Российский государственный гуманитарный университет
Russian State University for the Humanities

RSUH/RGGU BULLETIN
№ 1 (1)

Academic Journal

Series:
Information Science. Information Security.
Mathematics

Moscow
2018

ВЕСТНИК РГГУ
№ 1 (1)

Научный журнал

Серия
*«Информатика. Информационная безопасность.
Математика»*

Москва
2018

Ответственный за выпуск: АД. Козлов, канд. тех. н., проф. (РГГУ)

СОДЕРЖАНИЕ

CONTENTS

От главного редактора

Начало выпуска новой серии «Вестника РГГУ»

В современном мире трудно отыскать государство, которое распределяло бы финансовые и другие ресурсы в различные отрасли науки таким образом, чтобы удовлетворить все потенциальные запросы исследователей.

В начале текущего десятилетия в Указе Президента Российской Федерации от 7 июля 2011 г., № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники» были определены восемь приоритетных направлений научных исследований в России, включая индустрию наносистем, информационно-телекоммуникационные системы, космические и транспортные системы, безопасность и противодействие терроризму. Этот документ подтвердил то серьезное внимание, которое в нашей стране с начала XXI века стало уделяться целому ряду вопросов развития информационных технологий, а также обеспечению информационной безопасности объектов информатизации. А, как известно, основной составляющей информационных технологий является *информатика* – область научного знания, которая пронизывает практически все сферы экономики и науки и которую изучают в средней школе, колледже, университете и аспирантуре.

В июле 2017 г. Правительством Российской Федерации был принят важнейший документ: Распоряжение Правительства РФ от 28 июля 2017 г., № 1632-р «Об утверждении программы “Цифровая экономика Российской Федерации”», в соответствии с которым обозначены стратегические направления и технологии для страны: квантовые технологии, компоненты робототехники и сенсорика, большие данные, нейротехнологии и искусственный интеллект, технологии беспроводной связи и ряд других.

Но развитие информатики и информационных технологий в XXI веке немыслимо без обеспечения информационной безопасности предприятий и организаций, призванной если не свести к нулю, то хотя бы минимизировать уязвимость и угрозы личности, бизнесу и государству, связанные с применением современных не только информационных, но и инновационных технологий, а также уменьшить наблюдающийся в последние годы рост масштабов компьютерной преступности практически во всех отраслях экономики мира и России.

Утвержденный в России за последние три года ряд нормативно-правовых актов в области защиты информации, в числе которых «Стратегия национальной безопасности Российской Федерации»

(2015), «Доктрина информационной безопасности Российской Федерации» (2016), «О стратегии развития информационного общества Российской Федерации на 2017–2030 гг.» (2017) и др., также свидетельствует о повышении уровня внимания в нашей стране со стороны государства и общества к различным направлениям комплексного обеспечения информационной безопасности, включая ее правовые, организационные и программно-аппаратные аспекты.

Что касается математики, то еще Г. Галилей заметил, что природа формулирует свои законы языком математики, а М.В. Ломоносов подтвердил: «Все, что без этого было темно, сомнительно и неверно, математика сделала ясным, верным и очевидным».

Поэтому заключительным тематическим направлением настоящей серии журнала «Вестник РГГУ» стала «*математика* – наука, брошенная человеком на исследование мира в его возможных вариантах» (И. Кант).

От имени редакции желаю всем потенциальным авторам журнала «Вестник РГГУ» (серия «Информатика. Информационная безопасность. Математика») успехов в научной деятельности; редакция ожидает от авторов активного отражения в журнале своих достижений (в статьях с высоким уровнем оригинальности) в области всех трех отраслей науки: информатики, информационной безопасности и математики, а также в смежных с ними сферах знаний.

Валерий В. Арутюнов

From the chief editor

Issuing the new series of “RSUH/RGGU BULLETIN”

In nowadays world, it is difficult to find a state that would distribute financial and other resources to various branches of science in such a way as to satisfy all potential inquiries of researchers.

At the beginning of this decade, the Decree of the President of the Russian Federation dated July 7, 2011 No. 899 “On the approval of priority areas for the development of science, technology and engineering” determined eight priority areas for scientific research in Russia, including the industry of nano-systems, information and telecommunication systems, space and transport systems, security and countering terrorism. This document confirmed the serious attention that since the beginning of the 21st century has begun to be paid in our country to a number of issues of information technology development, as well as to ensuring information security of information objects. And, as you know, the main component of information technology is Informatics, an area of scientific knowledge that permeates virtually all areas of economics and science, and which is studied in high school, college, university and graduate school.

In July 2017, the Government of the Russian Federation adopted the most important document: Order of the Government of the Russian Federation of July 28, 2017 No. 1632-p “On Approval of the Program “Digital Economy of the Russian Federation” according to which strategic directions and technologies for the country are designated, they are quantum technologies; components of robotics and sensorics; big data; neurotechnology and artificial intelligence; wireless technology and several others.

But the development of informatics and information technologies in the 21st century is unthinkable without ensuring the Information security of enterprises and organizations, what is designed, at least minimize, if not to reduce to zero, the vulnerabilities and threats to the personality, business and government associated with the use of modern not only the information, but also the innovative technologies and also to reduce the growth of computer crime in recent years in almost all sectors of the economies of the world and Russia.

Over the past three years, a number of regulatory acts in the field of information security were approved in Russia, including “The National Security Strategy of the Russian Federation” (2015), “The Doctrine of Information Security of the Russian Federation” (2016), “On the Strategy for Developing an Information Society of the Russian Federation for 2017–2030” (2017) and others, that also testifies to an increase in the level of attention in our country from the state and society towards various areas of integrated information security, including its legal, organizational and software-hardware aspects.

As for mathematics, then G. Galilei noticed that nature formulates its laws in the language of mathematics, and M.V. Lomonosov confirmed: “Everything that without it was dark, doubtful and wrong, mathematics made clear, true and obvious.”

Therefore, the final thematic focus of this series of the Bulletin of the RSUH became “Mathematics – a science thrown by a man for the study of the world in its possible versions” (I. Kant).

On behalf of the editors, I wish a success in scientific work to all potential authors of the journal the Bulletin of the RSUH (the series “Informatics. Information Security. Mathematics”). The editors expect the authors to actively feature their achievements in the journal (in articles with a high level of originality) in the field of all three branches of the science: computer science, information security and mathematics, as well as in related fields of knowledge.

Valery V. Arutyunov

УДК 004.946

Информационная культура в виртуальном пространстве

Валерий В. Муромцев
Российский государственный гуманитарный университет, Москва, Россия, vvm44@inbox.ru

Анна В. Муромцева
Российский государственный гуманитарный университет, Москва, Россия, anmur37@yandex.ru

Аннотация. В статье рассматривается трансформация понятия «информационная культура» в контексте развития общей культуры человека в условиях современного виртуального пространства и виртуальных коммуникаций.

Ключевые слова: информационная культура, виртуальное пространство, информация, информационные технологии, виртуальные коммуникации, интернет вещей

Для цитирования: Муромцев В.В., Муромцева А.В. Информационная культура в виртуальном пространстве // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 11–19.

Information culture in the virtual space

Valery V. Muromtsev
Russian State University for the Humanities, Moscow, Russia, vvm44@inbox.ru,

Anna V. Muromtseva
Russian State University for the Humanities, Moscow, Russia, anmur37@yandex.ru

Abstract. The article discusses the transformation of the information culture concept in keeping with the personal general culture development in conditions of modern virtual space and virtual communications.

Keywords: information culture, virtual space, information, information technologies, virtual communications, Internet of things.

For citation: Muromtsev VV., Muromtseva AV. Information culture in the virtual space. *RSUH / RGGU Bulletin. “Information Science. Information Security. Mathematics” Series.* 2018;1(1):11-19.

Введение

Формирование информационной среды современного общества, включающей информационные ресурсы, информационные технологии и инфраструктуры, потребовало исследовать процессы, происходящие в рамках деятельности человека в данной среде.

Одним из понятий, которые появились при освоении человеком информационных технологий, является понятие информационной культуры.

Информационная культура современного общества основана на информационных технологиях, реализованных на виртуальных коммуникациях. При этом под виртуальной коммуникацией подразумевается «... такой процесс передачи информации, при котором искусственный канал связи создается неким сознанием, не являющимся статусным контрагентом данного информационного взаимодействия» [1].

Уровень информационной культуры человека все больше влияет на успешность его жизнедеятельности, расширяет его возможности и свободу действий. Сегодня, когда человек стал не просто созерцателем и получателем информации в виртуальном пространстве, а активным его участником, требуется изменить подходы к понятию информационной культуры, которая изначально относилась к потребностям одного человека.

Развитие сетевых информационных технологий, средств мобильной связи и, наконец, технологий Веб 2.0 требуют новых подходов к понятию информационной культуры в современном виртуальном пространстве.

Основываясь на определении информационной культуры как умении целенаправленно работать с информацией и использовать для ее получения, обработки и передачи компьютерную информационную технологию, современные технические средства и методы [2 с. 21], можно выделить основные составляющие информационной культуры:

- информационная грамотность;
- компьютерная грамотность;
- техническая грамотность.

Информационная культура может быть определена в рамках:

- государства;
- сообщества;

- организации (предприятия);
- отдельных категорий потребителей информации;
- человека.

Информационная культура выражается [3, 4 с. 184–190]:

- в умении извлекать информацию из различных виртуальных источников;
- в знании особенностей информационных потоков в своей области деятельности;
- в умении использовать различные виртуальные средства общения;
- в конкретных навыках по использованию технических устройств;
- в умении быстро осваивать новые информационные технологии;
- в умении работать с различными видами информации.

Доминирующая сегодня в обществе экранная культура складывалась на основе синтеза компьютерных и телекоммуникационных систем с видеотехникой. Для экранного мышления современного человека характерно сращивание логического и образного, понятийного и чувственно-наглядного рядов. Основой становится «экранная страница», которая является общечеловеческой и создает широкие возможности для общения, работы, развлечения и многого другого. Экранная культура тесно связана с информационной культурой, которая обеспечивает ее реализацию, используя информационно-коммуникационные технологии.

Письменный текст сегодня дополняется устной речью, видовыми изображениями, поведением изображаемых персонажей, анимационными методами, музыкальным звучанием и т. д. Как сам текст, так и любая программа может стать подвижной, многозначной и управляемой. Вместо однонаправленного потока информации реализуется диалог с элементами виртуального пространства, что находит выражение, например, в компьютерных играх, дистанционном обучении и т. д. [5 с. 538.].

Как в реальном, так и в виртуальном пространстве информационная культура современного человека формируется как понятие, интегрирующее несколько составляющих, и включает в себя такие компоненты, как [3, 6]:

- аудиовизуальная культура;
- логическая культура;
- семиотическая культура;
- понятийно-терминологическая культура;
- технологическая культура;
- коммуникационная культура;
- сетевая культура.

В рамках виртуального пространства в зависимости от того, чем занимается человек, можно говорить о делении информационной культуры на:

- технологическую;
- организационно-производственную;
- управленческую;
- научно-познавательную;
- информационную культуру словесного общения [7].

Все эти виды информационной культуры присутствуют у любого человека, однако один из них чаще всего является доминирующим, что зависит от вида его профессиональной деятельности.

В связи с широким распространением виртуальных коммуникаций культурное достояние общества человека утрачивает свое значение в том виде, в котором мы его привыкли видеть [8]. Для обычного человека становится важной не только сумма знаний, полученных в семье, школе, колледже, но и то, что он увидит по телевизору, в кино, прочтет в интернете, услышит по радио, узнает из разговора с сослуживцами или соседями. Таким образом, прежнее мировоззрение, составляющее целостную систему знаний и ценностей, дополняется набором переменчивых установок, на которые постоянно воздействуют различные виртуальные коммуникации.

Прежде всего следует обратить внимание на поведение человека в условиях виртуального коллектива, который включает не только людей, но и искусственные объекты и даже другие биологические объекты. Это вносит свои особенности в понятие информационной культуры.

Если ранее человек использовал информационную культуру исключительно в своих интересах, то сегодня он обязан взаимодействовать с другими участниками виртуальной реальности.

Человек в виртуальном пространстве не одинок, и его действия так или иначе отражаются на других участниках коммуникации. Это происходит из-за того, что информационные технологии используются по-другому, обеспечивая виртуальную реальность.

Реализуются они, например, средствами мобильного доступа в виртуальное пространство. Сегодня это массовое явление, практически у каждого человека имеются самые разнообразные средства мобильного доступа в виртуальное пространство. «Облачные технологии» освобождают современного человека от физических средств обработки информации, переводя этот процесс в виртуальное пространство [9 с. 455–458].

Разнообразные сервисы сети Интернет предлагают возможности доступа к ресурсам сети, осуществляют коммуникационное взаимодействие, реализуют информационные процессы в социальных сетях. Технологии Веб 2.0 просто предполагают для эффективного функционирования технологий участие как можно большего числа пользователей.

Процессы в денежно-финансовой сфере активно навязывают человеку уход от реальности в виртуальное пространство. Это и онлайн банкинг, и виртуальные валюты и т. д.

В области управления также все больше используется виртуальных инструментов, повышающих эффективность процесса управления. Это системы электронного документооборота, системы автоматизированного учета и распределения ресурсов, экспертные системы, системы поддержки управленческих решений и многое другое.

В виртуальном пространстве сегодня организуют свою деятельность предприятия, зачастую сами являющиеся виртуальными, осуществляются различные денежные операции, ведется общение на различных уровнях и др. Человек постоянно оказывается погружен в процессы работы с информацией и различными информационными технологиями. Все это отражается на информационной культуре человека.

Необходимо отметить, что деятельность человека в виртуальном пространстве сегодня небезопасна – его подстерегает множество угроз [10]. Это потеря конфиденциальности данных, их подмена, кража и т. д. Наверное, одной из главных опасностей является информационное воздействие – информационное управление, которое осуществляется как в открытом виде, так и воздействием на подсознание без контроля человека [11]. Формирование общественного мнения в социальных сетях, на телевидении, в радиопрограммах и т. д. является тому примером.

В рамках развития виртуальных сервисов интернета вещей [12 с. 231–237] создаются определенные проблемы, связанные с воздействием на реальное пространство действий в виртуальном пространстве.

Именно поэтому правомочно говорить об информационной культуре в виртуальном пространстве, которое всё больше проникает в нашу жизнь [13]. Информационное поле современного человека сверхнасыщено. Однако оно носит выборочный адресный характер в рамках виртуального пространства. Это выражается в увеличении числа каналов на телевидении, адресованных различным аудиториям, в уходе людей в различные социальные сети по профессиональным признакам, по интересам и др. Таким образом, происходит отход от централизованного распределения информации, и оно все больше становится персонализированным.

Одним из недостатков множества виртуальных коммуникаций в современном мире является доступность человеку во все большем объеме деструктивной информации, которую не всегда можно четко идентифицировать и отсеять. Поэтому выявить достоверную информацию из этого потока весьма сложно. Чем выше информационная культура человека, тем безопаснее его деятельность в виртуальном пространстве и тем сохраннее становятся ресурсы, которыми он пользуется.

Таким образом, процессы виртуализации деятельности требуют пересмотреть понятие информационной культуры с позиций деятельности человека в виртуальном пространстве.

Прежде всего человек в виртуальном пространстве сегодня не одинок, и от его действий зависит успех других участников. Это предъявляет определенные требования к его поведению в виртуальном пространстве. На аспекты информационной этики, эстетики, гигиены в рамках компьютерных информационных технологий и информационной безопасности, включающие меры по защите человеческой психики, обращает внимание в своих исследованиях Е.Н. Молчанова [14].

Другой исследователь информационной культуры, А.М. Атаян, предлагает при развитии информационной культуры личности выделять три уровня: общий (базовый), профессиональный и высший (логический).

Первый (общий, или базовый) уровень информационной культуры человека носит межпредметный характер и основан на наборе знаний, умений и навыков, которые дают возможность применения в различных сферах деятельности.

Второй, или профессиональный, уровень характеризуется ограниченностью области применения, но более высоким уровнем знаний, умений и навыков. Это связано с профессиональной деятельностью человека начиная с обучения его определенной профессии (колледж, вуз).

Для высшего уровня характерны реализация анализа, синтеза, комбинирования знаний, умений, навыков людей не только в своей профессиональной деятельности, но и в различных жизненных ситуациях, осуществление альтернативного поиска средств и способов решения поставленных задач [15].

Таким образом, от уровня информационной культуры зависит не только качество жизни человека, но и качество жизни людей, живущих рядом с ним, и организации, в которой он работает.

Информационная безопасность человека в виртуальном пространстве подвергается определенным угрозам как со стороны информационного контента, так и в психоинформационном плане. Информационное управление сопровождает человека в реальном и виртуальном мире. Контроль, за действиями человека в виртуальном пространстве более жесткий, чем в реальном мире.

Интернет вещей требует от человека определенной осторожности в действиях, которые могут нанести вред уже в реальном пространстве. И это не только сбор информации, кража личных данных, но и воздействие на устройства, подключенные к сети, которые могут нанести уже физический ущерб.

Таким образом, информационная культура в виртуальном пространстве – это совокупность знаний и умений безопасно действовать в виртуальном пространстве для достижения своих целей без ущерба другим участникам виртуального пространства.

Заключение

Сегодня развитие и активное использование информационных технологий привело к серьезным изменениям в жизни человека. Его коммуникации в реальном и, главное, в виртуальном пространстве приобрели совершенно иной смысл и возможности. Действия человека в виртуальном пространстве становятся более разнообразными с расширяющимися возможностями, но и не безопасными как для него самого, так и для других участников. Такое положение и привело к необходимости пересмотреть понятие информационной культуры.

Литература

1. *Батов В.И., Муромцев В.В., Муромцева А.В.* Виртуальная коммуникация как феномен культуры // Философские науки. 2008. № 7. С. 106.
2. Информатика: учеб. / под ред. Н.В. Макаровой. М.: Финансы и статистика, 2004. 768 с.
3. Информатика для гуманитариев: учеб. и практикум для академического бакалавриата / под ред. Г.Е. Кедровой. М.: Юрайт, 2018. 439 с. (Серия: Бакалавр. Академический курс).
4. *Муромцев В.В., Муромцева А.В.* Формирование информационной культуры в условиях доминирующей роли виртуальных коммуникаций // Социальное государство: Вызовы XXI века: Тр. XIII Чаяновских чтений. Москва, 14 марта 2013 / отв. ред. Н.И. Архипова. М.: РГГУ, 2013. 417 с.
5. *Ерасов Б.С.* Социальная культурология: Пособие для студентов высших учебных заведений. М.: Аспект Пресс, 1998. 591 с.
6. Информационная культура // Развитие сетевой журналистики. URL: https://sites.google.com/site/arzamastsevaks/home/informacionnaa-kultura (дата обращения 08 дек. 2018).
7. Информационная культура // UTMAG. URL: https://utmagazine.ru/posts/9829-informacionnaya-kultura (дата обращения 30 июля 2018).
8. *Моль А.* Социодинамика культуры. М.: Изд-во ЛКИ, 2008. 416 с.

9. *Гладков М.Ю.* Особенности внедрения «облачных» технологий в процессе управления организацией // Проблемы управления безопасностью сложных систем: Тр. междунар. конф. Москва, декабрь 2011 г. / под ред. Н.И. Архиповой, В.В. Кульбы. М.: РГГУ, 2011. 506 с.
10. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / под ред. Н.А. Кузнецова, В.В. Кульбы, Е.А. Микрина. М.: Наука, 2006. Т. 1. 495 с.
11. *Муромцев В.В., Немцова С.Р.* Проблемы психоинформационной безопасности в современном информационном пространстве // Информационные войны. 2014. № 2. С. 73–80.
12. *Гуриева М.Т.* Интернет вещей: анализ перспектив развития и проблем безопасности // Проблемы управления безопасностью сложных систем: Тр. XXV Междунар. науч. конф. Москва, декабрь 2017 г. / под ред. Н.И. Архиповой, В.В. Кульбы. М.: РГГУ, 2017. 652 с.
13. *Муромцев В.В., Немцова С.Р., Муромцева А.В.* Психоинформационная безопасность в медийном пространстве // Современные проблемы и задачи обеспечения информационной безопасности: Тр. Междунар. науч.-практ. конф. «СИБ – 2016». М.: МФЮА, 2016.
14. *Молчанова Е.Н.* Информационная культура как социокультурный конструкт информационного общества // SuperInf.ru. URL: https://superinf.ru/view_helpstud.php?id=3864 (дата обращения 08 дек. 2018)
15. *Атаян А.М.* Дидактические основы формирования информационной культуры личности в условиях информатизации общества: дис. ... канд. пед. наук. Владикавказ, 2001. 177 с.

References

1. Batov VI., Muromtsev VV., Muromtseva AV. Virtual communication as a phenomenon of culture // Philosophical sciences. 2008;7:106. (In Russ.)
2. Informatics. A textbook. 3rd ed. Makarova NV., ed. Moscow: Finansy i statistika Publ.; 2004. 768 p., Ill. (In Russ.)
3. Informatics for the humanities scholars. A textbook and a practical tutorial for bachelorship. Cedar GE., ed. Moscow: Yurait Publ.; 2018. 439 p. Bachelor. Academic course series. (In Russ.)
4. Muromtsev VV., Muromtseva AV. Forming the information culture under the dominant role of virtual communications. V: The welfare state. Challenges of the 21th century. Proceedings of the XIII Chayanov Conference. Moscow, March 14, 2013. Arkhipova NI., ed. Moscow: RGGU Publ.; 2013. 417 p. (In Russ.)
5. Erasov BS. Social cultural studies. A handbook for students in higher educational institutions. Moscow: Aspect Press Publ.; 1998. p. 538. (In Russ.)
6. Information Culture. Development of online journalism. [Internet]. [data obrashcheniya 08 dec. 2018]. URL: https://sites.google.com/site/arzamastsevaks/home/informacionnaa-kultura (In Russ.)
7. Information Culture. UTMAG. [Internet]. [data obrashcheniya 30 jul. 2018]. URL: https://utmagazine.ru/posts/9829-informacionnaya-kultura (In Russ.)
8. Mol' A. Sociodynamics of culture. Moscow: Izdatel'stvo LKI Publ.; 2008. p. 416. (In Russ.)

9. Gladkov MYu. Features of the introduction of “cloud” technologies in the management of the organization. V: Issues of security management of complex systems. Proceedings of the International Conference. Moscow, December 2011. Arkhipova NI., Kul’ba VV., eds. Moscow: RGGU Publ.; 2011. 506 p. (In Russ.)
10. Information security of organizational management systems. Theoretical foundations. In 2 vols. Kuznetsov NA., Kul’ba VV., Mikrin EA., eds. Moscow: Nauka Publ.; 2006. Vol. 1. 495 p. (In Russ.)
11. Muromtsev VV., Nemtsova SR. Issues of psycho-informational security in the modern information space. *Information warfare*. 2014;2:73-80. (In Russ.)
12. Gurieva MT. Internet of objects. Analysis of development prospects and security issues. V: Issues of managing the security of complex systems. Proceedings of the 25th International Scientific Conference. Moscow, December 2017. Arkhipova NI., Kul’ba VV., eds. Moscow: RGGU Publ.; 2017. 652 p. (In Russ.)
13. Muromtsev VV., Nemtsova SR., Muromtseva AV. Psycho-informational security in the media space. V: Contemporary issues and tasks of ensuring information security. Proceedings of the International Scientific and Practical Conference “NIB–2016”. Moscow: MFUA Publ.; 2016. (In Russ.)
14. Molchanova EN. Information culture as a sociocultural construct of the information society. SuperInf.ru. [Internet]. [data obrashcheniya 08 dec. 2018]. URL: https://superinf.ru/view_helpstud.php?id=3864 (In Russ.)
15. Atayan AM. Didactic foundations for forming the information culture of the person within the society informatization conditions. [diss. ... kand. ped. nauk], Vladikavkaz, 2001. 177 p. (In Russ.)

Информация об авторах

Валерий В. Муромцев, кандидат технических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; vvm44@inbox.ru

Анна В. Муромцева, кандидат филологических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; anmur37@yandex.ru

Information about the authors

Valery V. Muromtsev, PhD in Engineering, professor; Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993; Russia; vvm44@inbox.ru

Anna V. Muromtseva, PhD in Philology, associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993; Russia; anmur37@yandex.ru

УДК 004.45

Использование современных стандартов для описания архитектуры автоматизированной информационной системы

Леда А. Сысоева

Российский государственный гуманитарный университет, Москва, Россия, Leda@rggu.ru

Аннотация. Рассматриваются подходы к описанию архитектуры автоматизированных информационных систем, определенные в стандарте ГОСТ Р 57100-2016. Обоснована необходимость документированного описания архитектуры системы, представленной через множественные представления этой архитектуры. Приводится концептуальная модель описания архитектуры информационной системы.

Ключевые слова: автоматизированная информационная система, архитектура информационной системы, описание архитектуры информационной системы.

Для цитирования: Сысоева Л.А. Использование современных стандартов для описания архитектуры автоматизированной информационной системы // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. №1 (1). С. 20–27.

Use of modern standards for the description of architecture of the automated information system

Leda A. Sysoeva

Russian State University for the Humanities, Moscow, Russia, Leda@rggu.ru

Abstract. The approaches to the description of architecture of the automated information systems defined in the GOST R 57100-2016 standard are considered. Need of the documentary description of architecture of the system presented through multiple representations of this architecture is proved. The conceptual model for the description of architecture of an information system is given.

Keywords: the automated information system, architecture of an information system, the description of architecture of an information system.

For citation: Sysoeva LA. Use of modern standards for the description of architecture of the automated information system. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1): 20-27.

В настоящее время задача управления информационными системами организации не только относится к сфере управления информатизацией, но и становится важным компонентом при построении и управлении архитектурой предприятия в целом (Enterprise Architecture, EA).

За последние десятилетия был разработан ряд методологий в сфере управления архитектурой предприятия. Наибольшее применение в практической деятельности получили методология структуры Дж. Захмана для архитектуры предприятий (информационной системы), методология открытых групп TOGAF (The Open Group Architecture Framework), архитектура федеральной организации (FEA), обобщенная эталонная архитектура предприятия (GERA), методология Gartner (ранее именуемая Meta Framework) [1–4]. Для каждой методологии характерны свои концепции, подходы, наборы моделей, с помощью которых отражаются различные аспекты архитектуры, но в каждой из них применяется описание архитектуры. Рассмотрим нормативную базу для формирования описаний архитектуры.

Федеральным агентством по техническому регулированию и метрологии с 1 сентября 2017 г. был введен в действие национальный стандарт ГОСТ Р 57100-2016 «Системная и программная инженерия. Описание архитектуры» [5]. Стандарт направлен на всестороннее описание архитектуры сложной интегрированной информационной системы, способствует пониманию основных свойств, имеющих отношение к поведению, составу и развитию системы.

Объектами, на которые направлено действие стандарта, являются системы, которые созданы человеком и могут быть «сконфигурированы из одного или более следующих компонентов: аппаратных и программных средств, данных, людей, процессов, процедур, оборудования, материалов и образующихся сущностей» [5 с. 3].

Важно отметить, что стандарт ГОСТ Р 57100-2016 предназначен для различного круга лиц (сторон) – для тех, кто создает, применяет и управляет современными информационными системами, благодаря чему обеспечивается возможность совместной работы над совершенствованием и развитием системы в ходе ее жизненного цикла [6]. Для каждой из этих категорий работников создаются структуры архитектуры и языки описания архитектуры как средства систематизации соглашений и общих методов описания архитектуры в пределах их областей применения и сферы деятельности (см. рис. 2).

В основе методологии описания архитектуры лежат взаимосвязи между тремя составляющими: заинтересованными лицами, описываемой системой и ее архитектурой (рис. 1). Такая взаимосвязь обусловлена тем, что любая информационная система функционирует в некоторой окружающей среде и может быть представлена через описание архитектуры с позиций того или иного заинтересованного лица, имеющего определенный интерес к системе для реализации своих целей.

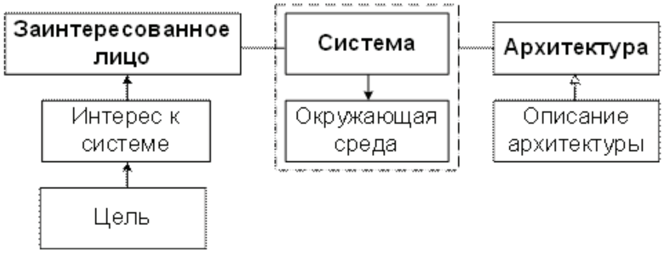


Рис. 1. Контекстная схема описания архитектуры [5 с. 3]

Термин «система» в контексте методологии ГОСТ Р 57100-2016 включает:

- «системы, которые созданы человеком и могут быть сконфигурированы из одного или более следующих компонентов: аппаратных и программных средств, данных, людей, процессов, процедур, оборудования, материалов и сущностей» [5 с. 3];
- программные продукты и услуги (ИСО/МЭК 12207) [6];
- программные системы.

Любую систему, в том числе программно-аппаратную, характеризуют:

- цели (взаимодействие всех элементов системы всегда направлено на достижение цели(ей));
- окружающая среда (система функционирует в окружающей среде).

В стандарте ГОСТ Р 57100-2016 окружающая среда системы определяет все множество воздействий на систему в ходе ее жизненного цикла, включая взаимодействие системы с самой окружающей средой, и ограничена определением и интересами заинтересованных сторон [5 с. 3]. Интересы сторон выражаются в виде конкретного результата или проблемы, которые могут быть получены или решены с использованием системы. Цели являются одним из видов выражения интересов.

Существует множество определений архитектуры системы. Приведем одно из наиболее общих определений: под архитектурой системы понимается «фундаментальная организационная структура, воплощенная в компонентах системы, их взаимоотношениях между собой и с окружением, и принципы, управляющие ее построением и эволюцией» [1].

В стандарте ГОСТ Р 57100-2016 отмечается, что «архитектура какой-либо системы представляет собой то, что является существенным относительно рассматриваемой системы в ее окружающей среде» [5 с. 3]. Следовательно, как сама архитектура, так и описание архитектуры системы зависит от того, что является существенным или основным для той или иной окружающей среды и с позиций заинтересованных сторон.

Схема взаимосвязей между компонентами, влияющими на процесс описания архитектуры информационной системы, приведена на рис. 2.

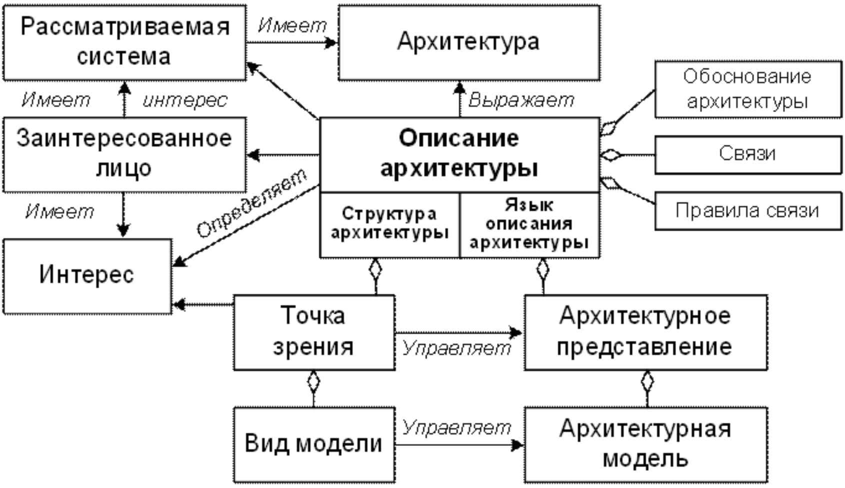


Рис. 2. Схема взаимосвязей между компонентами, влияющими на процесс описания архитектуры информационной системы [5]

Структура архитектуры определяет методологию создания описаний архитектуры, применение инструментальных средств моделирования архитектуры и методы создания, интерпретации, анализа и применения описания архитектуры сообществами заинтересованных лиц. Стандарт ГОСТ Р 57100-2016 рекомендует применять в качестве структуры архитектуры методологию структуры Дж. Захмана для информационной системы, методологию открытых групп TOGAF, обобщенную эталонную архитектуру предприятия (GERA) и др.

Выделяют несколько характеристик или групп характеристик, используемых при описании архитектуры:

– системные компоненты;
– взаимосвязи системных компонентов;
– обеспечение реализации бизнес-процессов;
– принципы организации системы;
– принципы управления развитием системы в ходе ее жизненного цикла.

В качестве языка описания архитектуры рекомендуется применять наборы различных видов моделей, позволяющих наиболее адекватно отражать характеристики системы и интересы сообществ заинтересованных сторон.

Концептуальную модель описания архитектуры информационной системы можно представить в виде схемы (рис. 3).

Описание архитектуры в соответствии с концептуальной моделью включает следующие этапы.

1. Определение группы характеристик, используемых при описании архитектуры (например, описание архитектуры с позиций обеспечения реализации бизнес-процессов организации).

2. Формирование групп заинтересованных лиц, которые имеют интересы, являющиеся важными для архитектуры системы (например: пользователи, операторы, разработчики, программисты, владельцы процессов, поставщики, сопровождающие систему, администрация и др.).

3. Выявление интересов для каждой группы заинтересованных лиц (например: цели системы, совершенствование архитектуры для достижения целей, оптимизация и совершенствование процессов, снижение потенциальных рисков, сопровождаемость и развитие системы, обеспечение реализации бизнес-процессов, распределение ответственности и др.).

4. Описание точек зрения, отражающих интересы каждой группы заинтересованных лиц (включает: методики процесса архитектуризации системы в течение ее жизненного цикла [7, 8]; процессы создания, интерпретации, анализа представлений, управляемых соответствующей точкой зрения; правила связи, критерии и методы проверки согласованности моделей; методы оценки и анализа представления архитектуры; методологии анализа и проектирования бизнес-процессов; принципы, методы, показатели, правила проектирования; регламенты процессов и др.).

5. Определение видов моделей, с помощью которых может быть описана каждая точка зрения (например: «ландшафт» процессов; карты стратегий; дерево целей и показателей; модели структурного, объектно-ориентированного анализа и моделирования;

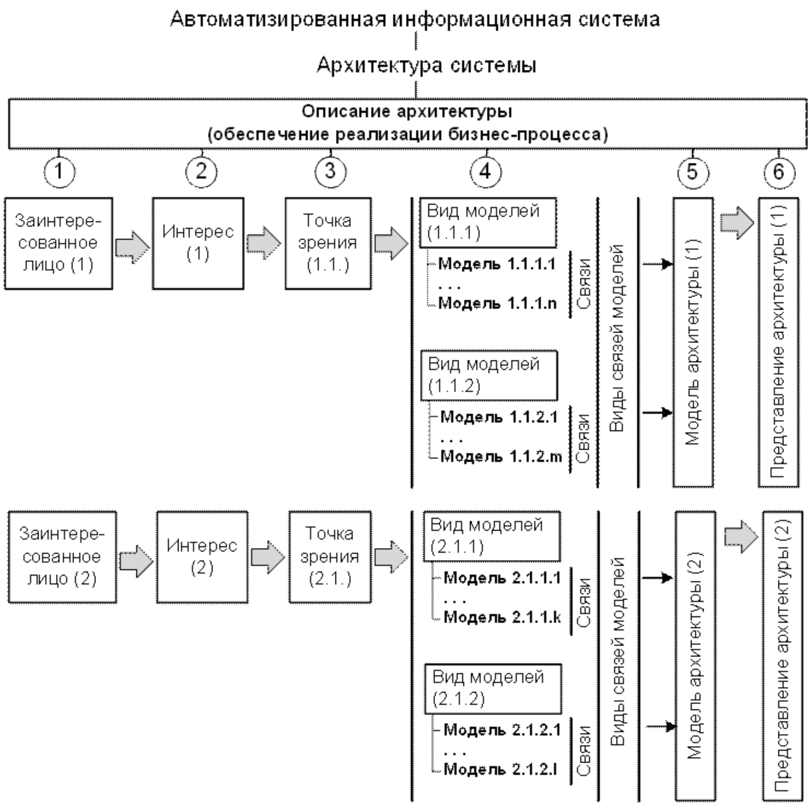


Рис. 3. Концептуальная модель описания архитектуры информационной системы

матрицы ответственностей; нотации представления процессов; стандарты взаимодействия и др.).

6. Описание видов связей и правил связи между элементами описания архитектуры (например: между моделями для обеспечения их согласованности, связности, интегрируемости, непротиворечивости).

7. Формирование модели архитектуры для каждой группы заинтересованных сторон на основе связанных между собой наборов моделей, отражающих определенные точки зрения.

8. Представление одной или нескольких моделей архитектуры.

Таким образом, в стандарте представлено, что одна и та же система может быть определена:

1) с помощью нескольких отличающихся архитектур (рассматривается система в различных окружающих средах);

2) с помощью нескольких отличающихся описаний архитектуры (имеются различные представления архитектур).

Данные положения подчеркивают, что архитектура системы наилучшим образом воспринимается через множественные представления этой архитектуры.

Каждое представление архитектуры определяется точкой зрения заинтересованных сторон. Точка зрения устанавливает условности для конструирования, интерпретации и анализа представления архитектуры.

Условности точки зрения включают: языки нотаций, виды моделей, правила проектирования и/или методы моделирования, методики анализа.

Необходимо отметить, что одним из требований к современным информационным системам, автоматизирующим реализуемые в организации бизнес-процессы, является быстрая адаптация ее функциональных возможностей к динамически изменяемым процессам [9]. Подобная адаптация АИС может быть выполнена при условии документированного описания архитектуры системы как целостной концепции основных ее свойств, представленной через множественные представления этой архитектуры.

Литература

1. ANSI/IEEE Std 1471-2000, IEEE Recommended practice for architectural description of software-intensive systems. URL: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf (дата обращения 20 окт. 2018).
2. The TOGAF Standard. URL: http://www.opengroup.org/togaf (дата обращения 20 окт. 2018).
3. ГОСТ Р ИСО 15704-2008. Промышленные автоматизированные системы. Требования к стандартным архитектурам и методологиям предприятия. Введ. 2010-03-15. М.: Стандартинформ, 2010. 48 с.
4. *Зиндер Е.З.* Архитектура предприятия в контексте бизнес-реинжиниринга. Часть 2 // Intelligent Enterprise. 2008. № 7. URL: http://www.iemag.ru/analitics/detail.php?ID=18024 (дата обращения 20 окт. 2018).
5. ГОСТ Р 57100-2016/ISO/IEC/IEEE 42010:2011. Системная и программная инженерия. Описание архитектуры. Введ. 2017-09-01. М.: Стандартинформ, 2016. 31 с.
6. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. Введ. 2012-03-01. М.: Стандартинформ, 2011. 100 с.
7. ГОСТ Р ИСО/МЭК 57102-2016. Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288. Введ. 2016-09-22. М.: Стандартинформ, 2016. 73 с.

8. ГОСТ Р 57193-2016. Системная и программная инженерия. Процессы жизненного цикла систем. Введ. 2016-10-16. М.: Стандартинформ, 2016. 98 с.
9. ITIL. URL: http://www.itil.co.uk / (дата обращения 20 окт. 2018).

References

1. ANSI/IEEE Std 1471-2000, IEEE Recommended practice for architectural description of software-intensive systems. [Internet]. [data obrashcheniya 20 oct. 2018]. URL: http://cabibbo.dia.uniroma3.it/ids/altrui/ieee1471.pdf
2. The TOGAF Standard. [Internet]. [data obrashcheniya 20 oct. 2018]. URL: http://www.opengroup.org/togaf.
3. GOST R ISO 15704-2008. Industrial automated systems. Requirements for standard enterprise architectures and methodologies. Intr. 2010-03-15. Moscow: Standartinform Publ.; 2010. 48 p. (In Russ.)
4. Zinder EZ. Enterprise architecture in business reengineering context. Part 2. Intelligent enterprise. 2008. № 7. [Internet]. [data obrashcheniya 20 oct. 2018]. URL: http://www.iemag.ru/analitics/detail.php?ID=18024 (In Russ.)
5. GOST R 57100-2016/ISO/IEC/IEEE 42010:2011. System and software engineering. Description of the architecture. Moscow: Standartinform Publ.; 2016. 31 p. (In Russ.)
6. GOST R ISO/IEC 12207-2010. Information technologies. System and software engineering. Software lifecycle processes. Intr. 2010-03-15. Moscow: Standartinform Publ.; 2011. 100 p. (In Russ.)
7. GOST R ISO/IEC 57102-2016. Information technologies. System and software engineering. Lifecycle management. Part 2. Usage guide ISO/IEC 15288. Moscow: Standartinform Publ.; 2016. 73 p. (In Russ.)
8. GOST R 57193-2016. System and Software Engineering. System Lifecycle Processes. Intr. 2016-10-16. Moscow: Standartinform Publ.; 2016. 98 p. (In Russ.)
9. ITIL [Internet]. [data obrashcheniya 20 oct. 2018]. URL: http://www.itil.co.uk /

Информация об авторе

Леда А. Сысоева, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; Leda@rggu.ru

Information about the author

Leda A. Sysoeva, PhD in Engineering, associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; Leda@rggu.ru

УДК 004.7

Анализ тенденций мирового патентования сетевых экранов

Ольга В. Маленкова
Российский государственный гуманитарный университет, Москва, Россия, ovm2030@yandex.ru

Игорь Н. Бычков
Всероссийская государственная библиотека иностранной литературы имени М.И. Рудомино, Москва, Россия, duke_199090@mail.ru

Аннотация. Проведен анализ патентования сетевых экранов. Для большинства культурно-просветительских организаций защита от угроз в сетевой инфраструктуре стала первоочередной для служб информационной безопасности. Большинство сетевых угроз в крупной сетевой инфраструктуре устраняется благодаря программно-аппаратным сетевым экранам. Выделены лидеры-патентообладатели среди стран, международных патентных союзов, частных организаций и государственных учреждений, а также изобретателей.

Для всех изобретений рассмотрена классификация по сферам применения. Относительно нее анализируется динамика патентования классов по годам подачи патентных заявок на изобретения. Дана оценка количественных показателей по данным классам, выделены наиболее востребованные в мире группы изобретений.

Ключевые слова: сетевые экраны, файрволл, брандмауэр, патенты, патентная динамика, патентная статистика, угрозы информационной безопасности, вычислительная сеть.

Для цитирования: Маленкова О.В., Бычков И.Н. Анализ тенденций мирового патентования сетевых экранов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. №1 (1). С. 28–38.

Trends analysis of global patenting for network firewalls

Olga V. Malenkova
Russian State University for the Humanities, Moscow, Russia, ovm2030@yandex.ru

Igor N. Bychkov
All-Russia State Library for Foreign Literature, Moscow, Russia, duke_199090@mail.ru

Abstract. The analysis of the network firewalls patenting is made. In most cultural and educational organizations the protection against threats to network infrastructure became a priority for information security services. The greater part of network threats in a large network infrastructure are eliminated thanks to software and hardware network screens. The article singles out leading patent owners among countries, international patent unions, private organizations, government agencies and inventors.

All inventions are classified by scope. The dynamics of class patenting by the year of filing patent applications for inventions is analyzed. The estimation of quantitative indicators according to those classes is given and the groups of the most demanded inventions in the world are highlighted.

Keywords: network screens, firewall, patents, patent dynamics, patent statistics, threats of information security, computer network.

For citation: Malenkova OV., Bychkov IN. Trends analysis of global patenting for network firewalls. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):28-38.

Введение

В век цифровых технологий, когда мировое сообщество глобализируется, становится более открытым и единым, любое государственное и частное учреждение культуры от районной библиотеки, выставочного зала, любительского театра, небольшого краеведческого до крупнейших национальных музеев, картинных галерей, киностудий и т. п. не может обходиться без собственной сетевой инфраструктуры.

Имея выход в Интернет благодаря локальной корпоративной сети учреждение автоматизирует не только повседневную деятельность, но и предоставляет онлайн-доступ для отечественных и зарубежных пользователей к шедеврам мировой изобразительной и театральной культуры, к историческим и литературным произведениям, к архивным памятникам и к новинкам беллетристики.

Главное в онлайн-доступе – это возможность самообразования для широкого круга пользователей. Помимо этого онлайн-доступ – это возможность прямого участия в жизни и развитии самого учреждения культуры путем шефской поддержки заинтересованных организаций, отдельных спонсорских дотаций, получение раритетов от дарителей, что способствует различным профильным исследованиям, реставрации помещений, расширению и обогащению экспозиций и архивов.

Говоря о великом открытии сетевого общения, нельзя забывать о тех угрозах, которые потенциально возможны в процессе функционирования сетевой инфраструктуры.

Одной из важнейших задач IT-специалистов является защита не только непосредственно целостной информации от модификаций и хищений, но также защита самой сетевой инфраструктуры как от внешних помех (в электропитании, на линиях связи, внедрение вирусов, хакерские атаки и др.), так и от внутренних сетевых сбоев, дестабилизирующих воздействий на информацию со стороны неопытных или умышленно вредоносных сотрудников и гостей культурных учреждений.

Не исключая использования таких защитных механизмов, как идентификация/аутентификация, разграничение доступа, протоколирование/аудит и др., не умаляя большой роли известных антивирусных программ, следует подробно остановиться на таком важном сервисе, как экранирование.

На периметрах сети устанавливаются так называемые сетевые экраны, представляющие собой «комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой, проводя анализ проходящего между ними трафика» [1].

Современный сетевой экран (файрволл, брандмауэр) позволяет реализовать более гибкую политику безопасности, комплексно охватывая сетевой, транспортный и прикладной уровни, анализируя трафик между компьютером и Интернетом или между компьютерами в разных подсетях или одной подсети. Главная функция межсетевых экранов – разграничение межсетевого доступа путем фильтрации информации с дополнительным контролем (например, по ip-адресам, антивирусным, с помощью механизмов аутентификации и др.).

Необходимость в сетевых экранах появилась относительно недавно, главным образом с развитием Интернета.

Определить тенденции развития межсетевых экранов, тренды рынков средств информационной безопасности, получить информацию по развитию производства межсетевых экранов позволяет анализ патентных баз.

Лидеры-патентообладатели

Самое раннее патентование изобретений для производства сетевых экранов зарегистрировано в 1993 г.

На сегодняшний день на рынке патентной собственности на производство сетевых экранов присутствуют две устойчивые группы патентообладателей:

– одна большая группа изобретателей включает коллективы, во главе которых стоят одна или несколько крупных государственных или частных организаций (например, университет, IT-корпорация, университет/госпредприятие и крупная IT-компания вместе, несколько частных корпораций и др.);
– штат другой группы составляют исключительно изобретатели.

Все сотрудники в обеих группах работают сообща и имеют минимум по четыре совместных патента. В табл. 1 представлены 10 крупнейших патентообладателей сетевых экранов по следующим группам: корпорации, государственные предприятия, изобретатели.

Классификация патентов в сфере сетевых экранов

Статистика утверждает, что количество патентов и заявок по сетевым экранам составляет около трех тыс. [2].

Все интересующие нас патенты, лежащие в основе производства сетевых экранов, можно разделить на три условных класса – Aggregate, Green, Orange.

Каждый класс имеет свои особенности и делится на соответствующие подклассы.

Рассмотрим конструктивно-функциональные возможности экранов каждого класса и подкласса в отдельности.

I. *Экраны класса Aggregate*. Все классы и подклассы взаимосвязаны с классом I Aggregate.

Специфика данного класса заключается в том, что изобретения, вошедшие в него, используются во всех сетевых экранах. Однако далее необходимо учесть, что подклассы Aggregate1–5 связаны только с классом Aggregate. А например подкласс Green1 (или Orange1) будет связан не только с Green (или Orange), но и с Aggregate.

В подкласс Aggregate1 вошли программно-аппаратные экраны, защищающие медиаустройства интерактивного контента.

Aggregate2 включает экраны, работающие по принципу создания избыточности (дополнительная маршрутизация, резервирование вычислительной нагрузки и пр.).

Aggregate3 – экраны, защищающие оборудование телефонных станций.

Aggregate4 – межсетевые экраны для защиты в цифровом ТВ.

Aggregate5 – для защиты систем видеотрансляций.

Таблица 1

ТОП-10. Известные корпорации, госпредприятия и изобретатели

№	Корпорации	Кол-во патентов	Государственные предприятия	Кол-во патентов	Изобретатели	Кол-во патентов
1	MICROSOFT CORP	188	UNIV WASHINGTON	14	RALEIGH GREGORY G	34
2	IBM	143	DISTRIBUTION SYSTEMS RES INST	13	ELLIS FRAMPTON ERROLL	33
3	AMAZON TECH INC	116	ZUK NIR	9	KOPONEN TEEMU	31
4	CISCO TECH INC	107	UNIV COLUMBIA	9	CASADO MARTIN	28
5	NICIRA INC	89	NEDERLAND PTT	4	RICHARDSON DAVID R	26
6	HEADWATER PARTNERS I LLC	85	COURT OF EDINBURGH NAPIER UNIVERSITY	3	LUNA MICHAEL	23
7	MCAFEE INC A DELAWARE CORP	61	UNIV MICHIGAN STATE	2	THAKKAR PANKAJ	17
8	JUNIPER NETWORKS INC	56	UNIV MICHIGAN	2	ERICSSON TELEFON AB L M	17
9	SEVEN NETWORKS INC	55	IND TECH RES INST	2	ALCATEL LUCENT	16
10	INTEL CORPORATION	54	UNIV WAKE FOREST	2	SIVASUBRAMANIAN SWAMINATHAN	14

II. *Экраны класса Green* с механизмами по обработке сетевых адресов на уровне ЭВМ, т.е. аппаратные устройства, занимающиеся анализом и обработкой сигналов на низком уровне.

Первый подкласс – это сетевые экраны, работающие на сетевом уровне сетевой модели ISO/OSI.

Второй подкласс экранов обрабатывает сигналы, поступающие по телефонным каналам связи.

Третий подкласс составляют специфические программно-аппаратные сетевые экраны, защищающие отдельные ЭВМ в сети.

Четвертый подкласс – экраны прикладного уровня, выполняющие проверку сетевых сообщений на уровне приложений (коммутация сообщений).

III. *Экраны класса Orange*. Разработаны для защиты конфиденциальной информации. Основной принцип таких устройств основан на механизмах авторизации отправителя и получателя информации. Единственный подкласс этого класса включает в себя самые «умные» экраны, способные выявлять и подавлять сетевые злоумышленные вторжения.

Укрупненная динамика патентования

Патентование по вышеназванным трем классам (рис. 1) показывает, что наибольшее количество патентов оформлено на сетевые экраны класса Green. Пик патентования отмечен в 2012 году. Такая тенденция отображает большую заинтересованность в мощных программно-аппаратных комплексах сетевой защиты, как правило, стоящей на рубеже сетевой инфраструктуры организаций между их внутренней инфраструктурой и сетью Интернет. Снижение количества подаваемых патентных заявок в 2008 и 2014 гг. объясняется мировыми экономическими кризисами.

Второе место по количеству патентов занимают «умные» сетевые экраны класса Orange. Разработки в данной сфере, как правило, сначала становятся достоянием различных служб безопасности крупных государственных институтов и корпораций и лишь после появления эффективных средств патентуются на мировом рынке «на экспорт». Данное предположение подтверждает динамика. До середины 2000-х график идет вверх вместе с графиком класса Green, что говорит о большом спросе на данные технологии со стороны рядового бизнеса на просторах Интернета. В середине 2000-х всемирная паутина активно внедряется в социум благодаря новым интернет-технологиям. Появляются социальные сети, бесплатная IP-телефония, набирает популярность интернет-банкинг, в большинстве стран активно развиваются свои

Рис. 1. Укрупненная динамика патентования по классам

электронные правительства, пользователи меньше смотрят телевизор и слушают радио, читая новости в Интернете; там же все чаще заказывают товары и получают дистанционное образование. Таким образом, если раньше интернет-преступник мог подорвать репутацию какого-нибудь банка или частного сайта, то после середины 2000-х через сеть Интернет уже можно подорвать национальную безопасность страны.

Наименьшим по количеству патентов является класс Aggregate. Скачок после 2011 года дают ему подклассы, связанные с видеотрансляциями и цифровым ТВ, ставшими в это время популярными благодаря активному вытеснению аналогового телевещания и внедрению онлайн-телетрансляций на популярных интернет-площадках и в социальных сетях.

Мировая статистика патентования по классам

На рис. 2 представлена диаграмма процентного распределения всех изобретений по вышеуказанным классам и подклассам.

На рисунке видно, что лидирующий интерес изобретателей был прикован к проблемам, которые по силам решить экранам типа Green (38,79%), Orange1 (14,16%), Aggregate (12,58%), Orange (9,8%), Green1 (9,37%) и Green3 (4,05%).

Рассмотрим динамику патентования классов (табл. 2). Самые малочисленные подклассы – Aggregate4, 1, 2; классы-лидеры – Green, Orange1, Aggregate. Самые ранние изобретения зарегистрированы в 1993 г. и были связаны с классами Green, Green1, Aggregate, Orange. Самые поздние (1998 г.) – Green2 и Agregate1.

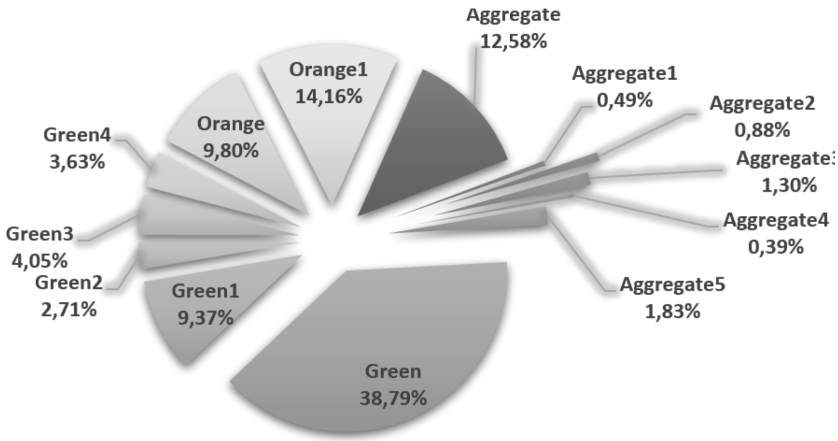


Рис. 2. Процентное соотношение патентов по классам сетевых экранов

Детальная динамика патентования по классам

В табл. 3 отображена динамика патентования по всем классам. Можно отметить, что первыми такие изобретения появились в классах Aggregate, Green, Green1 и Orange. В 1994 г. появляется изобретения в классе Orange1.

В 1995 г. в Web-технологиях наблюдается заметный рост развития, например появляется технология вызова различных приложений через окно WEB-браузера. Помимо этого в середине 1990-х появляются первые мультимедийные интернет-технологии, доступные как в ОС пользователей, так и в виде отдельных устройств, одновременно развиваются новые способы передачи сигналов в сети Интернет, что повлекло за собой новые сетевые угрозы и ответы на них изобретениями в 1996–1998 гг. Таким образом, в 1996 г. появляются первые изобретения в классах Green4, Aggregate4, 5. В 1997 г. – Green3, Aggregate3, в 1998 г. – Green2 и Aggregate2.

Интересна также картина динамики патентования за 2015–2017 гг. Отсутсвуют изобретения в классах Aggregate1 и 4, далее: на первом месте Green и Green1 (по 23%), второе место занимает Aggregate (19%), третье место Orange1 (13%) и Green3 (10%). Остальные классы занимают только 12%, а именно: 4% – Orange, 3% – Green4, 2% – Aggregate3, Aggregate2 и 5 по 1%.

Таблица 2

Динамика патентования классов по годам

Год/ Класс	G	O1	A	O	G1	G3	G4	G2	A5	A3	A2	A1	A4	Итог
1993	1		1	1	1									4
1994		1	1	1	1									4
1995	2	2	1	3	2									10
1996	11	3	7	9			3		1				1	35
1997	20	10	9	11	2	1	3			2			2	60
1998	16	6	6	13	2	4	9	5	2	1	1	2		67
1999	27	14	17	9	2	2	3	2	3			1	2	82
2000	53	10	21	11	3	1	6	2	3			1		111
2001	55	28	16	13	3	1	5	8	4	1	2	1	4	141
2002	59	28	10	13	13	5	4	9	5	1	2		1	150
2003	57	39	14	17	9	3	8	6	2	1	2			158
2004	67	43	11	17	5	1	3	3	4			3		157
2005	74	20	12	20	6	1	6	7	4	2		1	1	154
2006	72	22	19	22	7	3	8	2	1					156
2007	73	15	25	15	6	1	3	7	1					146
2008	43	13	7	14	10	1	6	1	3	3		1		102
2009	64	18	17	12	10	1	5	5	2	1	3			138
2010	75	13	22	13	8	7	1	3	2	2	1			147
2011	66	27	9	21	42	4	6	5	1		3			184
2012	103	19	24	18	18	21	8	6	2	6		1		226
2013	58	22	36	9	46	21	5	3	5	6	3	1		215
2014	52	18	27	6	17	14	4		4	7	6	2		157
2015	37	17	26	5	42	16	5	3	3	3	2			159
2016	12	12	12	4	7	6	2			1				56
2017	4	2	7	1	4	1								19
Итог	1101	402	357	278	266	115	103	77	52	37	25	14	11	2838

В табл. 3 можно увидеть распределение патентов между странами и международными патентными организациями. Самые активные страны – США (88%), Франция (0,87%) и Россия (0,59%); наименее активные – Корея и Нидерланды (всего по одному патенту); международные патентные организации ВОИС (WO) – 6%, Европейское патентное ведомство – 3% и Евразийская патентная организация – 0,173%.

Таблица 3

Распределение патентов между странами и международными патентными организациями

Страна	Кол-во
US	2521
WO	177
EP	99
FR	25
RU	17
CN	14
GB	11
AU	9
EA	5
JP	2
KR	1
NL	1

Заключение

В результате данного исследования можно сделать следующие выводы. Изобретениями в сфере сетевых экранов занимаются две устойчивые группы: лично изобретатели и группа, в которой материальную поддержку обеспечивают крупная частная или государственная организация и коллектив изобретателей. Больше всего патентуют изобретения крупные транснациональные организации, ведущие свой бизнес в сфере IT-технологий по трем группам: Aggregate (пять подклассов), Green (четыре подкласса), Orange (один подкласс). Укрупненная динамика патентования в данных классах показывает ответную реакцию изобретателей на рост угроз безопасности IT-инфраструктуры в сети в различных сферах жизни современного общества.

Большинство изобретений можно наблюдать в таких классах, как Green (38,79%), Orange1 (14,16%), Aggregate (12,58%), Orange (9,8%) и Green1 (9,37%). На сегодняшний день наиболее актуальными направлениями изобретатели считают сетевые экраны, обеспечивающие защиту по направлениям Green, Green 1 – первое место, Aggregate – второе место, Orange1 и Green3 – третье место.

Страны-лидеры патентования: первое место занимает США (2521 патент), второе – Франция (25 патентов), третье место с огромным отставанием от США – Россия (17 патентов).

Литература

1. Сетевые экраны // Компьютерные сети. Принципы, технологии, протоколы. URL: http://iptcp.net/setevye-ekrany.html (дата обращения 30 янв. 2019)
2. Патентная база «The Lens». URL: https://lens.org (дата обращения 30 янв. 2019)

References

1. etwork firewalls. Computer networks. Principles, technologies, protocols. [Internet]. [data obrashcheniya 30 jan. 2019]. URL: http://iptcp.net/setevye-ekrany.html. (In Russ.)
2. Patent base “The Lens”. [data obrashcheniya 30 jan. 2019]. URL: https://lens.org

Информация об авторах

Ольга В. Маленкова, кандидат технических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; Россия Москва, 125993, Миусская пл., д. 6; ovm2030@yandex.ru

Игорь Н. Бычков, научный сотрудник, Всероссийская государственная библиотека иностранной литературы имени М.И. Рудомино, Москва, Россия; Россия, Москва, 109240, ул. Николоямская, д. 1; duke_199090@mail.ru

Information about the authors

Olga V. Malenkova, PhD in Engineering, associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; ovm2030@yandex.ru

Igor N. Bychkov, researcher, All-Russia State Library for Foreign Literature, Moscow, Russia; bld. 1, Nikoloyamskaya st., Moscow, 109240, Russia; duke_199090@mail.ru

УДК 004.056

Многофакторная классификация угроз информационной безопасности киберфизических систем

Олег В. Казарин
Российский государственный гуманитарный университет, Москва, Россия,
Московский государственный университет
имени М.В. Ломоносова, Москва, Россия, okaz2005@yandex.ru

Ринат А. Шаряпов
Московский государственный университет имени М.В. Ломоносова,
Москва, Россия, Sharyapov@iisi.msu.ru

Валерий В. Ященко
Московский государственный университет имени М.В. Ломоносова,
Москва, Россия, iisi@iisi.msu.ru

Аннотация. В современном мире киберфизические системы, которые включают интернет вещей, индустриальный интернет, «умные» энергетические сети, системы больших данных, системы облачных и туманных вычислений, системы дополненной реальности и др., становятся основой научно-технологического развития. Киберфизические системы несут не только выгоды, но и серьезные угрозы для конкретного человека и общества в целом. Угрозы информационной безопасности киберфизических систем относятся к большим вызовам. Это определяет необходимость исследований и разработок в упреждающем режиме в области обеспечения информационной безопасности киберфизических систем.

Предложен многофакторный классификатор угроз информационной безопасности киберфизических систем. Для задач прогнозирования, обнаружения и оценки информационных угроз дана методология многофакторной классификации угроз информационной безопасности с указанием для выделенного фактора его возможных значений.

Рассмотрены концепция киберфизической системы и перспективы ее развития, показана взаимосвязь киберфизических систем с внутренними и внешними составляющими «общей картины мира», предложены основные технологические решения, относящиеся к таким системам. Приведена фактография, связанная с угрозами информационной безопасности киберфизических систем на примере интернета вещей. Проблема классификации угроз информационной безопасности киберфизических систем является задачей многофакторной экспертной классификации. На основе анализа угроз информационной безопасности определены уровни этих угроз, разработаны классификаторы угроз информационной безопасности, где эти системы выступают и как объект реализации, и как источник угроз.

Ключевые слова: информационная безопасность, угроза, фактор классификации угроз, многофакторная классификация, классификатор, киберфизическая система, интернет вещей, IoT устройство.

Для цитирования: Казарин О.В., Шаряпов Р.А., Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 39–55.

Multifactorial classification of threats to information security of cyber-physical systems

Oleg V. Kazarin

Russian State Humanities University, Moscow, Russia,
Lomonosov Moscow State University, Moscow, Russia, okaz2005@yandex.ru

Rinat A. Sharyapov

Lomonosov Moscow State University, Moscow, Russia, Sharyapov@iisi.msu.ru

Valery V. Yashchenko

Lomonosov Moscow State University, Moscow, Russia, iisi@iisi.msu.ru

Abstract. Nowadays cyber-physical systems which include Internet of things, Industrial Internet, “smart” energy networks, Big data systems, cloud and fog computing systems, augmented reality systems, etc., become the foundation of scientific and technological development. Cyber-physical systems bring not only the benefits, but also serious threats to an individual and the society as a whole. Threats to the information security of cyber-physical systems belong to grand challenges. This necessitates proactive research and development in the area of information security for cyber-physical systems.

A multifactorial classifier of the threats to the information security of cyber-physical systems is proposed. For the problems of forecasting, detection and evaluation of information threats the methodology of multifactorial classification of threats to information security is proposed with indication of possible values for the identified factor.

The article considers the cyber-physical system concept and the prospects for its development; there is an interrelation of cyber-physical systems and internal and external components of the “larger world picture”, and the main technological solutions related to cyber-physical systems are described. It gives some factual accounts with regard to threats to information security of cyber-physical systems by example of the Internet of things. The classification problem of threats to information security of cyber-physical systems is a problem of multifactorial expert classification. By the analysis of threats to information security the author proposes the levels of those threats, and also the information security threats classifiers where cyber-physical systems are acting both an object of realization and a source of threats.

Keywords: information security, threat, threat classification factor, multifactorial classification, classifier, cyber-physical system, internet of things, IoT device.

For citation: Kazarin OV., Sharyapov RA., Yashchenko VV. Multifactorial classification of threats to information security of cyber-physical systems. *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series.* 2018;1(1):39-55.

Введение

Угрозы информационной безопасности (ИБ) киберфизических систем (КФС) относятся к большим вызовам[1], еще не проявившимся и не получившим широкого общественного признания, для которых необходимы оценка рисков, обусловленных стремительным научно-технологическим развитием, и понимание процессов развития человеко-машинных систем [1].

На основе авторских концепций многофакторной классификации угроз ИБ и концепции киберфизической системы[2] в настоящей, некоторым образом прогнозной, работе предлагается многофакторный классификатор угроз ИБ КФС.

Сама по себе любая классификация, будучи научно обоснованной, является сравнительно новым итогом исследовательских работ подобного вида. И она во многом зависит от авторского миропонимания того, что же такое КФС, что они несут не только выгоды, но и серьезные угрозы для конкретного человека и общества в целом. А это часто угрозы, которые ранее не встречались и, следовательно, скорее всего на них нужно совершенно по-новому реагировать.

---

[1] Большие вызовы – объективно требующая реакции со стороны государства совокупность проблем, угроз и возможностей, сложность и масштаб которых таковы, что они не могут быть решены, устранены или реализованы *исключительно за счет увеличения ресурсов* [1].

[2] Которые, на взгляд авторов, представляют самостоятельный интерес.

1. Концепция многофакторной классификации угроз ИБ

В обновленной Доктрине информационной безопасности Российской Федерации дано следующее определение: «Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [2] .

Подчеркнем, что в настоящее время это определение имеет нормативно-правовой статус. В Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности. В частности, поставлены следующие задачи:

- прогнозирование, обнаружение и оценка информационных угроз;
- совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности.

Для решения указанных задач необходимо развивать методологию классификации угроз ИБ таким образом, чтобы классификация угроз была в большей мере ориентирована на принятие решений по обеспечению ИБ. А поскольку решения необходимо принимать разного уровня – стратегические, концептуальные, нормативно-правовые, нормативно-технические, организационные и др., то и классификация угроз должна быть по существу многофакторной.

Для выбора факторов классификации угроз ИБ был проведен системный анализ нормативно-правовой базы в области обеспечения ИБ [2–6], доступных материалов секции по информационной безопасности научного совета при Совете Безопасности Российской Федерации, обзорных материалов по состоянию ИБ России. На основе результатов проведенного анализа выбраны следующие факторы классификации угроз ИБ:

- уровень опасности последствий реализации угрозы (далее – уровень опасности);
- цели и мотивация источников угроз (далее – цели и мотивация);
- носитель угрозы (далее – носитель);
- признаки проявления реализации угрозы (далее – признаки);
- механизмы и инструменты реализации угрозы (далее – механизмы).

Определим теперь для каждого выделенного фактора множество его возможных значений (табл. 1).

Таблица 1

Факторы классификации угроз ИБ

Факторы	Множество возможных значений
Уровень опасности	Низкий («синий»)
	Высокий («желтый»)
	Критический («красный»)
Цели и мотивация	Военно- политические
	Террористические
	Криминальные
	Вмешательство во внутренние дела государств
	Экономические
Носитель	Специализированное программное и/или программно-техническое и/или техническое средство
	Контент (смысл информации)
Признаки	Нарушение устойчивости функционирования объекта, имеющего встроенные или конвергентные информационные и коммуникационные технологии
	Нарушение доступности информационных ресурсов
	Нарушение целостности данных
	Нарушение конфиденциальности данных
	Нарушение социально-экономической стабильности
Механизмы	Сетевые протоколы (стек TCP/IP, M2M, др.)
	Системы закупки/обновления установленного ПО и/или поставки/замены установленного оборудования
	Механизмы внедрения программных, программно-аппаратных, аппаратных закладок
	Устройства, используемые внутренними злоумышленниками (интрудерами)[3]
	Социальные сервисы (блоги, чаты, мессенджеры, социальные сети, др.)
	Другие механизмы

[3] Например, флеш-карты, радиомодули, трансиверы, встраиваемые в USB-кабели или USB-, WiFi-, Bluetooth-, GSM-устройства и соединения, подключаемые к атакуемому компьютеру, и др.

Таким образом, методология многофакторной классификации угроз информационной безопасности состоит в следующем:

- во-первых, для каждого выделяемого класса угроз необходимо определять значение каждого из пяти факторов классификации,
- во-вторых, нужно следить за тем, чтобы не было разных классов, у которых совпадают значения всех пяти факторов классификации.

Необходимо подчеркнуть, что значения факторов «уровень опасности» и «цели и мотивация» определяются в большей мере не техническими характеристиками угроз, а типом атакуемого объекта. Поэтому уровень опасности естественно определять, основываясь на категорировании значимых объектов критической информационной инфраструктуры, предусмотренных Федеральным законом от 26 июля 2017 г. № 187-ФЗ.

В следующих разделах эта методология конкретизируется с точки зрения КФС, для чего необходимо сначала определить, что же это такое.

2. Концепция киберфизической системы

В данном разделе концепция киберфизической системы (КФС) рассматривается как авторский способ описания, понимания и трактовки в заранее определенном смысле[4] этого сложного предмета (явления).

Киберфизическая система (от англ. – *Cyber-Physical System*, *CPS*), на наш взгляд, – это система, в которой осуществляется тесная (возможно, полная) конвергенция[5] физических[6] и информационно-вычислительных (компьютерных) процессов для создания качественно нового уровня (и охвата) управления и обеспечения функционирования естественных и/или искусственных объектов.

Многие исследователи, как и авторы настоящей работы, рассматривают КФС как следующий (естественный), эволюционный этап развития встроенных систем (Embedded Systems) [7–9]. При проектировании встроенных систем предполагалось их пусть и ограниченное, но включение в существующую систему. При проектировании КФС предполагается, что они являются неотъемлемой частью создаваемой системы, перестают быть в некотором смысле отдельной, автономной составляющей. В отличие от встроенных систем состав компонентов КФС и связей между ними, как правило, может меняться во времени.

---

[4] В том числе в смысле информационной безопасности.

[5] Включающая взаимопроникновение, взаимодействие, взаимосвязь, взаимозависимость процессов.

[6] Например, механических, биологических, химических и даже когнитивных процессов.

Будущие системы класса КФС объединят гетерогенные компоненты в единую систему с применением многочисленных контуров управления, состоящих из датчиков (сенсоров) и управляющих компьютеров (контроллеров). КФС смогут самостоятельно корректировать технологический процесс, проводить самодиагностику, самооптимизацию и самоконфигурацию, они станут активным компонентом, способным самостоятельно управлять этим процессом. Развитие КФС со временем увеличит их обучаемость, адаптируемость, эффективность и удобство использования, надежность, функциональную и информационную безопасность.

Перспективы развития КФС затронут большинство интересов индивида и общества и поэтому должны рассматриваться не только в технологическом, но и в более широком, социальном и гуманитарном измерении. Область применения КФС распространится практически на все виды человеческой деятельности, включая все многообразие промышленных, транспортных, энергетических систем, систем жизнеобеспечения, а также многих социотехнических систем.

Перечисленные системы скоро не будут соответствовать их строгому делению на системы физического и компьютерного мира, они будут вбирать в себя сопряжение физической модели их применения (использования, эксплуатации) и компьютерной модели управления ими.

На рис. 1 представлено видение взаимосвязи КФС с внутренними и внешними составляющими «общей картины мира» с их участием.

Рис. 1. Место КФС в «общей картине мира»

При этом особо подчеркивается, что КФС могут быть как объектом различных угроз[7], так и их источником.

К КФС уже сейчас можно отнести следующие решения:

- интернет вещей (Internet of Things, IoT);
- индустриальный интернет (Industrial Internet, II);
- «умные» энергетические сети (Smart Grid, SGr);
- системы больших данных (Big Data, BD);
- системы облачных и туманных вычислений (Cloud and Fog Computing, CFC);
- системы дополненной реальности (Augmented Reality, AR);
- робототехнические системы;
- системы 3D-печати и др.

КФС будут основой таких глубоко интегрированных решений, как:

- «умные» дома и города;
- «умные» фабрики и заводы;
- «умные» транспорт и логистика;
- «умная» медицина;
- «умные» боевые системы;
- «умные» сельское хозяйство и горнодобывающая промышленность и многих других.

Вполне закономерно предположить, что в будущем злоумышленники расширят спектр атак как на КФС, так и на другие системы с использованием КФС. Поэтому необходимы исследования и разработки в упреждающем режиме по обеспечению ИБ КФС. Классификация угроз ИБ КФС – лишь первый шаг в этом направлении.

3. Угрозы ИБ киберфизических систем

Рассмотрим некоторую фактографию, связанную с угрозами ИБ КФС, на примере интернета вещей, который может быть и источником таких угроз, и их объектом.

Недавняя активность IoT-ботнета Mirai, а также Hajime, BrickerBot, Persira [10], в котором основную массу устройств ботнета составляли «простейшие» IoT-устройства, в основном веб-камеры, дает основания предполагать, что уже сейчас существует зловредное ПО для потенциальных злоумышленников, которые, используя интернет вещей, могут осуществлять широкомасштабные атаки с серьезными последствиями.

Сегодня почти все IoT-устройства содержат критические уязвимости, которые могут легко эксплуатироваться злоумышленниками. Например, в настоящее время злоумышленники могут

---

[7] В том числе угроз ИБ.

потенциально получить доступ более чем к 3,5 млн камер по всему миру. При этом для доступа к видеоданным произвольно взятого пользователя требуется всего пара запросов к специализированной поисковой системе Shodan один – к Google и не более 60 сек времени. По разным оценкам, порядка 90% всех DVR-камер, которые используются для видеонаблюдения предприятиями малого и среднего бизнеса, содержат те или иные уязвимости и могут быть взломаны.

Не защищены от взлома компьютерные мыши и клавиатуры с радиоинтерфейсом и USB-трансивером. Собрать набор для проведения атаки можно всего за 300 руб., а вестись она может с расстояния до 1 км. Исследователи компании Positive Technologies протестировали безопасность устройств Logitech, A4Tech и Microsoft и смогли перехватить данные, передаваемые клавиатурами и мышами, дешифровать трафик и осуществить ряд других атак [11]. Обнаруженные уязвимости могут приводить к утечке паролей, платежных реквизитов, персональных данных и другой важной информации.

В ходе одного из исследований «умных» энергетических сетей (Smart Grid) эксперты обнаружили тысячи пользовательских Web-панелей управления системами мониторинга солнечных электростанций [12]. Примерно 5% систем вообще не требовали пароля для входа на страницу конфигурации, у остальных 95% систем пароль был, но его оказалось достаточно легко подобрать. Обойдя авторизацию, злоумышленник может удаленно установить модифицированную прошивку или просто поменять параметры системы, что может привести к аварии.

В 2017 г. в Интернет попали записи разговоров 800 тысяч клиентов компании Spiral Toys, производящей «умные» мягкие игрушки. Федеральное сетевое агентство Германии запретило «умных» кукол «Моя подруга Кайла», назвав игрушку шпионским устройством [13].

И, наконец, приведем специфичные угрозы, характерные исключительно для интернета вещей [14]. Недавно атаке подверглось одно из американских казино. Проникнуть в его сеть преступники смогли через «умный» аквариум, который игорное заведение установило для развлечения гостей. Аквариум с помощью специальных сенсоров регулировал температуру и соленость воды, а также кормил рыбок в автоматическом режиме. Предположительно преследовалась цель – получение персональных данных клиентов казино и/или нанесение материального ущерба владельцам казино.

Специалисты по безопасности после нескольких попыток сумели взломать «умный» холодильник Samsung модели RF28HMELBSR и получить учетные данные из аккаунта Gmail, так как компания-производитель не позаботилась о правильной проверке сертификата SSL при установке защищенного соединения с сервером Google. Аналогичной атаке подвергся и «умный» пылесос LG SmartThinkQ [10].

Таким образом, на наш взгляд, только эти примеры ярко характеризуют, насколько уязвим сегодня интернет вещей, составляющие его IoT-устройства и коммуникации между ними, насколько многообразен весь спектр таких уязвимостей.

Следовательно, возникает насущная необходимость в текущем и перспективном анализе потенциальных угроз для таких КФС, как интернет вещей, научно обоснованной их классификации. Попытка сделать это приводится ниже.

5. Многофакторная классификация угроз ИБ киберфизических систем

Из анализа предметной области следует, что задача классификации угроз ИБ КФС является задачей *многофакторной экспертной классификации*. Она заключается в выделении экспертами классификационных признаков, существенных в области угроз для КФС, и отнесении в соответствии с этими признаками угроз ИБ к выделенным группам и подгруппам (см. табл. 1).

Исходными данными для решения задачи составления классификатора угроз ИБ явились в том числе некоторые факторы классификации угроз ИБ (п. 1), типы и виды КФС (п. 2), информация о существующих угрозах ИБ (п. 3) и некоторый авторский прогноз их развития на видимую (среднесрочную) перспективу.

В результате ранжирования этих угроз по уровню опасности реализации их последствий как наиболее важной по мнению авторов составляющей классификации для КФС, можно установить следующие уровни:

- «красный» – возможны межгосударственные конфликты, техногенные катастрофы, нарушения социальной стабильности;
- «желтый» – возможны нарушения устойчивости функционирования объектов КФС как значимых объектов критической информационной инфраструктуры [6];
- «синий» – возможны нарушения устойчивости функционирования других объектов КФС.

При этом именно для КФС эти значения фактора «уровень опасности» являются определяющими.

В табл. 2 приведен классификатор угроз ИБ для КФС в соответствии с выделенными базовыми факторами. В табл. 3 источником угрозы является сама КФС, поэтому столбец «источник угрозы» классификации исключается.

Как и в почти любом классификаторе, желательно наличие элементов кодификации (см. 2-й столбец таблиц 2 и 3).

Таблица 2

Классификатор угроз ИБ, где объект реализации угрозы – КФС (с примерами)

Уровень опасности	Код угрозы	Источник угрозы (гипотезы, версии)	Объект реализации угрозы	Носитель	Признаки	Механизмы (гипотезы, версии)
1А. «Красный»	1А.а)	...	...	...	...	...
	1А.б)	Коллективы разработчиков, аффилированные со спецслужбами США и Израиля	АСУ ТП АЭС в г. Бушер (Иран)	Вредоносное ПО Stuxnet	Нарушение устойчивости функционирования системы управления центрифугами по обогащению урана, выход их из строя за счет недопустимого ускорения вращения	Системы обновления установленного ПО и замены установленного оборудования фирм Microsoft и Siemens
	1А.в)	...	...			
	...			...	...	...
1Б. «Желтый»	1Б.а)	Злоумышленники-любители	Система мониторинга солнечных электростанций	Вредоносное ПО	Нарушение устойчивости функционирования Web-панелей управления системами мониторинга солнечных электростанций	Протоколы удаленного и локального управления солнечными станциями (протоколы типа XUNBUS)
	1Б.б)	...		...	...	
	1Б.в)	...	...	...	...	...
			...			...

Продолжение таб. 2

Уровень опасности	Код угрозы	Источник угрозы (гипотезы, версии)	Объект реализации угрозы	Носитель	Признаки	Механизмы (гипотезы, версии)
1В. «Синий»	1В.а)	...	...	...	...	...
	1В.б)	...	...	...	...	...
	1В.в)	Злоумышленники – преступники, конкуренты	Аквариум, оборудованный выходом в Интернет и подключенный к локальной сети организации (казино)	Вредоносное ПО	Нарушение конфиденциальности информации за счет несанкционированного доступа к персональным данным клиентов, сотрудников, возможно, для вывода средств со счетов	Протоколы стека TCP/IP, протоколы типа Zeegbee, Z-Wave
	...	...	...	...	...	...

Таблица 3

Классификатор угроз ИБ, где источник угрозы – КФС (с примером)

Уровень опасности	Код угрозы	Объект реализации угрозы	Носитель	Признаки	Механизмы
2А. «Красный»	2А.а) 2А.б) 2А.в) ...				
2Б. «Желтый»	2Б.а) 2Б.б) 2Б.в) ...				
2В. «Синий	2В.а) 2В.б) 2В.в)	... Объекты-цели для ботнета, осуществляющего DDoS-атаки и использующего для этого IoT-устройства – DVR-камеры[8] ...	... Вредоносное ПО для организации DDoS-атак ...	... Нарушение доступности к системам Web-видеонаблюдения ...	... Протоколы стека TCP/IP ...

[8] Системы видеонаблюдения могут использоваться также для незаконного майнинга криптовалют и для спам-рассылок [15].

Приведенные классификаторы угроз ИБ КФС позволят на первых порах проанализировать их полноту и специфику. Со временем они естественным образом будут уточняться, конкретизироваться. Все это позволит, на взгляд авторов, оценить всю необычность такого нового технологического и социального явления, как КФС, и понять, какие специфичные угрозы ИБ возникают в связи с их развитием и становлением.

Заключение

Развитие КФС принципиально важно для любого государства, тем более поставившего одной из своих стратегических целей технологический прорыв, рывок в своем развитии.

Однако сейчас это удел фундаментально-поисковых и научно-исследовательских разработок, и задача государства на этом направлении – перевести имеющиеся проекты в практическое русло, например в рамках Стратегии научно-технического развития Российской Федерации [1] и правительственной программы «Цифровая экономика Российской Федерации» [16].

В настоящее время нет не только единого общепринятого определения КФС, но и нет единой мировоззренческой позиции по поводу того, что же это такое. Следовательно, нет и однозначного общепринятого понимания, что такое угрозы ИБ в их отношении, а в итоге – как, собственно, защищать КФС и их элементы. Некоторые первоначальные ответы на этот и подобные вопросы авторы и попытались дать в настоящей работе, которая скорее приглашает читателей к дальнейшему разговору, чем завершает такой разговор.

Литература

1. Стратегия научно-технического развития Российской Федерации (утв. Указом Президента Российской Федерации от 1 декабря 2016 года № 642) // АО «Кодекс». URL: http://docs.cntd.ru/document/420384257 (дата обращения 21 авг. 2018).
2. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 года № 646) // Российская газета. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения 21 авг. 2018).
3. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом Российской Федерации от 03 февраля 2012 года, № 803) // Законодательство РФ. URL: http://legalacts.ru/doc/

osnovnye-napravlenija-gosudarstvennoi-politiki-v-oblasti-obespechenija/ (дата обращения 21 авг. 2018).
4. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом Российской Федерации от 24 июля 2013 года № Пр-1753) // Законодательство РФ. URL: http://legalacts.ru/doc/osnovy-gosudarstvennoi-politiki-rossiiskoi-federatsii-v-oblasti/ (дата обращения 21 авг. 2018).
5. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (утв. Указом Президента Российской Федерации от 09 мая 2017 года № 203) // ГАРАНТ.РУ. URL: http://www.garant.ru/products/ipo/prime/doc/71570570/ (дата обращения 21 авг. 2018)
6. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 21 авг. 2018).
7. *Быковский С.В., Горбачев Я.Г., Ключев А.О.* и др. Сопряженное проектирование встраиваемых систем (Hardware/Software Co-Design). Часть 1. Учеб. пособие. СПб.: Университет ИТМО, 2016. 108 с.
8. *Майнцер К.* Исследуя сложность: от искусственной жизни и искусственного интеллекта к киберфизическим системам // Философия науки и техники. 2015. Т. 20. № 2. С. 85–105.
9. *Петров А.А.* Цифровая экономика: вызов России на глобальных рынках // Торговая политика. Trade policy. 2017. № 3/11. С. 46–74.
10. Эксперты об информационной безопасности в Интернете вещей // Индустрия 4.0. Цифровизация. 2018. № 1(1). С. 50–52.
11. Эксперты Positive Technologies прогнозируют рост угроз Интернету вещей // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/about/news/257662/ (дата обращения 21 авг. 2018).
12. Как обезопасить интернет вещи. Интервью Антона Тюрина и Павла Новикова // Информационная безопасность. 2017. № 3.URL: http://www.itsec.ru/articles2/focus/kak-obezopasit-internet-veschi (дата обращения 21 авг. 2018).
13. Кукол My Friend Cayla в Германии запретили за шпионаж // Defense Laboratory. Раздел «Новости». URL: http://deflab.ru/news/Kukol-My-Friend-Cayla-v-Hermanyy-zapretyly-za-shpyonazh.html (дата обращения 21 авг. 2018).
14. *Варфоломеева В.В., Казарин О.В., Климов А.А., Лисняк Е.О.* Подходы к классификации киберугроз и кибератак для Интернета вещей // Междунар. науч.-практ. конф. «Информационная безопасность: вчера, сегодня, завтра». Сб. трудов. М.: РГГУ, 2018. С. 149–156.
15. *Полевщиков А.А.* Кибербезопасность сетевого видеонаблюдения: теория и практика // Алгоритм безопасности. 2017. № 5. С. 30–32.
16. Программа «Цифровая экономика Российской Федерации» (утв. Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р). URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 21 авг. 2018).

References

1. Scientific and technological development strategy of the Russian Federation (approved by the Executive Order of the President of the Russian Federation № 642 of December 1, 2016). AO “Kodeks”. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://docs.cntd.ru/document/420384257. (In Russ.)
2. Information security doctrine of the Russian Federation (approved by the Executive Order of the President of the Russian Federation № 646 of December 5, 2016). Rossiiskaya gazeta. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. (In Russ.)
3. The main directions of the State Policy in the field of security of automated control systems of industrial and technological processes of critically important infrastructure objects of the Russian Federation (approved by the President of the Russian Federation on February 03, 2012, № 803). Zakonodatel’stvo RF. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://legalacts.ru/doc/osnovnye-napravlenija-gosudarstvennoi-politiki-v-oblasti-obespechenija/.(In Russ.)
4. Fundamentals of the Russian Federation’s State Policy of the in the field of international information security for the period until to 2020 (approved by the President of the Russian Federation on July 24, 2013, № Pr-1753). Zakonodatel’stvo RF. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://legalacts.ru/doc/osnovy-gosudarstvennoi-politiki-rossiiskoi-federatsii-v-oblasti/. (In Russ.)
5. Strategy for the development of an information society in the Russian Federation for the period of 2017–2030 (approved by the Executive Order of the President of the Russian Federation No. 203 on May 9, 2017). GARANT.RU. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://www.garant.ru/products/ipo/prime/doc/71570570/. (In Russ.)
6. Federal Law № 187-FZ “On Security of Critical Russian Federation Information Infrastructure” (approved on June 26, 2017). SPS “Konsul’tantPlyus”. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/. (In Russ.)
7. Bykovskiy SV., Gorbachev YaG., Klyuchev AO. and etc. Coupled design of embedded systems (Hardware/Software Co-Design). Part 1. Training manual. Saint-Petersburg: University ITMO Publ.; 2016. 108 p. (In Russ.)
8. Maintser K. Exploring complexity. From artificial life and artificial intelligence to cyberphysical systems. *Philosophy of Science and Technology*. 2015;20:85-105. (In Russ.)
9. Petrov AA. Digital economy: Russia’s challenge in global markets. *Trade policy*. 2017;3:46-74. (In Russ.)
10. Experts on information security in the Internet of things. *Industry 4.0. Digitalization*. 2018;1:50-52. (In Russ.)
11. Positive Technologies’ Experts forecast the growth of threats to the Internet of things. Positive Technologies. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: https://www.ptsecurity.com/ru-ru/about/news/257662/. (In Russ.)
12. How to Secure IoT devices. Interview with Anton Tyurin and Pavel Novikov. *Journal “Information Security”*. 2017;3. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://www.itsec.ru/articles2/focus/kak-obezopasit-internet-veschi. (In Russ.)

13. My Friend Cayla dolls have been banned in Germany for espionage. News. Defense Laboratory. [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://deflab.ru/news/Kukol-My-Friend-Cayla-v-Hermanyy-zapretyly-za-shpyonazh.html. (In Russ.)
14. Varfolomeeva VV., Kazarin OV., Klimov AA., Lisniak EO. Approaches to the classification of cyberthreats and cyber attacks for the Internet of things. V: International scientific and practical conference “Information security: yesterday, today, tomorrow”. Collected works. Moscow: RGGU Publ.; 2018. p. 149-156. (In Russ.)
15. Polevshchikov AA. Cyber security of network video surveillance. Theory and practice. *Algoritm bezopasnosti*. 2017;5:30-32. (In Russ.)
16. The Program “Digital Economy of the Russian Federation” (approved by the Government of the Russian Federation in its resolution №. 1632-r of July 28, 2017). [Internet]. [data obrashcheniya 21 aug. 2018]. URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf. (In Russ.)

Информация об авторах

Олег В. Казарин, доктор технических наук, старший научный сотрудник, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; Московский государственный университет имени М.В. Ломоносова, Москва, Россия; Россия, Москва, 119991, Ленинские горы, д. 1; okaz2005@yandex.ru

Ринат А. Шаряпов, кандидат политических наук, Московский государственный университет имени М.В. Ломоносова, Москва, Россия; Россия, Москва, 119991, Ленинские горы, д. 1; Sharyapovr@iisi.msu.ru

Валерий В. Ященко, кандидат физико-математических наук, старший научный сотрудник, Московский государственный университет имени М.В. Ломоносова, Москва, Россия; Россия, Москва, 119991, Ленинские горы, д. 1; iisi@iisi.msu.ru

Information about the author

Oleg V. Kazarin, Dr. in Engineering, senior researcher, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; Lomonosov Moscow State University, Moscow, Russia; bld. 1, Leninskie Gory str., Moscow, 119991, Russia; okaz2005@yandex.ru

Rinat A. Sharyapov, PhD in Political Sciences, Lomonosov Moscow State University, Moscow, Russia; bld. 1, Leninskie Gory str., Moscow, 119991, Russia; Sharyapovr@iisi.msu.ru

Valery V. Yashchenko, PhD in Physics and Mathematics, senior researcher, Lomonosov Moscow State University, Moscow, Russia; bld. 1, Leninskie Gory str., Moscow, 119991, Russia; iisi@iisi.msu.ru

УДК 004.056:378

Политика информационной безопасности высшего учебного заведения

Ирина А. Русецкая
Российский государственный гуманитарный университет, Москва, Россия, irkom@mail.ru

Александр В. Захаренков
Российский государственный гуманитарный университет, Москва, Россия, zakh007@gmail.com

Аннотация. Статья посвящена выявлению основных подходов к построению политики информационной безопасности в вузах. В статье рассматриваются основные требования, которые следует учитывать при создании политики информационной безопасности российских вузов, включая как требования законодательства, так и требования к построению системы информационной безопасности в высшем учебном заведении. Одной из задач работы является рассмотрение этапов создания политики информационной безопасности с учетом изученных требований. В статье также анализируется примерная структура политики информационной безопасности, рассматриваются разделы документа и основные подходы к определению содержания каждого раздела. В заключение определяется основной круг задач в области обеспечения защиты информации и информационной безопасности вуза, которые помогает решить грамотно составленная политика информационной безопасности.

Ключевые слова: политика информационной безопасности, информационная безопасность, угрозы защищаемой информации, вуз.

Для цитирования: Русецкая И.А., Захаренков А.В. Политика информационной безопасности высшего учебного заведения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 56–64.

Information security policy of a higher educational institution

Irina A. Rusetskaya
Russian State University for the Humanities, Moscow, Russia, irkom@mail.ru

Alexander V. Zakharenkov
Russian State University for the Humanities, Moscow, Russia, zakh007@gmail.com

Abstract. The article is devoted to identifying the main approaches to the construction of information security policies in universities. The main requirements that should be considered while creating an information security policy for Russian universities, including both legal requirements and requirements for building an information security system at a higher educational institution, are given. One of the tasks of the work is to consider the stages of creating an information security policy, taking into account the requirements studied. An analysis of the approximate structure of the information security policy was carried out, sections of the document and the main approaches to determining the content of each section were considered. In conclusion, the principal range of tasks in the field of information security and information security of the university is determined, which a correctly formulated information security policy helps to solve.

Keywords: information security policy, information security, threats of protected information, higher school.

For citation: Rusetskaya IA., Zakharenkov AV. Information security policy of a higher educational institution. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):56-64.

Введение

Важную роль при обеспечении информационной безопасности высших учебных заведений играют разработка и внедрение политики информационной безопасности вуза. Этот документ позволяет на концептуальном уровне определить приоритеты вуза в области информационной безопасности и наметить основные пути ее обеспечения.

Целью данной статьи является анализ основных подходов к построению политики информационной безопасности вузов.

Для реализации указанной цели необходимо решение определенных задач: выявление требований, которые необходимо учитывать при создании политики; анализ основных этапов ее построения; изучение основного содержания разделов, составляющих политику информационной безопасности.

Основные требования к политике информационной безопасности вуза

При разработке политики информационной безопасности должен учитываться ряд требований.

Требование законности предполагает, что внедряемая политика безопасности должна соответствовать существующей нормативно-правовой базе. Это касается не только российского законодательства, но и международных стандартов, принятых и одобренных на государственном уровне, внутренних распорядительных документов вуза или договоров, заключаемых с третьими лицами и сторонними организациями.

Требование персональной ответственности предполагает, что должно быть назначено ответственное лицо – сотрудник, который будет отвечать за политику безопасности на протяжении всего ее жизненного цикла, т. е. при планировании политики, контроле ее выполнения, пересмотре, обновлении и т. д.

Требование актуальности означает, что политика безопасности должна соответствовать постоянно меняющимся реалиям деятельности вуза, обновляться и пересматриваться в соответствии с ними. Процесс обеспечения информационной безопасности связан с непрерывной деятельностью, а не с разработкой определенного комплекса мер и мероприятий. При планировании политики информационной безопасности необходимо учитывать возможность возникновения новых угроз защищаемой информации и в связи с этим предусматривать внесение изменений в положения рассматриваемого документа.

Требование контроля за политикой информационной безопасности вуза означает, что политику следует подвергать независимому внешнему аудиту, чтобы подтверждать ее эффективность, правильность и соответствие стандартам и требованиям нормативных документов.

Таким образом, при разработке политики информационной безопасности в вузе должны быть учтены требования действующего законодательства, современный уровень и ближайшие перспективы развития информационной системы учебного заведения, а также проведен анализ системы обеспечения информационной безопасности. Положения и требования в отношении политики информационной безопасности должны распространяться на все структурные подразделения высшего учебного заведения, задействованные в работе с защищаемой информацией. Основные положения политики могут быть также распространены на подразделения сторонних организаций, взаимодействующих с вузом при передаче конфиденциальных сведений.

Основные этапы разработки политики информационной безопасности вуза

Обязательным требованием работ на каждом этапе является учет требований, содержащихся в нормативных документах, регламентирующих работу вуза в целом и мероприятия, осуществляемые в области информационной безопасности.

Первый необходимый этап разработки политики содержит анализ всех циркулирующих в вузе информационных потоков и их классификацию в соответствии с уровнями требуемой защиты. На этом этапе важно упорядочить имеющиеся в распоряжении вуза информационные ресурсы и их разумную локализацию.

Следующий этап должен включать в себя анализ угроз безопасности защищаемой информации. При этом последовательно должны быть рассмотрены все составляющие структуры угрозы, информационные риски и модели нарушителей информационной безопасности. Основная задача этого этапа – выявление, с одной стороны, наиболее вероятных, а с другой – наиболее опасных явлений и событий, от которых предстоит защищать информационную систему. Для этого представляется возможным использование различных методов оценки, ранжирования и категорирования потенциально опасных явлений и событий.

Следует количественно определить, что представляет наибольшую опасность для вуза, какие из нарушений информационной безопасности способны привести к серьезным негативным последствиям, чтобы в первую очередь сконцентрироваться на нейтрализации именно этих угроз. Иными словами, целью данного этапа является ранжирование возможных угроз нарушения информационной безопасности для определения порядка организации защиты информации.

Третий этап – анализ существующей системы обеспечения информационной безопасности высшего учебного заведения, включающий изучение всех используемых видов, методов и средств защиты различных носителей информации, в том числе сотрудников подразделений, работающих с конфиденциальной информацией.

Анализ структуры политики информационной безопасности вуза

Далее обратимся к рассмотрению основных элементов структуры политики информационной безопасности.

«За основу может быть взята схема, предложенная международными стандартами, но так как стандарты носят рекомендательный характер, то любая другая структура документа возможна и даже желательна, если она будет лучше и четче отражать специфику разработки политики безопасности и более понятна всем сотрудникам, непосредственно связанным работой, использованием информационных систем и управлением информационной безопасностью» [1 с. 196].

Политика информационной безопасности вуза может быть основана на рекомендациях стандарта ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности» [2] и будет включать в себя следующие разделы:

– Общие положения;
– Цели и задачи деятельности вуза по обеспечению информационной безопасности;
– Описание объекта защиты;
– Угрозы информационной безопасности вуза;
– Модель нарушителя информационной безопасности вуза;
– Меры и мероприятия, обеспечивающие необходимый уровень информационной безопасности вуза;
– Основные методы и принципы создания системы безопасности;
– Требования к подготовке и осведомленности сотрудников вуза в области информационной безопасности;
– Ответственность за нарушение политики информационной безопасности;
– Контроль за соблюдением положений политики информационной безопасности;
– Порядок утверждения, пересмотра, внесения изменений и дополнений в политику;
– Документация, способная поддержать политику информационной безопасности.
– Изучение подходов к составлению содержания отдельных разделов политики информационной безопасности.

В разделе «Общие положения» должны содержаться указания на нормативные акты, которым подчиняется деятельность по информационной безопасности высшего учебного заведения, а также определена область применения разработанной политики. Так, разработка политики должна основываться на следующих нормативных документах: Доктрине информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646); Федеральном законе «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ; Федеральном законе «О персональных данных» от

27.07.2006 № 152-ФЗ; Федеральном законе «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

Второй раздел политики определяет основную цель и задачи образовательного учреждения в области обеспечения информационной безопасности. Также внимание в разделе должно быть уделено действиям, благодаря которым данная цель и задачи могут быть достигнуты.

Раздел «Описание объекта защиты» должен содержать перечень объектов системы информационной безопасности в современном высшем учебном заведении, перечисление категорий информационных ресурсов, подлежащих защите в вузе, и мест их размещения и обработки.

Раздел «Угрозы информационной безопасности вуза» включает в себя актуальный для вуза перечень угроз, который может быть разбит на три группы по природе их возникновения: угрозы, зависящие от действий внутренних и внешних нарушителей (преднамеренные и непреднамеренные), техногенные и стихийные. Основное внимание при создании системы информационной безопасности на основе разработанной политики следует обратить на первую и вторую группу угроз как наиболее поддающихся контролю.

«Модель нарушителя информационной безопасности вуза» представляет собой описание внутренних и внешних нарушителей информационной безопасности образовательного учреждения, принимаемых во внимание вследствие их наибольшей реальной и потенциальной опасности. Также в разделе могут быть рассмотрены наиболее вероятные предположения о характере возможных действий указанных злоумышленников.

В разделе, посвященном мерам обеспечения требуемого уровня защищенности информационных ресурсов вуза, должен быть приведен перечень основных существующих мер обеспечения информационной безопасности, которые оказывают противодействие нарушителям правил разграничения доступа.

Следующий раздел содержит изложение основных принципов, используемых при создании системы обеспечения информационной безопасности вуза и при ее функционировании. Среди таких принципов, как правило, выделяют: законность, системность и комплексность, актуальность, непрерывность защиты, возможность внесения изменений и совершенствования, экономическую целесообразность, личную ответственность, простоту применения средств защиты, обязательность контроля и т. п.

Раздел «Требования к подготовке и осведомленности сотрудников вуза в области информационной безопасности» должен содержать список требований, предъявляемых к сотрудникам в области их знаний по обеспечению информационной безопасности вуза.

В этом же разделе указываются цель и задачи повышения уровня знаний сотрудников в области защиты конфиденциальной информации и предлагаются формы и методы такого обучения.

Особого внимания заслуживает раздел «Ответственность за нарушение политики информационной безопасности», в котором оговариваются формы и виды ответственности сотрудников за несоблюдение требований документов, регулирующих функционирование системы управления информационной безопасностью, а также порядка и правил использования информационных ресурсов вуза.

В разделе «Контроль за соблюдением положений политики информационной безопасности» устанавливается должностное лицо, ответственное за общий контроль состояния информационной безопасности высшего учебного заведения. Им является руководитель управления безопасности вуза. В конце раздела могут быть рассмотрены методы, с помощью которых осуществляется контроль.

Раздел «Порядок утверждения, пересмотра, внесения изменений и дополнений в политику» определяет дату вступления в законную силу разработанной политики, частоту пересмотра основных направлений и требований по защите информации в образовательном учреждении и устанавливает ответственным за данный пересмотр управление безопасности вуза.

В последнем разделе даются ссылки на документы вуза, детализирующие положения разработанной политики применительно к одному выделенному или нескольким различным аспектам информационной безопасности, а также к применяемым в деятельности учебного заведения технологиям обучения. Такими документами могут являться «Положение вуза об управлении по информатизации и информационным технологиям», «Положение об обработке и защите персональных данных работников, обучающихся и абитуриентов», «Положение о порядке отнесения сведений к конфиденциальной информации вуза», «Перечень сведений, составляющих коммерческую тайну вуза» и «Классификация рисков информационной безопасности вуза».

Однако одного только наличия разработанной политики информационной безопасности в вузе недостаточно для организации повышения уровня информационной безопасности. Для поддержания работоспособности системы защиты информации необходимы и аудит выполнения сотрудниками вуза уже существующей политики, и контроль ее выполнения. При этом в самой документации по политике безопасности должно быть указано, как часто она должна пересматриваться и обновляться.

Заключение

Политика информационной безопасности учебного заведения имеет ключевое значение для организации всех процессов обеспечения информационной безопасности вуза и позволяет рассматривать ее в качестве методологической основы:

– для организации и принятия единого комплекса мер в сфере создания системы информационной безопасности вуза;
– для выявления и нейтрализации потенциальных и реально существующих угроз информационной безопасности вуза;
– для разработки предложений по совершенствованию правового, организационного и технического обеспечения информационной безопасности вуза;
– для распределения полномочий различных структурных подразделений вуза, работающих с конфиденциальной информацией, и координации деятельности в этой сфере.

В современном мире существует насущная необходимость вести целенаправленную работу по подготовке политики информационной безопасности в рамках каждого вуза, а также по приведению локальных нормативных документов в сфере информационной безопасности в соответствие с требованиями такой политики.

Литература

1. *Кожина А.С., Некраха А.В., Ермакова А.Ю.* Разработка политики информационной безопасности вуза // Информационное противодействие угрозам терроризма. Науч.-практ. журн. 2010. № 14. С. 194–199.
2. ГОСТ Р ИСО/МЭК 27003-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М.: Стандартинформ, 2014.

References

1. Kozhina AS., Nekraha AV., Ermakova AYu. Development of the information security policy of the university. *Informatsionnoe protivodeistvie ugrozam terrorizma. Nauchno-prakticheskii zhurnal.* 2010;14:194-99. (In Russ.)
2. GOST R ISO / IEC 27003-2012. National standard of the Russian Federation. Information technology. Security techniques. Information security management systems. Implementation manual of information security management system. Moscow: Standartinform Publ.; 2014. (In Russ.)

Информация об авторах

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; Россия, 125993, Москва, Миусская пл., д. 6; irkom@mail.ru

Александр В. Захаренков, студент, Российский государственный гуманитарный университет, Москва, Россия; Россия, 125993, Москва, Миусская пл., д. 6; zakh007@gmail.com

Information about the authors

Irina A. Rusetskaya, PhD in History, associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; irkom@mail.ru

Alexander V. Zakharenkov, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; zakh007@gmail.com

УДК 517.9

Гипотеза Аль-Худжанди и последняя теорема Ферма

Аллаберди Г. Галканов
Государственный гуманитарно-технологический университет,
Орехово-Зуево, Московская область, Россия, agalkanov@yandex.ru

Аннотация. Рассмотрены некоторые факты из истории последней теоремы Ферма. Введены два новых понятия: плоскость Аль-Худжанди и числовая последовательность Аль-Худжанди. Показано, что все векторные решения уравнения Ферма лежат на плоскости Аль-Худжанди. Доказана сходимость числовой последовательности Аль-Худжанди, из которой следует ложность утверждения последней теоремы Ферма в предельном случае.

Ключевые слова: гипотеза Аль-Худжанди, гипотеза Ферма, последняя теорема Ферма, плоскость Аль-Худжанди, числовая последовательность Аль-Худжанди.

Для цитирования: Галканов А.Г. Гипотеза Аль-Худжанди и последняя теорема Ферма // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 65–73.

The Al-Khujandi hypothesis and Fermat's last theorem

Allaberdi G. Galkanov
State Humanitarian-Technological University, Orekhovo-Zuevo,
Moscow Region, Russia, agalkanov@yandex.ru

Abstract. Some facts from the history of Fermat's last theorem are considered. Two new concepts were introduced: the Al-Khujandi plane and the numerical sequence of Al-Khujandi. It is shown that all vector solutions of the Fermat equation lie in the Al-Khujandi plane. The convergence of the numerical sequence of Al-Khujandi is proved, from what the falsity of the assertion of Fermat's last theorem in the limiting case follows.

Keywords: Al-Khujandi hypothesis, Fermat's conjecture, Fermat's last theorem, Al-Khujandi plane, numerical sequence of Al-Khujandi

For citation: Galkanov AG. The Al-Khujandi hypothesis and Fermat's last theorem. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):65-73.

Введение

Математик и астроном средневекового мусульманского Востока Аль-Худжанди (X в.) высказал гипотезу (гипотеза Аль-Худжанди): сумма двух кубических чисел не есть кубическое число: $\left(x^3 + y^3 \neq z^3\right)$. Но доказать свою гипотезу ему не удалось. Сохранилось очень мало сведений об Аль-Худжанди кроме того, что он был математиком и астрономом, который жил на территории современных Афганистана, Туркменистана и Узбекистана. Также известно, что он создал один из крупнейших астрономических инструментов в IX–X веках.

В XI веке эту гипотезу попытался доказать Омар Хайям, но безуспешно (см., например, [1, 2]).

Французский юрист математик Пьер де Ферма (XVII в.) высказал гипотезу (гипотеза Ферма): «Невозможно разложить ни куб на два куба, ни биквадрат на два биквадрата, и вообще никакую степень, бóльшую квадрата, на две степени с тем же показателем» [1], т. е. $z^3 \neq x^3 + y^3$, $z^4 \neq x^4 + y^4, \ldots,$ $z^n \neq x^n + y^n$, где $n > 2$, x, y, $z -$ натуральные числа.

В дальнейшем вместо неравенства $z^n \neq x^n + y^n$ появилось равенство $x^n + y^n = z^n$, которое было названо уравнением Ферма, а утверждение «уравнение $x^n + y^n = z^n$ не имеет решения в натуральных числах, если $n > 2$» – теоремой Ферма (она же великая, знаменитая, большая, последняя теорема [1]). Позже объектом доказательства стало предложение: если $n > 2$, то в натуральных числах решение уравнения $x^n + y^n = z^n$ не существует, хотя Ферма свою гипотезу высказал о невозможности разложения натуральной степени z^n на сумму двух других натуральных степеней x^n и y^n.

Несмотря на отчаянные попытки математиков (Л. Эйлер, С. Жермен, А. Лежандр, Л. Дирихле, Г. Ламе, О. Коши, Э. Куммер, М. Краснер, Х. Брюкнер, П. Реморов, М. Айхлер, Г. Вандивер, А. Виферих, М. Мириманов, Ф. Фуртвенглер, Г. Фалтингс, И. Мияока, Ю. Танияма, Г. Симура, Г. Фрей, Ж.П. Серр, К. Рибет и др.) [1, 3, 4] и математиков-любителей доказать эту теорему, она долгое время оставалась недоказанной и получила ранг «одной из самых знаменитых проблем математики» [5].

Доказательства проводились методом от противного. Но «не были найдены противоречия ни с утверждениями из элементарной теории чисел, ни с утверждениями о числовых полях, ни с какими-либо другими утверждениями ...» [4]. Спустя более 350 лет, в 1995 г., доказательство, предложенное профессором Принстонского университета Э. Уайлсом, получило положительное заключение у шести рецензентов и было опубликовано в математическом журнале [6, 7]. Ключевыми понятиями доказательства Э. Уайлса являются «эллиптические кривые, модулярные формы и представления Галуа» [4], и оно включает следующие этапы.

(I) Связать эллиптическую кривую с гипотетическим нетривиальным решением уравнения Ферма с произвольным показателем $n \geq 5$.

(II) Выявить противоречие с предположением об истинности определенной гипотезы об эллиптических кривых и модулярных формах.

(III) Доказать истинность этой гипотезы.

Как видно из (I), доказательство построено для $n \geq 5$. Между тем проблема состояла в построении единого доказательства теоремы для всех $n > 2$.

Отметим, что доказательство Э. Уайлса занимает около 130 журнальных страниц и не является элементарным, если под элементарным доказательством понимать «доказательство, не вводящее новых идей и остающееся в рамках уже известных методов» [8].

Таким образом, спустя семь веков ту же проблему, что и Аль-Худжанди, сформулировал П. Ферма, но для любого $n > 2$, при этом, как и Аль-Худжанди, он ее не решил. Только в конце XX века, как уже отмечено выше, Э. Уайлс доказал гипотезу Ферма, но не для всех $n > 2$, а для всех $n \geq 5$, из чего следует, что единое доказательство гипотезы Ферма для всех $n > 2$, включающее в себя и гипотезу Аль-Худжанди, еще не получено. Так что гипотезу Аль-Худжанди можно охарактеризовать как открытие, через семь веков ставшее частным случаем одной из сложнейших проблем математики [9]. Поэтому имя Аль-Худжанди вполне заслуживает того, чтобы им было названо хотя бы одно математическое понятие, связанное с уравнением $x^n + y^n = z^n$. С этой целью автором данной статьи введены два понятия: плоскость и числовая последовательность Аль-Худжанди.

Плоскость Аль-Худжанди и геометрическая и физические интерпретации последней теоремы Ферма

Пусть N, Q, Q_+, IR – множества натуральных, рациональных, положительных рациональных и иррациональных чисел соответственно. И пусть $OXYZ$ – прямолинейная ортогональная система координат. В системе координат $OXYZ$ возьмем ортонормальный базис $\vec{e}_1, \vec{e}_2, \vec{e}_3$ и в этот базис введем векторы $\overrightarrow{K} = (1, 1, -1)$, $\overrightarrow{H_n} = (x^n, y^n, z^n)$, $n \in \mathbb{N}$, $x, y, z \in \mathbb{N}$, $\left(\overrightarrow{K}, \overrightarrow{H_n}\right)$ – скалярное произведение векторов $\overrightarrow{K}$ и $\overrightarrow{H_n}$.

Определение 1. Плоскость с нормальным вектором $\overrightarrow{K}$, проходящая через начало координатной системы $OXYZ$, называется плоскостью Аль-Худжанди.

Определение 2. Если $\exists n \in N\ \exists x, y, z \in N\left[\left(\overrightarrow{K}, \overrightarrow{H_n}\right) = 0\right]$, то $\overrightarrow{H_n}$ называется натуральным векторным решением уравнения Ферма степени n.

Геометрическая интерпретация векторных решений уравнения Ферма. Все векторные решения уравнения Ферма лежат на плоскости Аль-Худжанди.

Первая физическая интерпретация теоремы Ферма. Пусть P_1 – прибор, посылающий точечный сигнал на плоскость Аль-Худжанди из точки $A\left(x^n, y^n, 0\right) \in OXYZ$ параллельно оси OZ так, что путь, пройденный этим сигналом, может измеряться лишь в натуральных числах, где $n > 2$, $x, y \in N$. Тогда ни одна точка плоскости Ферма не может быть обнаружена прибором P_1.

Вторая физическая интерпретация теоремы Ферма. Ясно, что $\rho = (x + y)/\sqrt{3}$ – расстояние от точки $A(x, y, 0) \in OXYZ$ до плоскости Аль-Худжанди, где $x, y \in Q_+$. Пусть теперь P_2 – прибор, посылающий точечный сигнал на плоскость Аль-Худжанди из точки $A(x, y, 0)$ перпендикулярно той же плоскости Аль-Худжанди так, что путь, пройденный этим сигналом, может измеряться лишь в положительных рациональных числах. Тогда ни одна точка плоскости Аль-Худжанди не может быть обнаружена прибором P_2.

Таким образом, если предположить возможность существования столь фантастических приборов дискретного излучения P_1 и P_2, то плоскость Аль-Худжанди можно назвать плоскостью-невидимкой для этих приборов.

Числовая последовательность Аль-Худжанди

Прежде чем ввести понятие числовой последовательности Аль-Худжанди, сформулируем последнюю теорему Ферма и последнюю теорему Ферма в радикальной форме.

Последняя теорема Ферма (ПТФ):

$$n>2\left(n\in N\right)\;\Rightarrow\;\forall x,\;y,\;z\in N\left[x^n+y^n\neq z^n\right].$$

Радикальная форма ПТФ:

$$n>2\left(n\in N\right)\;\Rightarrow\;\forall x,\;y\in N\left[\sqrt[n]{x^n+y^n}\in IR\right].$$

Радикальная форма ПТФ и ПТФ эквивалентны. В самом деле,

$$\left(n>2\left(n\in N\right)\;\Rightarrow\;\forall x,\;y\in N\left[\sqrt[n]{x^n+y^n}\in IR\right]\right)\;\Leftrightarrow$$

$$\Leftrightarrow\;\left(n>2\left(n\in N\right)\;\Rightarrow\;\forall x,\;y,\;z\in N\left[\sqrt[n]{x^n+y^n}\neq z\right]\right)\;\Rightarrow$$

$$\Leftrightarrow\;\left(n>2\left(n\in N\right)\;\Rightarrow\;\forall x,\;y,\;z\in N\left[x^n+y^n\neq z^n\right]\right).$$

Здесь использован известный факт из теории чисел [5]:

$$\forall u\in N\;\forall n\in N\left[\sqrt[n]{u}\in N\;\vee\;\sqrt[n]{u}\in IR\right].$$

Пусть $a,\,b\in N$, где $a,\,b$ не зависят от n.

Определение 3. Числовая последовательность

$$\left\{\sqrt[n]{a^n+b^n}\right\}:\;a+b,\;\sqrt{a^2+b^2},\;\sqrt[3]{a^3+b^3},\ldots,\;\sqrt[n]{a^n+b^n},\ldots$$

называется последовательностью Аль-Худжанди.

Пусть $F_n=\sqrt[n]{a^n+b^n}$. Отметим частный случай. Если $b=a$, то $\left\{F_n\right\}:\;2a,\;\sqrt{2}a,\;\sqrt[3]{2}a,\ldots,\;\sqrt[n]{2}a,\ldots$.

Теорема. Последовательность Аль-Худжанди сходится и

$$\lim_{n\to+\infty}F_n=\max(a,\,b).$$

Теорему докажем после доказательства следующей леммы.

Лемма [10]. $\forall \lambda \in (0;\,1]\ \forall n \in N\left[\left(1+\lambda^{n+1}\right)^{n} < \left(1+\lambda^{n}\right)^{n+1}\right].$

Доказательство. При $\lambda = 1$ доказываемое неравенство очевидно: $2^{n} < 2^{n+1}$. Пусть $\lambda \in (0;\,1)$. Имеем

$$0 < \lambda < 1 \Rightarrow \lambda^{n+1} < \lambda^{n} \Leftrightarrow 1+\lambda^{n+1} < 1+\lambda^{n} \Leftrightarrow$$
$$\Leftrightarrow \left(1+\lambda^{n+1}\right)^{n} < \left(1+\lambda^{n}\right)^{n} \Rightarrow \left(1+\lambda^{n+1}\right)^{n} < \left(1+\lambda^{n}\right)^{n}\left(1+\lambda^{n}\right) \Leftrightarrow$$
$$\Leftrightarrow \left(1+\lambda^{n+1}\right)^{n} < \left(1+\lambda^{n}\right)^{n+1}.$$

Следствие 1.
$\forall n \in N\ \forall x,\, y \in N\,(x<y)\left[\sqrt[n+1]{x^{n+1}+y^{n+1}} < \sqrt[n]{x^{n}+y^{n}}\right].$

Доказательство. Если в доказанном неравенстве подставить $\lambda = \dfrac{x}{y}$, то

$$\left(1+\lambda^{n+1}\right)^{n} < \left(1+\lambda^{n}\right)^{n+1} \Leftrightarrow \frac{\left(x^{n+1}+y^{n+1}\right)^{n}}{y^{n(n+1)}} < \frac{\left(x^{n}+y^{n}\right)^{n+1}}{y^{n(n+1)}} \Leftrightarrow$$
$$\Leftrightarrow \left(x^{n+1}+y^{n+1}\right)^{n} < \left(x^{n}+y^{n}\right)^{n+1} \Leftrightarrow \left(x^{n+1}+y^{n+1}\right)^{\frac{n}{n(n+1)}} < \left(x^{n}+y^{n}\right)^{\frac{n+1}{n(n+1)}} \Leftrightarrow$$
$$\Leftrightarrow \sqrt[n+1]{x^{n+1}+y^{n+1}} < \sqrt[n]{x^{n}+y^{n}}.$$

Следствие 2. $\forall n \in N\ \forall x,\, y \in N\left[\sqrt[n+1]{x^{n+1}+y^{n+1}} < \sqrt[n]{x^{n}+y^{n}}\right].$

Доказательство. При $x<y$ применить следствие 1. Если $x=y$, то

$$\sqrt[n+1]{2} < \sqrt[n]{2} \Leftrightarrow x\cdot\sqrt[n+1]{2} < x\cdot\sqrt[n]{2} \Leftrightarrow \sqrt[n+1]{x^{n+1}+x^{n+1}} < \sqrt[n]{x^{n}+x^{n}} \overset{y=x}{\Leftrightarrow}$$
$$\overset{y=x}{\Leftrightarrow} \sqrt[n+1]{x^{n+1}+y^{n+1}} < \sqrt[n]{x^{n}+y^{n}}.$$

Если же $x>y$, то с учетом коммутативности сложения снова применить следствие 1.

Доказательство теоремы. Согласно следствию 2, для последовательности Аль-Худжанди имеет место цепочка неравенств

$$0 < \ldots < F_n < \ldots < F_3 < F_2 < F_1 = a + b,$$

откуда следуют ее монотонность, ограниченность и, как следствие, сходимость. При $a = b$ имеем $F_n = \sqrt[n]{2}a,$ откуда

$$\lim_{n\to+\infty} F_n = a = \max(a,\, a). \qquad (1)$$

При $a < b$: $F_n = b \cdot \sqrt[n]{1 + \left(\frac{a}{b}\right)^n}$, откуда

$$\lim_{n\to+\infty} F_n = b = \max(a,\, b). \qquad (2)$$

Если же $a > b,$ то $F_n = a \cdot \sqrt[n]{1 + \left(\frac{b}{a}\right)^n}$, откуда

$$\lim_{n\to+\infty} F_n = a = \max(a,\, b). \qquad (3)$$

Равенства (1), (2) и (3) завершают доказательство теоремы.

Следствие из теоремы. $\forall x,\, y\left[\lim\limits_{n\to+\infty} \sqrt[n]{x^n + y^n} \in N\right],$ где $x,\, y$ не зависят от $n.$

Таким образом, согласно радикальной форме ПТФ, хотя для каждого $n > 2$ и для любых $x,\, y \in N$ число $\sqrt[n]{x^n + y^n}$ иррационально, в предельном случае, когда $n \to +\infty,$ $\sqrt[n]{x^n + y^n}$ оказалось натуральным числом. А это в силу эквивалентности ПТФ и радикальной формы ПТФ означает, что в предельном случае, когда $n \to +\infty,$ последняя теорема Ферма перестает быть теоремой.

Заключение

В статье исследованы вопросы, связанные с ПТФ. Исторически гипотезе Ферма, сформулированной им в XVII в. предшествовала гипотеза Аль-Худжанди, высказанная им еще в X в. В связи с этим автором статьи поставлена задача отразить вклад

Аль-Худжанди в проблематику вокруг ПТФ. С этой целью введены такие математические понятия, как плоскость Аль-Худжанди и ее геометрическая и физические интерпретации, а также числовая последовательность Аль-Худжанди. Из сходимости последовательности Аль-Худжанди выведено важное следствие о ложности утверждения ПТФ в предельном случае, когда $n \to +\infty$.

Автор выражает признательность доктору педагогических наук, профессору В.К. Жарову за интерес и внимание к работе.

Литература

1. *Толстиков А.В.* Ферма теорема // Математическая энциклопедия / гл. ред. И.М. Виноградов. В 5 т. М.: Советская энциклопедия, 1982. Т. 5. 1228 стб.
2. *Острик В.В., Цфасман М.А.* Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые. М.: МЦНМО, 2005. 28 с.
3. *Сингх С.* Великая теорема Ферма. М.: МЦНМО, 2000. 288 с.
4. *Рибенбойм П.* Последняя теорема Ферма для любителей. М.: Мир, 2003. 229 с.
5. *Оре О.* Приглашение в теорию чисел. М.: Эдиториал УРСС, 2003. 128 с.
6. *Wiles A.* Modular elliptic curves and Fermat's last theorem // Ann. of Math. 1995. Vol. 122. P. 223–551.
7. *Taylor R., Wiles A.* Ring-theoretic properties of Gertain Hacke Algebras // Ann. of Math. 1995. Vol. 122. P. 553–572.
8. *Постников М.М.* Теорема Ферма. Введение в теорию алгебраических чисел. М.: Наука, 1978. 128 с.
9. *Галканов А.Г.* Из истории последней теоремы Ферма // Современные проблемы математики, физики и физико-математического образования. Орехово-Зуево: ГГТУ, 2017. С. 20–23.
10. *Галканов А.Г.* Метод от противоположного и его применение к доказательству теорем. М.: Издательство МГУ леса, 2011. 60 с.

References

1. Tolstikov AV. Fermat theorem. V: Vinogradov IM., head ed. Mathematical encyclopedia. In 5 vols. Moscow: Sovetskaya entsiklopediya Publ.; 1982. Vol. 5. 1228 col. (In Russ.)
2. Ostrik VV., Tsfasman MA. Algebraic geometry and number theory. Rational and elliptic curves. Moscow: MCNMO Publ.; 2005. 28 p. (In Russ.)
3. Singh S. Fermat's great theorem. Moscow: MCNMO Publ.; 2000. 288 p. (In Russ.)
4. Ribenboim P. The last theorem of Fermat for amateurs. Moscow: MIR Publ.; 2003. 229 p. (In Russ.)

5. Ore O. Invitation to number theory. Moscow: Editorial URSS Publ.; 2003. 128 p. (In Russ.)
6. Wiles A. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* 1995;122:223-551.
7. Taylor R., Wiles A. Ring-theoretic properties of Gertain Hacke Algebras. *Ann. of Math.* 1995;122:553-72.
8. Postnikov MM. Fermat's theorem. Introduction to the theory of algebraic numbers. Moscow: Nauka Publ.; 1978. 128 p. (In Russ.)
9. Galkanov AG. From the history of Fermat's last theorem. V: Actual issues of mathematics, physics and physico-mathematical education. Orekhovo-Zuevo: GGTU Publ.; 2017. P. 20-3. (In Russ.)
10. Galkanov AG. The Method from the contrary and its application to the theorem's proof. Moscow: MGU Lesa Publ.; 2011. 60 p. (In Russ.)

Информация об авторе

Аллаберди Г. Галканов, кандидат технических наук, доцент, Государственный гуманитарно-технологический университет, Орехово-Зуево, Московская область, Россия; 142600, Россия, Московская область, Орехово-Зуево, ул. Зеленая, д. 22; agalkanov@yandex.ru

Information about the author

Allaberdi G. Galkanov, PhD in Engineering, associate professor, State Humanitarian-Technological University, Orekhovo-Zuevo, Moscow Region, Russia; bld. 22, Zelenaya str., Orekhovo-Zuevo, Moscow Region, Russia, 142600; agalkanov@yandex.ru

УДК 512

Об алгебрах, порождаемых основными операторами анализа X, D, I

Валерий М. Максимов
Российский государственный гуманитарный университет,
Российский университет дружбы народов,
Москва, Россия, fpm@rggu.ru

Аннотация. В работе изучается алгебра $A_L\ (X, D, I)$, порожденная операторами: X(оператор умножения на переменную x), D (оператор дифференцирования), I (оператор интегрирования), заданными на некотором пространстве функций L. Рассмотрены подалгебры Вейля и Коши и соответствующие им операторные тождества. В частности, формула n-кратного интегрирования Коши представлена как алгебраическое тождество. Дано понятие расширенной алгебры Вейля и ее операторное представление в виде фактор-алгебры $A_L\ (X, D, I)$. Приведены формулы для некоммутативных биномов.

Ключевые слова: алгебра Вейля, алгебра Коши, соотношение Вейля, соотношение Коши, формула n-кратного интегрирования, некоммутативный бином.

Для цитирования: Максимов В.М. Об алгебрах, порождаемых основными операторами анализа X, D, I // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 74–93.

About the algebras generated by basic operators of mathematical analysis X, D and I

Valery M. Maksimov
Russian State University for the Humanities, Peoples' Friendship University of Russia, Moscow, Russia, vm_maximov@mail.ru

Abstract. This paper studies the algebra A_L (X, D, I) generated by the operators: X (the operator of multiplication by the variable x), D (the differentiation operator), and I (the integration operator) defined on a certain space of functions L. Weyl and Cauchy subalgebras and corresponding operator identities are studied. In particular, the formula for n-fold Cauchy integration is presented as an algebraic identity. A concept is given for the extended Weyl algebra and its operator presentation in the form of the quotient algebra A_L (X, D, I). Formulas for noncommutative binomials are given.

Keywords: Weyl algebra, Cauchy algebra, Weyl relation, Cauchy relation, the formula for n-fold integration, noncommutative binomial.

For citation: Maximov VM. About the algebras generated by basic operators of mathematical analysis X, D and I. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):74-90.

Введение

Рассмотрим некоторое линейное пространство действительных функций L, заданных на отрезке $[a; b]$. Предположим, что L замкнуто относительно основных операций X, D, I, то есть для любых f (x) ∈ L имеем:

1) $Df(x) = f'(x);$ (1)
2) $If(x) = \int_{x0}^{x} f(t)dt$, *где* $x_0 \in [a; b];$ (2)
3) $Xf(x) = xf(x).$ (3)

Тогда эти операции являются линейными операторами в L, порождающими алгебру $A_L\ (X, D, I)$ над полем действительных чисел R. Обозначим еще $\mathbf{1}$ как тождественный оператор, т. е. $\mathbf{1}f(x) = f\ (x)$, где $f(x) \in L$, и нулевой оператор $\mathbf{0}$, $\mathbf{0}f(x) = 0$, где $f(x)$ также принадлежит L. Здесь 0 обозначает функцию, тождественно равную 0 и принадлежащую L. Непосредственно из определений операций легко следуют основные свойства операторов, которые справедливы для функций из L:

1) $DDI = 1, ID \neq 1;$ (4)

2) $DX - XD = 1;$ (5)

3) $IX - XI = -I^2.$ (6)

Соотношение (1) показывает, что операции дифференцирования и интегрирования некоммутативны и поэтому формально не обратны. Соотношение (2) элементарно доказывается на с. 81 («Подалгебра (A_L(X, I)»). Оно называется соотношением Вейля. Ниже будет показано, что операторы X и D порождают алгебру Вейля. Соотношение (3) является частным случаем равенства Коши для n-кратного интегрирования и может быть легко получено непосредственно из соотношения Вейля.

Алгебра $A_L\,(X, D, I)$, порождаемая основными операторами анализа, играет важную роль в математическом анализе, поскольку в ней могут содержаться различные алгебраические соотношения, которые справедливы как формулы математического анализа, но могут получаться и чисто алгебраическим путем. Например, справедливы следующие формулы, которые выводятся чисто алгебраически:

$$X^n D^n = XD(XD - 1)(XD - 2) \dots (XD - (n - 1)) \tag{7}$$

или

$$D^n X^n = DX(DX + 1)(DX + 2) \dots (DX + (n - 1)). \tag{8}$$

В работе [1] указаны и другие соотношения между операторами X, D, I. Возможно, некоторые из них были опубликованы впервые, а другие были известны еще в первой половине XIX в.

Приведем еще одну формулу:

$$(X + I)^n = X^n + nX^{n-1}\,{}^{*}. \tag{9}$$

---

* Эта формула была сообщена автору несколько лет назад О.В. Висковым, сотрудником Математического института РАН им. В.А. Стеклова.

Отсюда следует, что n-кратное интегрирование вида $(X+I)^n$ в действительности требует лишь одного интегрирования (однократного интегрирования). Будет показано, что алгебра $A_L\ (X,D,I)$ не зависит от класса функций L, отрезка $[a;b]$ и точки $x_0 \in [a;b]$.

Алгебра $A_L\ (X,D,I)$ оказывается близка к алгебре Вейля, так как содержит собственный идеал, по отношению к которому операторы I и D коммутативны и обратимы. В таком случае фактор-алгебра $A_L\ (X,D,I)$ по этому собственному идеалу оказывается изоморфной расширенной алгеброй Вейля, которая легко строится из обычной алгебры Вейля.

Формально алгебра Вейля определяется как свободная фактор-алгебра с образующими a, b *и* $\mathbf{1}$ (единичный элемент) по идеалу, порожденному элементом $ba-ab-\mathbf{1}$. Если образы $a, b, \mathbf{1}$ при такой факторизации обозначить через $\tilde{a}, \tilde{b}, \tilde{\mathbf{1}}$, то получим $\tilde{b}\tilde{a}-\tilde{a}\tilde{b}=\tilde{\mathbf{1}}$. Полученное соотношение Вейля используется для построения алгебры Вейля, элементами которой могут быть всевозможные члены $\tilde{a}^{i_1}\tilde{b}^{j_1}, \tilde{a}^{i_2}\tilde{b}^{j_2}, \dots, \tilde{a}^{i_n}\tilde{b}^{j_n}$ и их линейные комбинации над полем действительных чисел R.

Здесь для удобства положим, что $\tilde{a}^0=\tilde{b}^0=\tilde{\mathbf{1}}$. Ниже будет показано, что базис такой алгебры состоит из элементов $\{\tilde{a}^k\tilde{b}^m\}$, где $k, m = 0, 1, 2, \dots$ Из соотношения $\tilde{b}\tilde{a}-\tilde{a}\tilde{b}=\tilde{\mathbf{1}}$ по индукции легко получить, что $\tilde{b}\tilde{a}^n-\tilde{a}^n\tilde{b}=\mathrm{n}\tilde{a}^{n-1}$, или

$$\tilde{b}P(\tilde{a})-P(\tilde{a})\tilde{b}=P'(\tilde{a}) \tag{10}$$

для любого полинома $P(\tilde{a})$ от переменной $\tilde{a}$, а $P'(\tilde{a})$ – формальная производная по символу $\tilde{a}$.

Расширенная алгебра Вейля строится присоединением элемента $\tilde{b}^{-1}$. Умножая соотношение $\tilde{b}\tilde{a}-\tilde{a}\tilde{b}=\tilde{\mathbf{1}}$ слева и справа на символ $\tilde{b}^{-1}$, получаем: $\tilde{a}\tilde{b}^{-1}-\tilde{b}^{-1}\tilde{a}=\tilde{b}^{-2}$, или $\tilde{b}^{-1}\tilde{a}-\tilde{a}\tilde{b}^{-1}=-\tilde{b}^{-2}$. Отсюда по индукции получим:

$$P\left(\tilde{b}^{-1}\right)\tilde{a}-\tilde{a}P\left(\tilde{b}^{-1}\right)=P'\left(\tilde{b}^{-1}\right), \tag{11}$$

где P – произвольный полином от $\widetilde{b}^{-1}$, а P' – формальная производная по символу $\widetilde{b}$.

Подалгебра $A_L(X, D)$

Операторы X *и* D, определенные на множестве функций L, удовлетворяют соотношению $DX - XD = \mathbf{1}$, что эквивалентно равенству $[xf(x)]' = f(x) + xf'(x)$, которое очевидно представляется в операторном виде:

$$[xf(x)]' = D\big(Xf(x)\big), f(x) = \mathbf{1}f(x),\ xf'(x) = X(Df(x)).$$

Отсюда

$$DXf(x) - XDf(x) = f(x)\ \forall f(x) \in L, \text{ или } (DX - XD - \mathbf{1})f(x) = 0, \forall f(x) \in L,$$

что означает равенство

$$DX - XD = \mathbf{1}.$$

В зависимости от выбора пространства L между операторами X, D *и* $\mathbf{1}$ возможны и другие соотношения, не являющиеся следствием соотношения $DX - XD = \mathbf{1}$.

Однако из специфичности соотношения Вейля будет следовать, что вся алгебра $A_L(X, D)$ изоморфна алгебре Вейля.

Теорема 1. Пусть в некоторой алгебре A с единицей $\mathbf{1}$ над полем действительных чисел имеются два элемента α *и* β, для которых выполнено соотношение Вейля: $\beta\alpha - \alpha\beta = \mathbf{1}$. Тогда элементы $\{\alpha^n\beta^m\}$, $n, m = 0, 1, 2, \ldots$, линейно независимы и алгебра, порожденная элементами α, β *в* A, изоморфна алгебре Вейля.

Доказательство. Допустим, что существует линейная зависимость между элементами $\{\alpha^n\beta^m\}$. Тогда возможно равенство $\sum C_{nm}\alpha^n\beta^m = 0$ при некоторых ненулевых коэффициентах C_{nm}. Это равенство можно записать в виде $\sum_{k=0}^{k_0} P_k(\alpha)\,\beta^k = 0$, где $P_k(\alpha)$ – полиномы, не все равные нулю. Из $\beta\alpha - \alpha\beta = 1$ и формулы (10) следует, что $\beta P(\alpha) - P(\alpha)\beta = P'(\alpha)$ или $\beta P(\alpha) = P(\alpha)\beta + P'(\alpha)$, где $P'(\alpha)$ – формальная производная по символу α.

Аналогично имеем $\beta^2\alpha - \alpha\beta^2 = 2\beta$ и $P(\beta)\alpha - \alpha P(\beta) = P'(\beta)$. Поэтому, умножив равенство $\sum_{k=0}^{k_0} P_k(\alpha)\,\beta^k = 0$ слева и справа на α и беря соответствующую разность, получим равенство

$$\sum_{k=0}^{k_0} kP_k(\alpha)\beta^{k-1} = 0.$$

Продолжая такой процесс, в конце концов получим: $k_0!\,P_{k_0}(\alpha) = 0$, или $P_{k_0}(\alpha) = 0$. Покажем, что все коэффициенты в $P_{k_0}(\alpha) = 0$ также равны нулю. Умножая равенство $P_{k_0}(\alpha) = 0$ слева и справа на β и беря их разность, получим $P'_{k_0}(\alpha) = 0$. Аналогично имеем

$$P''_{k_0}(\alpha) = P'''_{k_0}(\alpha) = \dots = P^{(m)}{}_{k_0}(\alpha)\ 0,$$

где m – степень полинома $P'_{k_0}(\alpha)$.

Так как α^m – наибольшая степень в $P_{k_0}(\alpha)$ с неравным нулю коэффициентом C_m, то имеем $P^{(m)}{}_{k_0}(\alpha) = 0 = C_m m!$. Из этого следует, что $C_m = 0$, и поэтому если $P_{k_0}(\alpha) = \mathbf{0}$, то и все коэффициенты в нем равны нулю. Итак, из равенства $\sum C_{nm}\alpha^n\beta^m = 0$ следует, что все коэффициенты C_{nm} должны быть равны нулю. Это означает, что все элементы $\{\alpha^n\beta^m\}$ линейно независимы в алгебре A.

В алгебре $A(\alpha,\beta)$, порожденной элементами α,β, в силу соотношения $\beta\alpha = \alpha\beta + \mathbf{1}$ набор $\{\alpha^n\beta^m\}$ образует базис, так как каждый элемент в $A(\alpha,\beta)$ можно представить в виде линейной комбинации элементов $\alpha^{i_1}\beta^{j_1}, \alpha^{i_2}\beta^{j_2}, \dots, \alpha^{i_k}\beta^{j_k}$. Поскольку, в силу доказанного выше, такое представление единственно, то набор $\{\alpha^n\beta^m\}$, $n,m = 0,1,2,\dots$ образует базис алгебры $A(\alpha,\beta)$. Отсюда сразу следует, что любые алгебры $A(\alpha,\beta)$ и $A(\alpha',\beta')$ изоморфны, если $\beta\alpha - \alpha\beta = \mathbf{1}$ и $\beta'\alpha' - \alpha'\beta' = \mathbf{1}'$.

Покажем теперь, что алгебра $A(\alpha,\beta)$ изоморфна алгебре Вейля. Действительно, пусть A – свободная алгебра с образующими $\tilde{a}, \tilde{b}$ и единицей $\tilde{\mathbf{1}}$. Рассмотрим фактор-алгебру по идеалу, порожденному элементами $\tilde{b}\tilde{a} - \tilde{a}\tilde{b} - \tilde{\mathbf{1}}$. Это и будет алгебра Вейля. Образующие $\tilde{a}, \tilde{b}, \tilde{\mathbf{1}}$ содержатся в некоторых смежных классах по идеалу и являются образующими алгебры Вейля. Обозначим их a, b *и* $\mathbf{1}$, соответственно. При этом факторизация дает соотношение $ba - ab = \mathbf{1}$. В силу доказанного базис фактор-алгебры состоит из элементов $\{a^n b^m\}$ и поэтому алгебра $A(\alpha,\beta)$ изоморфна алгебре Вейля. Теорема доказана.

Поскольку алгебра $A_L(X,D)$ порождается двумя операторами X *и* D, связанными соотношением $DX - XD = \mathbf{1}$, то, согласно теореме 1, алгебра $A_L(X,D)$ изоморфна алгебре Вейля и не зависит от выбора пространства функций L и точки $x_0 \in [a;b]$. В частности, L может состоять из всех многочленов. Из теоремы 1 также следует, что операторы $\{X^m D^n\}$, $m,n = 0,1,2,\ldots$, где $\{D^0 = X^0 = \mathbf{1}\}$, являются линейным базисом алгебры $A_L(X,D)$. Аналогично доказательству в теореме 1 из независимости $\{\alpha^n \beta^m\}$ следует и независимость элементов $\{\beta^n \alpha^m\}$. Следовательно, операторы $\{D^n X^m\}$ также образуют базис алгебры $A_L(X,D)$, так как каждый элемент из алгебры $A_L(X,D)$ в силу того же соотношения $DX - XD = \mathbf{1}$ представляется линейной комбинацией операторов $\{D^n X^m\}$.

Существует несколько доказательств этого факта, независимых от теоремы 1. Представляется, что простейшее доказательство основано на автоморфизме, переводящем оператор D в $-X$, а оператор X в D. При автоморфизме базис переходит в базис, при этом базисный элемент $X^n D^m$ переходит в базисный элемент $(-1)^m D^n X^m$. Поэтому операторы $\{D^n X^m\}$, $n,m = 0,1,2,\ldots$ также образуют базис.

Замена переменной x на оператор умножения X приводит к квантово-механическим вычислениям в алгебре Вейля и широко применяется в квантовой механике [2].

Если заменить в функции $f(x)$ из L переменную x на оператор X, то оператор $f(X)$ можно определить действием на функцию $\varphi(x) \in L$ как умножение $\varphi(x)$ на $f(x)$. Далее произведение $Df(X)$ можно было бы определить как операцию, действующую в L. При этом $Df(X)\varphi(x) = \big(f(x)\varphi(x)\big)' = (f'\varphi(x) + f\varphi'(x))$. Поскольку последнее равенство справедливо для всех $\varphi(x)$ *из* L, то имеем:

$$Df(X) = f(X)D + f'(X). \tag{12}$$

Аналогично получается и интерпретируется более общее равенство:

$$D^n f(X) = f(X)D^n + \binom{n}{1} f'(X)D^{n-1} + \binom{n}{2} f''(X)D^{n-2} + \cdots. \tag{13}$$

Эта формула эквивалента формуле Лейбница: $(f\varphi)^{(n)} = \sum_k \binom{n}{k} f^{(k)}\varphi^{(n-k)}$. Как следствие получим:

$$D^nX^m = X^mD^n + \binom{m}{1}\binom{n}{1}X^{m-1}D^{n-1} + \cdots \tag{14}$$

и

$$D^nX^n = X^nD^n + \binom{n}{1}^2 X^{n-1}D^{n-1} + \cdots. \tag{15}$$

Перейдем теперь к формулам (7) и (8). Легко видеть, что действуя обеими частями формулы (8) на x^n, мы получим равенства $(n+m)(n+m-1)\dots(n+1)x^n = (n+1)(n+2)\dots.(n+m)x^n, n = 0, 1, 2 \dots$ Поэтому формула (8) справедлива в алгебре Вейля в любом ее представлении $A_L(X, D)$. Из формулы (8) видно, что D^nX^n есть многочлен от оператора DX с целыми коэффициентами. Поэтому операторы D^nX^n и D^mX^m перестановочны, и в алгебре Вейля имеют место равенства:

$$D^nX^n\, D^kX^k = D^kX^kD^nX^n, \tag{16}$$

которые можно непосредственно проверить как тождество в алгебре Вейля.

Оператор DX порождает коммутативную подалгебру в алгебре Вейля. Легко видеть, что базис этой подалгебры состоит из операторов D^kX^k, $k = 0, 1, 2, \dots$, так как это следует из представления операторов $\{D^mX^m\}$ как полинома m-й степени от DX . Аналогично доказывается и формула (7).

Подалгебра $A_L(X, I)$

Алгебра $A_L(X, I)$ порождается операторами X *и* I, которые, как отмечалось во введении, связаны соотношением (6) $IX - XI = -I^2$, являющимся следствием формулы Коши:

$$\int_0^x (x-t)\, f(t)dt = -\iint_0^x f^2(t)\, dt \ \ [3].$$

Однако есть и другой взгляд на формулу (6): она является прямым следствием формулы Вейля (5). Действительно, умножая равенство $DX - XD = \mathbf{1}$ слева и справа на I, получим $(ID)XI - IX = I^2$. Оператор ID равен $\mathbf{1} - V_0$, где $V_0\, f(x) = f(x_0)$ для функций $f(x) \in L$. В самом деле, $IDf(x) = If'(x) = f(x) - f(x_0) = (\mathbf{1} - V_0)f(x)$. Поэтому $(ID)XI = (\mathbf{1} - V_0)XI = XI - V_0XI$. Но V_0XI равно нулю, так как $V_0XI\, f(x) = V_0x[F(x) - F(x_0)] = 0$, где $F(x)$ – первообразная от

$f(x)$, а $f(x)$ – произвольная функция из L. Итак, из формулы Вейля получаем $XI - IX = I^2$, или $IX - XI = -I^2$. Заметим, что это равенство не зависит от выбора пространства L. Поэтому возможен еще один подход к доказательству, который можно назвать комбинаторным. Действительно, в качестве пространства функций L на отрезке $[a;b]$, можно взять пространство всех полиномов, и тогда выполнение предполагаемого равенства достаточно проверить для всех степеней $\{x^n\}, n = 0, 1, 2 \ldots$. В данном случае, применяя левую и правую части (6) к полиному x^n, получим равенство:

$$\frac{x^{n+2}}{n+2} - \frac{x^{n+2}}{n+1} = -\frac{x^{n+2}}{(n+2)(n+1)}.$$

Алгебру $A_L(X, I)$ будем называть алгеброй Коши, а равенство (6) соотношением Коши.

Укажем две фундаментальные формулы ((17) и (18)), имеющие чисто алгебраическое представление и справедливые для любой пары операторов A и B, связанных соотношением $BA - AB = -B^2$. Например, кроме операторов X и I алгебра Коши применима и к паре операторов D $и$ $\overline{D}$, определенных, например, на полиномах, где D – дифференцирование, а $\overline{D}$ – понижение степени, т. е. $\overline{D}x^n = x^{n-1}$ и $\overline{D}1 = 0$, 1 – обычная единица, т. е. $\overline{D}f(x) = \frac{f(x)-f(0)}{x}$. При таком определении $\overline{D}$ легко проверить, что $D\overline{D} - \overline{D}D = -\overline{D}^2$ на степенях $\{x^n\}, n = 0, 1, 2 \ldots$. Указанные ниже формулы для пары X, I имеют характер математического фольклора и, возможно, были известны Коши или более ранним символистам XIX в. При этом их доказательства могли быть либо комбинаторными, либо аналитическими, так как в то время не было четкого понятия алгебры. Сформулируем далее две теоремы.

Теорема 2. Пусть $P(X)$ – произвольный полином от оператора X. Тогда имеют место равенства:

$$IP(X) = P(X)I - P'(X)I^2 + P''(X)I^3 - \cdots; \qquad (17)$$

$$P(X)I = IP(X) + I^2P'(X) + I^3P''(X) + \cdots, \qquad (18)$$

где $P'(X), P''(X), \ldots$ формальные производные полинома $P(X)$ по символу X. Например, $(X^n)' = nX^{n-1}$.

Теорема 3. Пусть $P(I)$ – произвольный полином от оператора I. Тогда верно равенство:

$$P(I)X = XP(I) - P'(I)I^2\,, \tag{19}$$

где $P'(I), P''(I), \dots$ – формальные производные полинома $P(I)$ по символу I.

Доказательство равенства (19) элементарно производится по индукции при $P(I) = I^n$, так как при $n = 0$ имеем $I^0 = \mathbf{1}$, а при $n = 1$ получаем формулу, которая совпадает с формулой (6). Если по индукции предположить, что $I^n X = XI^n - nI^{n+1}$, то, умножая слева на I , получим,

$$I^{n+1}X = (IX)I^n - nI^{n+2} = (XI - I^2)I^n - nI^{n+2} = XI^{n+1} - (n+1)I^{n+2}.$$

Теорема доказана.

Используем формулу (19) для доказательства теоремы 2. Формулу (17) достаточно доказать для всех степеней X^n. При $n = 1$ формула (17) совпадает с (6). Поэтому можно доказывать по индукции и предположить справедливым равенство:

$$IX^n = X^n I - nX^{n-1}I^2 + n(n-1)X^{n-2}I^3 - \cdots + (-1)^n n!\, I^{n+1}.$$

Умножив это равенство справа на X и используя равенство (19), получим:

$$IX^{n+1} = X^n(XI - I^2) + nX^{n-1}(XI^2 - 2I^3) +$$
$$+\, n(n-1)X^{n-2}(XI^3 - 3I^4) \dots + (-1)^n n!\,(XI^{n+1} - (n+1)I^{n+3}).$$

Складывая правую часть и приводя подобные члены, легко получаем (17). Аналогично доказывается формула (18). Теорема доказана.

Часто некоммутативные биномы имеют более глубокое содержание, нежели коммутативные, которые сводятся к комбинаторике сочетаний. В случае некоммутативной пары X, I имеем равенство $(X + I)^n = X^n + nX^{n-1}I$, см. (9), которое легко доказывается по индукции с помощью основного соотношения Коши. Действительно, при $n = 1$ имеем тождество $X + I = X + I$. Применяя по индукции равенство (9), получим:

$$(X + I)^{n+1} = (X^n + nX^{n-1}I)(X + I) =$$
$$= X^{n+1} + nX^{n-1}IX + X^n I + nX^{n-1}I^2 =$$
$$= X^{n+1} + nX^{n-1}(XI - I^2) + X^n I - nX^{n-1}I^2 = X^{n+1} + (n+1)X^n I.$$

Бином $(X+I)^n = X^n + nX^{n-1}I$ еще не осмыслен в анализе, хотя ясно, что слева имеем n-кратного интегрирование, а справа однократное. Тем более интересно, что формула Коши, связывающая однократное и n-кратного интегрирования, нашла многочисленное применение в анализе, в частности является ключевой в операторном исчислении Микусинского [3], и в то же время она является алгебраическим тождеством в алгебре $A_L(X,I)$ (алгебре Коши).

Формула n-кратного интегрирования Коши имеет вид:

$$\int_0^x \dots \int_0^x f(t)dt = \int_0^x \frac{(x-t)^{n-1}}{(n-1)!} f(t)dt. \qquad (20)$$

Если не считать коэффициента $\frac{1}{(n-1)!}$, то правая часть (20) является свёрткой двух функций x^{n-1} и $f(x)$. Поэтому данная формула нашла применение не только в анализе, но и в операционном исчислении Микусинского. Эта формула Коши эквивалентна алгебраическому тождеству в алгебре Коши $A_L(X,I)$. Действительно, ее можно представить в виде

$$I^n f(x) = \frac{1}{(n-1)!}\sum_{k=n-1}^{0}(-1)^k \binom{n-1}{k} X^k \int_0^x t^{n-1-k} f(t)dt =$$

$$= \frac{1}{(n-1)!}\sum_{k=n-1}^{0}(-1)^k \binom{n-1}{k} X^k I X^{n-1-k} f(x), \qquad (21)$$

эквивалентном алгебраическому тождеству

$$I^n = \frac{1}{(n-1)!}\sum_{k=n-1}^{0}(-1)^k \binom{n-1}{k} X^k I X^{n-1-k}. \qquad (22)$$

Эта формула легко устанавливается, если вместо IX^{n-k-1} подставить его представление (17), и потом привести подобные члены.

Наконец, выведем для бинома $(X-I)^n$ формулу, которая следует из основного равенства Коши (6).

Теорема 4. Имеет место равенство

$$(X-I)^n = X^n - nX^{n-1}I + n(n-1)X^{n-2}I^2 - \dots + (-1)^n n!\, I^n. \qquad (23)$$

Доказательство. Представим равенство $IX - XI = -I^2$ в виде $IX = (X - I)I$. Тогда $IX^2 = (X - I)IX = (X - I)^2 I$ и, следовательно, $IX^n = (X - I)^n I$. С другой стороны, если заменить IX^n по формуле (17), то получим:

$$X^n I - nX^{n-1} I^2 + n(n-1)X^{n-2} I^3 - \cdots + (-1)^n n!\, I^{n+1} = (X - I)^n I.$$

Оператор I можно вынести из этой формулы справа, но сократить оператор I нельзя, потому что $ID = \mathbf{1} - V_0$. Однако отсюда следует, что операторы $(X - I)^n$ и $X^n - nX^{n-1} I + nX^{n-2} I^2 + \cdots + (-1)^n n!\, I^{n+1}$ совпадают на всех степенях $x, x^2, \ldots$. Покажем, что они совпадают и на константах. Достаточно рассмотреть случай единичной константы. Тогда имеем:

$$(X - I)^n 1 = (X - I)^{n-1}(X - I)1 = (X - I)^{n-1}(x - (x - x_0)) =$$
$$= (X - I)^{n-1} x_0 = x_0 (X - I)^{n-1} 1 = \cdots = x_0{}^n.$$

С другой стороны,

$$[X^n - nX^{n-1} I + n(n-1)X^{n-2} I^2 - \cdots + (-1)^n n!\, I^n]1 =$$
$$= x^n - nx^{n-1}(x - x_0) + \frac{n(n-1)}{2!} x^{n-2}(x - x_0)^2 + \cdots + (-1)^n \frac{n!}{n!} (x - x_0)^n =$$
$$= (x - (x - x_0))^n = x_0{}^n.$$

Таким образом, имеем следующую формулу некоммутативного бинома:

$$(X - I)^n = X^n - nX^{n-1} I + n(n-2) X^2 I^2 + \cdots + (-1)^n n!\, I^n. \qquad (24)$$

Применяя (24) к различным специальным функциям, например, к степеням x^n, получим следующие комбинаторные формулы:

$$(X - I)^n x^m = (X - I)^{n-1}(X - I)x^m = (X - I)^{n-1}\left(x^{m+1} - \frac{x^{m+1}}{m+1}\right) =$$
$$= (X - I)^{n-1} \frac{m}{m+1} x^{m+1} = \cdots = \frac{m}{m+n} x^{m+n}.$$

Применяя правую часть формулы (24) к x^m и сокращая обе части на x^{m+n}, получим

$$[\,1 - \frac{n}{m+1} + \frac{n(n-1)}{(m+1)(m+2)} - \frac{n(n-1)(n-2)}{(m+1)(m+2)(m+3)} + \cdots +$$
$$+ \frac{(-1)^n n!}{(m+1)(m+2)(m+n)}] = \frac{m}{m+n}\ . \qquad (25)$$

Заметим, что формула (25) справедлива при любых натуральных m и n, а при $m = 0$ означает равенство суммы четных и нечетных биномиальных коэффициентов.

Другое следствие получим, если $\frac{n}{m} \to 1$. Тогда формула (25) дает следующее предельное выражение: $1 - 1 + 1 - \cdots = \frac{1}{2}$, что говорит и о возможной комбинаторной интерпретации такого равенства [4].

Перейдем к описанию базиса алгебры $A_L(X, I)$. Ясно, что базисы должны быть аналогичны базисам, указанным для алгебры Вейля.

Теорема 5. Множество операторов $\{I^n X^m\}$, $n, m = 0, 1, 2 \ldots$ и множество $\{X^n I^m\}, n, m = 0, 1, 2 \ldots$ являются базисами в алгебре $A_L(X, I)$.

Доказательство. Если допустить, что набор $I^{n_1}X^{m_1}, \ldots, I^{n_s}X^{m_s}$ (все пары (n_i, m_i), $i = 1, \ldots, s$ различны) линейно зависим, то после умножения слева элементов этого множества на $D^{\max n_i}$ должна получиться линейно зависимая система $D^{\max n_i - n_1}X^{m_1}, \ldots, D^{\max n_i - n_s}X^{m_s}$, которая на самом деле является линейно независимой в алгебре Вейля. Итак, первая часть теоремы будет доказана, если заметить, что в силу (6), (7) и (18) каждый элемент из $A_L(X, I)$ представляется в виде комбинации некоторых элементов $I^{i_1}X^{j_1}, \ldots, I^{i_m}X^{j_m}$.

Для доказательства второй части теоремы 5 воспользуемся формулой (18) для преобразования операторов $X^{n_i}I^{m_i}$ в линейную комбинацию операторов $I^k X^l$. Так как $X^n I = I X^n + n I^2 X^{n-1} + \cdots$, то $X^n I^2 = I X^n I + n I^3 X^{n-1} I + \cdots$. Отсюда легко видеть, что $X^n I^m = I^m X^n + \cdots$, где остальные члены имеют вид $I^{n-k}X^{m+k}$. Поэтому упорядочим линейно по возрастанию набор операторов $X^0 I^N, X^1 I^{N-1}, \ldots, X^N I^0$ и операторы $I^0 X^N, I^1 X^{N-1}, \ldots, I^N X^0$. Тогда, согласно вышесказанному, матрица перехода от второго набора к первому является обратимой. Поэтому из линейной независимости операторов $I^0X^N, I^1X^{N-1}, \dots, I^NX^0$ следует линейная независимость операторов $X^0I^N, X^1I^{N-1}, \dots, X^NI^0$. Теорема доказана.

Алгебра $A_L(X,D,I)$

Алгебра $A_L(X,D,I)$, порожденная операторами X,D,I, определена на некотором пространстве функций L, замкнутом относительно этих операций. Выше указывались три соотношения между этими операторами – (4), (5), (6). Это равенство Вейля, $DX - XD = \mathbf{1}$, равенство Коши $IX - XI = -I^2$ и соотношение односторонней обратимости операторов D и I, $DI = \mathbf{1}$, но $ID \neq \mathbf{1}$. Кстати, последнее соотношение, весьма существенно в понимании строения алгебры $A_L(X,D,I)$, так как иногда бытует представление об обратимости операций D и I, что, как уже указывалось выше, неверно. Далее будет рассмотрена факторизация алгебры $A_L(X,D,I)$, при которой образы операторов D *и* I обратимы, и дано описание такой алгебры в виде естественного расширения алгебры Вейля.

Элементы алгебры $A_L(X,D,I)$ состоят из произвольных констант, мономов, порожденных операторами X,D,I, т. е. операторов вида $X^{i_1}D^{j_1}I^{k_1}X^{i_2}D^{j_2}I^{k_2} \dots X^{i_s}D^{j_s}I^{k_s}$, где i_r, j_r, k_r, s – любые $0, 1, 2 \dots$, и из любых их конечных линейных комбинаций. При этом считается $X^0 = D^0 = I^0 = \mathbf{1}$.

Мономы разбиваются на два класса – правильных и неправильных мономов. Моном называется правильным, если в его записи нет оператора I, предшествующего оператору D. В противном случае, моном называется неправильным. В частности, по определению оператор $\mathbf{1}$ есть правильный моном. Линейное пространство всех правильных мономов обозначим через P.

Теорема 6. Операторы $\mathbf{1}, \{X^i\}, \{D^j\}, \{I^k\}, \{X^i D^j\}, \{X^iI^k\}$, где i,j,k в каждой системе операторов независимо принимают значения 1, 2, 3,..., образуют линейный базис пространства P.

Доказательство. Произвольную линейную комбинацию всех этих операторов, как легко видеть, можно однозначно представить в виде

$$P(X) + \sum_{m=1}^{m_1} q_m(X) D^m + \sum_{k=1}^{k_1} r_k(X) I^k, \tag{26}$$

где $P(X), q_m(X), r_k(X)$ – некоторые многочлены от оператора X. Если предположить, что сумма (26) равна нулю, то умножая ее справа на оператор I^{m_1}, получим:

$$P(X) I^{m_1} + q_{m_1}(X) + q_{m_1-1}(X) I + \cdots +$$
$$+ q_1(X) I^{m_1-1} + r_1(X) I^{m_1+1} + \cdots + r_{k_1}(X) I^{k_1+m_1} = 0. \tag{27}$$

Как видно из описания левой части (27), она состоит из различных мономов $X^i I^j$, которые в силу теоремы 5 линейно независимы. Теорема доказана.

Определим счетное число операторов:

$$V_0 = \mathbf{1} - ID, V_1 = \mathbf{1} - I^2 D^2, \ldots, V_{m-1} = \mathbf{1} - I^n D^n, \text{и т. д.}$$

Теорема 7. Операторы $V_0, V_1, \ldots$ образуют по умножению коммутативную полугруппу: $V_k V_m = V_{min(k,m)}, {V_k}^2 = V_k$ и $V_0 V_n = V_0$.

Доказательство. Действительно, согласно определению имеем

$$V_k V_m = (\mathbf{1} - I^k D^k)(\mathbf{1} - I^m D^m) = \mathbf{1} - I^m D^m - I^k D^k + I^m D^m I^k D^k =$$
$$= V_k + V_m - (\mathbf{1} - I^m D^m I^k D^k).$$

Если $k \leq m$, то $I^m D^m I^k D^k = I^m D^{m-k} D^k = I^m D^m$. Поэтому $V_k V_m = V_m + V_k - V_m = V_k$.

В случае $k > m$ аналогично получаем $V_k V_m = V_m$. Теорема доказана.

Таким образом, линейное пространство операторов $\{V_i\}$, $i = 0, 1, 2, \ldots$ образует коммутативную подалгебру в алгебре $A_L(X, D, I)$. Двусторонний идеал, порожденный этой подалгеброй, обозначим V. Ясно, что идеал V является линейным пространством.

Теорема 8. Линейное пространство алгебры $A_L(X, D, I)$ есть прямая сумма линейных пространств P и V.

Доказательство. Прежде всего покажем, что пространства P и V не пересекаются. Пусть A – некоторый оператор из пространства правильных мономов. Тогда образ $Af(x)$, где f пробегает функции пространства L, является бесконечномерным. Действительно, предположим противное, т. е. что образ $Af(x)$ для правильного монома A, когда f пробегает все бесконечномерное пространство функций L, является конечномерным. Тогда очевидно, что образ DAf, а следовательно, и образ $D^m Af$ при любом натуральном m также является конечномерным. Так как оператор A правильный, то в силу соотношений (5),(6) и (7) при достаточно большом m оператор $D^m A$ принадлежит алгебре $A_L(X, D)$. Покажем, что образ $D^m Af$, где f пробегает все бесконечное пространство L, не может быть конечномерным. Допустим противное, т. е. что образ $D^m Af$ конечномерен. Так как оператор $D^m A \in A_L(X, D)$, то он может быть представлен в виде

$$P_0(X) + P_1(X)D + \cdots + P_s(X)D^s,$$

где $P_k(X)$ – полиномы от оператора X.

Мы допустили, что образ пространства L при действии оператора $D^m A$ конечномерен. Тогда в L существует бесконечномерное подпространство, отображающееся оператором $D^m A$ в ноль.

Таким образом, линейное дифференциальное уравнение

$$P_0(x)f(x) + P_1(x)f'(x) + \cdots + P_s(x)f^{(s)}(x) = 0$$

должно иметь бесконечное пространство решений в L. Однако, как хорошо известно из теории таких уравнений, пространство решений является конечномерным, и за базис его решений можно взять решения этого уравнения с начальными условиями $f_j^{(i)}(x_0) = \delta_j^{\,i}$ (символ Кронекера), $i, j = 0, 1, 2, \dots, s-1, x_0 \in [a, b]$. К тому же не все эти решения принадлежат пространству функций L. Таким образом, приходим к противоречию. Следовательно, образ Af, где f пробегает все бесконечномерное пространство функций L, а оператор A является правильным мономом в $A_L(X, D, I)$, есть бесконечномерное подпространство в L.

В случае, если оператор $B \in V$, то пространство $Bf, \forall f \in L$ конечномерно. Для простоты доказательства предположим, что L

содержит константу, а следовательно, и все полиномы от переменного x. При этом очевидно, что $V_{k+1}x^n = (\mathbf{1} - I^k D^k)x^n = 0$, если $n \geq k$ и равно x^n при $n < k$. Таким образом, пространство образов V_k от всех полиномов имеет размерность k, т. е. оператор $V_k \notin P$. Всякий элемент идеала V является суммой операторов вида $A_1 V_{i_1} A_2 V_{i_2} \dots A_s V_{i_s} A_{s+1}$, где $A_1, \dots, A_{s+1}$ – правильные мономы. Так как операторы $A_1, \dots, A_{s+1}$ всякий многочлен переводят в многочлен, то образ пространства полиномов под действием операторов $A_1 V_{i_1} A_2 V_{i_2} \dots A_s V_{i_s} A_{s+1}$, где $A_1, \dots, A_{s+1}$ есть пространство полиномов степени не более $\min(i_1, i_2, \dots, i_s)$.

Покажем теперь, что все пространство алгебры $A_L(X, D, I)$ есть прямая сумма пространств P и V. Для этого достаточно показать, что всякий моном от операторов X, D *и* I есть сумма элементов из P и V. Если A есть правильный моном, то $A \in P$ из определения P. Если A неправильный моном, то $A = A_1\left(\mathbf{1} - V_{k_1}\right)A_2\left(\mathbf{1} - V_{k_2}\right)\dots$ $\dots A_s\left(\mathbf{1} - V_{k_s}\right)A_{s+1}$, где A_1, … A_{s+1} – правильные мономы. Раскрывая скобки, получим:

$$A = A_1 A_2 \dots A_{s+1} - A_1 V_{i_1} A_2 \dots A_s - A_1 A_2 V_{i_2} \dots A_s + \cdots .$$

В этой сумме оператор $A_1 \dots A_{s+1}$ имеет меньшую степень, чем оператор A. Здесь имеется в виду число множителей X *и* D. Оператор $A_1 A_2 \dots A_{s+1}$ может быть неправильным мономом. Остальные члены суммы очевидно принадлежат V. Продолжая действовать таким же образом с оператором $A_1 A_2 \dots A_{s+1}$, мы в конце концов за конечное число шагов придем к сумме, состоящей из правильного монома и элементов идеала V.Теорема доказана.

Теперь естественно возникает вопрос о строении алгебры, порожденной операторами X, D и I, в которой операторы D и I обратимы, т. е. $DI = ID = \mathbf{1}$. Естественно, такая алгебра получается факторизацией алгебры $A_L(X, D, I)$ по двустороннему идеалу V. При такой факторизации обозначим образы $\mathbf{0}, \mathbf{1}, X, D$ и I соответственно $\mathbf{0}, \mathbf{1}, a, b$ и b^{-1}.

Теорема 9. Фактор-алгебра $A_L(X, D, I)/V$ изоморфна расширенной алгебре Вейля, т. е. алгебре Вейля, порожденной элементами

a, b и $\mathbf{1}$ с соотношением $ba - ab = \mathbf{1}$ и расширенной элементом b^{-1}(обратным к b) с соотношением $b^{-1}a - ab^{-1} = -b^{-2}$ и с базисом $\{a^m b^n\}$, где $n = 0, 1, 2, \ldots$; $m = 0, \pm 1, \pm 2, \ldots$.

Доказательство. В силу теоремы 8 образами при факторизации будет пространство правильных мономов с заменой X на a, D на b, а I на b^{-1}, так как факторизация является гомоморфизмом и поэтому DI и ID переходят в $\mathbf{1}$. То есть если D переходит в b, то I должно переходить в b^{-1}. При гомоморфизме все алгебраические соотношения сохраняются. Поэтому соотношение $DX - XD = \mathbf{1}$ перейдет в $ba - ab = \mathbf{1}$, а соотношение $IX - XI = -I^2$ перейдет в $b^{-1}a - ab^{-1} = -b^2$. Очевидно, что и любые другие соотношения в алгебрах $A_L(X, D)$ и $A_L(X, I)$ перейдут в соответствующие соотношения. Таким образом, получаем расширенную алгебру Вейля. Линейный базис этой алгебры состоит из элементов $\{a^m b^n\}$, где $m = 0, 1, 2, \ldots$; $n = 0, \pm 1, \pm 2 \ldots$, или элементов $\{b^n a^m\}$, $n = 0, \pm 1, \pm 2, m = 0, 1, 2, \ldots$. Действительно, если $\sum_{k=-k_0}^{k_0} P(a) b^k = \mathbf{0}$ в расширенной алгебре Вейля, то умножив это равенство справа на b^{k_0}, получим $P_{-k_0}(a) + P_{-k_0+1}(a)b + \cdots + P_{k_0}(a) b^{2k^0} = \mathbf{0}$, которое является уже соотношением в алгебре Вейля. Следовательно, в силу теоремы 1 все многочлены $P_i(a) = \mathbf{0}$. Теорема доказана.

В заключение сделаем несколько важных замечаний.

1. Алгебру Вейля независимо от алгебры $A_L(X, D, I)$ можно естественно расширить элементами b^{-1} или a^{-1}. Действительно, пусть задана формальная алгебра Вейля с образующими $a, b, \mathbf{1}$ и $ba - ab = \mathbf{1}$. Введем для символа b обратный элемент b^{-1}. Умножая равенство $ba - ab = \mathbf{1}$ слева и справа на b^{-1}, получим: $ab^{-1} - b^{-1}a = b^{-2}$ или $b^{-1}a - ab^{-1} = -b^{-2}$. Продолжая аналогичным образом, мы придем к формуле $b^{-n}a - ab^{-n} = -nb^{-(n+1)}$.

В общем случае это будет выглядеть так: $P(b)a - aP(b) = P'(b)$, где $P(b)$ – полином от b с положительными и отрицательными степенями, а $P'(b)$ есть формальная производная по символу b. Аналогично алгебра Вейля расширяется символом a^{-1}.

2. Формула (17) переходит в соответствующую формулу в расширенной алгебре Вейля:

$$b^{-1}P(a) = P(a)b^{-1} - P'(a)b^{-2} + P''(a)b^{-3} - \cdots.$$

3. Аналогично формула (18) переходит в

$$P(a)b^{-1} = b^{-1}P(a) + b^{-2}P'(a) + b^{-3}P''(a) + \cdots,$$

где $P(a)$ – полиномы от a и $P'(a), P''(a), \ldots$, формальные производные по символу a.

Пользуясь случаем, выражаю благодарность В.К. Жарову за внимание к работе и В.И. Ремезовой за помощь в оформлении.

Литература

1. *Ващенко-Захарченко М.Е.* Символическое исчисление и приложение его к интегрированию линейных дифференциальных уравнений. Киев: Университетская типография, 1962. 90 с.
2. *Фок В.А.* Начала квантовой механики. М.: Наука, 1976. 367 с.
3. *Микусинский Я.* Операторное исчисление. М.: Изд-во иностр. лит., 1956. 366 с.
4. *Харди Г.* Расходящиеся ряды. М.: Изд-во иностр. лит., 1951. 504 с.

References

1. Vashchenko-Zakharchenko ME. Symbolic calculus and its application to the integration of linear differential equations. Kiev: Universitetskaya tipografiya Publ.; 1956. 90 p. (In Russ.)
2. Fock VA. The beginnings of quantum mechanics. Moscow: Nauka Publ.; 1976. 367 p. (In Russ.)
3. Mykusinskii Y. Operator calculus. Moscow: Izdatel'stvo inostrannoi literatury Publ.; 1956. 366 p. (In Russ.)
4. Hardy G. Divergent series. Moscow: Izdatel'stvo inostrannoi literatury Publ.; 1951. 504 p. (In Russ.)

Информация об авторе

Валерий М. Максимов, доктор физико-математических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; Российский университет дружбы народов, Москва, Россия; Россия, Москва, 117198, ул. Миклухо-Маклая, д. 6; vm_maximov@mail.ru

Information about the author

Valery M. Maksimov, Dr. in Physics and Mathematics, professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; Peoples' Friendship University of Russia, Moscow, Russia; bld. 6, Miklukho-Maklaya str., Moscow, 117198, Russia; vm_maximov@mail.ru

УДК 519.872

Предельные теоремы о сходимости к пуассоновскому закону распределения

Шакир К. Форманов
Институт математики им. В.И. Романовского АН Республики Узбекистан, Ташкент, Республика Узбекистан, shakirformanov@yandex.com

Байноза Б. Хусаинова
Институт математики им. В.И. Романовского АН Республики Узбекистан, Ташкент, Республика Узбекистан

Аннотация. В современной теории суммирования независимых случайных величин (с.в.) наряду с центральной предельной теоремой (аппроксимации распределения сумм независимых с.в. гауссовским распределением) важную роль играют предельные теоремы о сходимости к обобщенным пуассоновским распределениям.

Ключевые слова: обобщенные пуассоновские распределения, равномерная бесконечная малость случайных величин, классические и неклассические предельные теоремы, теоремы типа Линдеберга–Феллера.

Для цитирования: *Форманов Ш.К., Хусаинова Б.Б.* Предельные теоремы о сходимости к пуассоновскому закону распределения // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 94–110.

Ultimate theorems of convergence to Poisson distribution

Shakir K.Formanov
Romanovsky Institute of Mathematics, Academy of Sciences of Uzbekistan, Tashkent, Republic of Uzbekistan, shakirformanov@yandex.com

Bainoza B. Khusainova
Romanovsky Institute of Mathematics, Academy of Sciences of Uzbekistan, Tashkent, Republic of Uzbekistan

Abstract. In addition to the central limit theorem (approximations of the distribution for sums of independent random values by a Gaussian distribution) an important role in the modern theory of summation of independent random variables is played by ultimate theorems on convergence to generalized Poisson distributions.

Keywords: generalized Poisson distributions, uniform infinite infinitesimal smallness of random values, classical and nonclassical limit theorems, theorems of Lindeberg-Feller type.

For citation: Formanov ShK., Khusainova BB. Ultimate theorems of convergence to Poisson distribution. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):94-110.

Введение

Пусть

$$X_{n1},...,X_{nk},... \qquad n=1,2...$$

последовательность серий независимых случайных величин (с.в.), $\{k_n,\ n\geq 1\}$ – последовательность неотрицательных целочисленных чисел такая, что $k_n \to \infty$ при $n\to\infty$. Будем считать, что

$$EX_{nj}=0,\ EX_{nj}^2=DX_{nj}=\lambda_{nj},\ j=1,2,\ ...$$

$$S_n = X_{n1}+...+X_{nk_n},\quad \sum_{i=1}^{k_n}\lambda_{nj}=DS_n\to\lambda, \qquad n\to\infty.$$

Таким образом, $\{S_n,\ n\geq 1\}$ представляет собой последовательность сумм серий независимых с.в.

Положим $(x,t\in R)$;

$$F_n(x)=P(S_n<x),\ F_{nj}(x)=P(X_{nj}<x);$$

$$f_n(t)=Ee^{itS_n},\ f_{nj}(t)=Ee^{itX_{nj}},\ j=1,2,...$$

Таким образом, имеют место равенства

$$F_n(\cdot)=F_{n1}*...*F_{nk_n},\ f_n(t)=\prod_{j=1}^{k_n}f_{nj}(t),$$

где знак * обозначает свертку (композицию) распределений, т. е.

$$F*G=\int_{-\infty}^{\infty}F(x-u)dG(u)=\int_{-\infty}^{\infty}G(x-u)dF(u).$$

Закон распределения Пуассона со средним a и дисперсией $b>0$, т. е. закон с характеристической функцией (х.ф.)

$$\pi(a,b,t)=\exp\{iat+b(e^{it}-1-it)\},$$

мы будем обозначать $G(a,b,x)$. В дальнейшем рассматриваются следующие функции распределения (ф.р.):

$$G_{nj}(x)=G(0,\lambda_{nj},x),\ j=1,2,\ldots,$$

$$G_{\lambda}(x)=G(0,\lambda,x)\quad \lambda>0.$$

Соответствующие им х.ф. будем обозначать строчными буквами:

$$g_{nj}(t)=g(a,\lambda_{nj},t),\ j=1,2,\ldots.$$

В частности, $G_{\lambda}(x)$ обозначает ф.р. пуассоновского закона с параметром $\lambda=\sum_{j=1}^{\infty}\lambda_{nj},\quad \lambda=\lim_{n\to\infty}DS_n,$

и х.ф. $g_{nj}(t)=g(a,\lambda_{nj},t),\ j=1,2,\ldots$

Из приведенных обозначений следует, что имеют место равенства

$$G_{\lambda}=G_{n1}*\ldots*G_{nk_n}*\ldots=\prod_{j=1}^{\infty}G_{nj},$$

$$g_{\lambda}(t)=g_{n1}(t)*\ldots*g_{nk_n}(t)*\ldots=\prod_{j=1}^{\infty}g_{nj}(t)\cdot$$

Из последних рассуждений с учетом введенных обозначений имеют место равенства

$$\int_{-\infty}^{\infty}xdF_{nj}(x)=\int_{-\infty}^{\infty}xdG_{nj}(x)=0,$$

$$\int_{-\infty}^{\infty}x^2dF_{nj}(x)=\int_{-\infty}^{\infty}x^2dG_{nj}(x)=\lambda_{nj},\quad j=1,2,\ldots.,$$

$$DS_n=\lambda-\sum_{j=k_n+1}^{\infty}\lambda_{nj}.$$

Замечание 1. Число слагаемых с.в. k_n в сумме S_n можно считать равным бесконечности, предполагая при этом, что полученный ряд с.в. S_n сходится с вероятностью 1.

Хорошо известно (см. [1–4]), что расстояние Леви между двумя распределениями F и G, определяемое формулой

$$L(F,G) = \inf\left\{ \varepsilon > 0;\ F(x-\varepsilon) \le G(x) \le F(x+\varepsilon), \forall x \in R \right\}$$

метризирует слабую сходимость последовательности $\left\{F_n,\ n \ge 1\right\}$ к ф.р. G, т. е. имеет место импликация эквивалентности

$$\left\{F_n \Rightarrow G\right\} \sim \left\{L(F_n,G) \to 0,\ n \to \infty\right\}.$$

Здесь символ $\Longrightarrow$ означает слабую сходимость последовательности ф.р.

Напомним следующее хорошо известное определение равномерной бесконечной малости слагаемых сумм независимых с.в., играющее важную роль в теории предельных теорем.

Определение ([1–5]). Слагаемые X_{nj} сумм S_n называются равномерно бесконечно малыми, если для любого $\varepsilon > 0$

$$\lim_{n\to\infty} \max_{1\le j\le k_n} P\left(\left|X_{nj}\right| \ge \varepsilon\right) = 0. \qquad (1)$$

Из классического неравенства Чебышева следует, что если слагаемые X_{nj} суммы S_n удовлетворяют условию

$$\lim_{n\to\infty} \max_{1\le j\le k_n} DX_{nj} = \lim_{n\to\infty} \max_{1\le j\le k_n} \lambda_{nj} = 0, \qquad (2)$$

то выполняется предельное соотношение (1).

Условие Линдеберга и классическая предельная теорема о сходимости к пуассоновскому закону

В исследованиях по предельным теоремам соотношение для распределений сумм независимых с.в.

$$L_n(\varepsilon) = \sum_{j=1}^{k_n} \int\limits_{|x-1|>\varepsilon} x^2 dF_{nj}(x) \to 0, \quad n \to \infty, \qquad (L)$$

справедливое для любого $\varepsilon > 0$, называется условием Линдеберга. Присутствие в выражении $L_n(\varepsilon)$ суммы «хвостов» дисперсий слагаемых относительно точки $x = 1$ объясняется следующим образом: в силу известной теоремы Колмогорова о представлении

$$\log g_\lambda(t) = \lambda(e^{it} - 1 - it)$$

спектральная мера $\Psi_\lambda(\cdot)$ безгранично делимого распределения $G_\lambda(x)$ сосредоточивается в точке $x = 1$. Таким образом, имеет место равенство

$$\lambda(e^{it} - 1 - it) = \int_{-\infty}^{\infty} \frac{e^{itx} - 1 - itx}{x^2} d\Psi_\lambda(x).$$

Следовательно,

$$\Psi_\lambda(x) = \begin{cases} 0, & \text{при } x < 1 \\ \lambda, & \text{при } x \geq 1 \end{cases};$$

$$\Psi_\lambda(1+0) - \Psi_\lambda(1) = \lambda.$$

Замечание 2. Нетрудно видеть, что из условия (L) следует выполнение условия равномерной бесконечной малости дисперсий слагаемых (2). Действительно, при $0 < \varepsilon < 1$

$$\lambda_{nj} = \int_{-\infty}^{\infty} x^2 dF_{nj}(x) = \int_{|x-1| \leq \varepsilon} x^2 dF_{nj}(x) + \int_{|x-1| > \varepsilon} x^2 dF_{nj}(x) =$$

$$= \int_{1-\varepsilon}^{1+\varepsilon} x^2 dF_{nj}(x) + \int_{|x-1| > \varepsilon} x^2 dF_{nj}(x) \leq 2 \cdot (1+\varepsilon)^2 \cdot \varepsilon + L_n(\varepsilon).$$

Следовательно, при выполнении условия (L)

$$\limsup_{n \to \infty} \max_{1 \leq j \leq k_n} \lambda_{nj} \leq 2 \cdot (1+\varepsilon)^2 \cdot \varepsilon.$$

В силу произвольности числа ε из последнего неравенства следует, что

$$\max_{1 \leq j \leq k_n} \lambda_{nj} \to 0, \quad n \to \infty.$$

Таким образом, справедливость соотношения (2) доказана.

В книге В.И. Ротаря [6, 307] приведено доказательство следующей теоремы о сходимости к пуассоновскому закону распределения.

Теорема А. Пусть выполнено условие Линдеберга (L) и

$$\lim_{n\to\infty}\sum_{j=1}^{n} DX_{nj} = \lim_{n\to\infty}\sum_{j=1}^{\kappa_n}\lambda_{nj} = \lambda > 0 .$$

Тогда

$$F_n(x) = P(S_n < x) \Rightarrow G_\lambda(x) = \sum_{k<x+\lambda} e^{-\lambda}\cdot\frac{\lambda^k}{k!}. \qquad (3)$$

Приведенная теорема существенно обобщает классическую теорему о сходимости биномиального распределения к пуассоновскому закону. При этом следует заметить, что в силу знаменитой теоремы Бернулли о законе больших чисел эта сходимость возможна только в том случае, когда слагаемые суммы S_n образуют схему серии.

Приведенное утверждение получает свое подтверждение при рассмотрении следующего примера.

Пусть с.в.

$$X_{nj} = \begin{cases} 1-p_{nj}, & \text{с вероятностью } p_{nj} \\ -p_{nj}, & \text{с вероятностью } q_{nj} = 1-p_{nj} \end{cases} \qquad j = 1,2,\ldots$$

Легко вычислить, что

$$EX_{nj} = (1-p_{nj})\cdot p_{nj} - p_{nj}\cdot(1-p_{nj}) = 0,$$

$$\lambda_{nj} = DX_{nj} = (1-p_{nj})^2 p_{nj} + p_{nj}^2\cdot(1-p_{nj}) = p_{nj}\cdot q_{nj}, \quad j = 1,2,\ldots$$

Если

$$p_n = \max_{1\le j\le k_n} p_{nj} \to 0, \quad n\to\infty,$$

то при любом $\varepsilon > 0$

$$\left|1-p_{nj}-1\right| \le \varepsilon,$$

$$P\left(\left|X_{nj}\right| \ge \varepsilon\right) \le \frac{DX_{nj}}{\varepsilon^2} = \frac{\lambda_{nj}}{\varepsilon^2} \le \frac{p_n}{\varepsilon^2} \to 0, \quad j = 1,2,\ldots$$

В рассматриваемом случае условие (L) выполнено, и равенство (2) имеет место.

В последующих рассуждениях важную роль играет величина

$$A_n = \sum_{j=1}^{k_n} p_{nj}.$$

Исследуем три возможных случая:

a) $A_n \to 0$, b) $A_n \to \lambda$, $0 < \lambda < \infty$, c) $A_n \to \infty$, $n \to \infty$.

В случае (a) при $n \to \infty$

$$E\left|S_n\right| \le \sum_{j=1}^{k_n} E\left|X_{nj}\right| = 2 \cdot \sum_{j=1}^{k_n} p_{nj} \cdot (1 - p_{nj}) \le 2 \cdot A_n \to 0.$$

Следовательно, в этом случае имеет место сходимость к вырожденному распределению

$$F_n(x) = P(S_n < x) \Rightarrow E_0(x) = \begin{cases} 0, & x \le 0 \\ 1, & x > 0. \end{cases} \quad (4)$$

В случае (b)

$$A_n - DS_n = \sum_{j=1}^{k_n} p_{nj}^2 \le p_n \cdot A_n.$$

Следовательно,

$$1 - \frac{DS_n}{A_n} = O(p_n), \quad n \to \infty. \quad (*)$$

Из последнего соотношения следует, что

$$\lim_{n\to\infty} DS_n = \lim_{n\to\infty} A_n = \lambda.$$

Таким образом в случае (b) условие теоремы A выполняется, и согласно этой теореме

$$F_n(x) \Rightarrow G_\lambda(x), \ n \to \infty. \quad (5)$$

В случае (c) из соотношения (*) получаем, что

$$DS_n = \sum_{j=1}^{k_n} p_{nj} q_{nj} \to \infty, \quad n \to \infty. \quad (**)$$

Схема Бернулли с различными вероятностями успехов p_{nj} и q_{nj} называется биномиально-пуассоновский схемой. Хорошо известно, что для того чтобы в этой схеме имела место нормальная сходимость

$$P\left(\frac{S_n}{\sqrt{DS_n}} < x\right) = F_n\left(x\sqrt{DS_n}\right) \Rightarrow \Phi(x) = \frac{1}{\sqrt{2}\pi}\int_{-\infty}^{x} e^{-\frac{u^2}{2}}du, \ \ n \to \infty,$$

необходимо и достаточно выполнение соотношения (**). Окончательно из приведенных предельных соотношений (4)–(6) следует, что класс предельных законов в биномиально-пуассоновской схеме для ф.р. $F_n(x) = P(S_n < x)$ включает три следующих распределения: $E_0(x)$ – вырожденное, сосредоточенное в точке $x = 0$ распределение; $G_\lambda(x)$ – пуассоновское распределение с параметром $\lambda > 0$; $\Phi(x)$ – нормальное распределение с параметрами (0, 1).

Условие (L) не является необходимым для выполнения слабой сходимости распределения $F_n(x)$ к пуассоновскому закону, т. е. для выполнения предельного соотношения (3). Чтобы убедиться в этом, в теореме А положим

$$F_{n1}(x) = P(X_{n1} < x) = G_\lambda(x);$$

$$F_{nj}(x) = E_0(x) \ \text{для всех} \ \ j \geq 2.$$

Замечание 3. Условие Линдеберга (L) в «более вероятностном смысле» может быть записано в следующем виде: при $n \to \infty$ для любого $\varepsilon > 0$

$$L_n(x) = \sum_{j=1}^{k_n} E(X_{nj}^2 \cdot I(\left|X_{nj} - 1\right| > \varepsilon)) \to 0. \tag{L'}$$

Здесь и в дальнейшем $I(A)$ означает индикатор события A:

$$I(A) = I(\omega) = \begin{cases} 1, & \text{если элементарное событие} \quad \omega \in A \\ 0, & \text{если элементарное событие} \quad \omega \overline{\in} A. \end{cases}$$

Очевидно, что в любом вероятностном пространстве $(\Omega, \Im, \mathrm{P})$ $E\,I(A) = P(A)$ и для с.в. X

$$EX \cdot I(A) = \int_{\Omega} X \cdot I_A dP = \int_{A} XdP.$$

Теперь теорему А можно переписать в следующем виде.

Теорема A′. Пусть выполнено условие Линдеберга (L′) и

$$DS_n = \sum_{j=1}^{X_n} \lambda_{nj} \to \lambda, \;\; n \to \infty\,.$$

Тогда при $n \to \infty$

$$L(F_n, G_\lambda) \to 0. \qquad \text{(ПС)}$$

Это предельное соотношение называют «пуассоновской сходимостью (ПС)» ([1–4, 6]). Выше было доказано, что условие (L) не является необходимым для выполнения (ПС). В работах [2, 3] и [5] доказана следующая теорема.

Теорема B. Пусть выполнено условие (2). Тогда условие (L) является необходимым для выполнения (ПС).

Таким образом, с учетом того, что имеет место импликация $(L) \Rightarrow (2)$, путем сравнения теорем A′ и B получаем следующую импликацию эквивалентности:

$$(2) \cap \text{(ПС)} \Leftrightarrow (L)\,. \qquad (6)$$

Утверждение (6) может быть названо полным аналогом теоремы Линдеберга–Феллера для (ПС) распределения суммы S_n.

По В.М. Золотареву [4] предельные теоремы, доказанные с привлечением условия равномерной бесконечной малости слагаемых (2), называются классическими. В книге В. Ротаря [6 с. 307–310] доказан неклассический вариант теоремы A′.

Числовая характеристика Ибрагимова–Осипова–Эссеена и сходимость распределения $F_n(x)$ к пуассоновскому закону

Числовая характеристика Линдеберга $L_n(\varepsilon)$ обладает свойством универсальности при изучении предельных теорем для распределения $F_n(x) = P(S_n < x)$. Несмотря на это, условие (L) при доказательствах некоторых предельных теорем выглядит в определенном смысле «избыточным». Во-первых, справедливость соотношений $L_n(\varepsilon) \to 0,\ n \to \infty$ нужно проверить для любого $\varepsilon > 0$. На самом деле в силу монотонного убывания $L_n(\varepsilon)$ по ε достаточно проверить выполнение условия (L) для $0 < \varepsilon < 1$.

В работе В.В. Петрова ([5], 197) рассматривается величина

$$m_n = \sum_{j=1}^{n} E X_j^2 \cdot I(|X_j| > 1) + \left| \sum_{j=1}^{n} E X_j^3 \cdot I(|X_j| \le 1) \right| + \sum_{j=1}^{n} E X_j^4 \cdot I(|X_j| \le 1), \quad (7)$$

играющая существенную роль в задачах оценки скорости сходимости центральной предельной теоремы (т. е. в задачах оценки скорости стремления $F_n(x)$ к нормальному закону распределения). Стремление к нулю второго и третьего членов характеристики m_n проверяется одинаково. Поэтому их можно заменить одним выражением

$$m_n(\alpha) = \sum_{j=1}^{n} E |X_j|^{2+\alpha} \cdot I(|X_j| \le 1), \quad \alpha > 0.$$

Следовательно, в формуле (7) вместо выражения m_n можно использовать величину

$$M_n(\alpha) = L_n(1) + m_n(\alpha), \quad \alpha > 0. \quad (8)$$

Примечание. Введенные величины m_n и $M_n(\alpha)$ относятся к общей схеме суммирования независимых с.в., т. е. в формулах (7) и (8) надо полагать, что

$$X_j = X_{nj}, \quad j = 1, 2, \ldots, \quad n = 1, 2, \ldots .$$

На рубеже 60–70-х годов XX века Ибрагимовым, Осиповым, Эссееном опубликованы несколько работ, в которых авторы доказывают, что оценить остаточный член в центральной предельной теореме одной характеристикой Линдеберга $L_n(\varepsilon)$ или другой характеристикой «усеченных моментов» m_n невозможно. В последующем эти результаты названных авторов отражены в работе [5]. Таким образом, величины, определяемые формулами (7) и (8), можно называть числовыми характеристиками Ибрагимова–Осипова–Эссеена (И–О–Э).

В настоящей работе характеристика И–О–Э будет применена в предельных теоремах о сходимости к пуассоновскому закону распределения сумм независимых с.в. в S_n.

В связи со сказанным напомним, что в теории суммирования независимых с.в. предельное пуассоновское распределение возникает только при суммировании с.в. в схеме серии.

С учетом этого перепишем характеристику И–О–Э в виде

$$M_n(\alpha) = L_n(1) + m_n(\alpha), \quad \alpha > 0, \tag{8'}$$

где

$$L_n(\varepsilon) = \sum_{j=1}^{k_n} E\, X_{nj}^2 \cdot I(\left|X_{nj} - 1\right| > \varepsilon), \quad \varepsilon > 0;$$

$$m_n(\alpha) = \sum_{j=1}^{n} E\left|X_{nj}\right|^{2+\alpha} \cdot I(\left|X_{nj}\right| \le 1), \quad \alpha > 0.$$

Предварительно исследуем свойства сумм «усеченных» моментов порядка $2+\alpha$:

$$m_n(\alpha) = \sum_{j=1}^{k_n} \int\limits_{|x|\le 1} |x|^{2+\alpha}\, dF_{nj}(x), \quad \alpha > 0.$$

Лемма 1. Если $DS_n \to \lambda > 0, \quad n \to \infty$ и при некотором $\alpha = \alpha_0 > 0$

$$\lim_{n\to\infty} m_n(\alpha_0) = 0,$$

то $m_n(\alpha) \to 0$ для всех $\alpha > 0$.

Доказательство. Пусть $\alpha < \alpha_0$. При любом $0 < \varepsilon < 1$

$$m_n(\alpha) = \sum_{j=1}^{k_n} \int\limits_{|x-1|\le\varepsilon} |x|^{2+\alpha}\, dF_{nj}(x) + \sum_{j=1}^{k_n} \int\limits_{|x-1|>\varepsilon} |x|^{2+\alpha}\, dF_{nj}(x) = \tag{9}$$

$$= \sum{}_{n1} + \int\limits_{1-\varepsilon<|x|\le 1} |x|^{2+\alpha}\, dF_{nj}(x) = \sum{}_{n1} + \sum{}_{n2}.$$

Далее

$$\sum{}_{n1} \le \varepsilon^{\alpha} \sum_{j=1}^{k_n} \int\limits_{|x|\le\varepsilon} x^2 dF_{nj}(x) \le \varepsilon^{\alpha} DS_n \le \lambda\varepsilon^{\alpha}, \tag{9'}$$

$$\sum\nolimits_{n2} \le (1-\varepsilon)^{-(\alpha-\alpha_0)} \sum_{j=1}^{k_n} \int\limits_{1-\varepsilon<|x|\le 1} |x|^{2+\alpha_0}\, dF_{nj}(x) \le (1-\varepsilon)^{-(\alpha_0-\alpha)} \cdot m_n(\alpha_0). \quad (9'')$$

Теперь из (9′), (9′′) получаем, что при всех $0<\varepsilon<1$

$$\limsup_{n\to\infty} m_n(\alpha) \le \lambda \cdot \varepsilon^{\alpha}. \qquad (10)$$

Пусть $\alpha > \alpha_0$. Тогда

$$m_n(\alpha) = \sum_{j=1}^{k_n} \int\limits_{|x|\le 1} |x|^{2+\alpha_0} |x|^{\alpha-\alpha_0}\, dF_{nj}(x) \le m_n(\alpha_0) \to 0, \quad n\to\infty. \quad (10')$$

В силу произвольности $0<\varepsilon<1$ доказательство леммы 1 следует из соотношений (10) и (10′).

Из доказанной леммы следует, что удобнее считать условие $m_n(\alpha)\to 0,\ \ n\to\infty$ выполненным при $\alpha=1$, т. е.

$$m_n(1) = \sum_{j=1}^{k_n} \int\limits_{|x|\le 1} |x|^3\, dF_{nj}(x) \to 0, \quad n\to\infty.$$

Тогда условие $m_n(\alpha)\to 0,\ \ n\to\infty$ выполняется при любом $\alpha>0$. Сказанное продемонстрируем в случае «нарастающих» сумм одинаково распределенных независимых с.в. В связи со сказанным положим

$$M_n = L_n(1) + m_n(1) = L_n + m_n,$$

где $L_n = \sum_{j=1}^{k_n} \int\limits_{|x|>1} x^2 dF_{nj}(x).$

Содержание приведенной леммы проиллюстрируем в случае «нарастающих» сумм независимых одинаково распределенных с.в. Пусть $X_1, X_2, \ldots,$ – последовательность независимых с.в. с общей ф.р. $F(x)$. Будем считать, что

$$E\,X_1 = \int_{-\infty}^{\infty} x dF(x) = 0, \quad \sigma^2 = \int_{-\infty}^{\infty} x^2 dF(x) < \infty.$$

Введем обозначение

$$S_n = \frac{X_1 + \ldots + X_n}{\sigma\sqrt{n}} = X_{n1} + \ldots + X_{nn},$$

где $X_{nj} = \dfrac{X_j}{\sigma\sqrt{n}}, \quad j = 1, \ldots, n.$

В этом случае

$$L_n = L_n(1) = \int\limits_{|x| > \sigma\sqrt{n}} x^2 dF_n(x) \to 0, \; n \to \infty; \qquad (11)$$

$$m_n = m_n(1) = \frac{1}{\sigma\sqrt[3]{n}} \cdot \int\limits_{|x| \le \sigma\sqrt{n}} |x|^3 \, dF(x).$$

Далее при помощи несложных рассуждений нетрудно убедиться в справедливости следующей оценки $0 < \varepsilon < 1$:

$$m_n = \frac{1}{\sigma\sqrt[3]{n}} \cdot \left(\int\limits_{\left|\frac{x}{\sigma\sqrt{n}}\right| \le \varepsilon} |x|^3 \, dF(x) + \int\limits_{\varepsilon < \left|\frac{x}{\sigma\sqrt{n}}\right| \le 1} |x|^3 \, dF(x) \right) \le \varepsilon + \frac{1}{\sigma^2} \cdot \int\limits_{|x| > \varepsilon\sigma\sqrt{n}} x^2 dF(x).$$

Следовательно, при всех $0 < \varepsilon < 1$

$$\limsup_{n \to \infty} m_n \le \varepsilon. \qquad (11')$$

Таким образом, в силу произвольности $0 < \varepsilon < 1$ из предельных соотношений (11) и (11′) получаем, что

$$M_n \to 0, \quad n \to 0. \qquad (12)$$

В свою очередь, из последнего следует, что в случае одинаково распределенных независимых с.в. соотношение (12) выполняется, и согласно лемме 1 в этом случае имеет место соотношение

$$M_n(\alpha) \to 0, \quad n \to 0, \; \forall \alpha > 0. \qquad (12')$$

Теорема 1. Условие (M) и условие Линдеберга (L) эквивалентны (равносильны).

Доказательство. Утверждение теоремы 1 в схеме логических импликаций можно представить в виде

$$(M) \Leftrightarrow (L). \tag{13}$$

Пусть имеет место условие (M), т. е. при некотором $\alpha = \alpha_0 > 0$

$$m_n(\alpha_0) \to 0, \quad L_n(\varepsilon) \to 0, \; n \to \infty . \tag{14}$$

Согласно лемме 1 можно считать $\alpha_0 = 1$, и в силу монотонной убываемости характеристики Линдеберга $L_n(\varepsilon)$ достаточно доказать, что для всех $0 < \varepsilon < 1$

$$L_n(\varepsilon) \to 0, \quad n \to \infty. \tag{15}$$

Далее имеем

$$\begin{gathered} L_n(\varepsilon) = \sum_{j=1}^{k_n} \int\limits_{|x-1|>\varepsilon} x^2 dF_{nj}(x) = \\ = \sum_{j=1}^{k_n} \int\limits_{1-\varepsilon<|x|\le 1} x^2 dF_{nj}(x) + \sum_{j=1}^{k_n} \int\limits_{|x|>1} x^2 dF_{nj}(x) = \sum{}_n + L_n. \end{gathered} \tag{16}$$

Понятно, что оценка

$$\sum{}_n = \sum_{j=1}^{k_n} \int\limits_{1-\varepsilon<|x|\le 1} x^2 dF_{nj}(x) \le \frac{1}{1-\varepsilon} \cdot \int\limits_{|x|\le 1} |x|^3 \, dF_{nj}(x) = \frac{1}{1-\varepsilon} \cdot m_n \to 0 . \tag{17}$$

В свою очередь из (16) и (17) получаем, что при всех $0 < \varepsilon < 1$

$$\lim_{n\to\infty} L_n(\varepsilon) = 0.$$

Соотношение (15) доказано.

Далее имеем

$$m_n = \sum_{j=1}^{k_n} \int\limits_{|x|\le 1} |x|^3\, dF_{nj} \le \varepsilon \times \sum_{j=1}^{k_n} \int\limits_{|x|\le\varepsilon} x^2 dF_{nj} + \varepsilon^{-2} \times$$

$$\times \sum_{j=1}^{k_n} \int\limits_{\varepsilon<|x|\le 1} x^4 dF_{nj} \le \lambda\varepsilon + \varepsilon^{-2} L_n^*(\varepsilon),$$

где $L_n^*(\varepsilon) = \sum_{j=1}^{k_n} \int\limits_{|x|>\varepsilon} x^2 dF_{nj}(x)$.

Непосредственно из последних неравенств получаем, что

$$\limsup_{n\to\infty} m_n \le \varepsilon\lambda . \tag{18}$$

Теперь заметим, что при любом $\varepsilon > 0$

$$\left\{L_n(\varepsilon) \to 0\right\} \Leftrightarrow \left\{L_n^*(\varepsilon) \to 0\right\},\ n \to \infty.$$

Следовательно, из (18) следует, что $m_n \to 0,\ n \to \infty$.
Теорема 1 доказана.

Теорема 2. Если при некотором $\alpha > 0$

$$M_n(\alpha) \to 0, \quad n \to \infty, \tag{M}$$

то последовательность слагаемых $\left\{ X_{nj},\ j \ge 1 \right\}$ суммы S_n удовлетворяет условию равномерной бесконечной малости дисперсий (2).

Доказательство теоремы 2 проводится с применением следующего вспомогательное утверждения, доказательство которого можно проводить без сложных рассуждений.

Лемма 2. Пусть с.в. X с распределением $F(x)$ удовлетворяет условиям

$$EX = \int\limits_{-\infty}^{\infty} x dF(x) = 0;$$

$$DX = EX^2 = \int\limits_{-\infty}^{\infty} x^2 dF(x) = \sigma^2 < \infty.$$

Тогда при любом $0 < \varepsilon < 1$

$$\int\limits_{\{x;\, |x-1| \le \varepsilon\}} x^2 dF(x) = \int\limits_{1-\varepsilon}^{1} x^2 dF(x) \le 8\varepsilon\big(F(1) - F(1-\varepsilon)\big).$$

Применяя оценку, приведенную в лемме 2, имеем

$$\max_{1 \le j \le k_n} \int\limits_{|x-1| \le \varepsilon} x^2 dF_{nj}(x) \le \sum_{j=1}^{k_n} \int\limits_{|x-1| \le \varepsilon} x^2 dF_{nj}(x) \le 8\varepsilon \sum_{j=1}^{k_n}\big(F_{nj}(1) - F_{nj}(1-\varepsilon)\big) \le$$
$$\le 8\varepsilon\left[\sum_{j=1}^{k_n}\big(1 - F_{nj}(1)\big) + \sum_{j=1}^{k_n}\big(1 - F_{nj}(1-\varepsilon)\big)\right] \le \frac{16\varepsilon}{1-\varepsilon^2}\sum_{j=1}^{k_n}\lambda_{nj} \le \frac{16\varepsilon}{1-\varepsilon^2} DS_n \le \frac{16\varepsilon}{1-\varepsilon^2}\lambda\ . \tag{19}$$

Теперь доказательство теоремы 2 следует из последней цепочки оценок (19).

Следующая теорема является аналогом классической предельной теоремы Линдеберга–Феллера, относящейся к проблеме о справедливости центральной предельной теоремы.

Теорема 3. Для того, чтобы последовательность серий независимых случайных величин $\{X_{nj}, j \ge 1\}$ удовлетворяла условию равномерной бесконечной малости и функция распределения $F_n(x) = P\left(\sum_{j=1}^{\infty} X_{nj} < x\right)$ слабо сходилась к пуассоновскому закону, необходимо и достаточно выполнения условия (M).

Приведенная теорема 3 доказывается с привлечением результатов теорем 1 и 2.

Литература

1. *Гнеденко Б.В., Колмогоров А.Н.* Предельные распределения для сумм независимых случайных величин. М.: Гос. изд-во техн.-теор. лит-ры, 1949. 264 с.
2. *Линник Ю.В., Островский И.В.* Разложения случайных величин и векторов. М.: Наука, 1972. 478 с.
3. *Круглов В.М., Королёв В.Ю.* Предельные теоремы для случайных сумм. М.: МГУ, 1990. 208 с.

4. *Золотарёв В.М.* Современная теория суммирования независимых случайных величин. М.: Наука, 1986. 547 с.
5. *Петров В.В.* Предельные теоремы для сумм независимых случайных величин. М.: Наука, 1987. 317 с.
6. *Rotar V.* Probability theory. Singapore: World Sci., 1997. 414 p.

References

1. Gnedenko BV., Kolmogorov AN. Ultimate distributions for sums of independent random values. Moscow: Gosudarstvennoe izdatel'stvo tekhniko-teoreticheskoi literatury Publ.; 1949. 264 p. (In Russ.)
2. Linnik YuV., Ostrovsky IV. Decompositions of random values and vectors. Moscow: Nauka Publ.; 1972. 478 p. (In Russ.)
3. Kruglov VM., Korolyov VYu. Ultimate theorems for random sums. Moscow: MSU Publ.; 1990. 208 p. (In Russ.)
4. Zolotaryov VM. Modern theory of summation for independent random values. Moscow: Nauka Publ.; 1986. 547 p. (In Russ.)
5. Petrov VV. Ultimate theorems for sums of independent random values. Moscow: Nauka Publ.; 1987. 317 p. (In Russ.)
6. Rotar V. Probability theory. Singapore: World Sci., 1997. 414 p.

Информация об авторах

Шакир К. Форманов, академик Академии наук Республики Узбекистан, доктор физико-математических наук, профессор, Институт математики им. В.И. Романовского АН Республики Узбекистан, Ташкент, Республика Узбекистан; Республика Узбекистан, Ташкент, 100125, пр. Дурмон Йули, д. 29; shakirformanov@yandex.com

Байноза Б. Хусаинова, младший научный сотрудник, Институт математики им. В.И. Романовского АН Республики Узбекистан, Ташкент, Республика Узбекистан; Республика Узбекистан, Ташкент, 100125, пр. Дурмон Йули, д. 29

Information about the authors

Shakir K. Formanov, Full Member of Academy of Sciences of Republic of Uzbekistan, Dr. in Mathematics, professor, Romanovsky Institute of Mathematics, Academy of Sciences of Republic of Uzbekistan, Tashkent, Republic of Uzbekistan; bld. 29, Durmon Yoli av., Tashkent, 100125, Republic of Uzbekistan; shakirformanov@yandex.com

Bainoza B. Khusainova, junior researcher, Romanovsky Institute of Mathematics, Academy of Sciences of Republic of Uzbekistan, Tashkent, Republic of Uzbekistan; bld. 29, Durmon Yoli av., Tashkent, 100125, Republic of Uzbekistan

УДК 519.6

Об одном способе построения конструктивной математической модели: древняя и средневековая математика Китая

Валентин К. Жаров
Российский государственный гуманитарный университет, Москва, Россия, valcon@mail.ru

Аннотация. Статья посвящена представлению древней и средневековой китайской математики как хранилища различных мыслительных приемов, вычислительных операций, алгоритмов и собрания типов мышления. Автор предполагает, что внесет некоторое прояснение в проблему теоретического и практического начал китайской математики.

Ключевые слова: суань-пан, чоу-суань, счетное поле, мыслительные и логические операции, алфавит, схемы, алгоритмы.

Для цитирования: Жаров В.К. Об одном способе построения конструктивной математической модели: древняя и средневековая математика Китая // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика» 2018. № 1 (1). С. 111–147.

On one method of creating a constructive mathematical model. Ancient and Medieval mathematics of China

Valentin K. Zharov
Russian State University for the Humanities, Moscow, Russia, valcon@mail.ru

Abstract. The article is devoted to the representation of ancient and medieval Chinese mathematics as a repository of various thinking techniques, computational operations, algorithms and a collection of types of thinking. The author also assumes that he will bring some clarification to the issue of theoretical and practical beginning of Chinese mathematics.

Keywords: Suan-pan, Chou-suan, accounting field, thinking and logical operations, alphabet, schemes, algorithms.

For citation: Zharov VK. On one method of creating a constructive mathematical model. Ancient and Medieval mathematics of China. *RSUH / RGGU Bulletin. "Information Science. Information Security. Mathematics" Series.* 2018;1(1):111-147.

> В процессе мышления мы пытаемся постичь разумом истину; наш разум пытается просветить себя, исходя из своего опыта.
>
> *Г. Вейль*

Введение

В рассуждениях о происхождении математики является общепризнанным фактом утверждение о том, что математика древняя наука и образец логической строгости теоретических построений. Современная же математика скроена из различных кусков, которые созданы воплощенным мышлением выдающихся людей своего времени. В ней реализованы все операционные возможности мышления каждого из мыслителей конкретного периода времени. На вопрос, что же такое математика, многие выдающиеся математики нового времени пытались дать ответ. Мы же, вслед за А.С. Кузичевым [1], отметим, что в основании математики находятся вычислительная и дедуктивная ее составляющие; иначе, если более широко, современные математические теории имеют в основании вычислительную культуру и культуру конкретной страны в определенный период времени в целом. Проблема соотношения в математике теоретического и практического начал известна давно. Апологеты идеи исключительности теории перед практической математикой говорят об этом со времен античной греческой математики, при этом забывая о практическом происхождении геометрии и эталонного, теоретического воплощения этого знания в «Началах» Евклида. При обсуждении статуса древней и средневековой китайской математики исследователями было сломано много копий, и преобладает мнение, что китайская математика имеет только практический, прикладной статус и не является теоретической в западном понимании [2]. Это утверждение мы считаем некорректным, поскольку существуют два аргумента, без учета которых нельзя не усомниться в справедливости приведенного утверждения. Первый – известно ли нам, что такое математическое мышление[1]; и второй – что значит

---

[1] «Под математическим способом мышления я понимаю, во-первых, особую форму рассуждений, посредством которых математика проникает в науки о внешнем мире – в физику, химию, биологию, экономку и т. д. – и даже в наши размышления о повседневных делах и заботах, и, во-вторых, ту форму рассуждений, к которой прибегает в своей собственной области математик, будучи предоставленным самому себе» [3 с. 6]. Особенно интересна часть, определяемая со слов «во-вторых...», а первая часть фразы о чем? Видимо, о задачах математики как науки!

теоретическое в мыслительных традициях культуры, построенной на системе алгоритмических предписаний и уложений, в которой философия и по сей день имеет практический смысл! [4].

В данной статье мы рассматриваем развитие китайской математики до 1303 года – года написания Чжу Шицзе «Четырех яшмовых зеркал» [5]. Считаем по [6], что всего за две с половины тысячи лет до указанного года китайская математическая библиотека получила не более двадцати оригинальных трудов. Список трудов и обоснование этого утверждения можно найти в [7]. Мы же в своих исследованиях использовали пять работ из этого списка. Две работы переведены русский язык, одна частично на английский, а три полностью или частично переведены с древнекитайского языка автором статьи. Вот эти работы:

1) «Математика в девяти книгах» (Цзю Чжан Суань Шу) [6];
2) «Девять книг по математике» (Цинь Цзюшао)[6];
3) «Математический трактат о морском острове» (Лю Хуэй) [6];
4) «Математический трактат о морском зеркале» (Ли Е) [5];
5) «Суань Сюе Ци Мэн» Чжу Шицзе (первая книга этого автора) [6].

Анализ текстов этих источников приводит к определению ИПС[2] (информационно-педагогической среды) и созданию математической модели решения задач, представленных в рассматриваемых нами китайских текстах. Отметим, в частности, что исследование исторических следов имеет своей задачей и воссоздание различных сред изучаемой эпохи, а они естественным образом сохранены учебной и научной литературой.

Основное наше утверждение формулируется так: «развитие счетного инструмента с древнейшего времени до середины XIV века нашей эры в Китае предопределило стиль математического мышления китайских ученых, определивший, как бы теперь назвали, исчисление задач (конструктивная математика на традиционных вычислительных инструментах)»[8].

Еще одно утверждение состоит в том, что исследование текстов как памятников человеческой деятельности нужно понимать не только как историческую обработку материала (китайских трактатов), но и как превращенную форму мышления [8], а также как исчисление *разрешимых* задач.

---

[2] ИПС – окружающие человека физическое и социальное пространства (в целом – как макросреда, в конкретном смысле – как непосредственное социальное окружение, как микросреда), в которых происходит непрерывающийся обмен сообщениями, определяющий характер взаимодействия в процессе обучения, и связанная с этим процессом зона непосредственной активности индивида, его ближайшего развития и действия.

И, наконец, зададим обобщающий вопрос – каковы же китайская древняя и китайская средневековая математика?

1. Китайская традиционная математика

Различные ветви математики объединяются общим терминологическим словарем. Отсюда вытекает необходимость исследования терминологических словарей математики и словаря передачи и сохранения математической информации, т. е. глоссария обучения математике, а также стремление сопоставить научные словари различных эпох.

Основным методом представления математического знания в ИПС будет *метод составления минимальных словарей.*

1.1. Договоримся о понятиях

Напомним, что минимальный словарь (по Б. Расселу) должен удовлетворять двум условиям:

1) каждое предложение в данной системе знания может быть выражено посредством слов, принадлежащих данному словарю;

2) ни одно слово (атомарное слово) в этом словаре не может быть определено с помощью других слов этого словаря [9].

Под *словом* мы понимаем конструктивный объект, составленный по определенным правилам из букв конечного алфавита.

Буква – начальное понятие, удовлетворяющее следующим условиям: буква – это знак; буквы друг на друга не похожи, они различимы; буквы распознаваемы; буквы равноправны, т. е. они не подчиняются иерархическому принципу [10].

Знак – материальный предмет (явление, событие), выступающий в качестве представителя некоторого другого предмета, свойства или отношения и используемый для приобретения, хранения, переработки и передачи сообщений (выраженных в количестве информации и знаниях как значимых совокупностей текстов и текстур).

Смыслы – отраженные (зафиксированные) в текстах (носителях культуры) реальности (бытия, жизни). Как говорил В.В. Налимов – проявленность смыслов выражается через «человека в таких сферах его деятельности, как язык, воображение, наука» (цитируется по [11 с. 18]).

И еще одно соображение из цитируемой работы [11]: «*Смыслы* – это то, из чего создаются *тексты* с помощью *языка*. *Тексты* – это то, что создано из *смыслов* с помощью *языка*. *Язык* – это средство, с помощью которого рождаются *тексты*. Триада становится синонимом *сознания*».

> Человек извлекает смысл из мира-текста, переводит его на свой язык предметных, операциональных или вербальных значений. Процедура в целом носит название означивания смысла. Означивание смысла, построение знака и «размещение» его между собой и миром – это и есть Культура. Культура все превращает в знак, в язык, понимаемые в самом широком смысле. <...> Смысл означивается, так сказать, ответным действием, операциональным значением. [Цитируется В.П. Зинченко по: *Леонтьев А.А.* Деятельностный ум. М.: Смысл, 2001. С. 324].

Таким образом, движения, мыследействия, и тем самым образование потока сообщений возникают естественным путем, таким же путем возникает и коррекция сообщений посредством культурной среды.

Конечно, следует дать для полноты картины определение Культуры, но мы отошлем читателя к [12 с. 35].

Далее чрезвычайно важным в наших построениях является понятие «исчисление», которое означает

> ... систему изучения тех или иных областей объективного мира, в которой предметам какой-либо определенной области ставятся в соответствие материальные знаки (цифры, буквы и др.), с которыми затем по принятым в системе точным правилам производятся операции, необходимые для решения поставленной цели. Как показывает в своих трудах С.А. Яновская, возникшая 6 тысячелетий тому назад математика в древнем Египте и Вавилонии строилась прежде всего, как исчисление. Только в III в. до н. э. Евклид впервые построил математику в виде аксиоматической теории. Но и в современной школе изучение математики начинается еще с нумерации и четырех действий арифметики, т. е. с оперирования знаками (цифрами) [12 с. 31].

И наконец, необходимо обратить внимание читателя на понятие «счетный инструмент», которое является существенным в основном утверждении.

В [6] изображен на картинках чоу суань (рис. 1) – счетные палочки, народный счетный инструмент, для работы на котором требовались любая поверхность и сами палочки либо одного, либо нескольких цветов. Есть свидетельства, что чоу суань использовался еще в середине XX века менялами в Урумчи (автору рассказывал об этом Н.Е. Хохлов, преподаватель китайского языка ТашГУ им. В.И. Ленина).

Другой научный вычислительный инструмент – суань пан – представлен на рис. 2.

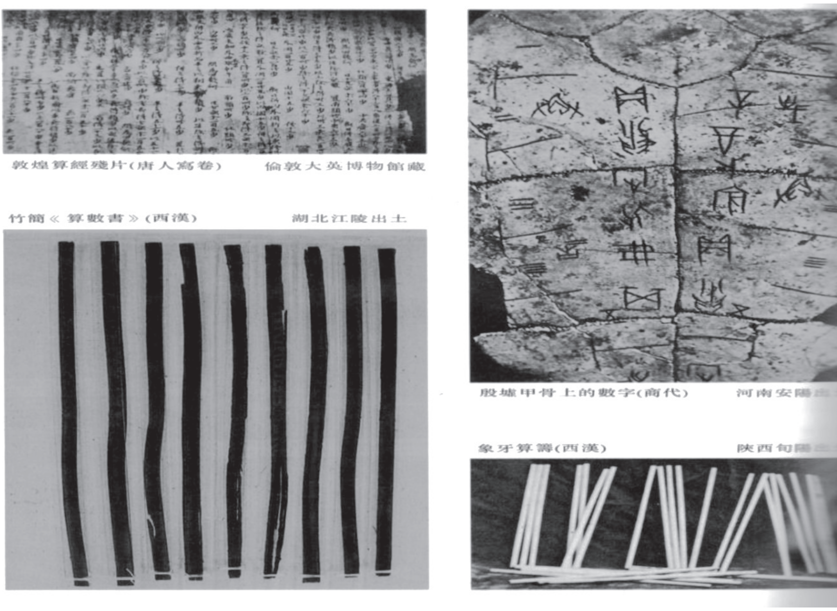


Рис. 1. Чоу суань

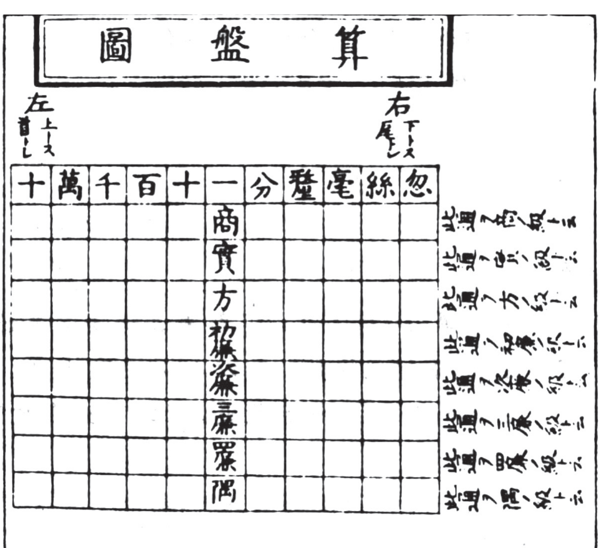


Рис. 2. Суань пан

К нему прилагаются вычислительные палочки (чоу суань). Конструкция суань пана и его свойства описаны в [7, 13]. На японской гравюре XVIII века (рис. 3) изображен процесс использования суань пана.

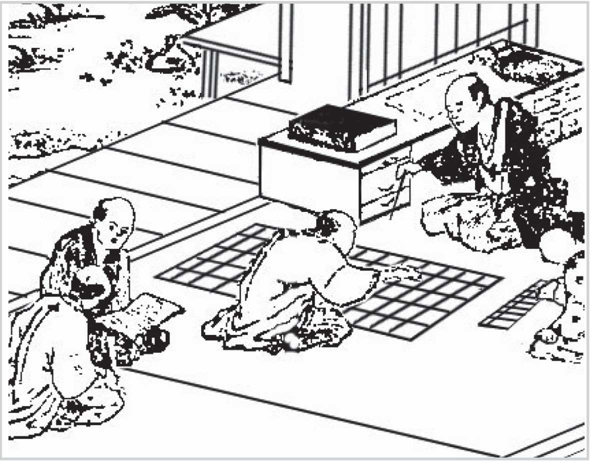


Рис. 3. Использование суань пана

Конструкцию суань пана (рис. 4.) образуют два основных компонента – расчерченная поверхность (вычислительное поле) и чоу сунь – набор палочек, раскладываемых на вычислительном поле или перебираемых в руках.

日本和算筹算图(据 1795 年木刻)

Рис. 4. Конструкция суань пана

1.2. Алфавит конструкции

Как строится модель изучаемого нами предмета – математических текстов традиционной китайской математики? В первом представлении она должна включить следующие этапы.

1. Всю обучающую (научную) литературу традиционной китайской математики разделить на две составляющие, а именно знаковую (универсальную знаковую систему, математический язык) и выраженный в них содержательный атрибут – алгоритмическую и культурологическую составляющие.
2. Показать возможные соответствия знаковых систем и их независимость в вычислительных конструкциях.
3. Совершить обратное отображение полученного представления в реальный историко-математический, историко-методический материал.

Анализ текстов перечисленных во введении трактатов привел к следующему результату.

Для проверки метода минимальных словарей были составлены минимальный словарь и словари последующих двух ступеней арифметико-алгебраических терминов трактата Цинь Цзюшао [14]. При этом использован сделанный раньше У. Либбрехтом [15] Glossary перевода части текста. Выполненный в 1988 г. автором статьи перевод трактата на русский язык до сих пор не опубликован. Однако для сравнения наших переводов этого оказалось вполне достаточно.

Рассмотрим *словарь первой ступени.*

1.	筹	чоу (chou) – счетная палочка
2.	一	и (yi) – один
3.	加 (并)	. цзя (jia)(бин (bin)) – прибавить, также добавить (этот иероглиф в “Чжоу би” можно перевести как «объединить» – термин, характерный для счетной доски)
4.	值	чжи (zhi) – установи на счетном поле
5.	退	туй (tui) – передвигай палочку влево
6.		чоу (chou) – передвигай палочку вправо
7.	位	вэй (wei) – место на вычислительном поле
8.	上	шан (shang) – верх
9.	中	чжун (zhong) – середина
10.	下	ся (xia) – низ
11.	进	цзин (jin) – доводить до

12.	除	чуй (chu) – исключать из
13.	实	ши (shi) – свободный член (место на счетном поле), подкоренное выражение, делимое
14.	方	фан (fang) – квадрат, место на счетной доске
15.	隅	юй (yu) – место на счетной доске
16.	廉	лянь (lian) – коэффициенты (о них ниже)
17.	负	фу (fu) – отрицательное число
18.	真	чжэн (zhen) – положительное число
19.	商	шан (shang) – место на счетной доске, также частное;
20.	分	фэнь (fen) – дробь
21.	元	юань (yuan) – неизвестная (включать этот термин в алгебраический словарь можно, но совершенно не обязательно; об этом ниже)

Словарь второй ступени – это производный словарь словаря первой ступени, в котором представлены термины, выражающие действия, определенные многократным повторением одной и той же операции, или слова, выражаемые комбинациями одного-двух слов минимального словаря.

1.	乘	чэн (cheng) – умножить
2.	行	синь (хан) (xin (hang)) – строка (столбец)
3.	减	цзянь (jian) – вычитать
4.	() 廉	(liang) лян – вспомогательные коэффициенты
5.	奇	цзи (ji) – остаток дроби, нечетное числа
6.		чуй (chui) – ступени
7.	实如法而•	ши жу фа эр – объедини делимое и делитель в одно число[3]
8.	重差	чжун ча (zhong cha) – двухслойная разность
9.	正负术	чжен фу шу (zheng fu shu) – определение положительных и отрицательных чисел
10.		гуй (gui) – метод деления

[3] Могут быть и другие версии точного перевода этого словосочетания, мы принимаем редакцию, предложеную Э.И. Березкиной.

Словарь третьей ступени состоит из правил, перечисленных в трактатах, например, цзянь фэнь (减分), чжун фэнь (重分), *пин фэнь* (平分), жу фан чэн (如方程), кай фан (开方), кай ли фан (开力方) и др.

Сделаем первое замечание.

Приведенный словарь третьей ступени обязательно дополняется названиями всех известных правил и методов китайской математики.

Принципиальное замечание: словари второй и третьей ступеней являются расширениями терминологического состава базы знаний средневековой и древней китайской математики.

Справедливость этого утверждения становится понятной, если учесть принцип организации словарей, следующих за минимальным словарем. Этот принцип состоит в последовательном повторении одного или нескольких правил или их суперпозиции.

Пользуясь указанными выше текстами и некоторыми переводами, составляя методом минимальных словарей сначала атомарный словарь каждого текста, затем его же минимальный словарь и проводя сравнение полученных таким образом словарей, мы получили подтверждение первого и второго наших утверждений.

К вышеизложенным замечаниям следует добавить, что кроме определения принципов составления минимального словаря следует упомянуть технологию составления словаря. Под технологией мы понимаем предварительный отбор иероглифического материала для последующего анализа. Критерием отбора служили частотность применения того или иного иероглифа, контекстность применения (арифметико-алгебраические тексты или части текстов), однозначность понимания (небольшая полисемия или ее отсутствие).

Отдельно целесообразно подчеркнуть, что мы исходили прежде всего из текста, и только создатель трактата и его мысли, зафиксированные в тексте, давали материал для исследования. Наша задача, как мы ее видели, найти адекватную модель или исторический прецедент явления, называемого китайской математикой. Возможно, «валидность» метода является предметом дискуссии. Однако методы отображения текстов с помощью алфавитов (иероглифов атомарного словаря) текстов, фиксирующих процесс создания уравнений по данным условиям задач, и вычисления их корней, строго определенная логика представления текстов с последующими комментариями являются традицией средневековой и древней китайской математики.

В связи с последним можно предложить утверждение: в нашем исследовании с помощью словарей и организации схем алгоритмов фиксируется чистое мышление вычислителя (средневекового и древнего мыслителя), отраженное в тексте.

1.3. Реализация алфавита

Алфавитом послужат иероглифы определенных выше групп минимального словаря, а именно: единицы (первая группа), знаки плюс и минус (вторая группа (отрицательные и положительные числа)) и четвертая буква q_{ij}^{s} (третья группа), т. е.

$\{ \quad 1, \oplus, (-), q_{ij}^{s}$, где q_{ij}^{s} – знак алфавита, определяющий место слова на счетной доске; его приписывают к слову справа или слева в зависимости от того, в какой части доски находится слово. Если слово находится в левой части, то оно является целым числом, а если справа, то дробным (см. рис. 2). Поэтому индексы определяют слово (дробное или целое число) и место данного слова на счетной доске:

$$s = \begin{cases} 1, & \text{если число дробное} \\ 0, & \text{если число целое} \end{cases}, \text{ а } \quad \begin{Bmatrix} 0 \le i < \infty \\ 0 \le j < \infty \end{Bmatrix}.$$

Например, если некоторое слово А=(| | | | | | | | |) записано как Аq_{12}^{1}, значит, слово А занимает место в дробной части доски и начинается (можно построить расположение слов на доске, используя глагол *находиться*, поскольку количество частей в каждой ячейке регулируется коэффициентом пропорциональности) с первой строки и второй колонки[4].

Далее, как обычно [16], определим знаки, использующиеся во вспомогательных построениях и не содержащиеся в данном алфавите. В нашем исследовании такими знаками были стрелка, стрелка с точкой, фигурные скобки, кавычки, скобки круглые.

За этими знаками идут следующие предписания и определения:

$\rightarrow$ – стрелка – «приписать (приставить) слева к палочке палочку»;

$\rightarrow.$ – стрелка с точкой – «приписать (приставить) слева к палочке палочку и закончить»;

{ – фигурная скобка – обозначение схемы алгоритма[5];

« » – кавычки – читать отмеченный ими знак;

( ) – круглые скобки – выделяют дополнительные условия существования алгоритма или текста.

---

[4] Однако заметим, что вообще говоря алфавит может быть и бесконечным. Этот вопрос обсуждался на с. 29 в работе А.И. Мальцева «Алгоритмы и рекурсивные функции». 2-е изд. М.: Наука, 1986.

[5] О понятии алгоритма см. работу А.А. Маркова [16 с. 8–9].

Запись вида $A \rightarrow B$, где A и B – слова одного алфавита, будет называться формулой. Иначе эту формулу называют простой формулой подстановки слова B вместо слова A.

Если $A \rightarrow \cdot B$, то это заключительная формула подстановки.

Под алгоритмом мы будем понимать точное предписание, которое задает вычислительный процесс (называемый в этом случае алгоритмическим), начинающийся с произвольного исходного данного (из некоторой совокупности возможных данных) и направленный на получение полностью определяемого этими исходными данными результата. Алгоритм должен удовлетворять нескольким условиям. Понятно, что список формул подстановок составляет существенную часть алгоритма.

Если есть некоторый алгоритм A, перерабатывающий при первом шаге применения слово P в слово Q из того же алфавита, то говорят, что A просто переводит слово P в Q, $(P \vdash Q)$, если же P переводится в слово Q по формуле заключительной подстановки, то говорят, что A заключительно переводит P в Q, $(P \vdash . Q)$.

Будем обозначать:

A: $(P \vdash Q)$ – (просто переводится P в Q);

A: $(P \vdash . Q)$ – (заключительно переводится P в Q).

Если алгоритм A не применим к слову P, то это обозначается A: $\neg$ P.

Если A: $P_1 \vdash P_2 \vdash P_3 \vdash P_4 \vdash P_5 \vdash ... \vdash P_n$,то эту цепочку переводов слова P_1 в P_n при условии ($P_1 = P$, $P_n = Q$) будем обозначать:

A: $P \models P_k$ – если применение алгоритма A обрывается на слове P_k;

A: $P \models . Q$ – если применение алгоритма A заключительно переводит слово P_1 в слово P_n ;

A: $P \models Q$ – если применение алгоритма A переводит слово P_1 в P_n.

Приведем простейший алгоритм приписывания слева одной палочки к другой A={$1 \rightarrow 1$ – это значит слева к единице (по аналогии, палочке на счетной доске), установленной на счетном инструменте (машина Тюринга, любое вычислительное поле), будет приписываться единица, и этот процесс по приписыванию единиц слева никогда не завершится, т .е. алгоритм неосуществим; если же алгоритм записать A = {$1 \rightarrow \cdot 1$, то алгоритм после первого шага осуществится, и результат будет иметь вид 11, так как это заключительная формула.

Ниже запишем алгоритмы, необходимые в моделировании процессов решения задач средневековой китайской математики (способов решений):

1) алгоритм, перерабатывающий слово P само в себя { $\rightarrow$.; A: P $\vdash$. P;
2) алгоритм A_1 приписывания слова P слева { $\rightarrow$. P; A_1 : W $\vdash$ PW . A(P)=AP;
3) частный случай алгоритма A_1 : { $\rightarrow$. 1; A_1 : P $\vdash$ 1P;
4) пустой алгоритм $\varnothing$, или A_2 : { $\rightarrow$ A.

Пусть требуется приписать (+) из алфавита *A* к единице. Эта задача решается алгоритмом A_1 (№2) { $\rightarrow$. (+); A_1 : 1 $\vdash$ (+)1, т. е. результатом будет (+)1.

Пусть необходимо убрать какой-то знак (букву) *a* из слова P. Этот алгоритм представляется схемой { *a* $\rightarrow$., так как присваивает знаку *a* пустое место на счетной доске, иначе из слова P этот алгоритм «выбрасывает» знак *a* . Понятно, что алгоритм, заданный схемой {(+) $\rightarrow$, аннулирует все знаки (+) в слове P. Присвоим этому алгоритму имя A_3.

Примеры. 1. B: {1 $\rightarrow$., этот алгоритм убирает из вычисления первую встретившуюся в слове единицу.

2. Пусть дано сложное слово P(+)Q, тогда алгоритм A_3 переработает это слово в слово вида PQ. Если слова P и Q состояли из единиц, как это сделано в нашей модели, то понятно, что PQ – слово, состоящее из двух наборов единиц или просто сумма, если полученное множество пересчитать (мощность множества).

Понятно, чтобы выполнить предписание, определенное иероглифом цзя (бин), достаточно применить алгоритм A_3, т. е. цзя (бин) 加(并): {(+)$\rightarrow$., тогда получим P1 (+) P2 $\vdash$ P1P2 – слово, состоящее из объединения единиц двух слов.

Чтобы записать иероглиф фу （负）, применяется упрощенная схема алгоритма {(-) $\rightarrow$., P $\vdash$ (-) P. Появление иероглифа фу одновременно определяет, что там, где нет этого иероглифа, число положительное и поэтому можно считать, что установлен иероглиф чжен 真) или по умолчанию число считается положительным.

Из теории алгоритмов известно следующее утверждение.

Если B: P $\vdash$ bP, где b – буква из расширения алфавита *A*, т. е. $A \cup \{b\}$.

Также справедливо, что:

1. B: P $\vdash$ Pb
2. B: bP $\vdash$ Pb (доказательство см. в [16 с.61]).

На основании этих утверждений далее можно интерпретировать весь минимальный словарь.

3. Чжи (值) (установи число) – схема алгоритма { $\rightarrow . \, q_{ij}^{s}$: P $\vdash$ q_{ij}^{s} P.

Этот алгоритм определяет место меткой на доске в виде q_{ij}^{s}, где нижние индексы по координатному принципу устанавливают соответствие между единицей (числом, в зависимости принципа построения числа) и клеткой счетной доски (вычислительного поля), а верхний индекс – это указатель правой или левой ее сторон: если s = 0, то левая («целая») часть счетной доски, если s=1, то правая («дробная») часть. Число q00 – пограничное число или начало системы координат счетной доски, прямая с координатами (q00,j) – делит счетную доску на две части – «целую» и «дробную» (рис. 2).

4. Алгоритм: установи позицию на счетной доске или место на счетной доске, что соответствует иероглифу вэй （位） : : P q_{ij}^{s} $\vdash$ q_{ij}^{s} P $\vdash$ q_{ij}^{s} $|P|$, где $|P|$ – длина слова в нашем алфавите, напомним – число единиц. Можно в общем случае определять длину слова P, в частности в нашем алфавите этот алгоритм очевидно упрощается.

5. Иероглиф ши (实). Этот иероглиф обладает свойством парности, т. е. рядом с ним необходимо располагать на счетной доске иероглиф юй (隅). Они вместе являются главными признаками наличия уравнения в решении задачи или, возможно, подбора значений множителей, удовлетворяющих равенству двух установленных на счетной доске чисел. Последнее можно трактовать как поиск числа (隅), произведение которого на коэффициент или возведение которого в соответствующую степень равно ши. Таким образом,

ши (实): (фиксированное место): { $\rightarrow . \, q_{ij}^{s}$ – (именное место);

юй (隅): { $\rightarrow .$ – (именное место – отличное от ши).

6. (туй): { $q_{ij}^{s} \rightarrow . \; q_{ij-1}^{s}$: 1 q_{ij}^{s} $\vdash .$ 1 q_{ij-1}^{s} .

7. (чао): { q $\rightarrow . \, q_{ij+1}^{s}$: 1 q_{ij}^{s} $\vdash .$ 1 q_{ij+1}^{s} .

8. чуй ( ): { $\rightarrow . \, q_{ij}^{s}$: P $\vdash .$ P q_{ij}^{s}; Q $\vdash .$ Q q_{ij}^{s};

{ $q_{ij}^{s} \rightarrow .$ (-) q_{ij}^{s} : P $q_{\boldsymbol{j}}^{s}$ $\vdash .$ -P q_{ij}^{s} ;

{ «jia»: Q q_{ij}^{s}(-P q_{ij}^{s}) $\rightarrow .$ Q q_{ij}^{s}; $Qq_{ij}^{s} \underset{-Pq_{ij}^{s}-k}{\mapsto .} \quad \underset{раз}{\ldots} \quad \mapsto . \, Qq_{ij}^{s}$.

9. шан (shang)(上) : { $q_{ij}^{s} \rightarrow . \; q_{i+1j}^{s}$: P q_{ij}^{s} $\vdash$ P q_{i+1j}^{s} .

10. ся (xia) （下）: { $q_{ij}^{s} \to . \ q_{i-1j}^{s}$: P $q_{ij}^{s} \vdash$ P q_{i-1j}^{s}.

11. чжун (zhong) （中） : { $q_{ij}^{s} \to . \ q_{ij}^{s}$: P $q_{ij}^{s} \vdash$ P q_{ij}^{s}.

Следует заметить: 1) позиция иероглифа чжун определяется по позициям иероглифов ся и шан; 2) сравнение чисел на доске легко осуществляется по месту, например, при сравнении длины слова (алгоритм 9 из [16]). Последним замечанием мы воспользуемся для определения алгоритма, соответствующего иероглифу цзинь (进).

12. Доводить до (进).

Иероглиф цзинь может быть определен алгоритмом сравнения; смысл действия, предписанного им, следующий:

а) исчерпание объекта (числа), обычно до пустого места на доске в данной строке (столбце);

б) сравнение числителя со знаменателем с учетом арифметических действий (в приведении дробей к общему знаменателю);

в) сопоставление результата вычисления с ранее определенным числом (возможно определенного дополнительными условиями).

Схема алгоритма, определенного этим иероглифом, выглядит так: { $\to . \ q_{ij}^{s}$: P $\vdash$ P q_{ij}^{s}; Q $\vdash$ Q q_{ij}^{s}

{ P $q_{ij}^{s} \to .$ Q q_{ij}^{s} : $\mathrm{P}_1 q_{ij}^{s} \vdash \mathrm{P}_2 q_{ij}^{s} \vdash \ldots \vdash$ Q q_{ij}^{s} или $\mathrm{P}_1 q_{ij}^{s} \models$ Q q_{ij}^{s}.

Определим алгоритмически дробь. Признаком дробности числа является верхний индекс s числа q_{ij}^{s}. Фэнь (分): { $\to . \ q_{ij}^{s}$. Это значит, что число размещено в правой части счетной (доски) поля. Такому размещению сопутствует следующая информация: поле в этой части уже «обработано», т. е. задана шкала мер. Можно, например, задать шкалу мер веса, длин, объема и т. д.

Ясно, что эта шкала продолжаема вправо, так же как и условием соглашения является то, что в любой колонке, независимо от части вычислительной плоскости, вычислителем произвольно устанавливается число позиций (система счисления). Это значит, что можно провести аналогию с арифметиками, имеющими различные основания счислений. В истории китайской математики важную роль играли фиксированные дроби, такие как 1/2, 1/3, 2/3 произвольных чисел. Их достаточно просто задать алгоритмически, используя соответствующие алгоритмы минимального словаря.

Наличие обширной математической литературы, выявление признаков, определяющих ее характер естественным образом, ставят вопрос о способах развития математического знания [7].

Можно сделать следующие важные выводы:

1) о терминологическом единстве рассматриваемой математической литературы, насчитывающей более полутора тысяч лет;

2) о способах развития базы математических знаний средневековой китайской математики;

3) о существовании в традиционной китайской математике последпвательности, типичной для европейского знания, а именно – «опыт, обобщение, отвлечение, опыт отвлечения, обобщение – знак (символ)», которая была реализована китайской знаковой системой.

2. Конструктивные модели мыслительной деятельности обучающегося по китайским трактатам

Тезис Пиаже о том, что знания об объекте не даны помимо познавательной деятельности субъекта, но конструируются в ходе его мыслительной деятельности, подвергнут критике со стороны априористов [17]. На самом же деле, следуя операционной установке в мышлении, к другому тезису, отличному от тезиса Пиаже, и невозможно прийти. При разборе операционного арсенала средневекового китайского математика вполне точно устанавливается разложение словарей на группы согласно предназначению их мыслительных процедур. Обратимость мыслительных операций по Пиаже весьма точно описывает комплекс операций, называемых в оригинальных текстах способами решения, правилами. Одной из гипотез создания столь лаконичных правил, а также составления сложных алгоритмов является предположение А.П. Юшкевича о решении задач «с конца» – это обратимость операций, обратимость результатов, изменение мест исходных данных (посылки и требуемого в задаче) и другие приемы, переходящие в приемы обучения математике (предмету).

Понятно, что познавательная деятельность (см. выше) субъекта обусловлена объектом познания, посредством процесса мышления объект определяет знание, к которому он приводит. Через посредство закономерностей процессов мышления, «конструирующих» научные понятия, и реализуется определяющая роль бытия, объекта познания.

Приведем некоторые пояснения к операционным действиям вычислителя.

1. Приставляя палочку к палочке, китайский вычислитель получал набор палочек: объединение же палочек (сначала из соображений удобства во время работы на счетном приборе) задаст конечное множество с соответствующим числом элементов; пере-

дача информации о наборе от вычислителя к вычислителю – первый сформулированный элемент базы знаний (с учетом свойства корпоративности). Иначе, возникала необходимость в обобщении конечного числа элементов, которая выражалась в присвоении знака, например Х, некоторому набору из четырех палочек или знаков ($\perp$) для шести единиц (десятков). Понятно, что замена количества палочек его представителем является первым шагом в процессе фиксации результата вычисления либо на бумаге (материале), либо в слое пыли, воска и т. п. В то же время эта замена является актом отвлечения от количества к его образу, требующего на этом шаге от «ученого сообщества» свойства корпоративности (передача и согласование информации в среде) [18–25].

2. Появление (в схеме развития китайской математики) алгоритма Евклида – алгоритма, обобщающего сочетание действий вычитания, умножения и сравнения чисел, перед дробями и уравнениями второй степени обосновывается прежде всего тем, что для работы с дробными числами и «решением» уравнений требуется высокая арифметико-алгоритмическая культура вычислений с целыми числами.

3. Дроби как естественное продолжение позиционности в «дробной» части счетной плоскости отличаются от целых чисел лишь характерным признаком – коэффициентом пропорциональности системы мер этой части плоскости (см. рис. 2).

Развитие алгоритмической культуры способствовало объединению обеих частей вычислительной плоскости. Это с очевидностью подтверждается базой знаний в «Математике в девяти книгах», а традиция, которую отмечали в [2, 13, 26–31], «действовать с дробными числами как с целыми», только подтверждает справедливость этого предположения. Предложенная схема ясно представляет историю появления отвлеченной дроби – от обычного сопоставления частей единичных мер (веществ, предметов) до результата объединения процессов деления чисел и применения дробных единиц в практической деятельности [2, 7, 30].

4. Сочетания слов из минимального словаря дополняют математический лексикон новыми словами, конструируют (конституируют) новые понятия. Степень сложности понятия определена вхождением в него количества слов основного и расширенных словарей. В то же время наблюдается явление компрессии как словосочетаний, так и оформленных в алгоритмы (сочетания слов со строго определенной последовательностью действий из основного и расширенных словарей) решений задач. Это значит, что созданы условия для иерархии словарей, вместе с ними алгоритмов, а следовательно, для дальнейшей возможности оценки логики их развития. Иными словами, выработаны мысли-

тельные процедуры, отличающиеся от операций простого вычисления на счетном поле.

Правила, позволяющие совершать указанные переходы, сами составляют подмножество элементов базы знаний, требующее обобщения результатов (конструкций), отражаемых в словарях более низкой ступени. При этом совершенная детерминированность возникающей системы является плодом не столько свойства традиционности в психологии мышления китайского ученого, сколько поддержки государством системы образования. То, что система китайского образования самая древняя из всех ныне существующих – это известный факт. Государственный контроль за образованием чиновников через систему государственных (императорских) экзаменов сложился в течение многих сотен лет и составлял необходимую часть государственной системы [32–39]. Из вышеизложенного можно предположить, что система передачи информации (рукописи, трактаты, устно, «школьно») была отлажена, и более того, существовал своеобразный институт «конференций», о чем свидетельствует относительное терминологическое однообразие текстов.

По возникшему минимальному словарю в п. 2.1 построены конструктивные модели (схемы) мыслительной деятельности обучающегося по китайским трактатам. В этом разделе делается попытка с помощью разработанной системы показать истинность гипотезы А.П. Юшкевича о непосредственной передаче информации и доказательств в процессе обучения специалистов – математиков и астрономов [28 с. 152].

2.1. Мыслительные процедуры в операционной деятельности китайского вычислителя

Перед нами стоит цель – уяснить, какие приемы мыслительной деятельности были в арсенале древнего вычислителя и какими из них он мог воспользоваться (пользовался, судя по ИПС) в обучении. Примеры из различных источников представляют существующие подходы к методам обучения.

Рассмотрим операцию как первоэлемент в решении задачи.

Прежде всего заметим, что применение тех или иных операций к тому или иному частному случаю предполагает процесс мышления (анализ, синтез, обобщение). Не операции порождают мышление, а процесс мышления порождает операции, которые затем в него включаются. «Каким бы аппаратом человек ни располагал, вопрос о применении тех или иных операций в каждом частном случае, к определенной задаче, не разрешается посредством этих же операций» [40 с. 51].

В историко-математической части исследования учтено, что исследование операционной деятельности вычислителя не тождественно полученному им результату. Вычисленный результат по примененному алгоритму прежде всего – цепочка силлогизмов, в ее начале находится проблема выбора/подбора необходимого алгоритма с последующим построением плана достижения поставленной задачи. Поэтому наблюдается некоторое огрубление, несоответствие получаемой модели настоящему мышлению. Мы также учитывали справедливость утверждения, что в психологическом исследовании, «всякая попытка признать операции чем-то первичным и свести процесс мышления к механическому функционированию так понимаемых операций принципиально неверна и неосуществима» [40 с. 50]. Заметим, что наше исследование относится к методико-педагогической сфере, психология играет значительную роль, но не главную, поскольку методические «следы», оставленные в математической литературе, только психолингвистическими методами исследованы быть не могут. Однако в тех же исследованиях психологов можно заметить и такие высказывания: «при предельной абстракции от особенностей предметного содержания операции выступают в их логической структуре. Мышление, совершающееся путем применения таких правил или соответствующих формул (логических, математических и т. д.), выступает непосредственно как функционирование определенных операций. Операцией в этом смысле является звено, т. е. звенья процесса мышления, совершающиеся по определенной формуле, возникают в ходе исторического развития сначала как результат мышления, открывающего соответствующее правило, и уже затем включаются в него» 40 с. 49].

Таким образом видно, что психологи разделяют мышление в способе отражения объекта (задачи) в познавательном процессе на «формулу» и «операцию». Другими словами, фиксируются различия в методике поиска формулы (алгоритма) и создании самой формулы (алгоритма) или получении результата в абстрактной сфере. В исследованиях по методике решения задач это обстоятельство выражается терминами «прием и операция» [41]. Под приемом, вслед за [41–44], будем понимать обобщенное знание о действиях или системе действий, необходимых при отыскании решения специфических для данной деятельности задач, причем это знание объективировано каким-либо образом, например, в виде словесного описания. Из этого определения следует, что алгоритм или формула, описанные любым способом, являются приемами в решении задач. В них приняты следующие определения.

Структурными элементами приема являются: предмет, цель и операционный состав приема.

Предмет приема – совокупность объектов, к которой можно применить данный прием.

Цель приема – это результат, на достижение которого направлен прием. В средневековой и особенно в древней китайской математике цель приема обозначена его названием.

Операционный состав приема – последовательность операций, предназначенных для достижения цели приема и входящих в его содержание, иначе совокупность операций, образующая законченный прием [42].

Способ выражения приемов, операций вообще зависит от языковой поддержки – от функционирующей знаковой системы. Математический же язык – это универсальная знаковая система, в которой слова (термины, понятия) упорядочены по степени абстракций. Однако формы выражения этого языка также различны.

Таким образом, операции мышления, составляющие приемы, и приемы решения задач нетождественны. В китайской математике, исследуя математическое мышление, разделим операции на две группы. Первая группа – операции анализа, синтеза, обобщения, сравнения, группировки, полагания; вторая – арифметические операции: сложения умножения, вычитания деления. Далее покажем, что операции второй группы являются сложными операциями по отношению к операциям первой группы. Психологи утверждают, что некоторые операции из первой группы также связаны между собой, например: сравнение выражается через анализ, синтез и сопоставление: мыслительная операция сравнения – прежде синтез (синтетический акт), а затем соотнесение и сопоставление явлений. Далее выделение в них общего и различного – выступающее в них общее в результате объединяет их, т. е. синтезирует. Сравнение – это та конкретная форма взаимодействия анализа и синтеза, посредством которого осуществляются эмпирическое обобщение и классификация явлений [40 с. 36, 55].

Проблема же обучения языку математики в современной школе исследовалась А.А. Столяром [43, 44], С.И. Шапиро [45], М.Ю. Колягиным [41, 46]. Эти исследования кроме самой постановки проблемы о значении математического языка и математической задачи в обучении потребовали решения и таких задач, как классификации приемов, оценка рациональности выбранной операции (выбранном методе), поиск решения и др.

Здесь интересны в историко-математическом аспекте зарождение постановки задачи и ее понимание в процессе обучения. Судя по материалам китайской математики процедура (операция) полагания (на счетном приборе – материализованная операция присваивания), наблюдаемая в различных видах вычислительной практики, развивалась от выделения места для числа в процессе операции деления до обозначения коэффициента в конструируемом уравнении. Можно предположить, что она одна из самых древних мыслительных операций[6] и является продолжением (расширением) операции «распространения». В европейской философии она явно оформилась в XVIII веке [10 с. 502].

Из этого следует распространение (расширение) приема (в терминах теории решения математических задач) на различные виды мыслительной деятельности. Постижение сущности явления – действие, состоящее из многих актов и соответствующее исключительно роду человеческому. Одним из таких актов является вычисление. Возможно, операция полагания является результатом (финальной частью) процесса сопоставления реальных объектов (по заранее выделенным свойствам). Во всяком случае, можно предположить, что ее истоки коренятся в процессе, где последовательно осуществляется переход от стадии сравнения объекта по внешним признакам до процедуры выделения сущности мыслимого.

Вычисления – порождение жизнедеятельности человека. В них отражаются пути развития цивилизаций. Основные древние цивилизации (Месопотамия, Древний Египет, Древняя Индия, Древний Китай) создали вполне обозримое множество вычислительных методов. Поскольку «основные мировые цивилизации образовались в руслах великих рек», то неудивительно, что в них ставились и решались одинаково сформулированные задачи [47]. «Технические средства» развивались согласно выдвигаемым жизнью требованиям, а в силу ограниченности «подручных» средств конструкционно похожи на вычислительные приборы, используемые в этих государствах [40].

Напомним: каждый акт мысли меняет соотношение субъект – объект, быть может, совершается некоторое физическое действие, например, изменяется положение счетных палочек на доске согласно предписанию, алгоритму или оформлению полученных результатов вычислений (снятие «кальки» с вычислительного поля). «Процесс – при осознании его цели – непрерывно переходит в деятельность мышления» [40 с. 28]. Но сам процесс мышления разрывается через соотношения тех продуктов, которые он дает на различных своих этапах. Таким образом, развитие технических средств – это развитие не только алгоритмического мышления,

---

[6] Отметим, отличия мыслительных процедур от действий на счетных инструментах сводятся к минимуму. Конечно же, понятие минимума условно, но в математических процедурах довольно сложно четко провести грань между действием физическим и умственным, тем более на заре зарождения математики.

но и прежде всего абстрактного, как видно на примере образования символики в китайской математике, т. е. «вершины» операции отвлечения.

Восхождение от абстрактного к конкретному – процесс синтетический. Суть его в соотнесении разнообразия абстрактных понятий и восстановлении конкретного. Подобная деятельность в общем случае является не чем иным, как представлением образа.

2.2. Логические операции в процессе вычислений

Логическая составляющая операционного мышления у китайского ученого (ученика) – результат социализации вычислительной деятельности. В пользу этого утверждения говорят исследования [7, 48]. Во втором из них показана целостная система методов мыслительной деятельности (рассуждений). Тань Цзефу говорил: «Учение о “методе” – это свод правил получения истинных знаний и способов применения последних в деятельности». В разделе «Семь методов» читаем:

«Вероятность» (хо). «Рассуждение потому называется вероятным, что оно не полностью охватывает истину» [48 с. 190].

«Предположение» (цзя) – форма рассуждения, аналогичная гипотезе. «Как предположение приводятся доводы, которые пока не обоснованы» [48 с. 191].

«Подражание образцу» (сяо). В этом случае рассуждение идет по образцу другого правильного рассуждения. «Подражание сводится к тому, что за образец берутся такие суждения, которые были правильными в похожей обстановке. Что соответствует образцу, то истинно, что не соответствует образцу – ложь» [48 с. 191].

«Сопоставление» (би) [возможно – сравнение]. «Сопоставление заключается в том, что данная вещь объясняется путем описания другой вещи». Таким образом, оно сводится к установлению аналогии между предметами рассуждения [48 с. 191].

«Сравнение» (моу). «Сравнение уподобляет два суждения и вместе их применяет» [48 с. 191].

«Ссылка на мнение оппонента» (юань) – указан прецедент. «Если ты можешь утверждать это, то почему я не могу сделать того же?» [48 с. 191].

«Распространение» (туй) – «заключается в том, чтобы путем совмещения положений, которые другой человек отвергает, с теми же положениями, которые он признает, согласие [спорящих сторон] распространялось на все положения» [48 с. 191].

Объекты рассуждений вступают в отношения друг с другом. Вот учение о видах отношений:

«“прямые отношения”: а) отношения равновесия; б) обратные; в) прямые; “отношение долженствования” (отсутствие свободы выбора); “отношение необходимости”. Если нет этого, то обязательно не будет и другого – это необходимость».

В целом же рассуждения должны удовлетворять принципу «сань у»: суждения должны иметь «причину», «основание» – *гу*. Необходимо придерживаться правил построения умозаключений – *ли*. И чтобы из суждений сделать вывод, нужно, чтобы эти суждения имели *родовое сходство – лэй* [48].

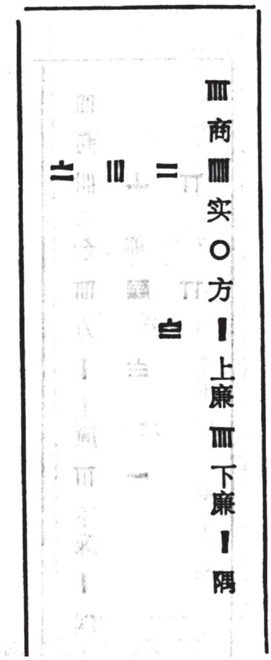
Необходимо напомнить, что основным объектом для критики Мо Ди и его последователей было учение Конфуция – первого учителя Китая. Современный китайский ученый Цзо Дахай, исследуя сохранившиеся фрагменты трактатов Мо Ди, обратил внимание на наличие в рассуждениях учителя инфинитезимальных идей [48].

Все вышеприведенное – система правил рассуждений, их классификация, оппонирование великому Учителю, переход к абстрактным по содержанию понятиям «малых изменений» – является вехами в совершенствовании мыслительной деятельности ученых Древнего Китая, в которой огромное место занимала, возможно, даже более чем в античных школах, дидактика. Она же (система правил) свидетельствует о том, что дидактика формировалась из таких логических приемов, как классификация понятий, определение понятий через род и сравнение видовых признаков, прием установления различных соотношений (больше, меньше или равно), прием обращения рассуждения, определения правдоподобного рассуждения, оценки полученного результата по соотнесению с таблицами (действия по образцу) и т. д. Поэтому в традиционной китайской математике логическая составляющая в процессе решения конкретной задачи формирует план решения, а затем вступает в силу отображение плана и цели на «вычислительную плоскость». Индуцирование логических приемов на вычислительную плоскость объясняет традицию решения задач от ответа, проверки промежуточных решений, комментирования полученных в процессе решения результатов и осторожного отношения к последним.

Весьма характерным примером развития «алгебраичности» в математике может служить средневековая китайская математика.

В самом деле, в силу ее алгоритмического характера, заметим, отнюдь не догматического, в ней были разработаны правила, которые условно можно назвать правилами «ценности вычислительных мест». Пусть решается некоторая задача, разрешимая биквадратным или иным алгебраическим уравнением. По типу задачи и рекомендуемому методу (способу решения) дана информация вычислителю об алгоритме, по которому необходимо будет составить (получить) коэффициенты соответствующего уравнения, а затем, следуя алгоритму, получить число (корень). Биквадратное уравнение на счетной доске показано в табл. 1.

Таблица 1

	9 – первая цифра корня шан 7324 – свободный член ши 0 фан – первый коэфф. при неизвестной 81 шан лянь – коэфф. при второй степени неизвестной 9 – ся лянь 1 юй – старший коэфф. при неизвестной

В табл. 2 показан принцип «записи» на счетном инструменте уравнений до десятой степени.

Таблица 2

Шан – искомый корень	Шан – искомый корень	Шан – корень уравнения
Ши a_2	Ши a_4	Ши a_{10}
Фан $a_1(x)$	Фан $a_3(x)$	Фан $a_9(x)$
Юй $a_0(x^2)$	Шан $a_2(x^2)$ лянь	Шан $a_8(x^2)$ лянь

	Ся $a_1(x^3)$ Лянь	Ци $a_7(x^3)$ Лянь
	Юй $a_0(x^4)$	⋮
		Ся $a_1(x^9)$ лянь
		Юй $a_0(x^{10})$

Логическая структура операции составления уравнений позволяют принципиально продолжить получение и других степеней. Как показано в задачах Цинь Цзюшао, уравнения высших степеней имеют дидактическую цель – обучить учащегося решать уравнения высших степеней [49].

Отметим, что уместен вопрос: «Но все же – как составлялось уравнение?».

Если допустить, что решение задачи находилось только методом обращения задач (или оформления вычислительных процедур «назад»), т. е. от ответа, то эта возможность была бы осуществима на не очень сложных вычислительных задачах, где использовались такие методы, как правило ложного положения, арифметические и геометрические прогрессии с небольшими номерами их членов, сложные пропорции и некоторые другие элементарные методы. Но способ обращения задач, решаемых методом «да янь», где используется прием, называемый сравнением по простому модулю, осуществим со значительно бóльшими трудностями. Однако как же составить уравнение, например десятой степени, «с хвоста», да так, чтобы можно было «выбирать» точность получаемого результата? Можно предположить, что хорошо разработанная библиотека алгоритмов помогала в решении стандартных задач, но для задач иного рода вычислитель (ученый) пользовался элементарной теорией в рамках логики привычных для него мыслительных операций, иначе математики, которая существовала в тот период.

Здесь мы еще раз хотим подчеркнуть, что речь идет не о подборе удовлетворительного в той или ной степени алгоритмического языка, который в той же степени описывает предмет исследования – китайскую средневековую математическую литературу, а об адекватном представлении мыслительных процедур древнего ученого, отраженных в терминологическом составе языка или в тезаурусе математических знаний. Основой создания такой модели являются оригинальные тексты, а не чувства и фантазии интерпретатора. Выбор же методов и идей конструктивной математики был предопределен историческим прецедентом в математике –

появлением труда А.А. Маркова «Теория алгорифмов» [16, 50, 51]. При этом мы хотим еще раз заметить, что алгоритмическая сущность обучения и проявление ее в индуктивной математике древнего Китая вовсе не обозначают уровень ее развития. Но, возможно, мыслительные стили, перенесенные в одинаковые среды, могут проявлять себя подобно и естественно с разными результатами [52]. Приняв за основу естественные группировки понятий, можно представить мыслительные схемы.

2.3. Об одном способе развития индуктивного знания в истории науки

Вычисление – один из самых ранних интеллектуальных приемов получения результатов в деятельности человека. В процессах вычисления сочетались как установки вычислителя на оценку результата, так и в осуществление прогноза деятельности.

Упоминания о древних цивилизациях вызывают различные ассоциации. Возможно, среди ассоциаций найдется место вавилонским и (или) египетским жрецам – авторам клинописных табличек и папирусов. В творениях последних, как известно, кроме астрономических таблиц, требующих весьма развитых систем счисления (вычисления с многозначными числами как в шестидесятеричной, так и десятичной системах счисления), сохранились задачи и вычисления на экономическую или хозяйственную тематику [53–57]. Выполнение таких расчетов предполагает наличие у древних счетного инструмента [55–58]. Примером такого инструмента является Саламинская доска – археологическое свидетельство счетного искусства у древних греков [18, 56].

Конечно, следуя логике реконструкций передачи информации от древних египтян к древним грекам, можно предположить заимствование греками приемов счетного искусства, впрочем, это возможно относится только к греческим купцам[7]. Подобное движение информации в реконструкциях от ассирийцев и шумеров к древним египтянам вполне допустимо, но оно все же входит в область предположений.

На основании анализа трактатов – памятников научной мысли, сохраненных китайской культурой, мы хотим предложить здесь интерпретацию способа развития индуктивного знания. Она заключается в том, что *развитие счетного инструмента в Китае с древнейшего времени до середины XIV в. н. э. предопределило стиль математического мышления китайских ученых*.

---

[7] Эта версия скорее всего не выдерживает критики.

Предполагая, что за последние две-три тысячи лет механизмы психики у человека не изменились, в терминах деятельного обучения (исследования мышления) попытаемся коротко изложить взгляд на историю развития китайской математики. Прежде всего будем считать, что математика в основе своей – особая форма мышления, при этом развиваемая. Напомним, что «мыслительная деятельность не только не отделена непреодолимой стеной от деятельности практической, напротив, постоянно совершаются переходы внутренних звеньев во внешние, и наоборот» [59 с. 23]. Процесс превращения внешних практических действий во внутренние принято называть интериоризацией, а обратный процесс – экстериоризацией. Понятие же превращенной формы при исследованиях мышления напрямую выводит нас в лингвистике на изучение текстов [60].

Таким образом, исследование текстов как памятников человеческой деятельности нужно понимать не только как историческую обработку материала (китайских трактатов), но и как превращенную форму [60].

Тезис 1. «Операционный состав действий определяется прежде всего (но не исключительно) условиями его выполнения» [61].

Считая доказанным наличие счетного инструмента у китайских ученых (суань-пан) к 1200 году нашей эры и исследуя операционный состав, а в текстах иероглифический состав предписаний (способов [решений]) и расчетов, можно утверждать, что указанный состав «Девяти книг по математике» (1247 г. н. э.) идентичен составу «Математики в девяти книгах» (примерно III в. до н. э.). А значит, наличие счетного инструмента, подобного суань-пану, в ранние века не должно вызывать сомнения. Однако его конструкция требует обсуждения. О ней можно судить не только по терминологическому составу текстов, но и по кальке с вычислений, например, из трактата Цинь Цзюшао «Девять книг по математике», озаглавленной автором трактата «расчеты». Все новые (в смысле применения методов решений) и громоздкие задачи снабжаются текстами, называемыми «расчетами»,

Сравнение терминологических составов источников не должно ограничиваться двумя или несколькими источниками, оно должно быть проведено со всем объемом китайских источников. Однако такая задача требует разработки метода. Некоторые результаты и методы сравнений изложены в [49]. Сочетание предложенного тезиса и исторического факта наличия терминологической базы математики показывает, что счетный инструмент занимал центральное место в развитии математики Китая до начала XIV века.

Тезис 2. Экономическое развитие древнего китайского общества способствовало использованию счетного инструмента. Подтверждение этого тезиса легко обнаруживаем в социальной составляющей задач древних и средневековых трактатов. В качестве определения задач примем, что цель, заданная *в определенных условиях*, называется задачей. При вычислении на счетном инструменте необходимо выполнить ряд действий: разместить (расположить) числа на счетной доске, перенести счетную палочку влево или вправо, довести число до исчерпания, сохранить число в специально отведенном месте (очень часто таких вспомогательных чисел в выполнении алгоритма не одно и не два), добавить или убрать палочки со счетного поля, следить за точностью перехода соответствий обозначениям чисел в разрядной сетке счетного инструмента и т. д.

Как утверждают психологи, действия становятся операциями тогда, когда они автоматизируются и перестают контролироваться сознанием. Поэтому громоздкость вычислений, выбор больших чисел и не всегда оптимальных методов решений, встречающихся в древних трактатах (с точки зрения современного математика), имеют вполне понятное обоснование, если рассматривать эти трактаты как учебные пособия по вычислительному искусству. Очевидно, что при реальном использовании инструмента необходимо операционное владение им. Сформированные технические навыки стали первыми знаниями, основанными на операционных умениях вычислителей, в индуктивном накоплении знания. Словесным оформлением такого знания явились предписания, на которых строились (создавались) способы решения конкретных задач. Именно последнее высказывание есть переформулировка темы, вынесенной в заглавие раздела. Здесь же, следует отметить, характер накопления информации был индуктивным, что соответствовало стилю мыслительных процедур, необходимых при работе на счетном инструменте.

Тезис 3. Кроме внешнего – экономического или общесоциального – фактора развития вычислительного инструмента существует и внутренний фактор. Иначе этот фактор можно назвать психологическим (человеческим) фактором [52]. Гальперин определяет его как управление формированием умственных действий, понятий и образов. Таким образом, внутренняя психическая деятельность имеет такой же орудийный, инструментальный характер, как и деятельность внешняя. В качестве этих орудий выступает система знаков (прежде всего язык), которая не изобретается индивидуумом, а усваивается им.

Следствием такого развития в индуктивно формирующемся знании при стабильной государственной структуре, контролирующей социальный запрос к этому виду деятельности, в которой институт образования играл важную роль, стала комментаторская деятельность выдающихся умов Китая.

Дополнить вывод можно и тем соображением, что постоянным средством проверки полученных результатов был инструмент, простой по форме, но по идейной насыщенности, возможно, неисчерпаемый. Созданная вычислителями и учеными Древнего и средневекового Китая знаковая система математики ориентирована на счетный инструмент. Она также является прямым подтверждением существовавшей средневековой китайской математической школы. Результатом ее развития можно объяснить расцвет алгебраическо-алгоритмической китайской школы XIV в. нашей эры.

Тезис 4. Интериоризация операционных и предметных знаний на основе знаковых систем (в первую очередь языковых) приводит к зарождению понятий (словесных значений). В случае индуктивного знания этот тезис приводит нас к прообразу выкристаллизовывающегося знания. В китайской математике таким прообразом является суань-пан. Действительно, вычислитель с необходимостью должен возвращаться в своей деятельности к рефлексии операций на счетной доске, формулировать полученные результаты, придавать им лаконичные формулировки, а таковыми являются тексты (комментарии) и способы решения задач. Поэтому понятия в китайской математике имеют формы алгоритмов (способов и правил). Можно считать, что поименованность мест на счетной доске – прием кодификации общеизвестного вычислителям знания о счетном инструменте. Таким образом, процесс экстериоризации знания «возвращает» его в виде кодов, точнее, сформированных знаков счетного инструмента, которые на нем же и аккумулировались.

Таким образом, из предложенных соображений можно сделать следующие выводы:

- китайская средневековая математика замкнута на счетный инструмент, операционный состав мыслительных действий определялся этим же инструментом;
- сформированная система знания также требовала рефлексии мышления в деятельности и в обучении, поскольку постоянно проверялась практикой вычислений;
- знаковая математическая система, оформленная в источниках, является доказательством индуктивного, а не дискретного характера отражения оформления знания;

- конструктивный принцип организации вычислительного инструмента в сочетании с принципом превращенной формы позволили сделать предположение относительно источника методических принципов обучения наблюдаемых нами в китайских трактатах, иначе, например, признанный историками науки метод обращения является не чем иным, как методом обучения будущих вычислителей в Древнем Китае.

Процессы интериоризации и экстериоризации знания должны были привести математиков к появлению теории в рамках среды, сформированной счетным инструментом и оформленной соответствующей знаковой системой и правилами представления результатов мыслительной деятельности.

Выводы

Из п. 1 можно сделать следующие сделать выводы.

Изучение психологии и истории математического образования в сочетании с анализом результатов в области классической китайской философии (нумерология и протологика) приводят нас к необходимости рассматривать математические тексты как сформированную среду, в которой все указанные науки вместе с историей китайской математики свидетельствуют о наличии в истории Китая развивающихся математического знания и научных методов.

Обращение к текстам как свидетельствам мыслительной деятельности, фиксирующим мыслительные операции, позволяет классифицировать их по признаку дидактической необходимости.

Возможность моделирования мыслительной деятельности, оформленной в виде алгоритмов, подобных не только алгоритму Евклида, но и многим другим, доказывает развитость алгоритмических начал китайской культуры; форма многих задач является подсказкой в выборе решений задач.

В преподавании китайской математики очень большое место отводилось самостоятельной работе учащегося «по образцу».

Комментаторская, псевдокомментаторская деятельность учащегося является одной из составляющих компонент в традиционной методике обучения, причем в полной мере отражающей философское представление о системе познания в данном этносе.

Оформление математических результатов развивало приемы абстрагирования, позволившие создать в рамках индуктивной математики совершенную знаковую систему.

Наличие информационно-педагогической среды в китайской математической литературе доказывает стабильность китайской математической школы.

Исследование методических приемов обучения приводит к убеждению в том, что к концу XIII и началу XIV века китайская математика обладала всеми атрибутами науки.

По источникам можно сформулировать следующие цели китайского математического образования в древности и в Средние века.

1. Уметь свободно пользоваться счетным инструментом, подобным суань пану.
2. Освоить все классические методы решения задач (но поскольку каждая из них являлась представителем своего фактор-класса, то вся «программа» обучения математике оказывалась факторизована по признаку применения задач в реальной жизни).
3. Научиться точно определять принадлежность задачи соответствующему классу разрешимых задач и выбирать соответствующий алгоритм среди многих алгоритмов (всего 26–27). Особенно эта цель была актуальна в древности и в Средние века.
4. Уметь объяснять и комментировать полученные результаты, а также доносить их до «заказчика».

В п. 2 приведены следствия из предложенной модели. Логика применения вычислительного инструмента в полной мере описывается логикой Мо Ди.

Литература

1. *Кузичева З.И., Кузичев А.С.* Вычислимость как стиль математических теорий // Социокультурная философия математики. СПб.: РХГИ, 1999. С. 377–390.
2. *Березкина Э.И.* Математика Древнего Китая. М.: Наука, 1980, 312 с.
3. *Герман В.* Математическое мышление. М.: Наука, 1989. 400 с.
4. *Фэн Ю-лань.* Краткая история китайской философии. СПб.: Евразия, 1998. 376 с.
5. *Чжу Шицзе* «Четыре яшмовых зеркала» / 中国科学技术典籍通汇(Zhong guo ke xue zhi shu dian ji tong hui) [Собрание китайских математических текстов: В 5 т. Китайская наука в первоисточниках]. Пекин, 1993. С. 1200–1280 (на китайском языке).
6. Там же.
7. *Жаров В.К.* Развитие методов преподавания традиционной китайской математики. (Опыт исследования информационно-педагогических сред). М.: Янус-К, 2002. 164 с.
8. *Жаров В.К.* Об одном примере развития математики // Годичная научная конференция, 2018. ИИЕТ им. С.И. Вавилова. М.: Янус-К, 2018. С. 203–207.

9. *Рассел Б.* Человеческое познание. Его сфера и границы. Киев: Ника-Центр, 1997. 560 с.
10. Философский энциклопедический словарь / под ред. Л.Ф. Ильичева, П.Н. Федосеева, С.М. Ковалева, В.Г. Панова. М.: Сов. энциклопедия, 1983. 840 с.
11. *Грановский Ю.В., Дрогалина Ж.А., Маркова, Е.В.* Я друг свобод... В.В. Налимов: вехи творчества. В 2 т. Т. 1. Томск; М.: Водолей Publishers, 2005. 376 с.
12. *Жаров В.К., Таратухина Ю.В.* Феноменология кросс-культурного образования. М.: Янус-К, 2016. 136 с.
13. *Жаров В.К.* О «Введении» к трактату Чжу Шицзе «Суань сюе ци мэн» // Историко-математические исследования. Вып. 6 (41). М.: Янус-К, 2001. С. 347–353.
14. *Цинь Цзюшао* «Девять книг по математике» (Цинь Цзюшао «Шу шу цзю чжан») (Шанхай,1937) /中国科学技术典籍通汇(Zhong guo ke xue zhi shu dian ji tong hui) [Собрание китайских математических текстов. В 5 т. Китайская наука в первоисточниках]. Т.1. Пекин. 1993. С. 430–724 (на китайском языке).
15. *Libbrecht U.* Chinese mathematics in the thirteenth century (The Shu-shu chiu-chang of Chin Chiu-shao). Cambridge, MA; London: MIT Press, 1973.
16. *Марков А.А.* Теория алгорифмов // Труды математического ин-та им. В.А. Стеклова. М.; Л., 1954. Вып. XLII. 374 с.
17. *Кричевец А.Н.* Априорность и адаптивность. М.: Российское психологическое общество, 1998. 130 с.
18. *Unguru S.* On the need to rewrite the history of Greek mathematics // Archive for history of exact science. 1976. Vol. 15 (2). P. 67–114.
19. *Wagner D.B.* An early Chinese derivation of the volume of the pyramid: Liu Hui, third century A.D. // Historia Math. 1979. Vol. 6 (2). P. 164–188.
20. *Морковкин В.В., Морковкина А.В.* Язык, мышление и сознание et vece versa // Русский язык за рубежом. 1994. № 1. С. 63–69.
21. *Розин В.М.* Типы и дискурсы научного мышления. М.: Эдиториал УРСС, 2000. 246 с.
22. *Сафронов М.В.* Введение в китайский язык. М.: Муравей, 1996. 256 с.
23. Чжун го шу сюе ши да си [Систематическая история китайской математики] / под ред. У Вэньцзюня. Пекин, 1998. Вып. 6. (на китайском языке)
24. *Стяжкин Н.И.* Становление идей математической логики. М.: Наука, 1964. 304 с.
25. *Сыма цянь.* Исторические записки (Ши цзи). Т. 3. М.: Наука, 1984. 944 с. (Памятники письменности Востока, XXXII).
26. *Lam Lay Yong.* Chu Shih-chiehs Suan-hsueh chi-meng (Introduction to mathematical studies) // Archive for history of exact sciences. 1979. Vol. 21 (1). P. 1–31.
27. *Березкина Э.И.* Древнекитайский трактат «Математика в девяти книгах» // Историко-математические исследования. Вып. X. М., 1957. С. 425–584.
28. *Юшкевич А.П.* Исследования по истории математики в Древнем Китае // Вопр. истории естествознания и техники. 1982. № 2. С. 125–137.
29. *Юнг Дж.В.А.* Как преподавать математику. М., 1924. 296 с.
30. *Юшкевич А.П.* История математики в средние века. М.: Физ.-мат. лит., 1961. 448 с.
31. *Юшкевич А.П.* О достижении китайский ученых в области математики // Из истории науки и техники Китая. М.: Изд-во АН СССР, 1955. С.130–160.

32. *Гессе-Вартег фон Эрнест.* Китай и китайцы. Жизнь, нравы и обычаи современного Китая. СПб.: Издание А.Ф. Девриена, 1900. 380 с.
33. *Девятов А.* Китайская специфика: как понял ее я в разведке и в бизнесе. М.: Муравей, 2002. 336 с.
34. История Китая с древнейших времен до наших дней. М.: Наука, 1974. 536 с.
34. История педагогики / под ред. А.И. Пискунова. М.: Сфера, 1998. Ч. 1. 192 с.
36. *Жаров В.К.* Теория и практика обучения математике в информационно-педагогической среде: По китайским математическим трактам XII–XIV вв.: дис. ... д-ра пед. наук., М., 2002.
37. *Сафронов М.В.* Введение в китайский язык. М.: Муравей, 1996. 256 с.
38. *Салмина Н.Г.* Знак и Символ в обучении. М.: МГУ, 1988. 288 с.
39. *Яо Фан.* Математические фрагменты из трактата «Чжоу би суань цзин» и комментария к нему Чжао Цзюнь-цина: дис. ... канд. физ.-мат. наук. М., 1995.
40. *Рубинштейн С.Л.* О мышлении и путях его исследования. М.: Изд-во АН СССР, 1958. 146 с.
41. *Колягин М.Ю.* Математические задачи как средство обучения и развития учащихся средней школы: автореф. дис. ... д-ра пед. наук. М., 1977. 55 с.
42. *Крупич В.И.* Теоретические основы обучения решению школьных математических задач. М.: Прометей, 1995. 166 с.
43. *Столяр А.А.* Педагогика математики. Минск, 1986. 414 с.
44. *Столяр А.А.* Методы обучения математике. Минск: Высшая школа, 190 с.
45. *Шапиро С.И.* От алгоритмов – к суждениям. (Эксперименты по обучению элементам математического мышления). М.: Сов. радио, 1978. 282 с.
46. *Колягин М.Ю.* Русская школа и математическое образование: Наша гордость и наша боль. М.: Просвещение, 2001. 318 с.
47. *Мечников Л.И.* Цивилизация и великие исторические реки. СПб., 1924.
48. *Титаренко М.Л.* Древнекитайский философ Мо Ди, его школа и учение. М.: Наука, 1985. 245 с.
49. *Жаров В.К.* О двух задачах трактата «Девять книг по математике» Цинь Цзюшао // Историко-математические исследования. Вып. XXX. М.: Наука, 1986. С. 338–343.
50. *Марков А.А.* О конструктивной математике // Труды математического ин-та им. В.А. Стеклова. М.; Л., 1962. Вып. LXVII. С. 2–14.
51. *Марков А.А.* О логике конструктивной математики. М.: Знание, 1972. 48 с.
52. Психологические критерии качества знаний школьников / ред. И.С. Якиманская. М., 1991. 142 с.
53. *Барабашев А.Г.* К проблеме возникновения теоретической математики // Методологические проблемы развития и применения математики. М.: АН СССР, 1985. С. 177–187.
54. *Waerden B.L.*, van der. Geometry and Algebra in Ancient Civilizations. Berlin; New York: Springer-Verlag, 1983.
55. *Вайман А.А.* Вавилонские числа // Историко-математические исследования. Вып. X. М., 1957.
56. *Ван дер Варден Б.Л.* Пробуждающееся наука. Математика Древнего Египта, Вавилона, Греции / пер. с гол. И.Н. Веселовского. М.: ГИФМЛ, 1959. 424 с.
57. *Нейгебауэр О.* Точные науки в древности. М.: Наука, 1968. 224 с.
58. *Выгодский М.Я.* Арифметика и алгебра в древнем мире. М.: Наука, 1967. 368 с.

59. *Брушлинский А.В.* Взаимосвязь процессуального и личностного аспектов мышления (методологический анализ) // Мышление: процесс, деятельность, общение. М., 1982. 286 с.
60. *Мамардашвили М.* Формы и содержание мышления. М.: Наука, 1968. 191 с.
61. *Брушлинский А.В.* Психология мышления и кибернетика. М.: Мысль, 1970. 202 с.

References

1. Kuzicheva ZI., Kuzichev AS. Computability as a style of mathematical theories / / Sociocultural philosophy of mathematics. Saint-Petersburg: RHGI Publ.; 1999. P. 377-90. (In Russ.).
2. Berezkina EI. The mathematics of Ancient China. Moscow: Nauka Publ.; 1980. 312 p. (In Russ.).
3. Hermann W. The mathematical way of thinking. Moscow: Nauka Publ.; 1989. 400 p. (In Russ.).
4. Feng Yu-Lan. A brief history of Chinese philosophy. Saint-Petersburg: Evraziya Publ.; 1998. 376 p. (In Russ.).
5. Zhu Sshijie. "Four Jasper Mirrors". 中国科学技术典籍通汇(Zhong guo ke xue zhi shu dian ji tong hui) [Collection of Chinese Mathematical Texts. In 5 vols. Chinese science in primary sources. Vol. 1.] Beijing, 1993. p. 1200-80. (In Chinese).
6. 中国科学技术典籍通汇(Zhong guo ke xue zhi shu dian ji tong hui) [Collection of Chinese Mathematical Texts. In 5 vols. Chinese science in primary sources. Vol. 1.] Beijing, 1993. (In Chinese).
7. Zharov VK. Development of methods of teaching traditional Chinese mathematics. (Experience in the study of information and pedagogical environments). Moscow: Yanus-K Publ.; 2002. 164 p. (In Russ.).
8. Zharov VK. On one example of the development of mathematics. V: Annual Scientific Conference, 2018. S.I. Vavilov IHST. Moscow: Yanus-K Publ.; 2018. p. 203-07. (In Russ.)
9. Russell B. Human knowledge. Its scope and boundaries. Kiev: Nika-Center Publ.; 1997. 560 p. (In Russ.)
10. Il'ichev LF., Fedoseev PN., Kovalev SM., Panov VG., eds. Philosophical encyclopedic dictionary. Moscow: Sov. etsiklopediya Publ.; 1983. 840 p. (In Russ.).
11. Granovskii, YV., Drogalina JA., Markova EV., eds. I am a friend of freedom... V.V. Nalimov. Milestones of creative work. In 2 vols. Vol. 1. Tomsk; Moscow: Vodolei Publishers Publ.; 2005. 376 p. (In Russ.)
12. Zharov VK., Taratukhina UV. Phenomenology of cross-cultural education. Moscow: Yanus-K Publ.; 2016. 136 p. (In Russ.)
13. Zharov VK. K. To "Introduction" to the treatise Zhu Shijie "Suan Xue qi Meng".V: Historical and mathematical research. Vol. 6 (41). Moscow: Yanus-K Publ.; 2001. p. 347-53. (In Russ.)
14. Qin Jiushao. "Nine books of Mathematics" (Qin Jiushao. "Shu Shu Ju Zhang") (Shanghai, 1937). 中国科学技术典籍通汇(Zhong guo ke xue zhi shu dian ji tong hui) [Collection of Chinese Mathematical Texts. In 5 vols. Chinese science in primary sources. Vol. 1.]. Beijing, 1993. p. 430-724. (In Chinese)

15. Libbrecht U. Chinese mathematics in the thirteenth century. The Shu-shu chiu-chang of Chin Chiu-shao. Cambridge, MA; London: MIT Press, 1973.
16. Markov AA. The theory of algorithms. V: Proceedings of Steklov Mathematical Institute. Moscow; Leningrad, 1954. Vol. 62. 374 p. (In Russ.)
17. Krichevets AN. Apriority and adaptability. Moscow: Rossiiskoe psikhologicheskoe obshchestvo Publ.; 1998. 130 p. (In Russ.)
18. Unguru S. On the need to rewrite the history of Greek mathematics. *Archive for history of exact science*. 1976;15:67-114.
19. Wagner DB. An early Chinese derivation of the volume of the pyramid: Liu Hui, third century A.D. *Historia Math*. 1979;6:164-88.
20. Morkovkin VV., Morkovkina AV. The language, thinking and consciousness et Vice Versa. *Russian Language Abroad*. 1994;1:63-9. (In Russ.)
21. Rozin VM. Types and discourses of scientific thinking. Editorial URSS Publ.; 2000. 246 p. (In Russ.)
22. Safronov MV. Introduction to the Chinese language. Moscow: Muravei Publ.; 1996. 256 p. (In Russ.)
23. Wu Wenjun, ed. Systematic history of Chinese mathematics (Zhong Guo Shu Xue Shi da XI). Beijing, 1998. Vol. 6. (In Chinese)
24. Styazhkin N. Formation of ideas of mathematical logic. Moscow: Nauka Publ.; 1964. 304 p. (In Russ.)
25. Sima Qian. Historical notes. (Shi JI). Vol. 3. M.: Nauka Publ.; 198. 944 p. (In Russ.). (Monuments of the writing of the East, XXXII)
26. Lam Lay Yong. Chu Shih-chiehs Suan-hsueh chi-meng (Introduction to mathematical studies). *Archive for history of exact sciences*. 1979;21:1-31.
27. Berezkina EI. Ancient Chinese treatise “Mathematics in nine books”. *Istoriko-matematicheskie issledovaniya*. Vol. 10. Moscow, 1957. p. 425-584. (In Russ.)
28. Yushkevich AP. Studies on the history of mathematics in Ancient China. *Problems in history of science and technology*. 1982;2:125-37 (In Russ.)
29. Yung Dzh. VA. How to teach mathematics. Moscow, 1924. 296 p. (In Russ.)
30. Yushkevich AP. History of mathematics in the Middle Ages. Moscow: Fiz.-mat.lit. Publ., 1961. 448 p. (In Russ.)
31. Yushkevich AP. On the achievement of Chinese scientists in the field of mathematics. V: From the history of science and technology of China. Moscow: Izd-vo AN SSSR Publ.; 1955. p. 130-60. (In Russ.)
32. Hesse-Wartag fon E. China and the Chinese. Life, morals and customs of modern China. Saint-Petersburg: A.F. Devrien Publ.; 1900. 380 p. (In Russ.)
33. Devyatov A. Chinese specifics. As I understood it in intelligence and business. Moscow: Muravei Publ.; 2002. 336 p. (In Russ.)
34. History of China from Ancient ages to the Present days. Moscow: Nauka Publ.; 1974. 536 p. (In Russ.)
35. Piskunov I., ed. History of pedagogy. Moscow: Sfera Publ.; 1998. Part 1. 192 p. (In Russ.)
36. Zharov V.K. Theory and practice of teaching mathematics in the information and educational environment. Following the Chinese mathematical paths of the 12th–16th centuries. [dis. ... d-ra ped. nauk.]. Moscow, 2002. (In Russ.)
37. Safronov MV. Introduction to Chinese Language. Moscow: Muravei Publ.; 1996. 256 p.

38. Salmina NG. Sign and symbol in training. Moscow: MGU Publ.; 1988. 288 p. (In Russ.)
39. Yao Fan. Mathematical fragments from the treatise “Zhou bi Xuan Jing” and Commentary on it by Zhao Jun-Qing. [dis. ... kand. fiz.-mat. nauk.]. Moscow, 1995. (In Russ.)
40. Rubinshtein SL. On thinking and ways of its research. Moscow: Izd-vo AN SSSR Publ.; 1958. 146 p. (In Russ.)
41. Kolyagin MYu. Mathematical problems as means of high school students training and development. [avtoref. dis. ... dr. ped. nauk.]. Moscow, 1977. 55 p. (In Russ.)
42. Krutich VI. Theoretical bases of teaching for school mathematical problems solving. Moscow: Prometei Publ.; 1995. 166 p. (In Russ.)
43. Stolyar AA. Pedagogics of mathematics. Minsk: Vysshaya Shkola Publ.; 1986. 414 p. (In Russ.)
44. Stolyar AA. Teaching methods in mathematics. Minsk: Vysshaya Shkola Publ.; 1966. 190 p. (In Russ.)
45. Shapiro SI. From algorithms – to judgments. (Experiments on learning elements of mathematical thinking). Moscow: Sov. Radio Publ.; 1978. 282 p. (In Russ.)
46. Kolyagin MYu. Russian school of mathematics and mathematical education. Our pride and our pain. Moscow: Prosveshchenie Publ.; 2001. 318 p. (In Russ.)
47. Mechnikov LI. Civilizations and great rivers in history. Saint-Petersburg, 1924. (In Russ.)
48. Titarenko ML. Ancient Chinese philosopher Mo Di, his school and teaching. Moscow: Nauka Publ.; 1985. 245 p. (In Russ.)
49. Zharov VK. On two problems of the treatise “Nine Books on Mathematics” Qin Jiushao. V: Historical and mathematical research. Vol. 30. Moscow, 1986. p. 338-43. (In Russ.)
50. Markov AA. On the constructive mathematics. V: Proceedings of Steklov Mathematical Institute. Moscow; Leningrad, 1962. Vol. 67. p. 2-14. (In Russ.)
51. Markov AA. On logic of the constructive mathematics. Moscow: Znanie Publ.; 1972. 48 p. (In Russ.)
52. Yakimanskaya IS., ed. Psychological criteria for quality of knowledge of schoolchildren knowledge. Moscow, 1991. p. 5-20. (In Russ.)
53. Barabashev AG. To the question of the emergence of theoretical mathematics. V: Methodological issues of development and application of mathematics. Moscow: AN SSSR Publ.; 1985. p. 177-87. (In Russ.)
54. Waerden B.L., van der. Geometry and Algebra in Ancient Civilizations. Berlin; New York: Springer-Verlag, 1983.
55. Vayman AA. The babylonian numbers. V: Historical and mathematical research. Vol. 10. Moscow, 1957. (In Russ.)
56. Waerden B.L., van der. The awakening science. Mathematics of Ancient Egypt, Babylon, Greece. Veselovskii IN., transl. from Dutch. Moscow: GIFML Publ.; 1959. 424 p. (In Russ.)
57. Neigebauer O. The exact sciences in antiquity. Moscow: Nauka Publ.; 1968. 224 p. (In Russ.)

58. Vygodskii MYa. Arithmetic and algebra in the ancient world. Moscow: Nauka Publ.; 1967. 368 p. (In Russ.)
59. Brushlinskii AV. Relationship of procedural and personal aspects of thinking (Methodological analysis). V: Thinking: process, activity, communication. Moscow, 1982. (In Russ.)
60. Mamardashvili, M. Form and content of thinking. Moscow: Nauka Publ.; 1968. 191 p. (In Russ.)
61. Brushlinskii AV. The psychology of thinking and cybernetics. Moscow: Mysl' Publ.; 1970. 202 p. (In Russ.)

Информация об авторе

Валентин К. Жаров, доктор педагогических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; Россия, Москва, 125993, Миусская пл., д. 6; valcon@mail.ru

Information about the author

Valentin K. Zharov, Dr. in Pedagogics, professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya sq., Moscow, 125993, Russia; valcon@mail.ru

Оформление серии
Е.В. Амосова

Корректор
Т.В. Рютина

Компьютерная верстка
М.Е. Заболотникова

Подписано в печать 19.11.2018.
Формат $60 \times 90^1/_{16}$.
Усл. печ. л. 9,2. Уч.-изд. л. 9,7.
Тираж 1050 экз. Заказ № 449

Издательский центр
Российского государственного
гуманитарного университета
125993, Москва, Миусская пл., 6
www.rggu.ru
www.knigirggu.ru