы консилиумов актуально, особенно для рассматриваемого в данной статье заболевания — рака поджелудочной железы (РПЖ).

В структуре онкологических заболеваний населения России РПЖ составляет 3 % [1] и считается наиболее фатальным заболеванием, от которого погибают 95 % всех заболевших РПЖ. Раннее диагностирование РПЖ случается крайне редко. Рак ПЖ чаще всего выявляется на терминальной стадии заболевания, при этом в момент диагностирования заболевания резектабельность опухоли не превышает 10—15 %, а у остальных 85—90 % пациентов выявляется нерезектабельная опухоль или отдаленные метастазы с летальным исходом в течение 1 года [2]. Низкая выявляемость рака на догоспитальном этапе приводит к снижению процента резектабельных опухолей. РПЖ выявляется случайно при обследовании по поводу другой патологии. При этом более 90 % заболевших погибают в результате прогрессирующего рака спустя 4 месяца — 1 год с момента выявления, пятилетняя выживаемость — 1—5 %. В настоящее время не существует скрининговых программ, которые могли бы быть рекомендованы.

Решение проблемы ранней оперативной диагностики РПЖ позволит улучшить результаты комплексного лечения пациентов с этим заболеванием.

Совместное решение задач. «Мышление в группе»

В зарубежных работах исследования «мышления в группе» [3] подразделяются на исследования проблем принятия решений группой (group decision making) и решения задач группой (group problem solving). Первое направление связано с исследованием динамики работы группы, принимающей решения. Здесь рассматривают такие вопросы, как описание стандартных проблем, их типология (рис. 1), влияние их характеристик на процесс решения и т. д.

Второе направление по большей части подразумевает постановку общепсихологических задач исследования самого процесса мышления в группе. Такие исследования в основном направлены на использование специальных методов (таких как мозговой штурм, синектика, морфологический анализ, деловые игры) в качестве вспомогательных для организации и активизации мышления в группе [4].

Предметом настоящей работы является коллективная деятельность медицинского консилиума.

Консилиум (лат. *consilium* — совещание, обсуждение) — это совещание врачей одной или разных специальностей с целью выработки заключения о состоянии здоровья обследуемого, установления диагноза болезни, определения ее прогноза, тактики обследования и лечения больного [5, с. 488].

Деятельность консилиума в медицине нацелена в зависимости от диагностической ситуации на решение дискуссионных, проблемных, творческих проблем, а также проблем, ориентированных на поиск правильного выбора.

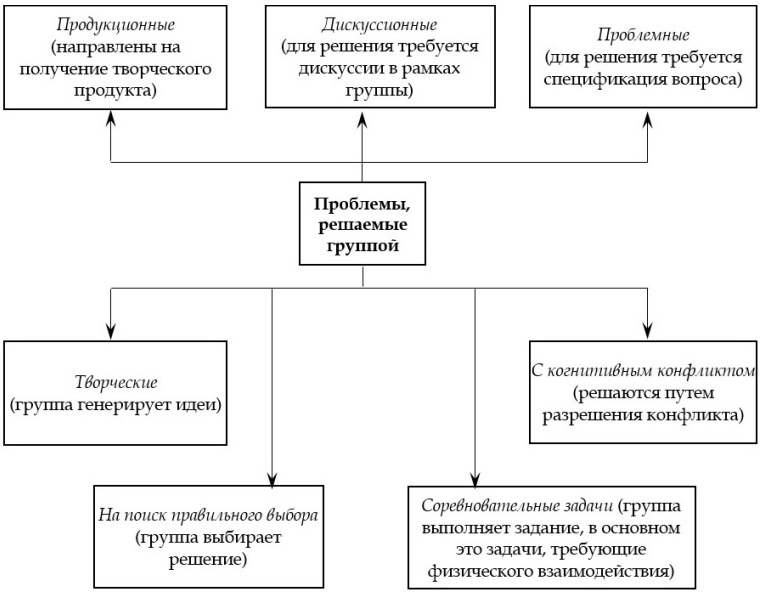


Рис. 1. Классификация проблем, решаемых в группе

Источник: [3].

В работе членов медицинского консилиума можно выделить следующие шаги [6]:

1. *Доклад лечащего врача* о состоянии больного на момент консилиума, его сопутствующих заболеваниях и осложнениях, о полученных результатах исследования и проведенного лечения. В завершение перечисляется список задач, которые выносятся для рассмотрения на консилиуме. Доклад делается в отсутствие пациента.

2. *Осмотр и опрос больного* – физикальное обследование больного (прослушивание, прощупывание, простукивание), при необходимости инструментальное обследование.

3. *Свободная дискуссия* (без больного). Дискуссия должна быть честной, открытой и доброжелательной. Вначале высказываются члены консилиума с меньшим опытом работы, а затем более именитые, чтобы не подавлять инициативу первых. Каждый выступающий имеет право на свою точку зрения, которую должен отстаивать. Все выступления конспектируются.

4. *Выработка заключения консилиума*.

Коллективная деятельность медицинского консилиума, преодолевающего проблему диагностики и лечения

Процесс созыва и работы консилиума рассматривался на примере диагностики рака поджелудочной железы (ПЖ). Построена схема (рис. 2) на основе результатов исследования процесса созыва консилиума и его проведения относительно неясного состояния больного: неточный диагноз, отсутствие эффекта от проведенного лечения, неясная степень резектабельности опухоли и т. д.

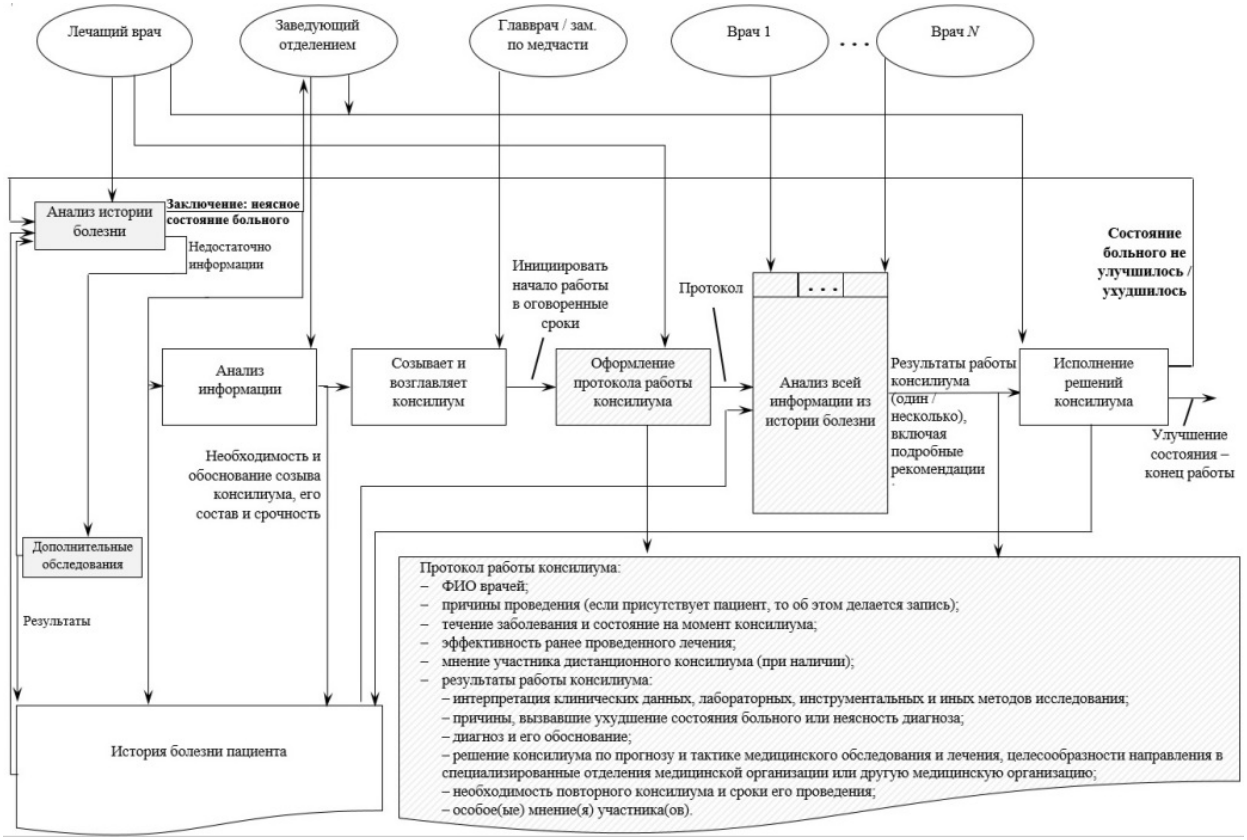


Рис. 2. Схема созыва и проведения консилиума при подозрении на рак поджелудочной железы

Работа консилиума включает в себя следующие этапы:

1. *Анализ истории болезни* лечащим врачом (на первых этапах это может быть участковый терапевт, далее — хирург или гастроэнтеролог). При этом симптоматика РПЖ на ранних стадиях малоспецифична и больные длительно наблюдаются у участкового терапевта по поводу хронического панкреатита, холецистита и т.д. Если имеет место недостаток информации, то переходят к этапу 2.

2. *Дополнительные обследования* (лабораторные инструментальные и иные методы обследования). Результаты записываются в историю болезни пациента.

3. Выход из цикла *Анализ истории болезни — Дополнительные обследования* происходит в случае, когда возможности медицинского учреждения в плане обследований исчерпаны, однако состояние пациента остается неясным (в том числе есть подозрение на РПЖ).

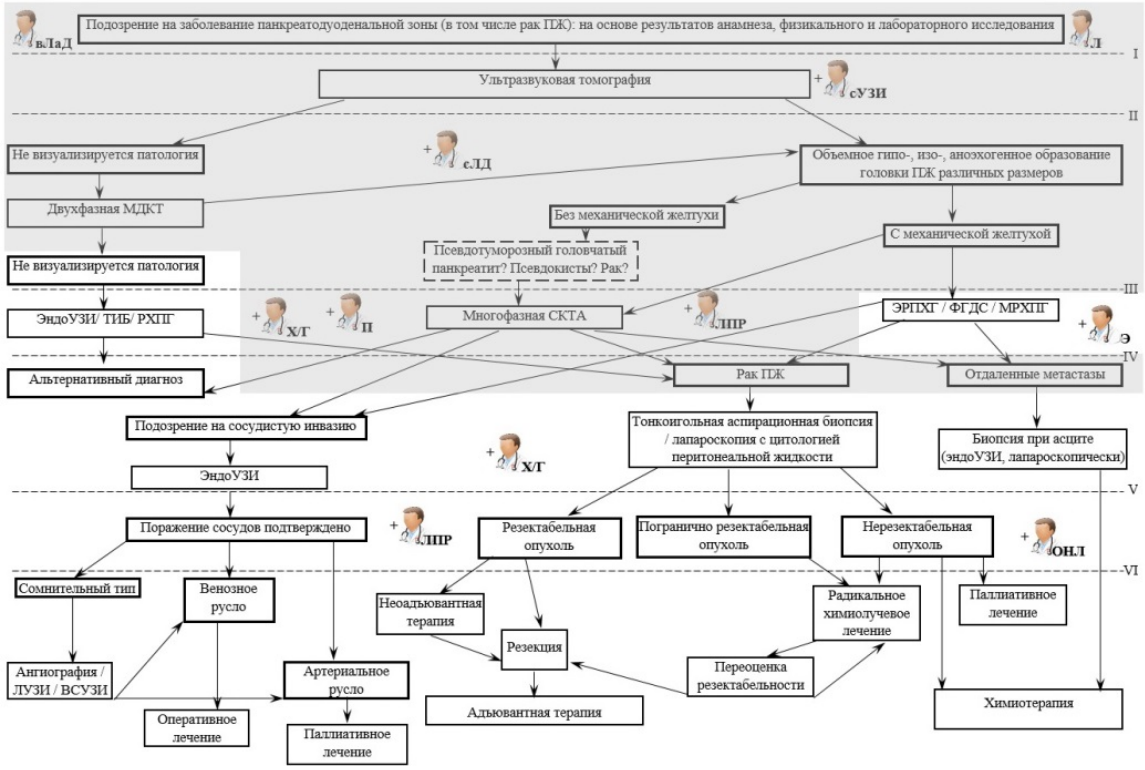
4. *Анализ информации*, поданной лечащим врачом заведующему отделением. Последний предоставляет главврачу или заместителю по медчасти заключение о необходимости созыва консилиума, его обоснование, данные по составу и срочности созыва.

5. Далее главврач либо заместитель по медчасти *созывает и возглавляет консилиум* и инициирует начало его работы в установленные сроки.

С момента появления первых симптомов до созыва консилиума проходит в среднем несколько месяцев, что значительно сокращает шансы пациента на положительный исход и приводит к высокой летальности.

Результатом анализа методов и особенностей процесса диагностики и лечения РПЖ стала схема процесса диагностики и лечения РПЖ, на которую наложен консилиум врачей (рис. 3).

В рисунке 3 использованы следующие сокращения: УЗИ — ультразвуковое исследование; МДКТ — Мультидетекторная компьютерная томография; МСКТА — мультиспиральная компьютерная ангиография, ЭндоУЗИ — эндоскопическое ультразвуковое исследование; ТИБ — тонкоигольная биопсия; РХПГ — ретроградная холангиопанкреатография; ФГДС — фиброгастродуоденоскопия; ЭРХПГ — эндоскопическая ретроградная холангиопанкреатография; МРХПГ — магнитно-резонансная холангиопанкреатография; ЛУЗИ — лапароскопическое ультразвуковое исследование; ВСУЗИ — внутрисосудистое ультразвуковое исследование; **Л** — лечащий врач (гастроэнтеролог или хирург); **Х/Г** — хирург и/или гастроэнтеролог; **ОНЛ** — онколог по нехирургическому лечению; **сЛД** — специалист по лучевой диагностике (чаще всего есть данные только по КТ); **сУЗИ** — специалист по ультразвуковому исследованию; **вЛаД** — врач лабораторной диагностики (интерпретирует данные лабораторных исследований); **П** — патологоанатом (исследует материал биопсии); **Э** — врач-эндоскопист; **ЛПР** — лицо, принимающее решение. Серой заливкой показаны те этапы диагностики, информацию и методы которых мы будем рассматривать на следующих этапах исследования. При этом процесс диагностики РПЖ и принятия решения о типе лечения на рисунке 3 условно разделен на шесть этапов. На каждом этапе в процесс диагностики включается очередной врач узкой специализации. В самом начале, когда пациент пришел с жалобами к лечащему врачу (хирургу или гастроэнтерологу), помимо него работает еще и врач лабораторной диагностики.



– заключение
– метод обследования/лечения
– несколько альтернатив

Рис. 3. Схема процесса диагностики и лечения рака поджелудочной железы, включающая консилиум врачей

Консилиум обычно собирают на VI этапе, но в сложных случаях и в отсутствие доступа ко всем многочисленным методам исследования, отраженным на рисунке 3, он может быть собран в первый раз и на IV этапе, если состояние больного остается неясным.

Сбор консилиума на рисунке 3 отмечен появлением врача-ЛПР — одного из руководящих административных работников (выполняет интеграционную функцию). Чаще всего это заместитель главного врача по медицинской части (начмед), имеющий специализацию «организатор здравоохранения», по специальности обычно терапевт.

Подозрение на заболевание панкреатодуоденальной зоны (в том числе РПЖ) возникает на основании клинических проявлений:

— самые ранние — боли в верхней половине живота (носят характер дискомфорта) и потеря веса. При этом создается ошибочное впечатление холецистита, язвенной болезни двенадцатиперстной кишки или заболевания правой почки;

— при местно-распространенной форме РПЖ — диспептические расстройства (анорексия, тошнота, отрыжка, изжога, чувство тяжести в эпигастрии, рвота, обильный частый зловонный стул глинисто-серого цвета, иногда поносы, запоры) и приступы резких панкреатических болей. На данном этапе часто ставят ошибочный диагноз хронического панкреатита с экзокринной недостаточностью. Здесь же развивается желтуха, которая в 10—30 % случаев становится практически единственным симптомом.

Заключение

В данной работе представлены результаты анализа коллективной деятельности членов медицинского консилиума. На примере РПЖ рассмотрен процесс созыва консилиума и взаимодействия врачей, входящих в него, знания которых требуются на протяжении всего процесса диагностики и формирования плана лечения больного с подозрением на РПЖ.

На следующем этапе исследования планируется разработка интегрированной модели (ИМ) работы консилиума для ранней диагностики РПЖ. Это позволит сократить сроки обследования пациентов за счет поддержки принятия решения на этапах цикла *Анализ истории болезни — Дополнительные обследования* (этапы с серой заливкой на рисунке 2) и ускорить выход из цикла с подозрением на рак к созыву консилиума. Предполагается реализация ИМ как функциональной гибридной интеллектуальной системы (ФГиИС) [7] с когнитивным моделированием диагностической проблемы, что даст возможность подойти к сглаживанию противоречивых показаний аппаратуры, снизит число врачебных ошибок, повысит качество и, соответственно, безопасность медицинских интеллектуальных систем поддержки принятия диагностических решений [8; 9]. Частично ФГиИС будет поддерживать работу реального консилиума (этапы с серой штриховкой на рисунке 2) в ситуации, когда неясен диагноз и консилиум созывается для подтверждения рака ПЖ.

Работа выполнена при поддержке гранта РФФИ № 19-07-00250А «Субъектно-ориентированное моделирование образа проблемной ситуации медицинской диагностики методами и средствами гибридных интеллектуальных систем».

Список литературы

1. *Клинические* рекомендации. Рак поджелудочной железы. URL: https://oncology-association.ru/files/clinical-guidelines-2020/rak_podzheludochnoj_zhelezy.pdf (дата обращения: 15.10.2020).

2. *Вардеванян О.П.* Комплексная оценка компьютерно-томографических критериев для оптимизации дифференциальной диагностики новообразований билиопанкреатодуоденальной зоны : дис. ... канд. мед. наук. Ереван, 2016.

3. *Матюшкина А.А.* Сравнительный анализ смыслообразования в индивидуальном и групповом мышлении : дис. ... канд. психол. наук. М., 2001.

4. *Спиридонов В.Ф.* Психология мышления: решение задач и проблем. М., 2006.

5. *Малая* медицинская энциклопедия : в 6 т. / под ред. В.И. Покровского. М., 1991.

6. *Тихилов Р.М., Кустов В.М.* Медицинский (врачебный) консилиум — история и практика // Здравоохранение. 2016. №8. URL: http://www.zdrav.by/organizatsiya-zdravoohraneniya/meditsinskij-vrachebnyj-konsilium-istoriya-i-praktika (дата обращения: 15.10.2020).

7. *Колесников А.В.* Гибридные интеллектуальные системы. Теория и технология разработки. СПб., 2001.

8. *Кобринский Б.А.* Значение визуальных образных представлений для медицинских интеллектуальных систем // Искусственный интеллект и принятие решений. 2012. №3. С. 3—8.

9. *Кобринский Б.А.* Аргументация и когнитивная графика в медицинской диагностической системе // XV национальная конференция по искусственному интеллекту с международным участием КИИ-2016 (3—7 октября 2016 г., Смоленск) : тр. конф. : в 3 т. Т. 2. Смоленск, 2016. С. 259—265.

Об авторе

София Борисовна Румовская — канд. техн. наук, науч. сотр., Калининградский филиал Федерального исследовательского центра «Информатика и управление» РАН, Россия.

E-mail: sophiyabr@gmail.com

The author

Dr Sophiya B. Rumovskaya, Research Fellow, Kaliningrad branch of the FRC «Computer Science and Control» of the RAS, Russia.

E-mail: sophiyabr@gmail.com

УДК 004.8

А. В. Колесников, С. Б. Румовская
Э. В. Ясинский, С. А. Солдатов

ИНТЕЛЛЕКТУАЛИЗАЦИЯ ОПЕРАТИВНО-ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ РЕГИОНАЛЬНОЙ ЭЛЕКТРОЭНЕРГЕТИКОЙ МЕТОДАМИ КОГНИТИВНЫХ ГИБРИДНЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

Часть 1

Оперативная работа с образом в интеллектуальных сложных динамических системах управления непосредственно не воспринимаемого объекта, проецирование на этот образ информации, поступающей извне, – трудная задача оператора. В связи с этим разработка компьютерной имитации когнитивных образований приведет к усилению человеческого интеллекта в оперативной работе путем дополнения естественных способностей оператора обрабатывать оперативно-технологическую информацию программно-аппаратными средствами (механизмами), расширяющими мыслительные процессы человека. В предлагаемой статье представлены результаты работы первого этапа второго года исследований по тематике когнитивных гибридных интеллектуальных систем, а именно результаты исследования системы оперативно-технологического управления региональной электроэнергетической системой, категоризации онтологической семантики объективной реальности и математической реальности объекта оперативно-технологической деятельности.

One of the most difficult task for an operator is the operational work with an image in intelligent complex dynamic control systems of a directly not perceptible object and projecting information from the outside onto this image. In this regard, the development of computer imitation of cognitive formations will lead to an increase in human intelligence in operational work, by supplementing the operator's natural abilities to process operational and technological information by software and hardware (mechanisms) that expand human thought processes. This paper presents the results of the work of the first stage of the second year of the research on the topic of cognitive hybrid intelligent systems. Namely, results of the study of the operational and technological control system of the regional electric power system, results of the categorization of the ontological semantics of the objective reality and the mathematical reality of the object of technology operations activities.

Ключевые слова: интеллектуальная электроэнергетическая система, система оперативно-технологического управления, онтологическая семантика объекта управления, объективная и математическая реальность объекта управления.

Keywords: intelligent power system, operational and technological control system, ontological semantics of a control object, objective and mathematical reality of the control object.

© Колесников А. В., Румовская С. Б., Ясинский Э. В., Солдатов С. А., 2020
Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2020. № 4. С. 57 – 87.

Человек — существо образное в реальности, в представлениях, в мечтаниях — в жизни и за пределами ее.
В. В. Козлов, И. А. Донченко

Введение

Российская Федерация обладает существенным потенциалом для того, чтобы стать одним из международных лидеров в развитии и использовании технологий искусственного интеллекта, чему способствует высокий уровень базового физико-математического образования, сильная естественнонаучная школа, наличие компетенций в области моделирования и программирования [2]. В Калининграде такая региональная школа сложилась и работает в рамках Российской ассоциации искусственного интеллекта под руководством доктора технических наук, профессора Института физико-математических наук и информационных технологий Балтийского федерального университета им. И. Канта А. В. Колесникова. В настоящее время работа школы сконцентрирована на интеллектуализации электроэнергетических систем и установок и медицинской диагностике методами гибридных интеллектуальных систем.

Искусственный интеллект — комплекс технологических решений для имитации когнитивных функций человека, включая самообучение и поиск решений без заранее заданного алгоритма, для результативного решения конкретных задач не хуже человека [2].

Интеллектуализация электроэнергетики — применение новых информационных технологий для создания интеллектуальной энергосистемы (ЭС) с системой управления, располагающей совокупностью моделей мира и обладающей «мыслительными способностями» в отношении управления режимными изменениями, свойственными человеческому разуму [3]. Интеллектуальная деятельность единых центров управления сетями (ЕЦУС), центров управления сетями (ЦУС), оперативно-диспетчерских служб (ОДС) «оживляет», изменяет и приспосабливает пассивные электрические сети к работе в условиях физической реальности. В составе интеллектуальной электроэнергетической системы (ИЭС) электрическая сеть из пассивного устройства транспорта и распределения электроэнергии превращается в активный элемент, параметры и характеристики которого изменяются в зависимости от режимов работы энергосистемы [4].

Настоящая работа содержит результаты моделирования когнитивных механизмов схематизации предметно-изобразительных, образных представлений о событиях, ситуациях, режимах и состояниях объекта управления у оперативных работников ЕЦУС, ЦУС и ОДС и развивает труды Д. А. Поспелова и В. Н. Пушкина, которые неразрывно связывают качество и надежность диспетчерского труда с построением в структурах мозга посредством «языка» информационных аналогов ресурсов той среды, в которой живет и действует человек-оператор. Воссоздавая тот или иной ресурс окружающей среды, оператор фиксирует его свойства относительно времени и в своем сознании изменяет отражаемый ресурс, преобразует его. Благодаря способности строить информационные модели («внутренние образно-концептуальные модели обста-

новки», по Г.В. Дружинину [5], «образно-концептуальные модели обстановки», по С.И. Магиду [6], «концептуальные модели деятельности», по С.А. Дружилову [7]), которые следует отличать от информационных моделей-мнемосхем на «языке мнемонического изображения» (по Д.А. Ошанину), оператор апробирует варианты поведения «про себя», прежде чем начать действовать.

В настоящей статье представлена первая часть работы, проведенной группой исследователей под руководством А.В. Колесникова. В ней изложены результаты анализа особенностей и структуры системы оперативно-технологического управления региональными электроэнергетическими системами на примере Калининградской области, а также результаты исследования объекта оперативно-технологического управления с онтологической и математической точек зрения.

Система оперативно-технологического управления региональными электроэнергетическими системами

Слово «описание» применительно к природе на протяжении веков постепенно теряло свой первоначальный смысл и сменилось «математическим описанием природы». В ясную картину мира привносился элемент абстрактности, наглядность исчезла, и оказалось, что математически сформулированные в квантовой теории законы природы относятся не к элементарным частицам как таковым, а к нашему знанию о них [8]. Характер техники особенно резко изменился с развитием теории электричества, в значительной мере использующей природные силы, эмпирически не известные человеку, хотя они и окружают нас повсюду. Сегодня электротехника для многих таинственна, жутковата и по меньшей мере непонятна (рис. 1).

а

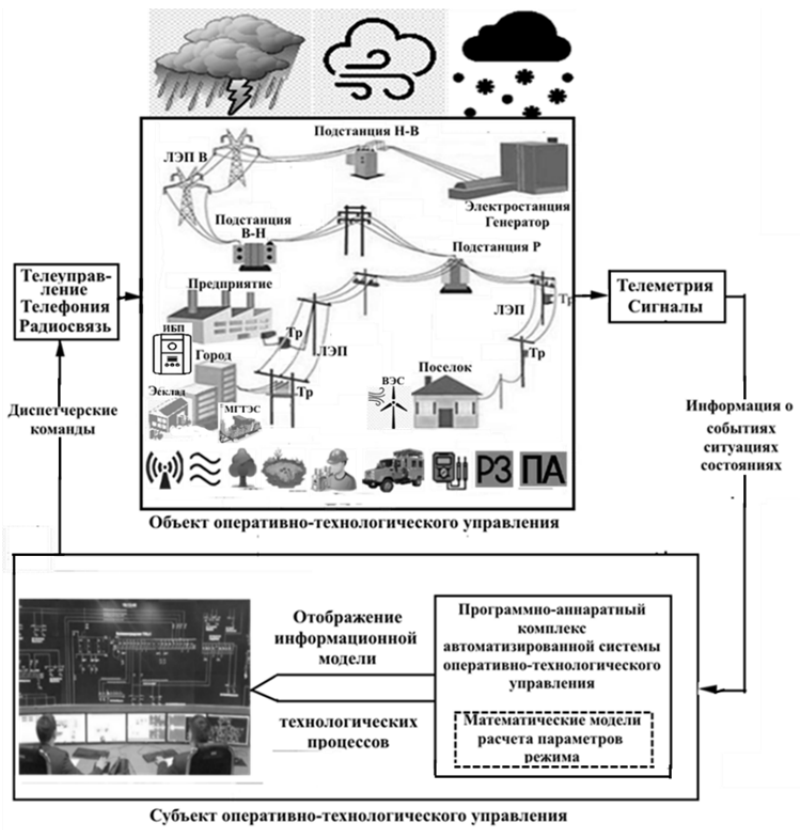
б

Рис. 1. Электротехника и человек:
а — люминисцентная лампа, горящая под ЛЭП напряжением 500 кВ в подмосковном Красногорске; *б* — современный сложный электрический аппарат — подстанция закрытого типа мощностью 50 МВА и напряжением 110 кВ «Береговая» в Калининграде, работающая в автоматическом режиме

Изменения, глубоко затронувшие в электротехническую эпоху окружающий мир, угрожающе деформировали и мышление субъекта оперативной деятельности в ЭС. Еще древний китайский философ Чжуан-цзы определил, что технократии свойственна утрата целостного восприятия мира в технической деятельности людей [9]. Вот рассказ о встрече ученика Конфуция Цзы-гуна со стариком-садовником, черпавшим воду для полива из колодца и носившим ее в горшке. Когда Цзы-

гун посоветовал садовнику воспользоваться водочерпалкой, тот ответил: «Я слышал от своего учителя, что тот, кто пользуется механизмами, будет все делать механически, а тот, кто действует механически, будет иметь механическое сердце. Если же в груди будет механическое сердце, тогда будет утрачена первозданная чистота, а когда утрачена первозданная чистота, жизненный дух не будет покоен…» [9, с. 134].

Отмеченные выше обстоятельства имеют самое непосредственное отношение к системе оперативно-технологического управления региональной электроэнергетической системой, функционирующей в условиях внешней среды, схема которой дана на рисунке 2.



Н-В — низкое напряжение — высокое напряжение
В-Н — высокое напряжение — низкое напряжение
Р — распределительная
ЛЭП В — высоковольтная линия электропередачи
Тр — трансформатор
ИБП — источник бесперебойного питания
Эсклад — склад инструментов и электрооборудования оперативно-выездных бригад
МГТЭС — мобильная газотурбинная электростанция
ВЭС — ветроэлектрическая электростанция
РЗ — релейная защита
ПА — противоаварийная автоматика

Рис. 2. Схема системы оперативно-технологического управления региональной электроэнергетической системой в условиях внешней среды

Эта схема, сохраняя в целом концептуализацию «объект управления», «субъект управления», «канал обратной связи», «регулятор», «внешняя среда», «вход», «выход», «управление», «информация» и др., общепринятую в теории управления, имеет следующие особенности:

1) ограничивается территориально-региональным уровнем ЕЭС;

2) специфицирует по отношению «род — вид» содержание концепта «управление» как оперативно-технологическое управление (ОТУ) / оперативно-диспетчерское управление (ОДУ);

3) разумно, в предметно-изобразительном и вербальном представлениях отображает состав и основную структуру объекта ОТУ региональной ЭС, актуальные для понимания онтологической семантики протекающих в нем микро- и макротехнологических процессов (при этом смысл части из них во избежание усложнения общего видения отражен изображениями-пиктограммами, расположенными в нижней части фигуры объекта ОТУ);

4) разумно, в тех же представлениях показан субъект ОТУ региональной ЭС (на рисунке 2 представлен фрагмент фотографии регионального центра управления сетями ОАО «Янтарьэнерго»: общая информационная модель-мнемосхема на видеостене из LCD-панелей и операторы за диспетчерским пультом);

5) терминология каналов прямой и обратной связи адаптирована к терминологии ОТУ и ОДУ региональной ЭС;

6) влияние внешней среды ограничено основными элементами природной среды, а также космическими, ионосферными и атмосферными воздействиями.

Онтологическая семантика объекта оперативно-технологического управления в региональной интеллектуальной электроэнергетике

В соответствии с определением ст. 3 ФЗ «Об электроэнергетике», *электроэнергетическая система* — совокупность объектов электроэнергетики и энергопринимающих установок потребителей электрической энергии, связанных общим режимом работы в едином технологическом процессе производства, передачи и потребления электрической энергии в условиях централизованного ОДУ [10]. *Объектами электросетевого хозяйства* (рис. 2) являются линии электропередачи, трансформаторные и иные подстанции, распределительные пункты и иное предназначенное для обеспечения электрических связей и осуществления передачи электрической энергии оборудование [10].

Производство электроэнергии в ЭС обладает особенностями, резко отличающими его от других отраслей промышленности:

1) производство электроэнергии, ее распределение и преобразование в другие виды энергии происходят одновременно, между мощностями энергосистемы оперативно поддерживается точный баланс;

2) относительная быстрота протекания переходных процессов составляет 10^{-4}—10^{-3} доли секунды; короткие замыкания, включения и отключения, качания, нарушения устойчивости идут от долей секунды

до нескольких секунд; сложность и высокая скорость технологического процесса приводят к большим психофизиологическим нагрузкам на оперативный персонал энергопредприятий и органов диспетчерского управления;

3) тесное взаимодействие со всеми отраслями промышленности, связью, транспортом и т.п. и актуальность надежности и резерва мощности во всех элементах ЭС.

Применительно к производству, технике и технологиям в ЭС в теории систем и системном анализе используется широкий спектр категорий, понятий и терминов, из которых наиболее употребимы «сложная система», «большая система» и «техноценоз». Однако применительно к ИЭС категоризацию нельзя считать завершенной.

Более 2 тыс. лет прошло с момента изложения в аристотелевском «Органоне» онтологической «категориальной сетки» субъектов или предикатов суждения (сущность, количество, качество, отношение, пространство, время, состояние, обладание, действие, претерпевание), которую древний мыслитель забросил в безбрежное море когнитивных абстракций человечества, сложив из добытого фундамент логики западного мышления.

Почти 60 лет назад вышла книга «Вещи, свойства и отношения» философа и логика А.И. Уёмова, обосновавшего три «узловые точки сети понятий», путем наложения которой на объективную реальность человек получает возможность отобразить последнюю во всей противоречивой действительности ее организованного бытия [11]. С тех пор понятия вещи, свойства, отношения представляют основные определения движущейся материи, занимают центральное положение в категориальной структуре знания и выполняют особые методологические функции — обеспечения концептуального единства знаний, регулирования и направления процесса познания, организации реального мира как системы вещей.

Прошло около 30 лет с момента появления онтологической инженерии — междисциплинарной отрасли исследований на основе философской онтологии, теории искусственного интеллекта, экспертных систем и баз данных, получившей широкое практическое приложение в индустрии [12].

Онтология, по Р. Мизогучи, — теория концептов или понятий, используемых как элементы для построения информационных систем [13], это вершина системы философского знания, она «гармонизирует», выстраивает в единое пространство, в единую систему различные части этого мира [12].

Появление и широкое применение термина «инженерная онтология» неслучайно, оно обусловлено осознанием того, что одно из самых уязвимых мест проектов интеллектуальных информационных систем – передача прикладной программе необходимых для диалога «оператор – машина» сведений о реальном мире. «Сознательное» построение онтологии предполагает для технических наук некоторый общий взгляд на структуру языковых смыслов, неформальную систематизацию интуитивных представлений общей структуры понятийной системы,

неизбежно выходит за рамки узкопрофессиональных границ, требует философской культуры и целевого использования прикладных умозрительных построений [14].

Построение онтологии знаний, по В.А. Лапшину, — процесс моделирования этих знаний (концептуализации), то есть построения модели мира решаемой задачи [15].

Понятие реальности объекта управления используется в обыденных рассуждениях, в конкретных науках и в философии в различных значениях [16; 24], хотя смысл его прозрачен и вытекает из противопоставления реального иллюзорному. Реально то, что существует независимо от сознания субъекта-оператора.

Реальный (от позднелат. *realis* 'вещественный, действительный') — действительный, существующий в действительности в противоположность вымышленному, воображаемому, фантастическому, ирреальному, существующему только в сознании [17].

Реальность — существующее в действительности; различают объективную реальность (материю) и субъективную (психику, ощущения, восприятия, волю, эмоции и представления), то есть явления сознания [18]. Синонимами являются вещественность, выполнимость, действительность, достижимость, истинность, конкретность, материальность, материя, осуществимость, осязаемость, очевидность, подлинность, предметность, реалия, субстанция, факт, фактичность и явь [19].

Действительность (от «действие») — осуществленная реальность во всей своей совокупности, реальность не только вещей, но и овеществленных идей, целей, идеалов, общественных институтов, общепринятого знания. Понятие «действительность» противоположно понятию «возможность», а не «иллюзия», «фантазия», которые также могут быть осуществлены [20]. Оно тесно связано с понятием «деятельности» — основы категориального отражения мира. Человек-оператор — «предметное существо», действующее «предметным образом». Перерабатывая природу, он создает предметный мир, а природа становится миром человеческой деятельности. Язык формируется в процессе деятельности как предметный, вещный язык, что делает категорию вещи центральной в его категориальной структуре. Понять, то есть объяснить, бытие вещи — значит образовать понятие вещи [21].

Объективный мир (*объективная реальность*), по А.Я. Райбекасу, — мир вещей, попавших в сферу человеческой деятельности [21].

Объект-реальность, по А.Я. Райбекасу, — вещь сама по себе, в действительности своего системного бытия, ставшая объектом человеческой деятельности. Понятие вещи — самое конкретно-всеобщее во всей категориальной структуре знания [21].

Объективная реальность — мир, существующий независимо от субъекта оперативной деятельности (оператора) и его сознания, представление о мире как о внешней (окружающей) реальности, не зависящей от позиции, понимания и восприятия субъекта ОТУ [22; 23]. «Движение, пространство, время, жизнь и т.д. — всё это свойства или проявления свойств и взаимодействий различных по степени сложности видов материи, которые в совокупности и образуют мир в целом или всю объ-

ективную реальность (бытие). Реальность, существование, действительность — более конкретные и глубокие, чем бытие, характеристики объективных процессов и явлений» [23].

Однако категория «объективная реальность» не является исчерпывающей для представления всех видов и форм реальности, в частности для раскрытия форм реальности, изучаемых физикой. Поэтому на стыке физики и философии, в области оснований физики возникло мировоззренческое понятие «физическая реальность». Это понятие имеет объективный статус, но не совпадает с категорией материи, конкретизируется в физических исследованиях.

Физическая реальность — отражение объективной реальности, изучаемое физикой, когнитивный, материально-идеальный объект, содержание которого формируют объективная реальность и человеческий фактор (практика экспериментов и теоретико-конструктивная деятельность). Физическая реальность, в отличие от объективной, включает в себя и черты человеческой деятельности (материальной и идеальной).

Физическая реальность, по Э.М. Чудинову, — «теоретизированный мир», совокупность «теоретизированных» объектов. Понятие физической реальности характеризует объективно-реальный мир не сам по себе, но в том его виде, как он «просматривается» через призму понятий физической теории [23].

Физическая реальность, по А.Я. Райбекасу, — мир эмпирических физических объектов, физических вещей, физических явлений (предметов) [21].

Выделение материального физического мира связано с выделением физических форм движения материи, а отсюда следует необходимость не отождествлять понятия «материя» и «материальный физический мир» и понятия «материальный физический мир» и «физическая реальность».

Материальный физический мир, по А.Я. Райбекасу, — мир естественных физических объект-реальностей, физический мир как таковой (сам по себе). Теоретическое представление материального физического мира — физическая картина мира [21].

Физическая реальность квантовой теории — форма реальности, в которой реальность проявляется в макроприборе, то есть предполагается явное и однозначное указание на экспериментальную установку, с помощью которой получаются результаты, относящиеся к данной физической реальности.

Физическая реальность объекта ОТУ региональной ЭС [25]. Движущийся электрический заряд порождает вокруг себя материальное магнитное поле. Сила, действующая на единичный заряд, принимается за количественную меру поля и называется напряженностью поля. Электрический ток обусловлен созданием и поддержанием напряжения (разности потенциалов) между двумя какими-либо точками, а также наличием проводящей цепи переноса зарядов между этими точками. Разность потенциалов создает электрическое поле, под действием которого в проводниках перемещаются электроны. С ним неразрывно связано электрическое поле, возникающее в результате изменения магнитного поля. Эти два вида материи — компоненты электромагнитных полей, заполняющих пространство вокруг заряженных частиц или за-

ряженных тел. Электрическое поле — самостоятельная физическая реальность, не сводимая ни к тепловым, ни к механическим явлениям [26]. Изменяющиеся во времени электрические и магнитные поля создают единое электромагнитное поле (электромагнитную волну, рис. 3, *а*), главная особенность которого — движение и перенос энергии.

а *б* *в*

Рис. 3. Знаки-изображения основных антропогенных силовых элементов объективной реальности объекта ОТУ в ЭС:
а — абстрактно-математическое представление электромагнитной волны как системы порождающих друг друга и распространяющихся в пространстве переменных электрического и магнитного полей ($\vec{E}$ — напряженность электрического поля; $\vec{B}$ — напряженность магнитного поля; $\vec{v}$ — скорость распространения электромагнитной волны в вакууме); *б* — предметно-изобразительная пиктограмма электромагнитной волны (излучения); *в* — пиктограмма (условное графическое обозначения) трехфазного переменного электрического тока

Начавшееся в одном месте движение зарядов через изменение электрического поля распространяется по всей цепи. Одни за другими все более удаленные носители заряда вовлекаются в движение, и передача действий от одних зарядов к другим происходит со скоростью света. Количественная мера тока — сила тока, физическая величина, равная количеству электричества, проходящему через сечение проводника за единицу времени. Электрон или ион двигаются почти всегда очень медленно, со скоростью меньше 1 мм/с. Следует различать понятия «скорость тока» и «скорость движения носителей заряда». В образной форме можно сказать, что энергию «несет» электромагнитная волна, и мчится она от источника к потребителю в пространстве, окружающем провод, со скоростью света. Провода только направляют поток энергии электромагнитного поля, провода с током — не «трубы» с текущей по ним энергией, а «рельсы» для потока энергии электромагнитного поля. Вместо термина «энергия электромагнитного поля» в физике используют понятие плотности энергии электромагнитного поля в определенной точке пространства.

Основной ток, получаемый генераторами электростанций, преобразуемый, передаваемый и распределяемый потребителям, — переменный ток трехфазной системы электрических цепей, в которых действуют переменные электродвижущей силы (ЭДС) одной и той же частоты, сдвинутые по фазе друг относительно друга на $^1/_3$ периода ($\varphi = 2\pi/3$). Каждую цепь называют фазой, а систему переменных токов — трехфазным током (пиктограмма трехфазного переменного тока изображена на рисунке 4, *в*). Технический ток в Российской Федерации меняет свое направление 100 раз в секунду и имеет частоту 50 Гц.

Объективная реальность объекта ОТУ в ЭС (антропогенные объекты – объекты, созданные человеком для обеспечения его социальных потребностей и не обладающие свойствами природных объектов) может быть специфицирована нижеследующим перечнем основных вещей, попавших в сферу электромеханической человеческой деятельности (рис. 3): основные (силовые) элементы; измерительные элементы — трансформаторы тока и напряжения, предназначенные для подключения измерительных приборов, средств управления и регулирования; средства управления — релейная защита, регуляторы, автоматика, телемеханика и связь.

Например, объективная реальность энергосистемы Калининградской области состоит из западного (60 энергообъектов) и восточного энергорайонов. ОАО «Янтарьэнерго» обслуживает территорию площадью более 15 тыс. км^2, эксплуатирует более 14,7 тыс. км ЛЭП и включает более 4 тыс. подстанций напряжением 60, 110, 330 кВ и суммарной мощностью 3949 МВт [27].

Основными силовыми элементами являются следующие:

1. Электростанции и блок-станции (рис. 2; 4, *а*) — синхронные генераторы, сборные шины, коммутационные аппараты, вспомогательное оборудование измерения, сигнализации, защиты и автоматики. Например, суммарная установленная мощность электростанций ЭС Калининградской области по состоянию на 1 января 2020 г. составляет 1715,628 МВт.

2. Мобильная газотурбинная установка (рис. 4, *б*) — передвижные электростанции с электрической мощностью от 5 до 25 МВт обычно размещаются в городах.

3. Ветроэлектрическая электростанция (рис. 4, *в*) — установка для преобразования кинетической энергии ветрового потока в механическую энергию вращения ротора с последующим ее преобразованием в электрическую энергию (обычно размещаются в сельской местности).

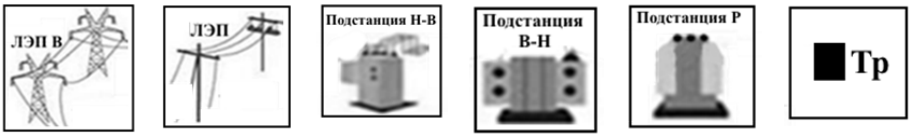
4. Фотоэлектрический преобразователь (рис. 4, *г*) — объект гелиоэнергетики, полупроводниковое устройство, прямо преобразующее солнечную энергию в постоянный электрический ток.

5. Бензиновая переносная электростанция (рис. 4, *д*) — компактные автономные силовые установки для производства электрической энергии, используемые в качестве основного или резервного источника электроснабжения.

а *б* *в* *г* *д*

Рис. 4. Знаки-изображения основных антропогенных силовых элементов объективной реальности объекта ОТУ в ЭС:
а — электростанция, генератор; *б* — мобильная газотурбинная электростанция; *в* — ветроэлектрическая электростанция; *г* — фотоэлектрический преобразователь (бытовой термин — «солнечная батарея», «солнечная панель»); *д* — бензиновая переносная электростанция

6. Кабельные и воздушные ЛЭП (рис. 2; 5, *а*, *б*) — сложные устройства для передачи энергии электромагнитного поля на расстояние, состоящие из многочисленных элементов с разными сроками службы: проводов, траверс, линейных изоляторов, арматуры (линейной, линейно-сцепной), опор, грозозащитных тросов, разрядников (молниезащиты), заземления, секционирующих устройств (пунктов секционирования или реклоузеров), волоконно-оптических линий связи. Во вспомогательное оборудование ЛЭП для нужд эксплуатации входят аппаратура ВЧ-связи, элементы маркировки для безопасных полетов воздушных судов, птицезащитные устройства, устройства плавки гололеда, гасители вибрации. Например, на территории Калининградской области, имеющей максимальную протяженность с востока на запад 205 км, с севера на юг — 108 км, эксплуатируется более 2 тыс. км воздушных ЛЭП напряжением 60—330 кВ, действуют электрические сети напряжением 330 — 110 — 60 — 15 — 10 — 6 кВ. Перечень из 106 ЛЭП напряжением свыше 60 кВ и их сводные данные представлены в [27].



а *б* *в* *г* *д* *е*

Рис. 5. Знаки основных антропогенных силовых элементов объективной реальности объекта ОТУ в ЭС:
а — высоковольтная ЛЭП; *б* — распределительная ЛЭП; *в* — электрическая подстанция «низкое — высокое» напряжения; *г* — электрическая подстанция «высокое — низкое» напряжения; *д* — распределительная электрическая подстанция; *е* — трансформатор

7. Электрические подстанции (центры питания, распределительные пункты, трансформаторные подстанции) (рис. 5, *в* – *д*) — сложные устройства для преобразования и распределения энергии магнитного поля. Термин «подстанция» возник на заре формирования больших сетей, когда каждая подстанция была частью своей электростанции и полностью от нее зависела. Подстанции состоят из многочисленных и, в свою очередь, сложных элементов: силовых трансформаторов (рис. 5, *е*) и автотрансформаторов, измерительных трансформаторов тока и напряжения, фазоповоротных трансформаторов, сборных шин, шинопроводов, коммутационных аппаратов (разъединителей, выключателей, заземлителей, короткозамыкателей, отделителей, дугогасителей, шунтирующих реакторов, ограничителей перенапряжений и предохранителей высоковольтных); устройств релейной защиты и автоматики, измерительных приборов, оборудования ВЧ-связи (конденсаторов связи, ВЧ-заградителей, фильтров присоединения); токоограничивающих, регулирующих устройств; преобразователей частоты, выпрямителей; системы заземления; молниезащитных сооружений; систем вентиляции, кондиционирования, обогрева; системы автопожаротушения; системы освещения территории; охранно-пожарной сигнализации; сис-

темы технологического видеонаблюдения; системы аварийного сбора масла; бытовой и ливневой канализации, водопровода; бытовых помещений; складов и мастерских. Например, первая в Калининградской области подстанция закрытого типа мощностью 50 МВА и напряжением 110 кВ ПС «Береговая», расположенная в Калининграде, существенно (в 5—10 раз) сокращает время оперативных переключений по сравнению с их выполнением сотрудниками оперативно-выездных бригад по голосовым командам оперативно-диспетчерского персонала.

Потребители электроэнергии (рис. 2, 6) сосредоточены «везде и всюду», в городах, поселках, на территории предприятий, на авто- и железных дорогах, газо- и нефтепроводах, в транспортных узлах и терминалах, на космодромах, территориях с ограниченным доступом. Кроме того, силовые элементы ЭС тратят электроэнергию на собственные нужды.

а *б* *в* *г* *д*

Рис. 6. Знаки-изображения основных потребителей электроэнергии объективной реальности объекта ОТУ в ЭС:
а — город со складами электрооборудования для обслуживания электросетевого хозяйства, городские электросети, инфраструктура городского хозяйства, электробытовое оборудование; *б* — поселок, деревня, сельскохозяйственная инфраструктура; *в* — предприятие, организация, испытательные полигоны, космодромы, железная дорога, транспортные магистрали; *г* — источники бесперебойного питания; *д* — установки и оборудование с электродвигателями

Электроприемник — устройство, преобразующее электрическую энергию в другие виды энергии для ее использования и характеризующееся различными параметрами. Режим его работы отражен в индивидуальном графике нагрузки [29].

Достигнув крупного потребителя (завод, населенный пункт), электроэнергия опять попадает на электроподстанцию, трансформируется в напряжение 6—10 кВ и передается по подземным кабелям.

Показательна структура потребления электроэнергии в Калининградской области по видам экономической деятельности за 2018 г.: население — 27,3 %, прочие виды деятельности — 27 %, промышленное производство — 24 %, потери в сетях — 14,2 %, транспорт и хранение — 3,0 %, сельское хозяйство, лесное хозяйство, охота, рыболовство и рыбоводство — 2,8 %, строительство — 1,7 %. Перечень основных крупных потребителей электроэнергии включает 133 предприятия, 12 из которых имеют максимальную мощность от 6,2 до 25 МВт. Максимум потребления мощности энергосистемы Калининградской области в 2019 г. составил 755 МВт [28].

В случае сельского электроснабжения электроэнергия подводится к большому количеству сравнительно маломощных потребителей, рас-

положенных на большой территории, радиальным построением сетей с большой протяженностью линий, применением проводов меньших сечений и трансформаторов меньшей мощности в сравнении с городскими распределительными сетями, что приводит к повышенному расходу электрической мощности и увеличению падения напряжения в сетях низкого напряжения [30].

Стабильное электроснабжение — больная тема для человечества. Аварии в ЭС могут привести к поломкам дорогостоящего оборудования, простоям в производстве, нарушению цепочки поставок, огромным счетам за сорванные сроки работ и за ремонт [31].

С потребителями связано понятие качества электроэнергии, устанавливаемого в РФ ГОСТ 13109-97. В частности, в нем определены следующие «нормы качества электрической энергии в системах электроснабжения общего назначения»: для напряжения (V) номинал 220 V±5 %, предельно 220 V±10 %; для частоты (Hz) номинал 50±0,2, предельно 50±0,4; для искажений (%) номинал 8, предельно 12; для провалов (с) номинал 3, предельно 30; для перенапряжений (V) номинал 280, предельно 380.

Источник бесперебойного питания — техническое средство с не менее чем двумя вводами от первичных источников тока и одним или несколькими выводами, обеспечивающими переход питания нагрузки с одного источника на другой для непрерывного питания потребителей в случае отключения или ухудшения качества электрической энергии на входе от первичного источника.

Качество электроэнергии ухудшают импульсные провалы, вызванные перегрузкой оконечных линий; постоянные провалы, низкое напряжение из-за перегрузки линии от подстанции до потребителя, плохого состояния трансформатора подстанции или соединительных кабелей; полные провалы (блекауты), пропадание напряжения в сети; постоянные перенапряжения, завышенное или циклично завышенное напряжение как следствие «перекоса фаз» — неравномерной нагрузки на разные фазы трансформатора подстанции; временное перенапряжение (импульсное, высокочастотное), возникающее при замыкании фазовых жил силового кабеля друг на друга и на нейтраль, при обрыве нейтрали, при пробое высоковольтной части трансформатора подстанции на низковольтную, при попадании молнии в кабель, подстанцию или рядом с ними [32].

Госдумой принят Федеральный закон №522-ФЗ, регулирующий развитие интеллектуальной системы учета электрической энергии (мощности) — компонентов и устройств для удаленного сбора, обработки, передачи показаний приборов учета электрической энергии.

Итак, мы рассмотрели основные структурные элементы объекта ОТУ в региональной ЭС, в большинстве своем и составляющие багаж когнитивных представлений и знаний об электрических система и сетях. Если провести параллель с объектом ОТУ пилотируемого аппарата гражданской авиации (или, проще, пассажирского самолета — более знакомого и понятного большинству транспортного средства по сравнению с транспортом электроэнергии к потребителю), то выше разговор не коснулся полетной среды, обслуживания летательного аппарата на земле, воздействия на него погодных факторов (температуры, ветра,

дождя, снега, состава атмосферы, магнетизма, грозы и др.), да и в целом он шел о самолетах начала века воздухоплавания — без автопилота, противоаварийной автоматики, средств информатики и вычислительной техники на борту, с плохо оснащенными техникой наземными диспетчерскими центрами, с пилотами и операторами, багаж знаний которых соответствовал своему времени. Восполним существенный пробел и обратимся к онтологической семантике природной среды, человеческого фактора и специального транспорта оперативно-выездных бригад (ОВБ) в объекте ОТУ, приборов и устройств технической электродиагностики, релейной защиты и противоаварийной автоматики, чьи значки-пиктограммы изображены в нижней части фигуры объекта ОТУ на рисунке 2.

Природная среда (природа) — совокупность компонентов природной среды, природных и природно-антропогенных объектов. Компоненты природной среды — земля, недра, почвы, поверхностные и подземные воды, атмосферный воздух, растительный, животный мир и иные организмы, а также озоновый слой атмосферы и околоземное космическое пространство, обеспечивающие в совокупности благоприятные условия для функционирования ЭС.

Природный объект (рис. 7, *а*) — естественная экологическая система, природный ландшафт и составляющие их элементы, сохранившие свои природные свойства.

а *б* *в* *г* *д* *е*

Рис. 7. Знаки-изображения основных элементов объективной реальности актуальных для эффективного и надежного функционирования объекта оперативно-технологического управления в электрических сетях и установках:
а — компоненты природной среды; *б* — оперативно-выездные бригады электромонтеров; *в* — специальный автотранспорт, устройства и оборудование оперативно-выездных бригад; *г* — приборы и устройства технической диагностики состояния электрических сетей и установок; *д* — системы и устройства релейной защиты; *е* — системы и устройства противоаварийной автоматики

Природно-антропогенный объект — природный объект, измененный в результате хозяйственной и иной деятельности, и/или объект, созданный человеком, обладающий свойствами природного объекта и имеющий рекреационное и защитное значение.

Эксплуатация природно-антропогенных ЭС оказывает воздействие на природную среду: при сжигании топлива на тепловых и электростанциях загрязняет воздух, воду и почвы отходами в виде газов, золы, серы и др.; выделяет в окружающую среду неиспользованную энергию в виде теплоты отходящих газов и нагрева охлаждающей воды; влияет посредством электромагнитного поля на живые организмы (гибель

птиц и насекомых, аномалии развития растений) и атмосферу; увеличивает шум; отчуждает из пользования земли и воды; нарушает эстетическую привлекательность среды (ЛЭП). Другой стороной вопроса являются жесткие требования к качеству профессиональных знаний, опыта, умений и навыков электромонтеров, соблюдению ими правил электробезопасности, а также возникающие затруднения со связью, радиопомехи, изрезанный ландшафт местности, отсутствие дорог вдоль ЛЭП, что вынуждает ремонтников-электромонтеров ОВБ в буквальном смысле бегать с грузом, инструментами по полям, лесам и болотам в любое время суток и усложняет исполнение оперативных диспетчерских команд и доклады, заставляют работать в условиях физических нагрузок и стресса.

Человеческий фактор и специальный транспорт оперативно-выездных бригад (рис. 7, *б*, *в*). Оперативно-выездные бригады — команды быстрого реагирования, которые создаются для оперативного обслуживания распределительной сети и состоят, как правило, из двух человек — дежурного электромонтера и электромонтера-водителя. Электромонтеры работают по сменам, в любое время дня и ночи может поступить сигнал об аварийной ситуации. Место базирования ОВБ имеет устойчивую телефонную и радиосвязь с диспетчером районной электросети. ОВБ обеспечивается автотранспортом. Основные ее задачи — определение мест повреждения сетей, их локализация; восстановление электроснабжения потребителей по временной или постоянной схеме; участие в проведении аварийно-восстановительных работ; производство переключений; систематический контроль состояния оборудования электросетей, нагрузок линий электропередачи, трансформаторов, а также показателей качества электроэнергии. Техническое обслуживание ОВБ заключается в обходах и осмотрах воздушных линий, трансформаторных подстанций и секционирующих пунктов, расчистке трасс воздушных линий от кустарников, обрезке ветвей деревьев, устранении мелких неисправностей на линиях и трансформаторных подстанциях. Электромонтеры ОВБ одними из первых прибывают на пожары, отключают электроэнергию, напряжение. Устройства и оборудование ОВБ включают в себя изолирующие штанги (оперативные или универсальные), сигнализаторы напряжения, изолирующие и электроизмерительные клещи и инструмент, диэлектрические перчатки, ковры, изолирующие накладки, боты, изолирующий инструмент, переносные заземления, защитные щитки, очки, каски, плакаты и знаки безопасности, указатель напряжения для проверки совпадения фаз, респираторы, предохранительный пояс.

Приборы и устройства технической диагностики [33] (рис. 7, *г*) представляют собой сложное, зачастую электронное оборудование: многофункциональные цифровые регистраторы, амперметры, вольтметры, вольтамперметры, ваттметры, частотомеры, автоматизированные диагностические устройства, измерители емкости (мосты), рефлектометры, пирометры, мосты переменного тока, газовые хроматографы,

виброанализаторы, электронно-оптическое дефектоскопы, устройства рентгеноскопии изоляторов, летательные аппараты и лаборатории для оценки общего состояния трассы (высота поросли, наличие пожароопасного мусора, строений, состояние пересечений с другими ЛЭП, автодорогами, подтопления, заболоченность, состояние обволовки фундаментных опор), состояния опор (изгибы, поломки, некомплектность), проводов и контактных соединений (общий вид, геометрия положения, локальные перегревы проводов и шлейфов, негабарит шлейфов, местные истирания, нарушение верхнего повива, места перекрытия), арматуры (перекосы и поломки распорок, гасителей вибрации, экранов, зажимов, лодочек, изоляции, тросов и их изоляции), аппаратуры регистрации электромагнитного излучения разрядных процессов. Также используются приборы видеосъемки и цифрового фотографирования, аэросъемки естественного гамма-фона Земли по трассам ЛЭП.

Релейная защита (рис. 8, *д*) — комплекс устройств для быстрого автоматического выявления и отделения от ЭС поврежденных элементов посредством силовых выключателей для обеспечения нормальной работы всей системы. Реле — автоматический аппарат, контролирующий значение какой-либо управляющей физической величины и воздействующий на значение другой, управляемой физической величины [34—39]. Релейная защита — основной вид электрической автоматики, сегодня она оснащена программируемым микроконтроллером.

Противоаварийная автоматика (рис. 7, *е*) — совокупность технических устройств, обеспечивающая измерение и обработку параметров режима ЭС, передачу информации и команд управления и реализацию управляющих воздействий в соответствии с заданными алгоритмами и настройкой, предназначенная для выявления, предотвращения развития и ликвидации аварийного режима ЭС [40]. Она позволяет осуществлять дистанционное управление с удаленного поста (щита, пульта); местное управление от местной кнопки или ключа управления, расположенных вблизи коммутационного аппарата; автоматическое включение через устройство автоматического повторного включения (АПВ).

Устройства защиты ЛЭП: токовые и направленные; от замыкания на землю; трансформаторов напряжения контроля изоляции; дистанционные; дифференциальной токовой продольной и поперечная (балансной); плавкими предохранителями.

Устройства автоматики ЛЭП: АПВ; автоматического включения резерва; автоматической частотной разгрузки; автоматика деления; системная противоаварийная автоматика; автоматические воздушные выключатели и их устройства защиты (расцепители); устройства защитного отключения.

Защита и автоматика элементов электростанций, подстанций и потребителей электроэнергии. Защита синхронных генераторов: релейная защита от замыканий на землю на стороне генераторного напряжения, многофазных замыканий в обмотке статора генератора и на его

выводах, замыканий между витками одной фазы в обмотке статора турбогенератора, внешних коротких замыканий, перегрузки генератора токами обратной последовательности, симметричной перегрузки обмотки статора генератора, перегрузки обмотки ротора генератора током возбуждения, повышения напряжения на статоре генератора, замыканий на землю в одной точке цепи возбуждения; асинхронного режима с потерей возбуждения. Автоматика: автоматические регуляторы частоты вращения турбины; вторичное регулирование частоты и мощности агрегата; устройства группового регулирования мощности; аварийная режимная автоматика специального назначения; автоматика ликвидации асинхронного режима; автоматическое ограничение отклонения частоты и напряжения сверх допустимых пределов. Защита и автоматика подстанций: газовая; токовые и направленные от коротких замыканий; дифференциальные токовые; открытыми плавкими вставками, плавкими и управляемыми предохранителями. Устройства противоаварийной автоматики трансформатора: автоматическое включение резерва и повторное включение; автоматическая аварийная разгрузка, отключение и включение для уменьшения потерь энергии; автоматическое регулирование напряжения. Защита и автоматика конденсаторных установок. Защита и автоматика шин. Токовая защита. Дуговая защита.

В XXI в. наибольшее значение приобретут компьютеры, силовая электроника (транзисторные реле, тиристорные коммутационные аппараты и регуляторы переменного тока) и электропривод. Компьютеры будут выполнять функции «разума», а силовая электроника и электропривод — «мускулов» [41—43].

На объективную реальность объекта ОТУ в электрических сетях и установках сильное влияние оказывают космические, ионосферные и атмосферные воздействия (рис. 8).

Грозовые явления и атмосферные перенапряжения [44] (рис. 8, *а*). Грозовые перенапряжения возникают при разряде молнии в оборудование ЭС или рядом с ним в землю, что приводит к волне напряжений, распространяющейся по линии к подстанциям. Молнии оказывают значительные электромагнитные, термические и механические воздействия на изоляторы ЛЭП при прохождении через них, приводят к авариям и отказам оборудования. На изоляцию электрооборудования воздействует как рабочее напряжение, так и возможные внешние и внутренние перенапряжения, импульсы или волны напряжения, накладывающиеся на номинальное напряжение сети. Грозовые перенапряжения являются наиболее кратными, короткими по времени воздействия и тяжелыми для электроустановок. Например, при прямом ударе молнии в провод воздушной ЛЭП напряжением 110 кВ почти всегда происходит перекрытие изоляции. Даже высокая импульсная прочность линейной изоляции воздушных линий напряжением 500—1150 кВ не может обеспечить грозоупорность линии при прямом ударе молнии в провод. Одна из эффективных защитных мер — применение вентильных разрядников или нелинейных ограничителей перенапряжений.

а *б* *в* *г* *д*

Рис. 8. Знаки-изображения основных космических, ионосферных и атмосферных воздействий на объективную реальность объекта ОТУ в ЭС: *а* — воздействие грозовых атмосферных перенапряжений; *б* — влияние ветра; *в* — влияние гололедно-изморозевых образований; *г* — воздействие геомагнитных бурь; *д* — воздействие аномальной жары

Влияние ветра (рис. 8, *б*). Главная помеха для воздушных ЛЭП — горизонтальная слагающая ветра, давление на провода, тросы и опоры. Кроме того, создавая поперечную нагрузку на провода и тросы, ветер увеличивает их натяжение. Появляются дополнительные изгибающие усилия на опоры, что может вызвать их поломку и падение с вырыванием фундаментов. Вибрации наиболее подвержены провода, расположенные высоко над землей и на открытой ровной местности, где равномерное движение воздушного потока не нарушается рельефом или наземными препятствиями. Вероятность возникновения вибрации растет с увеличением длины пролета более 120 м. Особенно опасна вибрация проводов при переходах через реки и водные пространства с пролетами более 500 м. Опасность вибрации заключается в обрывах отдельных проволок на участках их выходов из зажимов. Пляска проводов, так же как и вибрация, возбуждается ветром, но отличается от вибрации большой амплитудой и длиной волны. При этом колебания проводов отдельных фаз, проводов и тросов происходят несинхронно. Часто провода перемещаются в противоположных направлениях, сближаются и схлестываются, что вызывает значительные динамические усилия в линейной арматуре и в траверсах опор, повреждение линейной арматуры, изоляторов, перекос или сброс распорок, заброс подвесных гирлянд на траверсы [45].

Влияние гололедно-изморозевых образований (рис. 8, *в*) проявляется в отложениях чистого гололеда, инея, зернистой изморози и мокрого снега, а также их сочетаниях. Иней для проводов воздушных линий не представляет существенной нагрузки и не влияет на механическую прочность. Зернистая изморозь способствует закручиванию провода, прочно сцепляется с ним и своими размерами увеличивает парусность провода, что при поперечном ветре приводит к дополнительным нагрузкам на опоры и провода ЛЭП. Ледяная корка плотно сцепляется с проводом воздушной линии. В случае несимметричного образования гололед вызывает закручивание провода, а при большой толщине стенки гололеда его вес может во много раз превысить вес самого провода. Мокрый снег выпадает при плюсовой температуре и оседает на проводах, покрывая их большим слоем. При понижении температуры воздуха в область отрицательных значений, налипший влажный снег замерзает, кристаллизуется и прочно сцепляется с проводами ЛЭП, нагружая их.

Техносферные аварии в периоды геомагнитных бурь (рис. 8, *г*). На подстанциях геомагнитоиндуцированные токи текут в земле через трансформаторные обмотки и по заземлению там, где нет РЗ и ПА. Это активирует опасные эффекты: насыщение трансформаторов, их перегрев и разрушение; генерацию паразитных гармоник переменного тока; нарушение работы стандартных РЗ и, как следствие, отключение ЛЭП; колебания активной и реактивной мощности в энергосистеме и, как следствие, ложное срабатывание либо несрабатывание РЗ и ПА, массовые нарушения электроснабжения в узлах нагрузок. Проявление эффектов ионосферных возмущений (ионосферных токов) нарушает радиосвязь [46].

Аномальная жара (рис. 8, *д*). Воздействие аномальной жары не гарантирует бесперебойного электроснабжения: из-за перегрева оборудование и подстанции выходят из строя, срабатывает РЗ и ПА, неплановo отключаются потребители. В период жары горожане активно используют кондиционеры, в торгово-ресторанном секторе на полную мощность работают холодильные установки, что в разы повышает нагрузку на электросети. Температура воздуха влияет на степень натяжения либо провисания проводов воздушных ЛЭП.

Математическая реальность объекта оперативно-технологического управления региональной интеллектуальной электроэнергетики

И.М. Яглом подчеркивает, что математика предоставляет естественным и гуманитарным наукам адекватный аппарат (язык) описания, классификации и сопоставление фактов и явлений [47]. *Математическая реальность,* по А.И. Панченко, — реальность чисто идеального характера [16].

Уровень зрелости электротехники в значительной мере определяется степенью использования математического аппарата, содержательностью математических моделей. Использование в математическом моделировании геометрического языка и геометрической интуиции сводится к пониманию любых физических, химических, биологических, экономических, социологических и иных систем как точек в пространстве состояний ЭС, а их изменений — как точечных преобразований в рассматриваемом пространстве. Связь математики и жизни опосредована творцами математики — живыми людьми (например, операторами ЭС, разработчиками математических моделей, математиками), неразрывно связанными с окружающим их миром. Математические объекты создаются путем абстрагирования и идеализации. Чтобы формализовать проблему, необходимо «оторвать» ее от жизни, кое-что упростить, чем-то пренебречь, то есть использовать лишь конечное число понятий. При этом все выражено через понятия, имеющие однозначно определенный смысл: слова, величины, отношения и пр. Формула — это совокупность символов (слов, знаков и т.д.), каждому из которых дано четкое определение.

Структура математической модели — это совокупность переменных и параметров, записанных в математическом выражении. Пара-

метры — количественные характеристики внутренних свойств объекта, которые отражаются его структурой, а в математической модели являются коэффициентами, входящими в математическое выражение.

Рассматривая объекты моделирования, часто ограничиваются исследованием физических свойств одного рода: тепловых, электрических, магнитных, механических и т.д. Но в тех случаях, когда в объекте происходит передача или преобразование энергии, требуется учет свойств различного рода, например электромагнитных, теплоэлектрических, тепломеханических, электромеханических и др. Каждое устройство и ЭС в целом могут моделироваться на микро-, макро- и метауровне восприятия человеком окружающего мира.

Рассмотрим модели ЭС на микроуровне [48]. Это распределенные модели (с распределенными параметрами), представленные системами дифференциальных уравнений в частных производных. При их анализе исходят из основных физических законов в их наиболее «чистом», фундаментальном виде (законы сохранения массы, количества движения и энергии), что обеспечивает адекватное описание объектов, протекания процессов и явлений в ЭС.

Начало XIX в. изобиловало захватывающими открытиями в математическом моделировании микроуровневой электродинамики: Х.К. Эрстед показал, что текущий по проводнику ток порождает магнитные эффекты, опыты А. Ампера подтвердили наличие сил притяжения или отталкивания между двумя проводниками с током (еще в XVIII в. И. Ньютон сформулировал закон гравитационного притяжения между любыми двумя материальными телами). М. Фарадей и Д. Генри открыли явление электромагнитной индукции и продемонстрировали связь магнетизма и электричества, Д.К. Максвелл разработал электромагнитную теорию разнообразия свойств электромагнитных полей с помощью величин напряженности электрического и магнитного полей и сформулировал ее в виде системы нескольких уравнений. Исправление, внесенное Максвеллом в известные уравнения электромагнетизма, привело к устранению противоречий и может быть записано системой уравнений для электромагнитного поля в вакууме в интегральной форме [49]:

$$\oint \mathrm{E}d\mathrm{S} = 4\pi \int \rho dV, \tag{1}$$

$$\oint \mathrm{B}d\mathrm{l} = \frac{4\pi}{c} \int \mathrm{j}d\mathrm{S} + \frac{1}{c}\frac{\partial}{\partial t} \int \mathrm{E}d\mathrm{S}, \tag{2}$$

$$\oint \mathrm{B}d\mathrm{S} = 0, \tag{3}$$

$$\oint \mathrm{E}d\mathrm{l} = -\frac{1}{c}\frac{\partial}{\partial t} \int \mathrm{B}d\mathrm{S}, \tag{4}$$

где B — магнитная индукция магнитного поля; ρ — плотность электрического заряда; j — плотность тока; E — напряженность электрического поля; S — площадь произвольной замкнутой поверхности конечных размеров в магнитном поле; V — объем, окруженный замкнутой поверхностью S.

Уравнения Д.К. Максвелла в интегральной форме соотносятся с теми экспериментальными законами, которым они обязаны своим происхождением. Уравнение (1) — теорема К.Ф. Гаусса, которая оказывается справедливой не только для статического, но и для зависящего от времени поля *E* (поток вектора электрической индукции через произвольную замкнутую поверхность равен алгебраической сумме свободных зарядов, находящихся внутри этой поверхности). Уравнение (2) обобщает закон А. Ампера (с добавлением к нему максвелловского тока смещения): циркуляция вектора напряженности электрического поля по произвольному контуру равна алгебраической сумме токов проводимости и токов смещения, охватываемых эти контуром. Уравнение (3), теорема К.Ф. Гаусса для магнитного поля, выражает отсутствие в природе магнитных зарядов (поток вектора магнитной индукции через произвольную замкнутую поверхность равен нулю). Наконец, (4) — закон электромагнитной индукции М. Фарадея: циркуляция вектора напряженности электрического поля по произвольному контуру равна минусу скорости изменения магнитного потока через поверхность, ограниченную этим контуром. Общее следствие из уравнений Максвелла — существование энергии электромагнитного поля.

Теория Д.К. Максвелла — теория близкодействия (в те времена в физике была принята концепция дальнодействия И. Ньютона), то есть электромагнитное взаимодействие происходит с конечной скоростью, равной скорости света. В этой теории решается основная задача электродинамики: по заданному распределению зарядов и токов отыскиваются основные характеристики создаваемых ими электрических и магнитных полей. При проектировании высоковольтной ЛЭП на большие расстояния уравнения Д.К. Максвелла помогают создать систему с минимальными потерями.

Математическое моделирование ЭС системами дифференциальных уравнений в частных производных сталкивается со значительными трудностями: число уравнений в системе может достигать 10^6 и более. Поэтому в ЭС переходят от распределенных параметров к сосредоточенным: выделяют крупные элементы ЭС и их параметры сосредоточивают в одной точке; поле потенциалов представляют величиной одного напряжения, поток электронов моделируется электрическим током и т.п., то есть создают макроуровневые математические модели в дискретных пространствах и непрерывном времени, используя аппарат обыкновенных дифференциальных или интегро-дифференциальных уравнений.

Поведение (состояние) моделируемой ЭС характеризуется фазовыми переменными потенциала (электрическое напряжение) и потока (электрический ток). Такие уравнения называют компонентными. Способ связи элементов ЭС отражается другими, топологическими уравнениями с переменными одного типа — либо потенциала, либо потока. Топологические уравнения выражают законы сохранения, условия непрерывности, равновесия, баланса и т.п. Математические модели объ-

ектов ЭС — совокупность компонентных и топологических уравнений. Основные фазовые переменные ЭС — напряжения и токи в различных элементах систем. Компонентные уравнения элементов имеют вид

$$U = RI, \quad I = C\frac{dI}{dt}, \quad U = L\frac{dI}{dt},$$

где U — напряжение; I — ток; R — сопротивление; C — емкость; L — индуктивность.

При соединении резисторов, емкостей, индуктивностей между собой образуется схема замещения, соединение элементов в которой отражается уже топологическими уравнениями — законами Г. Кирхгофа:

$$\sum_j I_j = 0, \quad \sum_i U_i = 0,$$

где уравнения токов записываются для узлов, а уравнения напряжений — для контуров ЭС. Сложные элементы при их моделировании замещаются схемами из сопротивлений, емкостей и индуктивностей.

Графы и матрицы — модели представления схем и компактной записи уравнений для электрические сетей современных ЭС — насчитывают тысячи ЛЭП и трансформаторов для расчетов режимов [48]. Линии, трансформаторы и другие элементы ЭС представляются в расчетах схемами замещения. Все шины подстанций – узловые точки сети. Графы – топологические модели схем электрических цепей. Графовое представление повторяет изображение схемы, но без элементов электрической цепи. Узлы (вершины графа) соединяются непрерывными линиями (ребрами), на которых при необходимости указывается положительное направление тока или потока мощности. Элементы ЭЭС, которые моделируются ребрами графа (рис. 9), — ЛЭП, трансформаторы, реакторы, батареи конденсаторов и др. Как правило, все они представляются П-образными схемами замещения и поэтому имеют элемент связи между двумя граничными узлами (продольную ветвь) и элементы, связывающие узлы с нейтральной точкой системы N (поперечные ветви).

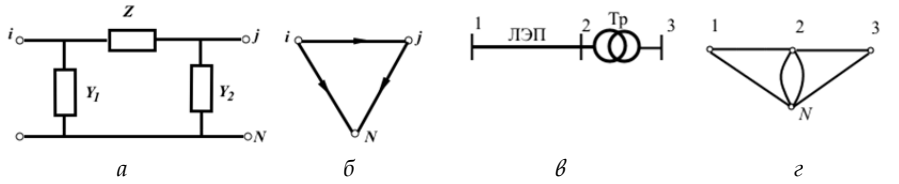


Рис. 9. Моделирование элементов ЭС графами:
а — П-образная схема замещения (имеет продольную ветвь как элемент связи между двумя граничными узлами i и j и поперечные ветви как элементы, связывающие узлы с нейтральной точкой системы N; Z и Y — векторные величины);
б — граф П-образной схемы замещения; *в* — схема замещения электрической сети, состоящей из ЛЭП и трансформатора (две соединенные между собой П-образные схемы замещения); *г* — граф из двух графов П-образных схем

Аналогично представляются схемами замещения электрические нагрузки. Для моделирования топологии схем электрических сетей используют матричные модели, отражающие свойства графов. Это матрицы инциденций и смежности. Каждая продольная ветвь в графе электрической сети характеризуется сопротивлением $Z_j = R_j + jX_j$, а поперечная — проводимостью $Y_i = G_i + jB_i$ ($j = 1,2,...,m$; $i = 1,2,...,n$), где n — количество узлов (шин) схемы сети, m — количество ветвей, соединяющих шины. Значения продольной и поперечной проводимости образуют матрицы параметров электрической сети: матрицу сопротивлений продольных ветвей и матрицу-столбец проводимостей поперечных ветвей — шунтов. Кроме пассивных ветвей в сети существуют активные ветви с источниками ЭДС и тока. Эти ветви, как правило поперечные, моделируют генераторы электростанций и потребителей электрической энергии и представляются матрицами ЭДС (E) и потребителей J.

Эти матрицы задают режим работы электрической сети и представляют собой векторы независимых переменных — режимных параметров. Зависимыми переменными режимных параметров являются напряжения в узлах, токи и напряжения в продольных ветвях и др.; U — матрица напряжений в узлах (узловые напряжения); I — матрица токов ветвей; $U_в$ — матрица напряжений в ветвях (падения напряжения на сопротивлениях ветвей); $S_в^{(н)}$ — матрица потоков мощности в начале ветвей; $S_в^{(к)}$ — матрица потоков мощности в конце ветвей; $S_в$ — матрица потерь мощности в ветвях. Тогда, умножив матрицу соединений на матрицу токов ветвей, имеем соотношение — первый закон Кирхгоффа в матричной записи $M \cdot I = J$. Умножая транспонированную матрицу соединений M^T на матрицу узловых напряжений, получим $\Delta U = M^T \cdot U$, и после преобразований получим $Y \cdot U = J$ — уравнение узловых напряжений (потенциалов) в матричной записи. Матрицу Y называют матрицей узловых проводимостей электрической сети.

Теория автоматического регулирования (ТАР) представляет ЭС и их элементы как динамические системы, процессы в которых описываются дифференциальными уравнениями, взаимосвязывающими значения регулируемых величин со значениями возмущающих и управляющих воздействий.

Впервые математическое определение динамической системы (ДС) было предложено в 1931 г. А. А. Марковым.

Свободная динамическая система — трехэлементное множество $\langle E, T, \Theta \rangle$, где E — пространство состояний (фазовое пространство), T — ось времени, а Θ — движение, представляющее собой отображение $\Theta: E \otimes T \otimes T \to E$, удовлетворяющее трем условиям-аксиомам движения: начальных условий, припасовывания и непрерывности; $\Theta(x_0\ t_0, t)$ — состояние системы в момент времени t, если ее состояние в момент времени t_0 было x_0. Таким образом, $\Theta(x_0\ t_0, t)$ — значение отображения Θ, каждой тройке $\langle x_0\ t_0, t \rangle$ ставящего в соответствие состояние

$y = \Theta(x_0\ t_0, t)$. Если обозначить множество всех троек через $E \otimes T \otimes T$, где $x_0 \in E$, $t_0 \in T$, $t \in T$, то зависимость $\Theta : E \otimes T \otimes T \to E$ состояния от времени называется движением.

Целая траектория, проходящая через точку x_0 пространства состояний E стационарной динамической системы $\langle E, T, \Theta \rangle$, — множество $L(x_0)$ всех состояний, которые проходит ДС в процессе движения Θ_{x_0}, соответствующего начальным условиям x_0, так, что $L(x_0) = \{\Theta(x_0, t) | t \in T\}$. Множество всех целых траекторий — фазовый портрет.

Будем рассматривать движение ДС в n-мерном евклидовом пространстве состояний E и полагать, что функция $\Theta_x : T \to E$ непрерывно дифференцируема по t. Производная $\dot{\Theta}_x$ этой функции по t — $\dot{\Theta}_x(t) = \lim\limits_{\Delta t \to 0} \dfrac{\Theta_x(t) + \Theta_x(t + \Delta t)}{\Delta t}$ называется фазовой скоростью, то есть скоростью изменения состояний. По аксиоме припасовывания $\dot{\Theta}_x(t)$ зависит только от состояния, в котором эта система находится. Фазовую скорость в точке $\boldsymbol{x}$ обозначают обычно $\dot{x}$ и записывают ее зависимость от состояния в виде дифференциального уравнения

$$\dot{x} = \frac{dx}{dt} = f(x). \tag{5}$$

Теоремы существования решений для дифференциальных уравнений определяют условия их единственности и непрерывности зависимости от начальных условий. Если $x(t)$ — частное решение (5), то есть если при подстановке $x(t)$ в правую и левую часть соотношение (5) обращается в тождество, то можно записать $x(t) = \Theta(x_0, t)$, где $\boldsymbol{x}_0 = \boldsymbol{x}(0)$ — начальные условия, однозначно определяющие вид решения.

Управляемая ДС — пятиэлементное множество $\langle E, T, \Theta, U^*, \eta \rangle$, где E — фазовое пространство, T — время, Θ — движение, U^* — множество допустимых законов управления, η — выходное преобразование. При этом должны выполняться следующие условия: η — непрерывная функция, U^* — множество измеримых функций $u : Y \otimes T \to U$, заданных на $Y \otimes T$ и ставящих в соответствие каждому вектору $y \subset Y$ и каждому моменту времени $t \in T$ точку $u(y, t)$ из конечномерного векторного пространства U; движение Θ — непрерывная функция $E \otimes T \otimes T \otimes U^* \to E$, ставящая в соответствие каждому моменту времени t, начальным условиям x_0, взятым в момент времени t_0, и каждому закону управления $u \in U^*$ точку $x(t) = \Theta(x_0, t_0, t, u)$ — состояние ДС в момент времени t. Допустимый закон управления $u \in U^*$ называется управлением: временным, программным, без обратной связи, если u не зависит от выходного сигнала y.

В зачаточном виде многие положения ТАР содержатся в общей теории линейных регуляторов Д.К. Максвелла и И.А. Вышнеградского (1868—1876). Параллельно с А. Пуанкаре А.М. Ляпунов создал теорию устойчивости движения и заложил основы качественной теории дифференциальных уравнений. Одна из первых в мире книг по автоматическому управлению вышла в 1938 г. — «Автоматическое управление электрическими установками и системами» Б.И. Доманского. В 1963 г. А.А. Вавилов и А.И. Солодовников публикуют работу «Экспериментальное определение частотных характеристик автоматических систем». К началу XXI в. появились методы структур и алгоритмов ТАР в трудах В.Н. Антонова, В.А. Терехова, И.Ю. Тюкина, И.В. Мирошника, В.О. Никифорова, А.Л. Фрадкова, А.А. Воронова, Я.З. Цыпкина, Л.А. Растригина, В.В. Солодовникова, А.Г. Ивахненко и др. В.А. Терехов и И.Ю. Тюкин с начала XXI в. развивают идеи и методы построения систем ТАР с обучаемыми многослойными нейронными сетями, выполняющими функцию адаптивного регулятора. Вскоре пришло понимание, что традиционные технологии уже не могут обеспечить повышение качества управления ЭС, поскольку не учитывают всех неопределенностей, воздействующих на систему, и уже в 2001 г. были опубликованы результаты разработки интеллектуальных систем автоматического управления [50]. Значительный вклад в автоматику ЭС внесли работы [51; 52].

Гибридная система (ГС) — записанная на математическом языке комбинация двух автономных методов, один из которых имеет преимущества в моделировании непрерывных процессов, а другой — дискретных. Подробный анализ ГС дан в [53]. Состояние ГС представляется вектором двух переменных — непрерывной и дискретной. Непрерывная динамика ГС в непрерывном, дискретном и/или смешанном времени задается обычно дифференциальными уравнениями, а дискретная управляется цифровым автоматом или передаточной функцией с конечным количеством состояний. Оба процесса, непрерывный и дискретный, взаимодействуют в моменты возникновения «событий» или «переключений», когда очередное состояние достигает некоторых заданных множеств в непрерывном пространстве состояний. Иными словами, ГС — это индексированная совокупность динамических систем и таблица «скачков» между ними.

Гибридная природа таких систем, например автоматики с реле, ключами и гистерезисом, контроллеров перемещения, роботов, гибких производственных систем, автопилотов определяется непрерывно-дискретным характером их поведения, для описания которого недостаточно аналитических знаний в виде дифференциальных уравнений и необходимо комбинировать их со знаниями из дискретной математики, математической статистики и логики. Например, в [54] предложена управляемая событиями, последовательная, детерминированная модель, включающая объект, цифровой управляющий автомат и интерфейсы (аналого-цифровой — *AD* и цифро-аналоговый — *DA*) и изображенная на рисунке 10.

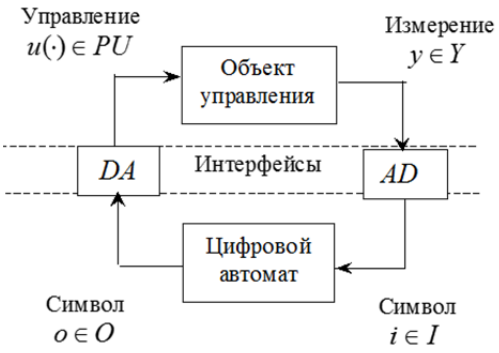


Рис. 10. Гибридная система

Источник: [55].

В H_{NK}-гибридной системе объект управления описывается как $\dot{x} = f(x(t)),\ u(t),\ y(t) = h(x(t)),$ где $x(t) \in X \subset \Re^n$, $u(t) \in U \subset \Re^m$, $y \in Y \subset \Re^p$, $f : \Re^n \otimes \Re^n \to \Re^n$, а $h : \Re^n \to \Re^p$, и представляется конечным автоматом, состояние которого принадлежит $\Re^n$. Входной алфавит — множество пар $(u(\cdot), \delta_k)$, где δ_k — положительный скаляр, задающий время до следующего события, а $u(\cdot)$ — элемент множества U^w кусочно-непрерывных функций в $U^{[0,\infty)}$.

Предположим, что объект управления находится в состоянии x_k в момент времени t_k. Тогда «очередное состояние» вычисляется в соответствии с функцией переходов с учетом текущего состояния и символа $(u(\cdot), \delta_k)$ на входе следующим образом: $x_{k+1} = x(t_k + \delta_k)$, где $x(\cdot)$ — решение уравнения $\dot{x}(t) = f(x(t), u(t - t_k)),\quad x(t_k) = t_k$ на интервале $[t_k, t_k + \delta_k]$. После вычисления $x_{k+1} = t_k + \delta_k$ процесс продолжается. Цифровой управляющий автомат — конечный символьный автомат (Q, I, O, v, h), где Q — пространство состояний, I — входной алфавит, O — выходной алфавит (Q, I, O — изоморфные подмножества натуральных чисел), $v : Q \otimes I \to Q,\ \ h : Q \otimes I \to O.$

Оба автомата объединяются с помощью интерфейса, то есть отображений $AD : Y \otimes Q \to I$ и $DA : O \to PU,$ где PU для кусочно-непрерывного U обозначает конечное множество.

Динамика ГС похожа на модель [55]. Однако появляются новые элементы: во-первых, вход и выход как для объекта управления, так и для управляющего автомата и, во-вторых, отображения AD и DA. В итоге имеем:

$$\dot{x}(t) = f[x(t), DA(o(t))(t - [t])],\ \ y(t) = h[x(t)], \tag{6}$$

$$q(t) = v[q(t^-), AD(y(t), q(t^-))],\quad o(t) = \eta[q(t), AD(y(t), q(t^-))], \tag{7}$$

где $q(t^-)$ — левый предел функции q в момент t; $[t]$ — момент времени, меньший или равный t, в который произошли скачок или событие.

Комбинированная динамика модели следующая. Непрерывное состояние x изменяется в соответствии с (6), а дискретное состояние q — по (7). Затем $AD(\cdot, q)$ присваивается выходу $y(t)$ — символу из I. Когда этот символ изменится, то есть управляющий автомат выполнит переход в новое состояние, то его выходной символ $o \in O$ также изменится. Связанное с этим символом управление $DA(o)$ рассматривается как входной параметр дифференциального уравнения до тех пор, пока входной символ управляющего автомата опять не изменится.

Оценка соотношений математики и реальности дана, например В.Я. Перминовым [56]. В частности, по его мысли, развитие математики в XVII, XVIII и в особенности в XIX в. убедительно продемонстрировало тот факт, что математические понятия непосредственно не соотносятся с реальностью. Уже Лейбниц осознавал, что математические понятия скорее конструируются самим разумом, чем извлекаются из опыта абстрагированием. В математике нет места для представлений опыта: математические понятия — либо априорные представления, либо логические конструкции. Разрыв между математикой и реальностью аргументируется существованием природных связей, в принципе не допускающих математического описания. Хорошо согласовываясь с механикой и другими физическими науками, где выполняется принцип аддитивности, математика остановилась перед онтологическим барьером законов биологии, социологии и других системных и гуманитарных наук, где такой принцип нарушается в соединении элементов, что и определило принципиальный предел продвижения к математическому описанию реальности.

Логика синтеза математических понятий входит в неустранимое противоречие с реальным синтезом, протекающим в объекте исследования большой сложности. Математический метод перспективен при описании неживой материи, то есть тех сфер реальности, в которых преобладает аддитивный синтез систем, но он не может быть ведущим для сфер реальности, основанных на системности, и целевых воззрений на мир. Как полагает В.Я. Перминов, есть все основания утверждать, что сложные явления природы, связанные с системностью и неаддитивностью, никогда не будут объясняться в теориях, подобных теориям математической физики. Математическая реальность должна быть понята как специфический организм, приспособляющийся к своей естественной среде — к системе содержательных понятий.

Заключение

Рассмотрены основные результаты исследования системы оперативно-технологического управления региональной электроэнергетической системы, а также категоризация онтологической семантики объективной реальности объекта ОТУ региональной ЭС как «сложной системы», «большой системы» и «техноценоза», функционирующих в «аг-

рессивных» условиях внешней среды. Особое внимание обращено на специфику человеческого фактора, наличие систем релейной защиты и противоаварийной автоматики в объекте ОТУ, которые значительно повышают степень уверенности в том, что конечный потребитель получает качественную электроэнергию благодаря результатам электротехники, автоматического регулирования и деятельности оперативно-выездных бригад.

Рассмотрена математическая реальность мира оперативно-технологической деятельности: от представлений теории электродинамики Д. К. Максвелла, аппарата динамических и гибридных систем до средств интеллектуальных систем автоматического управления. Дана оценка соотношений математики и реальности, показывающая, что логика синтеза математических понятий входит в неустранимое противоречие с реальным синтезом, протекающим в объекте ОТУ ЭС большой сложности и высокой динамичности.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-07-00208.

Список литературы

1. *Козлов В. В., Донченко И. А.* Направленные визуализации: теория и метод. Запорожье, 2015.

2. *О развитии* искусственного интеллекта в Российской Федерации и Национальная стратегия развития искусственного интеллекта на период до 2030 г. [Электрон. ресурс] : указ Президента Российской Федерации № 490 от 10 октября 2019 г. Доступ из справ.-правовой системы «КонсультантПлюс».

3. *Зеленохат Н. И.* Интеллектуализация ЕЭС России: инновационные предложения : практ. пособие. М., 2013.

4. *Концепция* интеллектуальной электроэнергетической системы с активно-адаптивной сетью / ОАО «Федеральная сетевая компания Единой Электроэнергетической системы». М., 2012.

5. *Дружинин Г. В.* Человек в моделях технологий : учеб. пособие : в 3 ч. Ч. 1 : Свойства человека в технологических системах. М., 1996.

6. *Магид С. И.* Подготовка персонала энергопредприятий: о целесообразности использования «Компьютерных тренажеров» // Энергетика и промышленность России. 2002. № 11 (27).

7. *Дружилов С. А.* Формирование модели мира человека в новой информационной реальности // Психология, социология и педагогика. 2011. № 1. URL: http://psychology.snauka.ru/2011/10/15 (дата обращения: 02.01.2019).

8. *Гейзенберг В.* Шаги за горизонт / сост. А. В. Ахутин ; общ. ред. и вступ. ст. Н. Ф. Овчинникова. М., 1987.

9. *Малявин В. В.* Чжуан-цзы. М., 1985.

10. *Об электроэнергеетике* [Электрон. ресурс] : федер. закон № 35-ФЗ от 26.03.2003 г. (ред. от 27.12.2019 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

11. *Уёмов А. И.* Вещи, свойства, отношения. М., 1963.

12. *Заковоротная М. В.* Онтологическая инженерия, философская онтология: проблемы и перспективы // Научная мысль Кавказа. 2013. № 2. С. 13—20.

13. *Mizoguchi R.* Tutotial on Ontological Engineering: Part 1: Introduction to Ontological Engineering // New Generation Computing. 2003. Vol. 21 (4). P. 365—384.

14. *Рубашкин В.Ш.* Онтологическая семантика. Знания. Онтологии. Онтологически ориентированные методы информационного анализа текстов. М., 2013.

15. *Лапшин В.А.* Онтологии в компьютерных системах. М., 2010.

16. *Панченко А.И.* Философия, физика, микромир. М., 1988.

17. *Ивина А.А.* Философия : энцикл. словарь М., 2004.

18. *Большой* Российский энциклопедический словарь. М., 2009.

19. *Мудрова А.Ю.* Словарь синонимов русского языка. М., 2009.

20. *Жуковский В.И.* Теория изобразительного искусства. СПб., 2011.

21. *Райбекас А.Я.* Вещь, свойство, отношение как философские категории. Томск, 1977.

22. *Smith B.* Constraints on Correspondence // Traditionen und Perspektiven der analytischen Philosophie / eds. H. Rutte, W. Sauer, W. Gombocz. Vienna, 1989. P. 415—430.

23. *Фролова И.Т.* Философский словарь. 7-е изд., перераб. и доп. М., 2001.

24. *Чудинов Э.М.* Природа научной истины. М., 1977.

25. *Жилейко Г.И.* Техническая электродинамика. М., 1994.

26. *Элементарный* учебник физики : в 3 т. / под ред. Г.С. Ландсберга. Т. 2 : Электричество и магнетизм. М., 2001.

27. *Янтарьэнергосбыт* к 2023 г вложит более 1 млрд руб. в установку «умных» счетчиков в многоэтажках Калининградской области // Интерфакс. 2020. URL: https://www.interfax-russia.ru/northwest/news/ (дата обращения: 14.10.2020).

28. *Схема* и программа перспективного развития электроэнергетики Калининградской области на 2021—2025 годы // Правительство Калининградской области : [офиц. сайт]. URL: https://infrastruktura.gov39.ru/upload/165P_3004 2020.pdf (дата обращения: 14.10.2020).

29. *Карманова Т.Е.* Приемники и потребители электрической энергии систем электроснабжения : учеб. пособие. Архангельск, 2015.

30. *Ханин Ю.И.* Повышение эффективности электропередачи в сельских сетях 0,38 кВ с коммунально-бытовой нагрузкой посредством компенсации неактивных составляющих полной мощности : дис. … канд. техн. наук. Зерноград, 2017.

31. *Убытки*, поломки, простои: последствия аварийного отключения электричества и способы их нивелировать // Хабр : [сайт]. URL: https://habr.com/ru/company/eaton/blog/514856/ (дата обращения: 14.10.2020).

32. *Данилин А.* Негативные явления в электросети - их влияние на нагрузку и способы борьбы // iXBT.com : [инф.-аналит. сайт]. URL: https://www.ixbt.com/power/ups/electric_power.shtml (дата обращения: 14.10.2020).

33. *Михеев Г.М.* Электростанции и электрические сети. Диагностика и контроль электрооборудования. М., 2010.

34. *Федосеев А.М., Федосеев М.А.* Релейная защита электроэнергетических систем : учебник для вузов. 2-е изд., перераб. и доп. М., 1992.

35. *Федоров В.А.* Библия релейной защиты и автоматики. Новосибирск, 2014.

36. *Андреев В.А.* Релейная защита и автоматика систем электроснабжения : учебник для вузов. 3-е изд., перераб. и доп. М., 1991.

37. *Автоматика* энергосистем : учеб. пособие / Ю.С. Боровиков, А.С. Гусев, М.В. Андреев, А.О. Сулайманов. Томск, 2015.

38. *Автоматика* электроэнергетических систем : учеб. пособие для вузов / О.П. Алексеев, В.Е. Казанский, В.Л. Козис. М., 1981.

39. *Павлов Г.М., Меркурьев Г.В.* Автоматика энергосистем. СПб., 2001.

40. *Автоматическое* противоаварийное управление режимами энергосистем. Противоаварийная автоматика энергосистем. Условия организации процесса. Условия создания объекта. Нормы и требования : стандарт ОАО «СО ЕЭС». URL: http://so-ups.ru/fileadmin/files/laws/standards/sto_emerg_control_2011_izm_2014.pdf (дата обращения: 17.10.2020).

41. *Белов М.П., Новиков В.А., Рассудов Л.Н.* Автоматизированный электропривод типовых производственных механизмов и технологических комплексов. М., 2004.

42. *Розанов Ю.К., Лепанов М.Г.* Силовая электроника : учебник и практикум. М., 2019.

43. *Исследование* электронных коммутационных аппаратов и регуляторов : учеб.-метод. пособие / В.И. Лузгин, С.Ю. Кропотухин, А.С. Коптяков, Д.А. Глушков. Екатеринбург, 2017.

44. *Малахова Т.Ф., Захаренко С.Г., Захаров С.А.* Грозовые явления и защита систем электроснабжения от атмосферных перенапряжений // Вестник Кузбасского государственного технического университета. 2017. №4. С. 110—116.

45. *Крюков К.П., Новгородцев Б.П.* Конструкции и механический расчет линий электропередачи : учебник. Ленинград, 1979.

46. *Авакян С.В., Воронин Н.А., Дубаренко К.А.* Влияние магнитных бурь на аварийность систем электроэнергетики, автоматики и связи // Научно-технические ведомости СПбГПУ. 2012. №3 (154), ч. 2. С. 253—266.

47. *Яглом И.М.* Математика и реальный мир. М., 1978.

48. *Лыкин А.В.* Математическое моделирование электрических систем и их элементов : учеб. пособие. 2-е изд., перераб. и доп. Новосибирск, 2009.

49. *Мамро С.И., Фролов М.В.* Лекции по электродинамике : учеб. пособие для вузов. Ч. 1. Воронеж, 2007.

50. *Макарова И.М., Лохин В.М.* Интеллектуальные системы автоматического управления. М., 2001.

51. *Козис В.Л., Овчаренко Н.И.* Автоматика электроэнергетических систем : учеб. пособие для вузов М., 1981.

52. *Павлов Г.М., Меркурьев Г.В.* Автоматика энергосистем. СПб., 2001.

53. *Колесников А.В.* Гибридные интеллектуальные системы. Теория и технология разработки / под ред. А.М. Яшина. СПб., 2001.

54. *Nerode A., Kohn W.* Models for Hybrid Systems: Automata, Topologies, Stability // Technical Report 93-11. Cornell University, 1993.

55. *Tavernini L.* Differential Automata and their discrete simulators // Nonlinear Analysis, Theory, Methods, and Applications. 1987. Vol. 11 (6). P. 665—683.

56. *Перминов В.Я.* Математика и реальность: Гносеологические проблемы математизации знания // Вестник МГУ. Сер. 7: Философия. 2014. №1. С. 42—68.

Об авторах

Александр Васильевич Колесников — д-р техн. наук, проф., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: avkolesnikov@yandex.ru

София Борисовна Румовская — канд. техн. наук, науч. сотр., Калининградский филиал Федерального исследовательского центра «Информатика и управление», Россия.
E-mail: sophiyabr@gmail.com

Эрик Викторович Ясинский — асп., Балтийский федеральный университет им. И. Канта; ведущий разработчик, ООО «Роуттех», Россия.
E-mail: ejasinski96@gmail.com

Сергей Александрович Солдатов — канд. техн. наук, ведущий разработчик ООО МТС ИТ, Россия.
E-mail: ssacompany@mail.ru

The authors

Prof. Alexander V. Kolesnikov, Immanuel Kant Baltic Federal University, Russia.
E-mail: avkolesnikov@yandex.ru

Dr Sophiya B. Rumovskaya, Research Fellow, Kaliningrad branch of the FRC «Computer Science and Control» of the RAS, Russia.
E-mail: sophiyabr@gmail.com

Eric V. Jasinski, PhD Student, Immanuel Kant Baltic Federal University, Lead Developer, Ltd «Routtech», Russia.
E-mail: ejasinski96@gmail.com

Dr Sergei A. Soldatov, Lead Developer, «MTS IT», Russia.
E-mail: ssacompany@mail.ru

УДК 621.396.677

Е. В. Волхонская, Е. В. Коротей, К. В. Власова

МОДЕЛЬНЫЕ ИССЛЕДОВАНИЯ НАПРАВЛЕННЫХ СВОЙСТВ ОДНОЗЕРКАЛЬНОЙ АНТЕННЫ С ДВУХДИАПАЗОННЫМ ЛОГОПЕРИОДИЧЕСКИМ ОБЛУЧАТЕЛЕМ В СРЕДЕ MathCAD

Приведены результаты оптимизации геометрических параметров однозеркальной антенны с двухдиапазонным логопериодическим облучателем и исследования ее диапазонных свойств в среде MathCAD. Использованная авторами модель поля излучения зеркальной антенны построена на базе методов поверхностных токов и наведенных ЭДС, а также теории цепей с распределенными параметрами. Результаты исследований показали адекватность построенной модели и соответствие направленных свойств зеркальной антенны предъявляемым к ним требованиям.

The results of single-mirror antenna with a dual-band log-periodic irradiator geometric parameters optimization and model researches of it's range properties in MathCAD are presented in this article. The model of the mirror antenna radiation field used by the authors is based on the base of the surface currents method, the method of induced EMFs and theory of electric circuits with distributed parameters. The results of the research showed the adequacy of the constructed model and the compliance of the directional properties of the mirror antenna with the requirements imposed on them.

Ключевые слова: зеркальная антенна, логопериодическая антенна, двухдиапазонный облучатель, характеристики излучения.

Keywords: mirrorantenna, log-periodic antenna, dual-band irradiator, radiation characteristics.

Введение

Развитие телекоммуникационных технологий приводит к непрерывному расширению спектра предоставляемых услуг в области передачи голосовых сообщений и данных, доступа в интернет, телевизионного вещания, навигационных услуг и прочего. По состоянию на 2019 г. на геостационарной орбите было задействовано 379 активных спутников связи, имеющих транспондеры, функционирующие в диапазонах L, S, C, X, Ku и Ka. В 2020—2022 гг. запланирован ввод в эксплуатацию еще 28 спутников [1].

Увеличение числа спутников-ретрансляторов приводит к необходимости решать задачу пространственного разделения данных источников сигналов, а значит, к необходимости уменьшения ширины диаграммы направленности антенны по мере перехода на более высокочастотные диапазоны Ku и Ka [2].

© Волхонская Е. В., Коротей Е. В., Власова К. В., 2020
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 88 – 95.

Порядка 10 % всех активных спутников-ретрансляторов одновременно функционируют в нескольких частотных диапазонах. Необходимость одновременного приема сигналов нескольких частотных диапазонов делает актуальной задачу синтеза многодиапазонных облучателей зеркальных антенн. Традиционные облучатели зеркальных антенн представляют собой рупорные или логопериодические антенны. Проведенный анализ технических решений таких облучателей показал, что совмещение нескольких частотных диапазонов в рамках единой конструкции, как правило, приводит либо к серьезному усложнению конструкции [3], либо к непостоянству направленных свойств [4].

Конструкция облучателя

В рамках проводимой авторами статьи НИОКР «Разработка электродинамических моделей облучателей больших зеркальных антенн в составе системы ГМССБ для исследования качества решения задач спутниковой радиосвязи и радионавигации» была предложена конструкция логопериодической антенны, функционирующей в смежных диапазонах частот С и Х (рис. 1). Прототипом конструкции данной антенны послужила микрополосковая логопериодическая антенна С-диапазона [5].

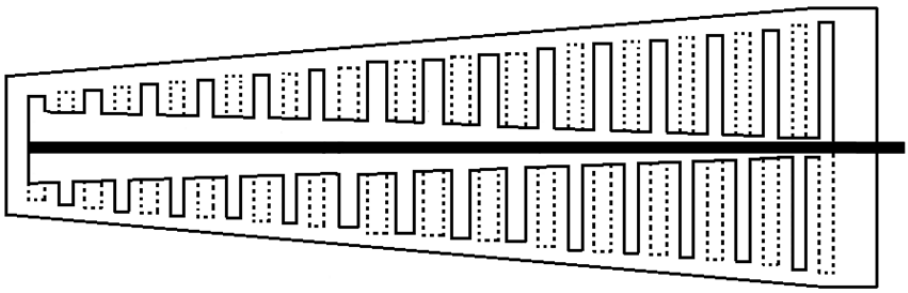


Рис. 1. Конструктивное исполнение двухдиапазонного логопериодического облучателя, функционирующего в С и Х диапазонах

Конструкция такого облучателя была оптимизирована с применением алгоритма, реализованного в работе [6]. Исследование направленных свойств и электрических параметров данной антенны показало относительную стабильность характеристик в пределах всего рабочего диапазона частот. Ниже, на рисунках 2 и 3, приведены диаграмма направленности (ДН) и частотные зависимости активной и реактивной составляющих входного сопротивления, коэффициента стоячей волны (КСВ) в коаксиальном фидере, ширины ДН антенны, максимального относительного уровня боковых лепестков (УБЛ) ДН и коэффициента направленного действия (КНД) антенны в двух главных плоскостях.

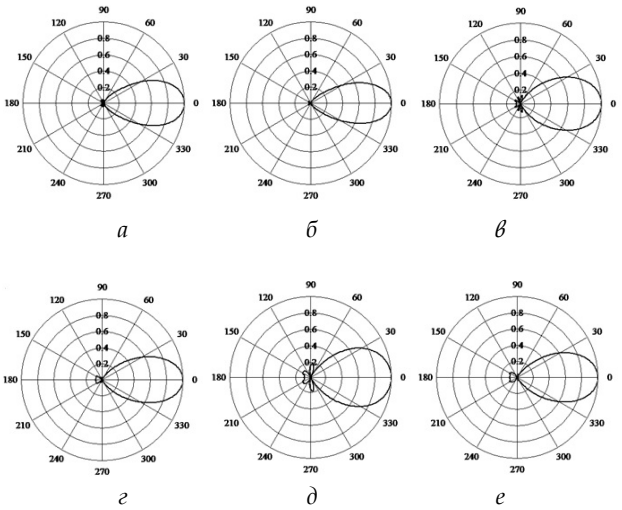


Рис. 2. Нормированная ДН логопериодического облучателя для рабочих частот 5,721 ГГц (*а*, *б*), 7,185 ГГц (*в*, *г*) и 8,364 ГГц (*д*, *е*) в плоскостях, содержащей излучающие элементы (*а*, *в*, *д*) и перпендикулярной им (*б*, *г*, *е*)

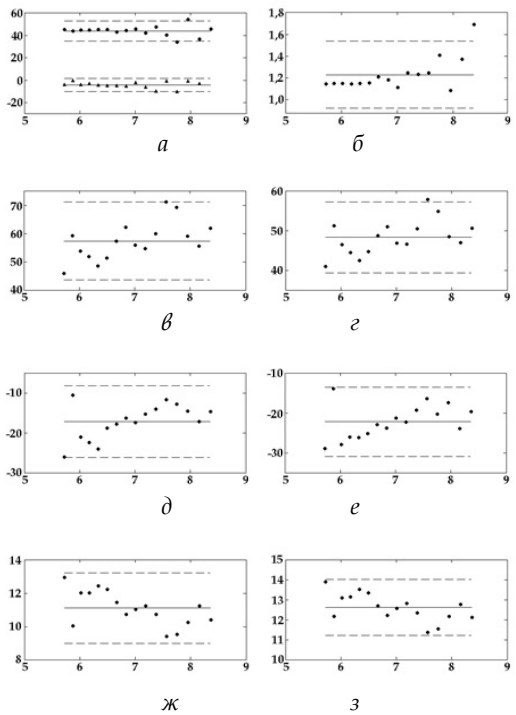


Рис. 3. Частотные зависимости активной и реактивной частей входного сопротивления, Ом (*а*), КСВ в питающем фидере (*б*), ширины ДН, градусы (*в*, *г*), максимального относительного УБЛ, дБ (*д*, *е*) и КНД, дБи (*ж*, *з*) в плоскости, содержащей элементы антенны (*в*, *д*, *ж*) и перпендикулярной им (*г*, *е*, *з*). По оси абсцисс отложены значения рабочей частоты в ГГц

Оптимизация конструкции зеркальной антенны

В работе проведена оптимизация конструктивных параметров однозеркальной антенны с выбранным двухдиапазонным логопериодическим облучателем в соответствии с процедурой оптимизации, описанной в работе [7].

В качестве оптимизируемых конструктивных параметров были выбраны радиус раскрыва зеркала (рефлектора) и его фокусное расстояние. В качестве исходных данных выбраны:

1) диапазон изменения радиуса рефлектора — от 1 до 4 м;

2) диапазон изменения фокусного расстояния рефлектора — от 2 до 6 м;

3) рабочая частота f = 8,364 ГГц.

Результаты исследования направленных свойств однозеркальной антенны при изменении фокусного расстояния зеркала приведены в таблице 1.

Таблица 1

Результаты оптимизации фокусного расстояния зеркала при R_0 = 3 м

f_0, м	$\Delta\theta_{0,707}$, градусов	ξ, дБ	D, дБи	$\nu\cdot\chi$
2	0,433	– 27,121	47,803	0,203
2,5	0,404	– 26,600	48,226	0,221
3	0,389	– 23,522	48,424	0,234
3,5	0,378	– 21,921	48,652	0,237
4	0,372	– 20,844	48,766	0,232
4,5	0,368	– 20,096	48,848	0,214
5	0,364	– 19,594	48,907	0,207
5,5	0,362	– 19,237	48,953	0,186
6	0,360	– 18,975	48,988	0,175

В соответствии с процедурой оптимизации, изложенной в [7], было выбрано оптимальное фокусное расстояние f_0 = 3,5 м, соответствующее наибольшему значению произведения коэффициента использования поверхности (КИП) рефлектора ν на эффективность облучения рефлектора χ, которые определяются выражениями вида

$$\nu = \left(\frac{\lambda}{2\pi R_0} \right)^2 \cdot D \,, \tag{1}$$

где λ — рабочая длина волны, м; R_0 — радиус раскрыва рефлектора, м; D — коэффициент направленного действия (КНД) зеркала, дБи;

$$D = \frac{4\pi}{\int\limits_0^{2\pi}\int\limits_0^{\pi} \left|F(\theta,\varphi)\right|^2 \sin(\theta)\, d\theta d\varphi}, \tag{2}$$

где $F(\theta, \varphi)$ — нормированная пространственная амплитудная характеристика направленности зеркальной антенны; (θ,φ) — сферические углы в системе координат, совмещенных с фокусом рефлектора;

$$\chi = \frac{\int_0^{2\pi}\int_0^{\theta_{\max}} \left|F(\theta,\varphi)\right|^2 \sin(\theta)\, d\theta d\varphi}{\int_0^{2\pi}\int_0^{\pi} \left|F(\theta,\varphi)\right|^2 \sin(\theta)\, d\theta d\varphi}, \quad (3)$$

где $\theta_{\max}$ — угол, под которым видна кромка рефлектора из фокуса.

Результаты исследования направленных свойств однозеркальной антенны при изменении радиуса раскрыва зеркала при оптимальном фокусном расстоянии приведены в таблице 2.

В соответствии с аналогичным критерием был выбран оптимальный радиус раскрыва рефлектора $R_0 = 1{,}75$ м.

Таблица 2

Результаты оптимизации радиуса раскрыва зеркала при $f_0 = 3{,}5$ м

R_0, м	$\Delta\theta_{0{,}707}$, градусов	ξ, дБ	D, дБи	$\nu\cdot\chi$
1	1,061	–18,024	44,959	0,264
1,25	0,853	–18,290	46,881	0,364
1,5	0,716	–18,620	48,448	0,467
1,7	0,635	–18,885	49,521	0,567
1,75	0,617	–18,969	49,768	0,615
1,8	0,601	–19,085	49,992	0,612
2	0,545	–19,402	49,144	0,466
2,5	0,444	–20,564	48,243	0,287
3	0,378	–21,921	48,652	0,237
3,5	0,332	–23,653	49,249	0,205
4	0,299	–25,635	48,840	0,143

Модельные исследования

На последнем этапе работы проведены модельные исследования направленных свойств зеркальной антенны в пределах рабочего диапазона частот облучателя, охватывающего С- и Х-диапазоны.

Результаты исследования направленных свойств однозеркальной антенны при изменении рабочей частоты при оптимальных фокусном расстоянии и радиусе раскрыва приведены в таблице 3.

Таблица 3

Частотная зависимость параметров излучения зеркальной антенны с параметрами $R_0 = 1{,}75$ м, $f_0 = 3{,}5$ м

f, ГГц	$\Delta\theta_{0{,}707}$, градусов	ξ, дБ	D, дБи	χ
5,721	0,901	–18,875	46,482	0,804
5,868	0,881	–19,020	46,694	0,596
6,018	0,856	–18,836	46,922	0,760
6,173	0,836	–18,888	47,139	0,731
6,331	0,815	–18,912	47,356	0,763
6,493	0,795	–18,900	47,577	0,770

Окончание табл. 3

f, ГГц	$\Delta\theta_{0,707}$, градусов	ξ, дБ	D, дБи	χ
6,660	0,775	–18,909	47,796	0,715
6,831	0,756	–18,946	48,013	0,642
7,006	0,739	–19,077	48,227	0,642
7,185	0,719	–18,976	48,451	0,673
7,370	0,701	–18,974	48,670	0,652
7,559	0,685	–19,105	48,882	0,559
7,752	0,666	–18,984	49,109	0,549
7,951	0,650	–18,998	49,329	0,575
8,155	0,635	–19,068	49,544	0,675
8,364	0,617	–18,969	49,768	0,609

В соответствии с полученными результатами построены частотные зависимости ширины ДН, максимального относительного УБЛ, КНД и эффективности облучения рефлектора. Эти зависимости приведены на рисунке 4, где точками отмечены модельные результаты, а сплошными линиями — критические значения данных параметров, рассчитанные в соответствии с требованиями, предъявляемыми к характеристикам зеркальных антенн земных станций спутниковой связи [8].

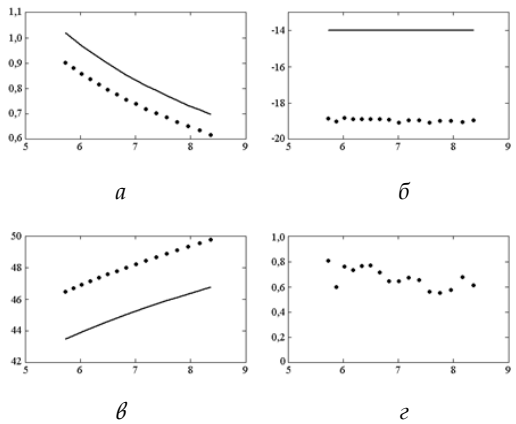


Рис. 4. Частотные зависимости:
а — ширины ДН, градусов; *б* — максимального относительного УБЛ, дБ;
в — КНД, дБи; *г* — эффективности облучения рефлектора
(по оси абсцисс отложены значения рабочей частоты в ГГц)

Из приведенных зависимостей видно, что ширина ДН зеркальной антенны не превосходит максимально допустимого значения, определяемого выражением [8]

$$\Delta\theta_{\max} = \frac{68 \cdot \lambda}{2R_0} \qquad (4)$$

в пределах всего рабочего диапазона частот.

Требование к максимальному относительному УБЛ (не должен превышать –14 дБ) выполняется с большим запасом. Также можно отметить существенную разницу в модельных и критических значениях КНД порядка 3 дБ, благодаря чему значение КНД всегда выше минимально допустимого, определяемого выражением вида

$$D_{\min} = 20 \cdot \lg\left(\frac{2R_0}{\lambda}\right) + 7 . \quad (5)$$

Что касается полученных значений эффективности облучения рефлектора, то они лежат в диапазоне от 0,6 до 0,8. В случае использования зеркальной антенны в режиме передачи это привело бы к переливу излучаемой энергии за кромку зеркала и, соответственно, к уменьшению коэффициента усиления зеркальной антенны на величину порядка 5—15 % [8]. Однако примененный в составе конструкции логопериодический облучатель микрополоскового исполнения находит применение только в режиме приема, когда уровень принимаемых сигналов мал. В режиме приема данный эффект может привести к приему шумов земной поверхности и атмосферы, однако в диапазоне СВЧ эти шумы существенно меньше собственных шумов антенной системы.

Заключение

Проведенные модельные исследования направленных свойств однозеркальной параболической антенны с разработанным двухдиапазонным логопериодическим облучателем показали, что антенная система исправно функционирует во всем рабочем диапазоне частот, а ее параметры излучения находятся в пределах допустимых значений.

Исследование выполнено в рамках государственного задания на выполнение НИОКР «Разработка электродинамических моделей облучателей больших зеркальных антенн в составе системы ГМССБ для исследования качества решения задач спутниковой радиосвязи и радионавигации», приказ № 279-л от 21.04.2020 г.

Список литературы

1. *SATBEAMS*. URL: https://www.satbeams.com/satellites (дата обращения: 05.09.2020).

2. *Волхонская Е. В., Коротей Е. В.* Разработка математической модели поля излучения двухзеркальной антенны Грегори в рамках метода поверхностных токов // Морские интеллектуальные технологии : тр. VII междунар. Балтийского морского форума. Вып. 4 (46). Калининград, 2019. Т. 2. С. 188—193.

3. *Двухдиапазонный* облучатель с комбинированным преобразователем мод : пат. RU 2680424 C1 МПК H01Q 5/00 (2015.01) Рос. Федерация. № 2018102630 ; заявл. 23.01.2018.

4. *Сверхширокополосная* логопериодическая антенна : пат. RU 2663264 C2 МПК H01Q 11/00 (2006.01) Рос. Федерация. № 2017101490 ; заявл. 17.01.2017.

5. *Микрополосковая* логопериодическая антенна : пат. RU 2571607 C1, МПК H01Q 10/11 (2006.01) Рос. Федерация. № 2014129990/08 ; заявл. 21.07.2014.

6. *Свидетельство* о государственной регистрации программ для ЭВМ № 2015619811 Российская Федерация. Оптимизация геометрических парамет-

ров логопериодической антенны микрополоскового исполнения для C и Ku диапазонов / Е.В. Коротей, Е.В. Волхонская, Д.В. Кужекин. № 2015615296 : заявл. 15.09.2015 ; опубл. 20.10.2015.

7. *Волхонская Е.В., Коротей Е.В., Скридлевский А.В.* Оптимизация конструкции двухзеркальной антенны Грегори с логопериодическим облучателем Ku-диапазона для повышения качества решения задач спутниковой связи // Радиотехника. 2020. № 2 (4). С. 3—15.

8. *Фролов О.П., Вальд В.П.* Антенны для земных станций спутниковой связи. М., 2008.

Об авторах

Елена Вячеславовна Волхонская — д-р техн. наук, проф., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: volkhonskaya_e@mail.ru

Евгений Владимирович Коротей — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: eugeny_korotey@mail.ru

Ксения Валерьевна Власова — канд. физ.-мат. наук, доц., Балтийская государственная академия рыбопромыслового флота, Россия.
E-mail: p_ksenia@mail.ru

The authors

Prof. Elena V. Volkhonskaya, Immanuel Kant Baltic Federal University, Russia.
E-mail: volkhonskaya_e@mail.ru

Evgeny V. Korotey, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: eugeny_korotey@mail.ru

Dr Kseniya V. Vlasova, Associate Professor, Baltic Fishing Fleet State Academy, Russia.
E-mail: p_ksenia@mail.ru

УДК 621.315.615:665.3

Ж. В. Кадолич, С. В. Зотов

РАСШИРЕНИЕ АРСЕНАЛА ФИЗИЧЕСКИХ МЕТОДОВ ИССЛЕДОВАНИЯ ЖИДКИХ ДИЭЛЕКТРИКОВ НА ПРИМЕРЕ ЭКЗОТИЧЕСКИХ ВИДОВ РАСТИТЕЛЬНЫХ МАСЕЛ

Тема исследования: применимость физического метода – электретно-термического анализа – к изучению жидких диэлектриков, которые представлены некоторыми экзотическими видами пищевых растительных масел.

Цель научного исследования: установление взаимосвязи токового отклика на нагрев образцов масел с их жирнокислотным составом.

Описание методологии исследования: для анализа образцов растительных масел (тыквенного, грецких орехов, черного тмина) использован широко применяющийся в физике конденсированного состояния метод электретно-термического анализа. При реализации этого метода в ходе нагрева образцов фиксируется токовый отклик на протекающие в них физико-химические изменения, который сопоставляется с жирнокислотным составом масел.

Основные результаты, выводы исследовательской работы: на основании существования отличного от нуля токового отклика выдвинута гипотеза, в соответствии с которой в образцах происходит термически стимулированное и сопровождающееся протеканием тока разрушение малостабильных надмолекулярных образований – ассоциатов триглицеридов жирных кислот. Установлено, что вид спектра термостимулированного тока находится в очевидном соответствии с тем, триглицериды каких именно специфических жирных кислот превалируют в составе того или иного масла. Изменение токового спектра в сравнении с характеристическим спектром для данного вида масла может считаться маркером порчи или фальсификации.

Research topic: the applicability of an external feature – electret-thermal analysis – to the study of liquid dielectrics, which are exotic types of edible vegetable oils.

The purpose of scientific research: to establish the relationship of the current response with heating of oil samples with their fatty acid composition.

Description of the research methodology: for the analysis of samples of vegetable oils (pumpkin, walnuts, black cumin), the method of electret-thermal analysis, that is widely used in condensed matter physics, was applied. When this method is implemented, during the heating of samples, a current response to the physicochemical changes occurring in them is recorded, which is compared with the fatty acid oils composition.

The main results, conclusions of the research work: based on the existence of a non-zero current response, a hypothesis is put forward that thermally stimulated and accompanied by the flow of current destruction of unstable supramolecular formations – associates of fatty acid triglycerides – occur in the samples. It has been established that the spectrum type of the thermally stimulated current is in obvious accordance with the fact which triglycerides of which specific fatty acids prevail in the composition of a particular oil. A change in the current spectrum in comparison with the characteristic spectrum for this oil type can be considered a marker of damage or falsification.

© Кадолич Ж. В., Зотов С. В., 2020

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 96 – 107.

Ключевые слова: жидкие диэлектрики, растительные масла, жирнокислотный состав, электретно-термический анализ.

Keywords: liquid dielectrics, vegetable oils, fatty acid composition, electret-thermal analysis.

Введение

Потребительский рынок растительных масел в течение последних десятилетий активно обновляется. Помимо традиционных и привычных для постсоветского покупателя видов масел (подсолнечное, рапсовое, кукурузное, оливковое), ему предлагается все больше новых, среди которых льняное, тыквенное, кунжутное, кедровое, тминное и др. Можно предполагать, что данный ассортимент, призванный удовлетворить любым запросам потребителя, будет постоянно обновляться. Поэтому существует актуальность в расширении арсенала методов исследования, позволяющих судить о показателях качества масел. Кроме того, необходимость установления преграды на пути проникновения фальсификата — один из важных аргументов в пользу совершенствования классических методов анализа любой продукции.

Оценка качества — сложная аналитическая задача, при ее решении следует не только правильно выбрать метод анализа, но и учитывать особенности состава, физико-химической структуры и свойства исследуемого объекта, которые в значительной мере определяют параметры, регистрируемые в ходе лабораторного эксперимента. Для оценки качества растительных масел применяют широкий арсенал методов исследования, позволяющих определить вкус, запах, прозрачность, кислотное, перекисное и йодное числа, показатель преломления, содержание влаги, число омыления и др. [1; 2]. Для определения физико-химических показателей масел используют спектр лабораторных методов анализа (ИК-спектроскопия, термогравиметрия, хроматография, УФ-спектрометрия и т.д.). Кроме того, ведутся исследования, основанные на методе рентгеновской флуоресцентной спектроскопии, явлении ядерного магнитного резонанса, измерении проводимости, вязкости, диэлектрической проницаемости и др. показателей, отражающих степень окисления масла, его загрязненность продуктами окисления, гидролиза и т.д. [3]. Общая окислительная стабильность натуральных масел и жиров может быть определена методом Rancimat, основанном на окислении молекул масла или жира с образованием первичного (пероксиды) и вторичного (образовавшиеся после разложения жирных кислот низкомолекулярные органические кислоты) продуктов окисления, которые растворяются в воде, после чего по изменению электропроводности судят о содержании кислот, а по продолжительности индукционного периода до появления вторичных продуктов — об индексе стабильности масла [4].

Основной фактор, определяющий потребительские свойства растительных масел, — их химический состав. Он преимущественно представлен триглицеридами моно-, полиненасыщенных и насыщенных

жирных кислот [5]. Результаты комплексного экспериментального исследования физико-химических свойств полученных из различных масел смесей эфиров жирных кислот даны в работе [6]. Однако использованные лабораторные методы позволили получить информацию только о совокупном содержании остатков жирных кислот, но не о специфических для каждого масла особенностях их связывания в триглицериды, взаимодействия с другими компонентами масел и др., что особенно важно при определении признаков порчи или фальсификаций продукта. Существует необходимость использования метода анализа, который позволил бы получить и интерпретировать некий сигнал, характеризующий тот или иной вид растительного масла [2], причем отступление от этого сигнала было бы обоснованным признаком несоответствия анализируемого образца заявленным характеристикам.

Цель работы — продемонстрировать естественнонаучный подход к оценке растительных масел с помощью стандартного для изучения диэлектриков физического метода исследования — метода электретно-термического анализа (ЭТА), который в данной работе применен в отношении экзотических (деликатесных) разновидностей масел.

Материалы и методы исследований

В качестве исследуемых объектов выбраны масла тыквенное, грецких орехов и черного тмина (табл. 1). Перечисленные разновидности масел, сравнительно недавно появившиеся в свободном доступе на отечественном рынке, можно отнести к группе деликатесных или экзотических. Ряд исследований указывает на их высокую пищевую и биологическую полезность, особенно ввиду наличия сочетания уникальных жирных кислот.

Таблица 1

Характеристика исследуемых образцов масла

Разновидность масла	Номер образца	Особенность образца
Тыквенное нерафинированное	1	Изготовитель — ООО «Натуральные масла», Россия, Московская обл., г. Солнечногорск; масло приобретено в торговой сети
	2	Изготовитель — ООО «Золотой кедр», Россия, г. Новосибирск; масло приобретено в аптечной сети; класс экстра
Грецких орехов пищевое нерафинированное	3	Изготовитель — ООО «Натуральные масла», Россия, Московская обл., г. Солнечногорск; масло приобретено в торговой сети
Черного тмина	4	Изготовитель — фабрика «Аль Жасмин», Египет, провинция Эль-Файюм; масло приобретено в фирменном объекте торговой сети по месту изготовления

Тыквенное масло — одно из самых полезных для здоровья. В его состав помимо триглицеридов входят эфирные масла, белки, пектины, стерины, гормоноподобные вещества, фосфолипиды, флавоноиды, токоферолы, каротиноиды, витамины А, Е, F, С, К, B_1, B_2, Р. Как видно из таблицы 2, жирнокислотный состав достаточно сложен.

Таблица 2

Жирнокислотный состав тыквенного масла

Название кислоты	Общая формула	Класс	Содержание, %
Миристиновая	$C_{13}H_{27}COOH$	Насыщенная	0,2
Пальмитиновая	$C_{15}H_{31}COOH$	Насыщенная	6—15
Пальмитолеиновая	$C_{15}H_{29}COOH$	Мононенасыщенная	< 0,5
Стеариновая	$C_{17}H_{35}COOH$	Насыщенная	6—7,5
Олеиновая	$C_{17}H_{33}COOH$	Мононенасыщенная	18—47
Линолевая	$C_{17}H_{31}COOH$	Поли(ди-)ненасыщенная	30—48
Линоленовая	$C_{17}H_{29}COOH$	Поли(три-)ненасыщенная	15
Арахиновая	$C_{19}H_{39}COOH$	Насыщенная	< 0,8
Гадолеиновая	$C_{19}H_{37}COOH$	Мононенасыщенная	< 0,5
Бегеновая	$C_{21}H_{43}COOH$	Насыщенная	< 0,4
Эруковая	$C_{21}H_{41}COOH$	Мононенасыщенная	< 0,3
Лигноцериновая	$C_{23}H_{47}COOH$	Насыщенная	< 0,5

Источник: [7; 8].

Масло грецких орехов содержит фосфор, медь, цинк, магний, железо, кальций, йод, кобальт, фитостерины, сфинголипиды и фосфолипиды, каротиноиды, витамины В, РР, А, К, С и в рекордных количествах витамин Е. Группа насыщенных жирных кислот представлена пальмитиновой (6 %), стеариновой (2 %), арахидиновой (0,2 %) кислотами. Из мононенасыщенных жирных кислот в составе идентифицирована олеиновая (22 %), из полиненасыщенных — линолевая (54 %) и альфа-линоленовая (10 %) [9].

Масло черного тмина содержат более 100 различных компонентов и около 50 катализаторов естественного биосинтеза клеток, которые ускоряют биологические реакции. Среди них липаза (помогает переваривать и растворять жиры, обеспечивая таким образом доставку жирных кислот к тканям организма), токоферолы (являются главным питательным веществом-антиоксидантом, участвуют во всех репродуктивных процессах), флавоноиды (участвуют в окислительно-восстановительных реакциях организма), дубильные вещества (препятствуют распространению инфекции), алкалоиды (защищают организм от внешних воздействий), катехины (сильные антиоксиданты, укрепляют иммунную систему), цитокинины (стимулируют деление клеток), энзимы (катализируют химические реакции в организме, регулируя обмен веществ), минеральные соли, провитамины групп А, В, Р, Е, минералы, кальций, железо, медь, цинк, фосфор. В состав масла входят насыщенные жирные кислоты — стеариновая (до 3,5 %) и пальмитиновая (до 14 %), мононенасыщенные жирные кислоты — олеиновая (15—18 %),

полиненасыщенные жирные кислоты — линолевая (55—65 %). Также присутствуют миристиновая, бегеновая, маргариновая, арахиновая, пентадекановая, пальмитолеиновая кислоты [10].

Часто встречающиеся утверждения о перспективности электрофизических и/или электромагнитных методов при оценке свойств и структуры жидких сред [11; 12] предопределили выбор метода исследования — стандартизированный метод ЭТА [13]. Данный метод основан на нагревании анализируемого образца, размещенного между заземленным и измерительным электродами, и получении графиков зависимости протекающего во внешней цепи электрического тока от температуры — спектров термостимулированных токов (ТСТ), по характеру которых анализируют процессы релаксации в образце электретного заряда. Ток возникает в образце при его нагреве с постоянной скоростью, поляризованные компоненты образца деполяризуются, вследствие чего происходит движение носителей электрических зарядов. Фактически ЭТА пригоден для изучения диэлектрических объектов (сред) различного химического состава и происхождения, в структуре которых существуют связанные электрические заряды, способные высвободиться при нагревании [14—16].

Функциональная схема измерительного комплекса для проведения ЭТА представлена на рисунке 1.

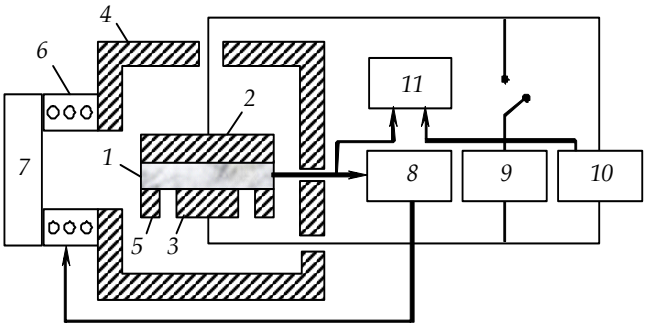


Рис. 1. Блок-схема установки для проведения ЭТА:
1 — исследуемый образец; *2* и *3* — измерительные электроды; *4* — измерительная камера; *5* — охранный электрод; *6* — нагреватель; *7* — система охлаждения; *8* — регулятор температуры; *9* — вольтметр; *10* — усилитель; *11* — устройство вывода результатов

Обоснование применимости метода ЭТА для анализа некоторых популярных видов растительных масел впервые дано в работе [2]. Растительные масла являются диэлектрическими средами благодаря следующим своим особенностям:

— содержат триглицериды жирных кислот, имеющие ненасыщенные фрагменты (то есть избыточный заряд) и обладающие дипольным моментом (то есть способные поляризоваться);

— содержат надмолекулярные малостабильные структуры (ассоциаты), в которых вышеупомянутые триглицериды определенным образом связаны, за счет чего создается определенная пространственная ориентация ненасыщенных фрагментов и диполей.

Проведенные авторами исследования позволили установить, что отличный от нуля ТСТ в диапазоне 20—120 °С фиксируется при ЭТА подсолнечного, рапсового, льняного, пальмового и других разновидностей растительных масел, причем вид токового спектра коррелирует с жирнокислотным составом этих масел [17; 18]. В процессе исследований также решена одна из методологических проблем применения ЭТА для анализа жидкостей, связанная с опасностью растекания жидкой среды по электроду с нарушением принципа взаимной изоляции электродов. Применен «носитель» диэлектрической жидкости — мелкодисперсный порошок кварца или диоксида титана [19]. Методика эксперимента предусматривала предварительное интенсивное механическое смешение диэлектрического носителя с анализируемым образцом растительного масла в соотношении 2:1 при общей массе смеси до 0,5 г, размещение полученной смеси на нижнем электроде (рис. 2), размещение поверх смеси диэлектрического зазора в виде пленки из политетрафторэтилена толщиной 10 мкм, помещение поверх пленки верхнего электрода с прижатием, размещение электродной системы в ячейке, равномерный нагрев, регистрацию спектра ТСТ и сохранение данных в цифровом виде с помощью компьютерной программы. Предложенная схема призвана обеспечить более высокую воспроизводимость результатов анализа с получением точных значений положения токовых максимумов по температурной шкале. Представленные далее на рисунках 3—5 спектры ТСТ являются графическим усреднением 10 спектров образцов.

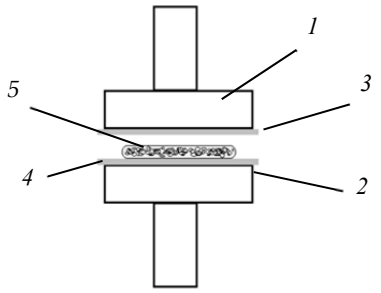
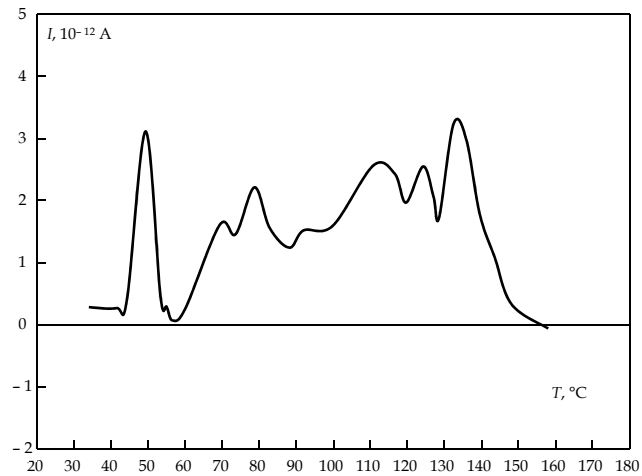


Рис. 2. Экспериментальный вариант расположения образцов растительных масел в системе электродов:
1 — верхний (измерительный) электрод; *2* — нижний (заземленный) электрод;
3 — тефлоновая прокладка для обеспечения регулируемого зазора;
4 — алюминиевая фольга (необходима для облегчения очистки электрода после ЭТА);
5 — образец масла (с «носителем»)

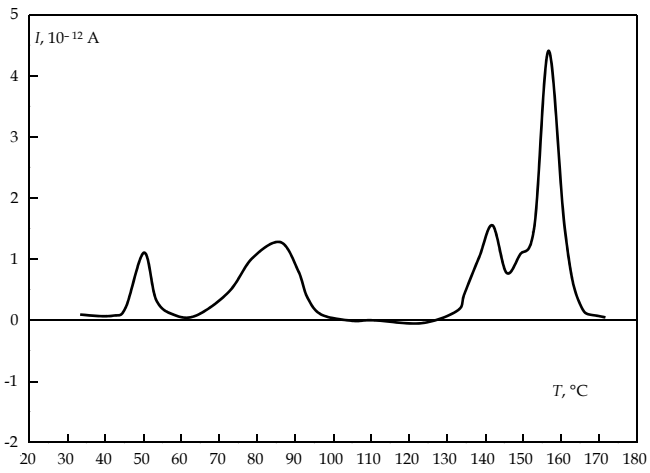
Результаты и их обсуждение

1. Тыквенное масло. Результаты ЭТА образцов тыквенного масла представлены на рисунке 3. Анализ полученных экспериментальных данных позволяет сделать вывод о наличии на спектре ТСТ трех выраженных групп токовых пиков, интенсивность которых находится в пределах нескольких пикоамперов (10^{-12} А): низкотемпературные пики (как правило, один) в сравнительно узком диапазоне 40—50 °С, среднетемпературные пики (как правило, один, реже два) в более широком диапазоне 65—90 °С и последующие высокотемпературные пики. Эти

данные согласуются с тремя видами жирных кислот, триглицериды которых превалируют в составе тыквенного масла: насыщенными, мононенасыщенными и полиненасыщенными. В подтверждение ранее выдвинутой гипотезы о существовании ассоциатов, в которые связываются триглицериды определенных жирных кислот, можно полагать, что наименее термически стабильными будут ассоциаты триглицеридов насыщенных кислот (тип 1) как содержащие наименьшее число способных к межмолекулярным взаимодействиям активных центров, относительно более стабильными — ассоциаты триглицеридов мононенасыщенных кислот (тип 2), а наиболее стабильными — ассоциаты триглицеридов полиненасыщенных кислот (тип 3). На основании этого следует соотнести низкотемпературную группу ТСТ с распадом малостабильных ассоциатов типа (1), среднетемпературную — типа (2) и высокотемпературную — типа (3) [8].



а



б

Рис. 3. Спектры ТСТ образцов тыквенного масла:
а — образец 1; *б* — образец 2

Пик ТСТ, отвечающий ассоциатам типа (3), является мультиплетным. Это может быть обусловлено следующими причинами:

— высокой термической стабильностью и значительным содержанием в тыквенном масле ассоциатов триглицеридов линолевой кислоты;

— способностью триглицеридов линолевой кислоты связываться в ассоциаты с триглицеридами других кислот, что усложняет структуру координационных связей и повышает стабильность кооперативных образований;

— вероятностью того, что в температурном диапазоне до 100 °С происходит не только терморазпад малостабильных ассоциатов, но и рекомбинация триглицеридов различных кислот в более сложные и несколько более стабильные структуры, повторное разложение которых идет при более высоких температурах.

При анализе спектра ТСТ на рисунке 3, *б* обращает на себя внимание перекрывание нескольких токовых пиков в среднетемпературной области. Вероятно, образец 2 отличается усложненным характером связывания триглицеридов в ассоциаты, которые могут содержать остатки кислот разных типов, а не одного, как предполагалось ранее. Подобное поведение может быть обусловлено особенностями производства тыквенных масел различного сорта, спецификой проведения рафинации и доведения до категории качества «экстра».

2. Масло грецких орехов. Масло грецких орехов демонстрирует в ходе ЭТА спектры ТСТ, представленные на рисунке 4.

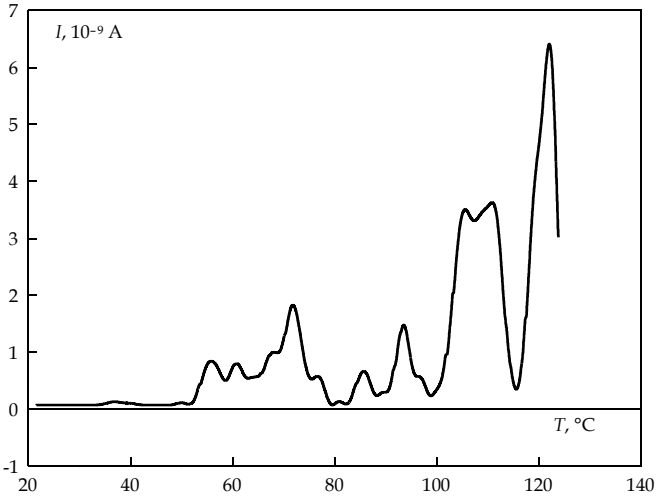


Рис. 4. Спектр ТСТ масла грецких орехов (образец 3)

Имеют место несколько выраженных групп токовых пиков — в диапазонах 50—60, 75, 85 и 95 °С, которые могут быть соотнесены с несколькими группами нестабильных ассоциатов, сформированными по принципу взаимодействия триглицеридов определенных жирных кислот. Высокотемпературные (выше 100 °С) пики ТСТ, как и для тыквенного масла, могут быть связаны со вторичными процессами распада более

сложных, в том числе вторичных, структур. Обращает на себя внимание аномально сильный сигнал ТСТ масла грецких орехов — до 10^{-9} А, причиной чего может быть более высокая степень координации триглицеридов жирных кислот в ассоциаты с образованием большего количества внутри- и межмолекулярных связей. Этому может способствовать, например, каталитическое воздействие некоторых веществ, в малой концентрации присутствующих в масле грецких орехов.

3. Масло черного тмина. Масло черного тмина в ходе ЭТА демонстрирует спектр ТСТ, представленный на рисунке 5. Имеются три основные группы пиков: низкотемпературная (40—45 °С), интерпретируемая нами как относящаяся к распаду ассоциатов насыщенных жирных кислот, среднетемпературная (75—85 °С), иллюстрирующая распад ассоциатов мононенасыщенных кислот, и высокотемпературная (выше 100 °С), отвечающая распаду ассоциатов полиненасыщенных жирных кислот и, дополнительно, еще более устойчивых ассоциатов смешанного состава. Токовый сигнал превышает таковой для тыквенного масла и находится в диапазоне 10^{-11} А, что, как и для масла грецких орехов, может свидетельствовать о каталитическом действии веществ, присутствующих в масле помимо триглицеридов жирных кислот.

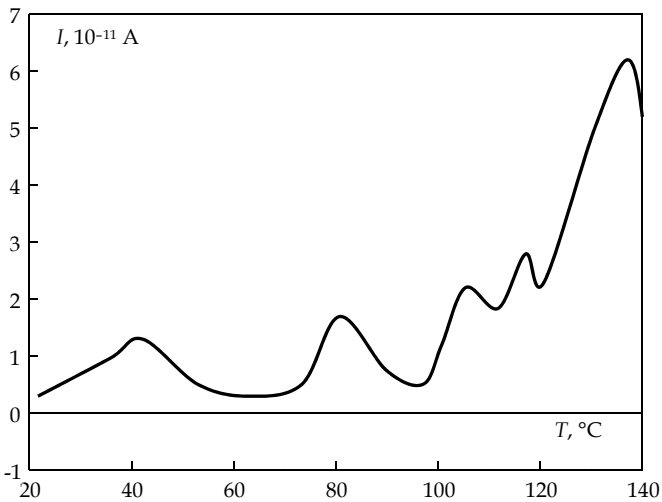


Рис. 5. Спектр ТСТ масла черного тмина (образец 4)

Заключение

Полученные экспериментальные результаты иллюстрируют возможности, которые предоставляет физический метод исследования (ЭТА) в отношении недостаточно изученных, но набирающих популярность на отечественном потребительском рынке экзотических видов растительных масел. Установлено, что спектр ТСТ масел фиксирует отличный от нуля токовый отклик, который интерпретируется с точки зрения появления инициированных нагревом физико-химических процессов распада малостабильных ассоциатов — структур, тем или

иным образом связывающих триглицериды жирных кислот. Распад ассоциатов, построенных из остатков определенных жирных кислот, происходит в определенном температурном диапазоне и находится в соответствии с прочностью связывания триглицеридов, которая, в свою очередь, зависит от наличия в остатках жирных кислот активных центров, определяющих характер подобного связывания. С учетом структуры триглицеридов, где глицерин по принципу этерификации связывает и блокирует карбоксильную группу, такими активными центрами могут служить преимущественно ненасыщенные связи в жирных кислотах. Поэтому ассоциаты триглицеридов насыщенных кислот оказываются наименее стабильными (малая вероятность физического и крайне малая вероятность физико-химического взаимодействия), мононенасыщенных кислот — среднестабильными (высокая вероятность физико-химического межмолекулярного связывания по принципу доноро-акцепторного взаимодействия с перераспределением электронной плотности по всему надмолекулярному образованию), а полиненасыщенных кислот — наиболее стабильными (наибольшая возможность донорно-акцепторного взаимодействия с участием большего количества ненасыщенных групп). При этом вполне вероятно, что при общем превалировании ассоциатов, содержащих триглицериды одной определенной кислоты (что может быть связано с биохимией процессов формирования масла в семенах соответствующих растений), в составе растительных масел имеются ассоциаты более сложного состава, связывающие триглицериды разных кислот. Однако последние надмолекулярные образования, как правило, более стабильны, разрушаются при более высоких температурах и не вносят заметных искажений в спектр ТСТ растительных масел в температурных диапазоне по меньшей мере до 100 °С.

Целесообразно сделать вывод о том, что метод ЭТА позволяет получить результат в виде токового сигнала, находящегося в соответствии с жирнокислотным составом того или иного растительного масла. Можно полагать, что несоответствие пиков ТСТ анализируемого образца данного товара полученному на нативном образце «характеристическому» токовому спектру, включая сдвиг пиков или резкое изменение их интенсивности, может считаться как критерием несоответствия жирнокислотного состава заявленному, так и признаком начавшейся или уже произошедшей окислительной порчи конкретного вида масла.

Современная мировая наука нацелена на получение фундаментальных знаний, на основе которых со временем можно создать некий коммерческий продукт. Проведенный эксперимент по ЭТА растительных масел иллюстрирует новое направление в исследовании этого товара. Промежуточным этапом подобных исследований может быть составление словаря-справочника с перечислением жирнокислотного состава различных растительных масел, представления характеристического спектра ТСТ для конкретных видов и описания экспериментально установленных физико-химических соответствий между ними. Ввиду доказанной эффективности метода ЭТА при анализе самых различ-

ных материалов и веществ, содержащих диэлектрические компоненты [8; 14—18], авторы ставят перед собой задачу и далее адаптировать этот метод, применяя его к различным объектам [20].

Список литературы

1. *Касторных М.С., Кузьмина В.А., Пучкова Ю.С.* Товароведение и экспертиза пищевых жиров, молока и молочных продуктов : учебник для вузов. М., 2018.

2. *Кадолич Ж.В., Деликатная И.О., Цветкова Е.А.* Растительные масла: свойства и методы контроля качества // Потребительская кооперация. 2010. №4 (31). С. 78—84.

3. *Криштафович В.И., Криштафович Д.В., Еремеева Н.В.* Физико-химические методы исследования : учебник для бакалавров. М., 2015.

4. *Жиры* и масла животные и растительные. Определение устойчивости к окислению (ускоренное испытание на окисление) : ГОСТ Р 53160-2008 (ISO 6886:2006). М., 2009.

5. *Беззубов Л.П.* Химия жиров. М., 1975.

6. *Антонова З.А., Крук В.С., Максимук Ю.В., Курсевич В.Н.* Исследование составов и физико-химических свойств смесей эфиров жирных кислот // Свиридовские чтения : сб. ст. Вып. 10. Минск, 2014. С. 163—177.

7. *Тыквенное* масло: черное золото // Масложировая промышленность. 2008. №6. С. 27—28.

8. *Кадолич Ж.В.* Экспериментальное обоснование применения метода электретно-термического анализа для исследования тыквенного масла // Пищевая промышленность: наука и технологии. 2017. №3 (37). С. 102—108.

9. *Остриков А.Н., Горбатова А.В., Филипцов П.В.* Анализ жирнокислотного состава масел арахиса и грецкого ореха // Технологии пищевой и перерабатывающей промышленности АПК — продукты здорового питания. 2016. №4 (12). С. 37—42.

10. *Бондаренко Е.Ю., Пелипенко Т.В.* Масло черного тмина — источник ненасыщенных жирных кислот // Физико-химический анализ свойств многокомпонентных систем. 2007. №5. С. 10.

11. *Магнитные* жидкости в машиностроении / Д.В. Орлов, Ю.О. Михалев, Н.К. Мышкин [и др.]. М., 1993.

12. *Иголкин Б.И., Васильева Л.К., Васипов В.В. и др.* Электропроводность растительных масел в зависимости от температуры и частоты электромагнитных колебаний // Научно-технические ведомости СПбГПУ. 2011. №2. С. 278—282.

13. *Пластмассы* и пленки полимерные. Методы определения поверхностных зарядов электретов : ГОСТ 25209-82. М., 1982.

14. *Кравцов А.Г., Гольдаде В.А., Пинчук Л.С., Зотов С.В.* Возможности термоактивационной токовой спектроскопии при изучении электрофизических свойств материалов // Материалы, технологии, инструменты. 2006. №2 (11). С. 104—108.

15. *Pinchuk L.S., Goldade V.A., Sessler G.M.* Electret-thermal analysis of blood // Medical Eng. and Phys. 2002. Vol. 24. P. 361—364.

16. *Кадолич Ж.В.* Физическое модифицирование сопряжений полимер-металл для повышения их износостойкости на основе модифицирования биофизических свойств естественных суставов : автореф. дис. ... канд. техн. наук. Гомель, 2002.

17. *Кадолич Ж.В., Зотов С.В., Гольдаде В.А.* Экспериментальное обоснование выбора идентификационного признака пальмовых масел // Приборы и методы измерений. 2015. №1 (10). С. 99—104.

18. *Кадолич Ж.В., Зотов С.В.* Иллюстрация возможностей метода электретно-термического анализа при исследовании растительных масел // Стандартизация. 2018. №4. С. 61—68.

19. *Способ* термоактивационной токовой спектроскопии пищевого растительного масла : пат. РБ 21764 Респ. Беларусь. №a20150180 ; заявл. 06.04.2015.

20. *Кадолич Ж.В., Зотов С.В.* Возможности электретно-термического анализа при исследовании полисахаридов и пищевых жиров // Вестник технологического университета. 2018. №9 (21). С. 16—21.

Об авторах

Жанна Владимировна Кадолич — канд. техн. наук, доц., Белорусский торгово-экономический университет потребительской кооперации, Республика Беларусь.

E-mail: cilodak@mail.ru

Сергей Валентинович Зотов — канд. техн. наук, ведущ. науч. сотр., Институт механики металлополимерных систем им. В.А. Белого Национальной академии наук Беларуси, Республика Беларусь.

E-mail: zotov-1969@mail.ru

The authors

Dr Zhanna V. Kadolich, Associate Professor, Belarusian Trade and Economic University of Consumer Cooperation, Republic of Belarus.

E-mail: gki@mail.gomel.by

Dr Sergey V. Zotov, Leading Research Fellow, V.A. Belyi Metal-Polymer Research Institute, National Academy of Sciences of Belarus, Republic of Belarus.

E-mail: zotov-1969@mail.ru

УДК 539.143.539.183

А. А. Персичкин, С. Г. Шпилевая, Н. В. Персичкина

ОСОБЕННОСТИ СТЫКОВКИ ИЗМЕРИТЕЛЬНЫХ ПРИБОРОВ С ПРОГРАММНЫМ ПАКЕТОМ MATLAB

Описан алгоритм интеграции цифровых измерительных приборов с персональным компьютером в составе многофункционального приборного комплекса для использования ресурсов пакета прикладных программ Matlab при регистрации и обработке принимаемых сигналов. В качестве базового прибора выбран запоминающий осциллограф производства компании Tektronix, хорошо зарекомендовавший себя в лабораторных экспериментах по радиоспектроскопии. Предлагаемая процедура стыковки осциллографа с программным пакетом представляет собой последовательность вполне доступных любому пользователю действий. Вместе с тем она позволяет существенно повысить эффективность использования цифровых измерительных приборов в экспериментальной технике.

The paper describes an algorithm for integrating digital measuring devices with a personal computer as part of a multifunctional instrument complex for using the resources of the Matlab application software package for recording and processing received signals. The basic device is a memory oscilloscope manufactured by «Tektronix», which has proven itself in laboratory experiments on radio spectroscopy. The proposed procedure for connecting the oscilloscope to the software package is a sequence of actions that are quite accessible to any user. At the same time, it can significantly increase the efficiency of using digital measuring devices in experimental technology.

Ключевые слова: цифровой измерительный комплекс, программные средства математического моделирования, обработка принимаемых сигналов, повышение точности измерений.

Keywords: digital measuring system, software for mathematical modeling, processing of received signals, improving the accuracy of measurements.

Современные измерительные приборы, в том числе осциллографы, предоставляют возможность высококачественного приема и оцифровки сигналов в широкой полосе частот [1]. Это относится в том числе к регистрации относительно слабых сигналов, наводимых в радиочастотных контурах при выполнении измерений по ядерному спиновому резонансу, возбуждаемому в образцах со сложной геометрией [2—4], а также при решении других прикладных задач из области радиоспектроскопии [5—7]. Однако ресурсы цифровых измерительных приборов по обработке и визуализации исследуемых сигналов значительно уступают возможностям программных средств математического моделирования (СММ), например пакета прикладных программ Matlab [8].

Важным преимуществом обработки информации с помощью СММ является более высокая точность конечных результатов, чем при оценке параметров сигнала, получаемых непосредственно с измерительного прибора [8] (в этом случае на точность измерений влияют погрешности, связанные с дополнительной оцифровкой сигнала перед выводом

© Персичкин А. А., Шпилевая С. Г., Персичкина Н. В., 2020
Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 108 – 113.

его на экран и т.п.). Реализация преимущества СММ в указанных случаях возможна при построении аппаратно-программных комплексов, включающих как измерительные приборы (блоки), интегрированные с персональным компьютером, так и специализированное программное обеспечение, выполняющее обработку информации. Существуют два основных принципа реализации таких комбинированных установок [1]: 1) объединение автономных измерительных приборов в систему, обеспечивающую необходимый обмен данными с персональным компьютером; 2) использование ПК, дополненного измерительными преобразователями в виде встроенных плат ввода/вывода, включенных в системную шину компьютера.

Основные компании-производители цифровых измерительных приборов (Tektronix, Agilent Techologies, LeCroy и др.) стали внедрять возможность стыковки своих приборов, прежде всего осциллографов, с СММ, используя для обмена информацией между прибором и компьютером порт универсальной последовательной шины USB. Однако материалов по практическому применению СММ совместно с конкретными измерительными средствами в свободном доступе встречается крайне мало.

В связи с этим мы поставили целью отработать процедуру интеграции измерительных приборов с программным пакетом Matlab, используя в качестве аппаратного средства цифровой запоминающий осциллограф TDS-2022C, выпускаемый компанией Tektronix (рис. 1).

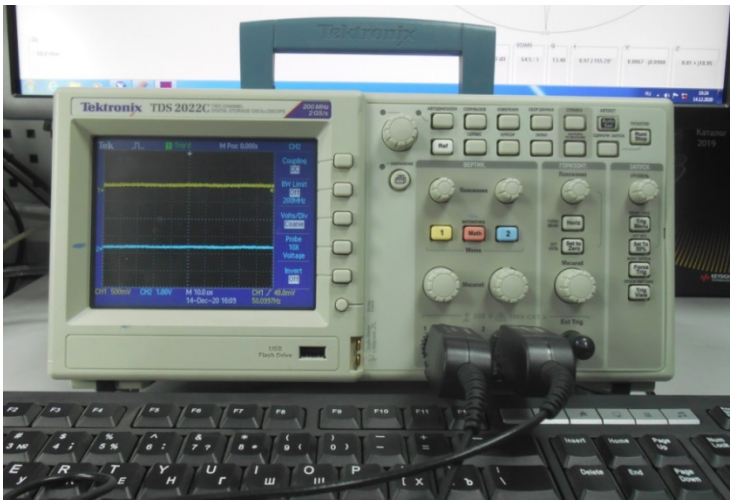


Рис. 1. Внешний вид лицевой панели осциллографа TDS-2022C
в комплексе с персональным компьютером

Выбранный нами прибор в значительной степени отвечает необходимым требованиям для его использования в качестве лабораторного средства регистрации данных в масштабе реального времени: полоса пропускания до 50 МГц, частота дискретизации 500 Мвыб/с, одинаковая длина памяти при всех значениях временной развертки, возможность выполнения быстрого преобразования Фурье (БПФ) и других математических функций, высокая надежность работы.

Стыкуемый с компьютером осциллограф Tektronix должен иметь USB-разъем Type-B, а также управляющее программное обеспечение OpenChoice, которое зачастую входит в комплект поставки либо его можно загрузить с сайта компании-производителя. Указанное программное обеспечение выполняет функции организации обмена информацией с прибором и вывода снимков изображения с экрана осциллографа на экран компьютера. Обмен информацией с Matlab поддерживает специальный пакет расширения Instrument Control Toolbox. При этом обеспечивается поддержка виртуальных инструментов стандартной архитектуры VISA (Virtual Instrument Standard Architecture).

Перейдем к описанию процедуры стыковки осциллографа с СММ Matlab.

Шаг 1: устанавливаем на компьютер программное обеспечение OpenChoice (рис. 2), подключаем осциллограф и проверяем его успешную совместную работу с ПК.

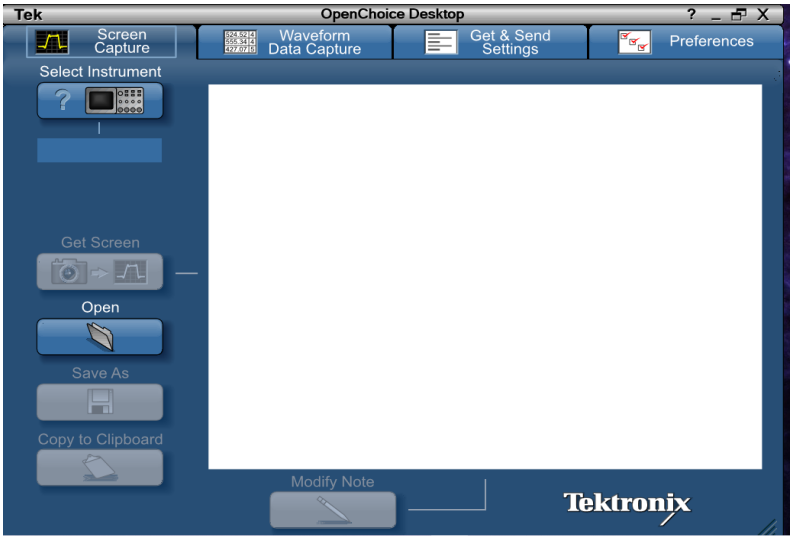


Рис. 2. Управляющее окно ПО OpenChoice

Шаг 2: устанавливаем драйвер работы Matlab с прибором (при следующей стыковке этот шаг можно пропустить). В последних версиях Matlab есть предустановленные драйверы для некоторых измерительных приборов. Они имеют расширение ***.mdd** и находятся по пути: *'корневой каталог Matlab'*\toolbox\instrument\instrument\drivers*.mdd

Чтобы узнать предустановленные в СКМ драйверы, можно воспользоваться командой **tmtool** Matlab, о которой будет рассказано ниже.

Если драйвер отсутствует, то его, как правило, можно найти на сайте производителя оборудования.

Шаг 3: инсталяция драйвера. В рабочем поле Matlab набираем команду **midedit**, которая вызывает окно утилиты инсталляции драйвера нового оборудования (рис. 3). Для этого открываем папку с драйвером устройства и сохраняем его в каталог.

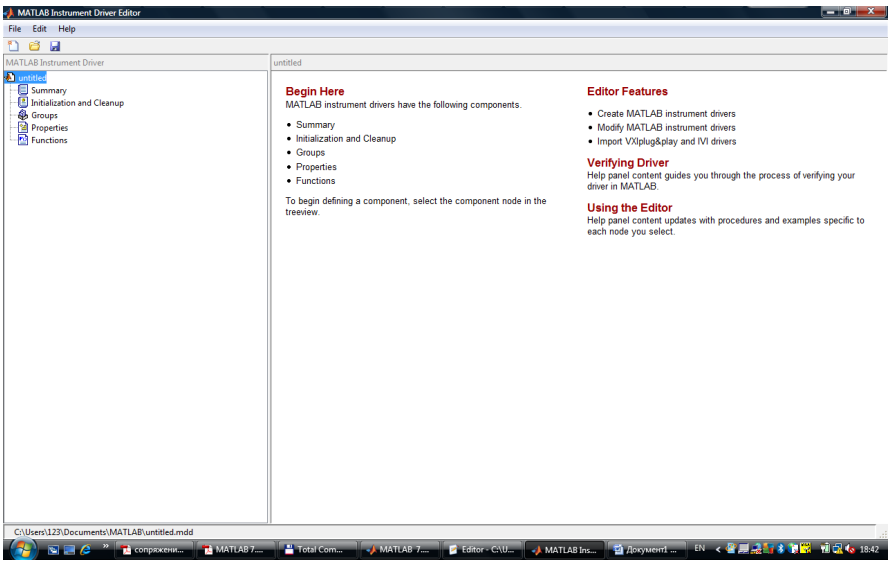


Рис. 3. Окно утилиты инсталляции драйвера

Шаг 4: подключение прибора к Matlab. Для этого можно использовать команду **tmtool** и вызываемое ею окно утилиты тестирования измерительных приборов (рис. 4).

В «дереве» левой части окна нужно последовательно обеспечить выбор USB-устройств, а также создание интерфейсного (interface) и приборного (device) объектов. После выбора необходимого объекта производим окончательную стыковку оборудования с Matlab активацией кнопки Connect в правом верхнем углу утилиты.

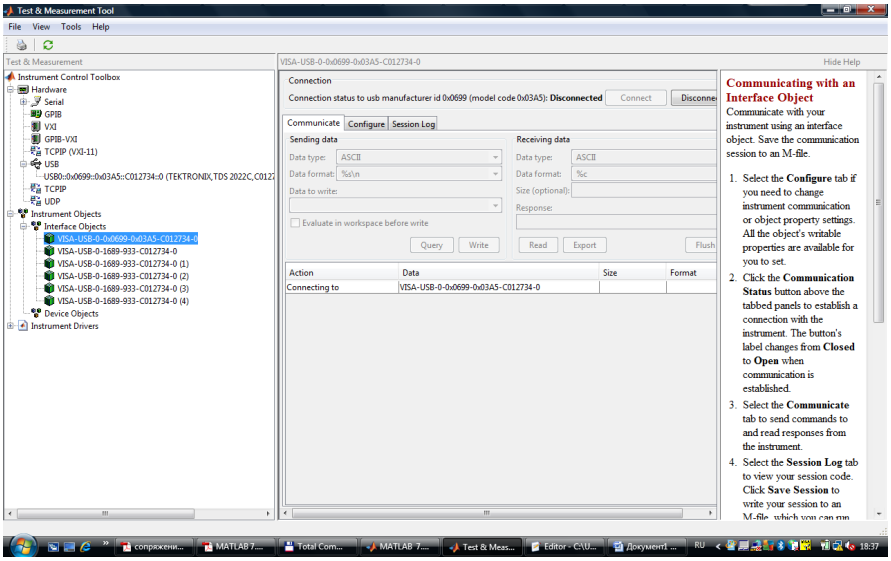


Рис. 4. Окно утилиты тестирования измерительных приборов

Далее можно переходить к разработке программы, обеспечивающей обработку сигналов, поступающих с осциллографа. Пакет расширения Instrument Control Toolbox предоставляет для этого следующие основные функции:

• instrhwinfo — возвращает информацию о подключенном к ПК устройстве;
• visa — конструирование VISA-объекта;
• fopen — подключение VISA-объекта к прибору;
• query — запись или чтение форматированных данных с прибора;
• fprintf — запись текста в прибор;
• fclose — отключает связь с прибором;
• binblockread — чтение поблочно данных с прибора.

Прежде чем приступить непосредственно к программированию, нужно сконструировать VISA-объект, который выглядит так:

ob = visa('*производитель*','*спецификация оборудования производителя* ')

Перечень возможных '*производителей*':
• 'ni' — National Instruments;
• 'agilent' — Agilent Technologies;
• 'tek' — Tektronix.

Информацию о спецификации оборудования можно получить в правой части окна утилиты тестирования измерительных приборов. В случае рассматриваемого осциллографа TDS-2022 компании Tektronix она будет иметь вид

Visa-usb-0-0x0699-0x03a5-c012734-0,

где **usb-0** — номер порта; **0x0699** — код производителя в шестнадцатеричной системе (в десятичной **1689**); **0x03a5** — код оборудования в шестнадцатеричной системе (в десятичной **933**).

Окончательно VISA-объект для TDS-2022 будет выглядеть следующим образом:

vu=visa('tek','USB0::1689::933::C012734::0::INSTR').

После создания VISA-объекта открываем его командой **fopen** и считываем данные, которые далее можно обрабатывать средствами Matlab [1].

Использование предлагаемого алгоритма позволяет максимально реализовать возможности СММ и повысить эффективность использования цифровых измерительных приборов в экспериментальной технике [1], предполагающей высокую точность измерений.

Список литературы

1. *Аминев А.В., Блохин А.В.* Измерения в телекоммуникационых системах. Екатеринбург, 2015.

2. *Белый Ю.И., Поцепня О.А., Семин Г.К.* Аппаратура для борьбы с терроризмом на основе эффекта ЯКР // Специальная техника. 2002. №2. С. 22—31.

3. *Устройство* контроля электромагнитного поля вторичных излучателей : пат. 2527315 Рос. Федерация. №2013108753 ; заявл. 08.07.2014.

4. *Устройство* исследования электромагнитного поля вторичных излучателей : пат. 2538318 Рос. Федерация. №2013114517 ; заявл. 19.11.2014.

5. *Устройство* обнаружения сигналов ядерного квадрупольного резонанса : пат. 2697023 Рос. Федерация. № 2018142728 ; заявл. 08.08.2019.

6. *Гречишкин В.С., Шпилевой А.А., Бурмистров В.И.* О возможности применения ЯКР для обнаружения взрывчатых веществ на теле человека // Специальная техника. 2004. № 5. С. 29—35.

7. *Синявский Н.Я., Шпилевой А.А.* Особенности косвенной регистрации сигналов ядерного квадрупольного резонанса взрывчатых веществ // Радиотехника. 2009. № 2. С. 131—134.

8. *Дьяконов В.П.* MATLAB 7.* /R2006/R2007 : самоучитель. М., 2008.

Об авторах

Андрей Андреевич Персичкин — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: a.persichkin@kgnic.ru

Светлана Геннадьевна Шпилевая — канд. пед. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: SSHpilevaya@kantiana.ru

Наталья Витальевна Персичкина — ст. преп., Балтийский федеральный университет им. И. Канта, Россия.
E-mail: VPersichkina@kantiana.ru

The authors

Andrey A. Persichkin, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: a.persichkin@kgnic.ru

Dr Svetlana G. Shpilevaya, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: SSHpilevaya@kantiana.ru

Natalia V. Persichkina, Assistant Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: VPersichkina@kantiana.ru

ТРЕБОВАНИЯ И УСЛОВИЯ ПУБЛИКАЦИИ СТАТЕЙ В ВЕСТНИКЕ БФУ ИМ. И. КАНТА

Правила публикации статей в журнале

1. Представляемая для публикации статья должна быть актуальной, обладать новизной, содержать постановку задач (проблем), описание основных результатов исследования, полученных автором, выводы, а также соответствовать правилам оформления.

2. Материал, предлагаемый для публикации, должен быть оригинальным, не публиковавшимся ранее в других печатных изданиях. При отправке рукописи в редакцию журнала автор автоматически принимает на себя обязательство не публиковать ее ни полностью, ни частично без согласия редакции.

3. Рекомендованный объем статьи для докторантов и докторов наук — 20—30 тыс. знаков с пробелами, для доцентов, преподавателей и аспирантов — не более 20 тыс. знаков.

4. Список литературы должен составлять от 15 до 30 источников, не менее 50 % которых должны представлять современные (не старше 10 лет) публикации в изданиях, рецензируемых ВАК и (или) международных изданиях. Оптимальный уровень самоцитирования автора — не выше 10 % от списка использованных источников.

5. Все присланные в редакцию работы проходят ***внутреннее*** и ***внешнее рецензирование***, а также проверку системой «Антиплагиат», по результатам которых принимается решение о возможности включения статьи в журнал.

6. Статья на рассмотрение редакционной коллегией направляется ответственному редактору по e-mail. Контакты ответственных редакторов: *http://journals.kantiana.ru/vestnik/contact_editorial/*

7. Статьи на рассмотрение принимаются в режиме онлайн. Для этого авторам нужно зарегистрироваться на портале Единой редакции научных журналов БФУ им. И. Канта *http://journals.kantiana.ru/submit_an_article* и следовать подсказкам в разделе «Подать статью онлайн».

9. Решение о публикации (или отклонении) статьи принимается редакционной коллегией журнала после ее рецензирования и обсуждения.

10. Автор имеет право публиковаться в одном выпуске «Вестника Балтийского федерального университета им. И. Канта» один раз; второй раз в соавторстве — в исключительном случае, только по решению редакционной коллегии.

Комплектность и форма представления авторских материалов

1. Статья должна содержать следующие элементы:

1) индекс УДК — должен достаточно подробно отражать тематику статьи (основные правила индексирования по УДК см.: *http://www.naukapro.ru/metod.htm*);

2) название статьи строчными буквами на русском и английском языках *(до 12 слов)*;

3) аннотацию на русском и английском языках *(150 – 250 слов, то есть 500 печатных знаков)*. Располагается перед ключевыми словами после заглавия;

4) ключевые слова на русском и английском языках *(4 – 8 слов)*. Располагаются перед текстом после аннотации;

5) список литературы *(примерно 25 источников)* оформляется в соответствии с ГОСТ Р 7.0.5. — 2008;

7) сведения об авторах на русском и английском языках (Ф. И. О. полностью, ученые степени, звания, должность, место работы, e-mail, контактный телефон);

8) сведения о языке текста, с которого переведен публикуемый материал.

2. Ссылки на литературу в тексте статей даются только в квадратных скобках с указанием номера источника из списка литературы, приведенного в конце статьи: первая цифра — номер источника, вторая — номер страницы (например: [12, с. 4]).

3. Рукописи, не отвечающие требованиям, изложенным в пункте 1, в печать не принимаются, не редактируются и не рецензируются.

Общие правила оформления текста

Авторские материалы должны быть подготовлены ***в электронной форме*** в формате листа А4 (210 × 297 мм).

Все текстовые авторские материалы принимаются исключительно в формате *doc* и *docx* (Microsoft Office).

Подробная ***информация о правилах оформления текста***, в том числе ***таблиц, рисунков, ссылок и списка литературы***, размещена на сайте Единой редакции научных журналов БФУ им. И. Канта: *http://journals.kantiana.ru/vestnik/monograph/*.

Рекомендуем авторам ознакомиться с информационно-методическим комплексом «Как написать научную статью»: *http://journals.kantiana.ru/authors/imk/*.

Порядок рецензирования рукописей статей

1. Все научные статьи, поступившие в редколлегию Вестника БФУ им. И. Канта, подлежат обязательному рецензированию. Отзыв научного руководителя или консультанта не может заменить рецензии.

2. Ответственный редактор серии определяет соответствие статьи профилю журнала, требованиям к оформлению и направляет ее на рецензирование специалисту, доктору или кандидату наук, имеющему наиболее близкую к теме статьи научную специализацию.

3. Сроки рецензирования в каждом отдельном случае определяются ответственным редактором серии с учетом создания условий для максимально оперативной публикации статьи.

4. В рецензии освещаются следующие вопросы:

а) соответствует ли содержание статьи заявленной в названии теме;

б) насколько статья соответствует современным достижениям научно-теоретической мысли;

в) доступна ли статья читателям, на которых она рассчитана, с точки зрения языка, стиля, расположения материала, наглядности таблиц, диаграмм, рисунков и формул;

г) целесообразна ли публикация статьи с учетом ранее выпущенной по данному вопросу литературы;

д) в чем конкретно заключаются положительные стороны, а также недостатки статьи, какие исправления и дополнения должны быть внесены автором;

е) рекомендуется (с учетом исправления отмеченных рецензентом недостатков) или не рекомендуется статья к публикации в журнале, входящем в Перечень ведущих периодических изданий ВАК.

5. Рецензирование проводится конфиденциально. Автор рецензируемой статьи может ознакомиться с текстом рецензии. Нарушение конфиденциальности допускается только в случае заявления рецензента о недостоверности или фальсификации материалов, изложенных в статье.

6. Если в рецензии содержатся рекомендации по исправлению и доработке статьи, ответственный редактор серии направляет автору текст рецензии с предложением учесть их при подготовке нового варианта статьи или аргументированно (частично или полностью) их опровергнуть. Доработанная (переработанная) автором статья повторно направляется на рецензирование.

7. Статья, не рекомендованная рецензентом к публикации, к повторному рассмотрению не принимается. Текст отрицательной рецензии направляется автору по электронной почте, факсом или обычной почтой.

8. Наличие положительной рецензии не является достаточным основанием для публикации статьи. Окончательное решение о целесообразности публикации принимается редколлегией серии.

9. После принятия редколлегией серии решения о допуске статьи к публикации ответственный секретарь серии информирует об этом автора и указывает сроки публикации.

Текст рецензии направляется автору по электронной почте, факсом или обычным почтовым отправлением.

10. Оригиналы рецензий хранятся в редколлегии серии и редакции «Вестника Балтийского федерального университета им. И. Канта» в течение пяти лет.

Научное издание

ВЕСТНИК
БАЛТИЙСКОГО ФЕДЕРАЛЬНОГО УНИВЕРСИТЕТА
им. И. КАНТА

2020

Серия

Физико-математические и технические науки

№ 4

Редактор *Д. А. Малеванная.* Корректор *С. В. Ильина*
Компьютерная верстка *Г. И. Винокуровой*

Подписано в печать 23.03.2021 г.
Формат 70×108 1/16. Усл. печ. л. 10,2
Тираж 1000 экз. (1-й завод 41 экз.). Цена свободная. Заказ 27
Подписной индекс 94112

Издательство Балтийского федерального университета им. Иммануила Канта
236022, г. Калининград, ул. Гайдара, 6