ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

1
2022

VESTNIK RGGU. Seriya “Informatica. Informacionnaya bezopasnost. Matematica”

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” Series Academic Journal

There are 4 issues of the printed version of the journal a year.

Founder and Publisher
Russian State University for the Humanities (RSUH)

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is included: in the Russian Science Citation Index; in the List of leading scientific magazines journals and other editions for publishing PhD research findings peer-reviewed publications fall within the following research area:

20.00.00 Informatics

81.93.29 Information security, data protection

27.00.00 Mathematics

Objectives and areas of research

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series publishes the results of research by scientists from RSUH and other universities and other Russian and foreign academic institutions. The areas covered by contributions include theoretical and applied computer science, up-to-date IT, means and technologies of information protection and information security as well as the issues of theoretical and applied mathematics including analytical and imitation models of different processes and objects. Special emphasis is put on articles and reviews covering research in indicated directions in the areas of social and humanitarian problems and also issues of personnel training for these directions.

RSUH/RGGU BULLETIN. “Information Science. Information Security. Mathematics” series is registered by Federal Service for Supervision of Communications Information Technology and Mass Media. 25.05.2018, reg. No. FS77-72977

Editorial staff office: 6, Miusskaya sq., Moscow, Russia, 125047

tel: +7 (916) 250-90-85

e-mail: adkozlov@mail.ru

ВЕСТНИК РГГУ. Серия «Информатика. Информационная безопасность. Математика»
Научный журнал

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», включен: в систему Российского индекса научного цитирования (РИНЦ); в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям и соответствующим им отраслям науки:

20.00.00 Информатика

81.93.29 Информационная безопасность, защита информации

27.00.00 Математика

Цели и область

В журнале «Вестник РГГУ», серия «Информатика. Информационная безопасность. Математика», публикуются результаты научных исследований ученых и специалистов РГГУ, а также других университетов и научных учреждений России и зарубежных стран. Направления публикаций включают теоретическую и прикладную информатику, современные информационные технологии, методы, средства и технологии защиты информации и обеспечения информационной безопасности, а также проблемы теоретической и прикладной математики, включая разработку аналитических и имитационных моделей процессов и объектов различной природы. Особое внимание уделяется статьям и обзорам, посвященным исследованиям по указанным направлениям в области социальных и гуманитарных проблем, а также вопросам подготовки кадров по соответствующим специальностям для данных направлений.

ВЕСТНИК РГГУ, серия «Информатика. Информационная безопасность. Математика», зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций 25.05.2018 г., регистрационный номер ПИ № ФС77-72977.

Адрес редакции: 125047, Россия, Москва, Миусская пл., 6

Тел: +7 (916) 250-90-85

электронный адрес: adkozlov@mail.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

А.Д. Козлов, кандидат технических наук, доцент (РГГУ)

CONTENTS

СОДЕРЖАНИЕ

УДК 004
DOI: 10.28995/2686-679X-2022-1-8-34

Международная премия А.М. Тьюринга Ассоциации вычислительной техники: информационный анализ

Вячеслав М. Тютюнник
Международный Информационный Нобелевский Центр (МИНЦ), Тамбов, Россия, vmtyutyunnik@gmail.com

Аннотация. Представлены краткие сведения об английском математике и криптографе А.М. Тьюринге, о старейшей и мощнейшей в сообществе компьютерщиков Ассоциации вычислительной техники, о премии имени Тьюринга – высшей награде по компьютерной науке, которая считается аналогом Нобелевских премий в информатике. Приведен полный список лауреатов премии Тьюринга с 1966 по 2020 г. на русском языке и языке оригинала, даты жизни. Анализ достижений лауреатов показывает полную и интереснейшую историю развития информатики и вычислительной техники в XX – начале XXI в. За это время лауреатами стали 74 человека, в том числе три женщины. Приведены точные формулировки награждающего комитета для каждого лауреата, а также их ученые степени, места и даты получения. Приведены также некоторые статистические данные по лауреатам (распределение по странам, перечень тематических направлений, по которым присуждены премии, средний возраст лауреатов).

Ключевые слова: премия А.М. Тьюринга, Ассоциация вычислительной техники, компьютерная наука (информатика), лауреаты, информационный анализ

Для цитирования: Тютюнник В.М. Международная премия А.М. Тьюринга Ассоциации вычислительной техники: информационный анализ // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 8–34. DOI: 10.28995/2686-679X-2022-1-8-34

International A.M. Turing Award of the Association for Computing Machinery. Information analysis

Viacheslav M. Tyutyunnik
International Nobel Information Centre (INIC), Tambov, Russia, vmtyutyunnik@gmail.com

Abstract. The article presents the brief information on the English mathematician and cryptographer A.M. Turing, about Association for Computing Machinery, the oldest and most powerful in the computer science community, and about the A.M. Turing Award, the highest prize in computer science, which is considered the equivalent of the Nobel Prizes in computer science. A complete list of A.M. Turing Award winners from 1966 to 2020 is given in Russian and original languages, dates of life. Analysis of the achievements of the laureates shows a complete and interesting history of the development of informatics (computer science) in the 20th and early 21st centuries. During this time, 74 people became laureates, including three women. The exact formulation of the award committee for each laureate is given, as well as their academic degrees, places and dates of receipt. Some statistical data on the laureates are also given (distribution by country, a list of thematic areas for which prizes were awarded, the average age of the laureates).

Keywords: A.M. Turing Award, Association for Computing Machinery, computer science (informatics), laureates, information analysis

For citation: Tyutyunnik, V.M. (2022), "International A.M. Turing Award of the Association for Computing Machinery. Information analysis", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 8–34, DOI: 10.28995/2686-679X-2022-1-8-34

Введение

Награждение особо отличившихся представителей человечества с древних времен было прерогативой государственных и частных организаций. Бесчисленное количество премий, орденов и иных наград отражает как в зеркале исторические эпохи и нравы, политические и социальные интересы, научные и технологические направления, художественные и эстетические моды. Международные, национальные и местные награды рождаются и исчезают с течением времени, но в каждый конкретный период четко выражают потребности данного сообщества [Тютюнник 1978], [Тютюнник, Федотова 1988].

Редкие награды переживают свое 50-летие, но есть и исключения. Самые почетные и самые известные международные награды – Нобелевские премии – присуждаются уже 120 лет [Тютюнник 1975], [Тютюнник 1991], [Наука 2019], [Тютюнник, Силиванец 2019], [Тютюнник 2020a], [Тютюнник 2020b], [Тютюнник, Силиванец 2020a], [Тютюнник, Силиванец 2020b], [Тютюнник 2021a], [Тютюнник 2021b]. Сообщество информатиков также имеет большое количество наград, высшей из которых является Международная премия Тьюринга, которая присуждается Ассоциацией вычислительной техники (*ABT*; Association for Computing Machinery, *ACM*), более 50 лет и по праву считается аналогом Нобелевских премий в информатике [Cacm Staff 2014].

Выдающийся английский математик и криптограф, член Лондонского Королевского общества Алан Мэтисон Тьюринг (23.06.1912–07.06.1954) прожил очень короткую, но насыщенную знаменательными событиями жизнь [Leavitt 2007], [Ходжес 2015] (рис. 1). Он по праву считается одним из основателей науки информатики или компьютерной науки, как ее называют в англоязычных странах. Еще в 1936 г. он предложил и аналитически описал модель абстрактной вычислительной «Машины Тьюринга», которая впоследствии была использована для создания компьютеров с формализацией представлений об алгоритме (процедуре) и искусственном интеллекте: эмпирический «тест Тьюринга» для оценки уровня искусственного интеллекта компьютера. Затем он прославился в период Второй мировой войны, возглавляя специальную великобританскую правительственную группу криптоанализа, занимавшуюся задачами взлома шифров и кодов, использовавшихся в переписке военно-морского флота Германии. Именно его группа разработала алгоритмы взлома, на основе которых была создана машина «Бомбе» (ирония от *Bombe glacee*), взломавшая немецкий шифратор «Энигма» (Enigma). Это была первая в современной истории хакерская сенсация, расценённая как исключительная математическая гениальность Алана. В третий раз Тьюринг прославился участием с 1948 г. в разработке новых электронных компьютеров, из которых «Манчестерский Марк 1» был запущен уже в 1949 г. Наконец, на закате своей короткой жизни он прославился еще раз основополагающей работой в зарождающейся области математической биологии (химический морфогенез), в которой предсказал новый класс химических реакций, протекающих в колебательном режиме. Экспериментально автоколебания в химических системах впервые обнаружил Б.П. Белоусов в 1951 г. (это знаменитые реакции Белоусова-Жаботинского).

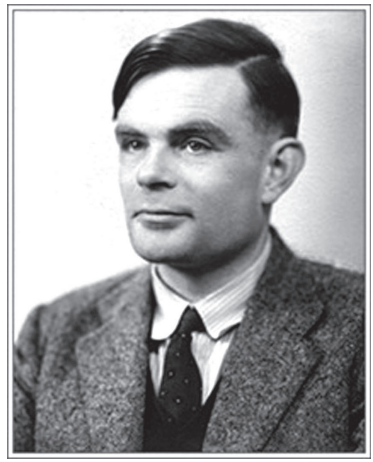


Рис. 1. Алан Тьюринг

Рис. 2. Марки (в блоках) с изображениями Тьюринга и некоторых лауреатов

Эти достижения сделали Тьюринга знаменитостью (рис. 2). Однако в 1952 г. он был осужден за гомосексуализм, подвержен принудительной гормональной терапии, а в 1954 г. отравлен цианидом. Позже он стал одной из самых известных жертв гомофобии в Великобритании, и лишь в конце 2013 г. королева Великобритании посмертно принесла ему официальные извинения. Годом раньше стало известно, что еще в 1945 г. Тьюринг был секретно награжден Орденом Британской империи.

Из истории АВТ и премии Тьюринга

Старейшая и мощнейшая в сообществе компьютерщиков Ассоциация вычислительной техники основана в США (штаб-квартира в Нью-Йорке) в эпоху вычислительных машин, уже на следующий год после введения в строй первой электронной вычислительной машины ENIAC. Главная идея этой организации сформулирована на организационном собрании в Колумбийском университете 15 сентября 1947 г.: «Цель этой организации будет заключаться в продвижении научных исследований, разработок, конструирования и применения нового оборудования для вычислений, рассуждений и другой работы с информацией». Первый и последующие уставы Ассоциации развили эти начальные идеи, хотя основной смысл остается. В настоящее время ее цель гласит:

> Ассоциация является международной научной и образовательной организацией, занимающейся продвижением искусства, науки, инжиниринга и применения информационных технологий, служа как профессиональным, так и общественным интересам, способствуя открытому обмену информацией и продвигая самые высокие профессиональные и этические стандарты.

АВТ быстро объединяла вокруг себя наиболее талантливых и известных компьютерщиков мира и к 1960-м годам превратилась в крупнейшее международное профессиональное сообщество, правда, во многом игнорирующее специалистов из СССР и стран советского блока. Даже в настоящее время, когда Ассоциация представляет весь спектр исследований и достижений в области информационных технологий, а членами АВТ являются более 100 тыс. представителей почти всех стран мира, россиян всего 370 чел., что меньше, чем, например, греков. Из всех бывших союзных республик количество членов АВТ составляет 458 чел.

Ассоциацией управляет совет, возглавляемый президентом, которого избирают на два года без права переизбрания. В настоящее время президентом является Габриэль Котсис, профессор компьютерных наук Университета им. Иоганна Кеплера (Линц, Австрия), почетный член АВТ. Структура Ассоциации сложна и разветвлена: более 170 региональных отделений, более 500 отделений в колледжах и университетах, издательский совет, цифровая библиотека, редколлегии множества специальных журналов и др. Основная деятельность осуществляется через специальные тематические группы (SIG – special interest group), которые соответствуют пол-

ному перечню научных и прикладных направлений информационных технологий и которых сейчас около 70. Наиболее известный журнал “Journal of the ACM” (учрежден в 1954 г.) в 2021 г. имел импакт-фактор в Scopus 7,0 (Q1), в WoS – 1,7.

Ассоциация учредила к настоящему времени более трех десятков наград, каждая из которых чрезвычайно почетна среди наиболее талантливых специалистов по информационным технологиям. В 2021 г., к примеру, обладателем наград стал 71 член АВТ. Ее главная и старейшая награда имени Тьюринга учреждена в 1966 г. и присуждается за вклад «в длительное и важное техническое достижение для компьютерной области». Это общая формула премии, каждое награждение имеет свою формулировку, однако неизменное условие – долгосрочность выдающегося достижения. Премией награждает специальный комитет, который состоит из председателя (в 2022 г. эту должность занимает 67-летний профессор Массачусетского технологического института Родни Аллен Брукс, знаменитый робототехник, член Австралийской академии наук, писатель и предприниматель в области робототехники, наиболее известный популяризацией акционистского подхода к робототехнике) и десяти членов, представляющих крупнейшие компьютерные центры мира.

Первоначально размер премии составлял 100 тыс. долл. США, в 2007 г. увеличен до 250 тыс., а в 2014 г. – до 1 млн долл. США (транспортные расходы лауреатов к месту вручения оплачиваются дополнительно к основной награде). Первым спонсором премии была корпорация Intel (создана в 1968 г. как NM Electronics), затем к ней присоединился Google Inc., который в настоящее время является единственным спонсором премии. Премия вручается ежегодно на специальном банкете в различных точках США, обычно в июне. Кроме денежной части, каждый лауреат получает символический серебряный кубок (рис. 3) и обязан прочитать «Лекцию лауреата премии А.М. Тьюринга» (не путать с Тьюринговскими чтениями, ныне называемыми Тьюринговскими лекциями, которые организованы, спонсируются и проводятся ежегодно с 1999 г. Институтом инженерии и технологий (IET) и Британским компьютерным обществом (BCS) в различных местах Великобритании). За первые 20 лет лекции изданы и в русском переводе [Лекции 1993]. Номинирование на премию осуществляется выдающимися учеными в области информационных технологий, последнее время возможно в онлайн-варианте, и завершается ежегодно 15 декабря. Обычно принимается от четырех до восьми писем-поддержек.

Рис. 3. Варианты серебряного кубка, вручаемого лауреатам, и бюст Тьюринга, изготовленный к 50-летию премии

Лауреаты премии Тьюринга

Анализ достижений лауреатов премии Тьюринга с 1966 по 2020 г. показывает полную и интереснейшую историю развития информатики и вычислительной техники. За это время лауреатами стали 74 чел., в том числе три женщины (рис. 4). К сожалению, в этом списке пока нет ни одного представителя нашей страны (табл. 1), однако эта ситуация характерна для любой высшей награды – претендентов много, а премия одна. К примеру, даже самых выдающихся представителей компьютерной науки насчитывается не менее 150 чел., т. е. в два раза больше, чем лауреатов.

Рис. 4. Женщины-лауреаты премии Тьюринга (слева направо): Ф. Аллен, Б.Дж. Лисков, Ш. Гольдвассер

Таблица 1

Полный список лауреатов премии Тьюринга

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
1966	Алан Дж. **Перлис** (Alan J. Perlis) (1.4.1922–7.2.1990)	За влияние в области передовых методов программирования и построения компиляторов	США	PhD по математике, Массачусетский технологический институт, 1950
1967	Морис В. **Уилкс** (Maurice V. Wilkes) (26.1.1913–29.11.2010)	Профессор Уилкс наиболее известен как конструктор и дизайнер EDSAC, первого компьютера с внутренне хранимой программой. Построенный в 1949г., EDSAC использовал память с ртутной линией задержки. Он также известен как автор, вместе с Уилером и Гиллом, книги «Подготовка программ для электронных цифровых вычислительных машин» (1951 г.), в котором эффективно внедрены программные библиотеки	Великобритания	PhD по физике, Колледж Святого Джонса Кембриджского университета, 1937
1968	Ричард У. **Хэмминг** (Richard W. Hamming) (11.2.1915–7.1.1998)	За работу по численным методам, системам автоматического кодирования, кодам обнаружения и исправления ошибок	США	PhD по математике, Иллинойский университет, 1942
1969	Марвин Л. **Мински** (Marvin L. Minsky) (9.8.1927–24.1.2016)	За центральную роль в создании, формировании, продвижении и развитии области искусственного интеллекта	США	PhD по математике, Принстонский университет, 1954

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
1970	Джеймс Х. **Уилкинсон** (James H. Wilkinson) (27.9.1919–5.4.1986)	За исследования в области численного анализа, способствовавшие использованию высокоскоростного цифрового компьютера, получив особое признание за работу по вычислениям в линейной алгебре и «обратному» анализу ошибок	Великобритания	BS по математике, Кембриджский университет, 1940
1971	Джон **МакКарти** (John McCarthy) (4.9.1927–24.10.2011)	Лекция доктора МакКарти «Современное состояние исследований в области искусственного интеллекта» охватывает область, в которой он добился значительного признания за свою работу	США	PhD по математике, Принстонский университет, 1951
1972	Эдсгер В. **Дейкстра** (Edsger W. Dijkstra) (11.5.1930–6.8.2002)	За фундаментальный вклад в развитие программирования как высокой интеллектуальной задачи; за красноречивое настаивание и практическую демонстрацию того, что программы должны быть составлены правильно, а не просто отлажены до корректности; за просветление восприятия проблем, лежащих в основе проектирования программ	Нидерланды	PhD по физике, Лейденский университет, 1956
1973	Чарльз У. **Бахман** (Charles W. Bachman) (11.12.1924–13.7.2017)	За выдающийся вклад в развитие технологии баз данных	США	PhD по электротехнике, Калифорнийский университет (Беркли), 1967

1974	Дональд Э. **Кнут** (Donald E. Knuth) (10.01.1938)	За крупный вклад в анализ алгоритмов и разработку языков программирования и, в частности, за вклад в «искусство программирования для ЭВМ» благодаря своим известным книгам в продолжающейся серии под таким названием	США	PhD по математике, Калифорнийский технологический институт, 1963
1975	Ален **Ньюэлл** (Allen Newell) (19.3.1927–19.7.1992) Герберт А. **Саймон** (Herbert A. Simon) (15.6.1916–9.2.2001)	В совместной научной работе, продолжавшейся более двадцати лет, сначала в сотрудничестве с Дж.К. Шоу в корпорации RAND, а затем с многочисленными преподавателями и студентами университета Карнеги-Меллон, Ньюэлл и Саймон внесли фундаментальный вклад в искусственный интеллект, психологию человеческого познания и обработку списков	США США	MS по математике, Принстонский университет, 1950 PhD по политическим наукам, Чикагский университет, 1943
1976	Михаэль О. **Рабин** (Michael O. Rabin) (1.9.1931) Дана С. **Скотт** (Dana S. Scott) (11.10.1932)	За совместную работу «Конечные автоматы и проблема их решения», в которой представлена идея недетерминированных автоматов, оказавшаяся чрезвычайно ценной. Их классическая статья была постоянным источником вдохновения для последующих работ в этой области	США США	PhD по компьютерной науке, Принстонский университет, 1956 PhD по математике, Принстонский университет, 1958
1977	Джон У. **Бэкус** (John W. Backus) (3.12.1924–17.3.2007)	За глубокий, влиятельный и долгосрочный вклад в разработку практических систем программирования высокого уровня, в частности благодаря работе над FORTRAN, и за фундаментальную публикацию формальных процедур для спецификации языков программирования	США	BS по математике, Колумбийский университет, 1949

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
1978	Роберт У. **Флойд** (Robert W. Floyd) (8.6.1936–25.9.2001)	За явное влияние на методологию создания эффективного и надежного программного обеспечения, а также за вклад в основание следующих важных областей информатики: теория синтаксического анализа, семантика языков программирования, автоматическая проверка программ, автоматический синтез программ и анализ алгоритмов	США	BS по физике, Чикагский университет, 1958
1979	Кеннет Ю. **Айверсон** (Kenneth E. Iverson) (17.12.1920–19.10.2004)	За новаторские усилия в области языков программирования и математической нотации, результатом которых стал язык программирования APL, за вклад в реализацию интерактивных систем, в образовательное использование APL, а также в теорию и практику языков программирования	США	PhD по прикладной математике, Гарвардский университет, 1954
1980	Ч. Энтони Р. **Хоар** (C. Anthony R. Hoare) (11.1.1934)	За фундаментальный вклад в определение и разработку языков программирования	Великобритания	BS по классической литературе и языкам, Оксфордский университет, 1956
1981	Эдгар Ф. **Кодд** (Edgar F. Codd) (23.8.1923–18.4.2003)	За фундаментальный и продолжительный вклад в теорию и практику систем управления базами данных	США	PhD по теории связи, Университет штата Мичиган, 1965

ISSN 2686-679X • RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series, 2022, no. 1

1982	Стефен А. **Кук** (Stephen A. Cook) (14.12.1939)	За значительное и глубокое развитие нашего понимания сложности вычислений. Его фундаментальная статья «Сложность процедур доказательства теорем», представленная в 1971 г. на симпозиуме ACM SIGACT по теории вычислений, заложила основы теории NP-полноты. Последующее исследование границ и природы класса NP-полных задач стало одним из наиболее активных и важных направлений исследовательской деятельности в информатике в последнее десятилетие	Канада	PhD по математике, Гарвардский университет, 1966
1983	Деннис М. **Ритчи** (Dennis M. Ritchie) (9.9.1941–12.10.2011) Кеннет Л. **Томпсон** (Kenneth L. Thompson) (4.2.1943)	За разработку общей теории операционных систем и конкретно за реализацию операционной системы UNIX	США США	PhD по математике, Гарвардский университет, 1968 MS по электротехнике, Калифорнийский университет (Беркли), 1966
1984	Никлаус Э. **Вирт** (Niklaus E. Wirth) (15.2.1934)	За разработку последовательности инновационных компьютерных языков: EULER, ALGOL-W, MODULA и PASCAL. PASCAL стал педагогически значимым и заложил основу для будущих исследований в области компьютерных языков, систем и архитектуры	Швейцария	PhD по электротехнике, Калифорнийский университет (Беркли), 1963

ISSN 2686-679X • Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
1985	Ричард М. **Карп** (Richard M. Karp) (3.1.1935)	За постоянный вклад в теорию алгоритмов, включая разработку эффективных алгоритмов для сетевого потока и других проблем комбинаторной оптимизации, отождествление вычислимости полиномиального времени с интуитивным понятием алгоритмической эффективности и, что особенно важно, вклад в теорию NP-полноты. Карп ввел ставшую стандартной методику доказательства NP-полноты проблем, которая привела к идентификации многих вычислительно трудных теоретических и практических проблем	США	PhD по прикладной математике, Гарвардский университет, 1959
1986	Джон Ю. **Хопкрофт** (John E. Hopcroft) (7.10.1939) Роберт Э. **Тарьян** (Robert E. Tarjan) (30.4.1948)	За фундаментальные достижения в разработке и анализе алгоритмов и структур данных	США США	PhD по прикладной математике, Стэнфордский университет, 1964 PhD по компьютерной науке, Стэнфордский университет, 1972
1987	Джон **Кок** (John Cocke) (30.5.1925–16.7.2002)	За значительный вклад в разработку и теорию компиляторов, архитектуру больших систем и развитие компьютеров с сокращенным набором команд (RISC); за открытие и систематизацию многих фундаментальных преобразований, используемых сегодня при оптимизации компиляторов, включая сокращение действия операторов, устранение общих подвыражений, распределение регистров, распространение констант и устранение «мертвого кода»	США	PhD по математике, Университет Дюка, 1953

ISSN 2686-679X • RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series, 2022, no. 1

1988	Айвен Э. **Сазерленд** (Ivan E. Sutherland) (16.5.1938)	За новаторский и дальновидный вклад в компьютерную графику, начавшийся со Sketchpad и продолжавшийся после него	США	PhD по электротехнике, Массачусетский технологический институт, 1963
1989	Уилльям М. **Кэхэн** (William Kahan) (5.6.1933)	За фундаментальный вклад в численный анализ. Один из ведущих экспертов по вычислениям с плавающей запятой. Кэхэн посвятил себя тому, чтобы «сделать мир безопасным для численных вычислений»!	США	PhD по математике, Университет Торонто, 1958
1990	Фернандо Х. **Корбато** (Fernando J. Corbato) (1.7.1926–19.7.2019)	За новаторскую работу по формулировке концепций и руководству разработкой крупномасштабных компьютерных систем общего назначения с совместным использованием времени и ресурсов, CTSS и Multics	США	PhD по физике, Массачусетский технологический институт, 1956
1991	Артур Дж. Робин Г. **Милнер** (Arthur J.R. Robin G. Milner) (13.1.1934–20.3.2010)	За три отдельных и полных достижения: 1) LCF, механизация логики вычислимых функций Скотта, вероятно, первый теоретически обоснованный, но практический инструмент для машинного построения доказательств; 2) ML – первый язык, включающий полиморфный вывод типов вместе с безопасным для типов механизмом обработки исключений; 3) CCS – общая теория параллелизма. Кроме того, он сформулировал и значительно продвинул полную абстракцию, изучение отношений между операционной и денотативной семантикой	Великобритания	MS по математике, Кембриджский университет, 1957

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
1992	Батлер Р. **Лэмпсон** (Butler W. Lampson) (23.12.1943)	За вклад в развитие распределенных персональных вычислительных сред и технологий их реализации: рабочих станций, сетей, операционных систем, систем программирования, дисплеев, безопасности и публикации документов	США	PhD по электротехнике, Калифорнийский университет (Беркли), 1967
1993	Юрис **Хартманис** (Juris Hartmanis) (5.7.1928);	В знак признания их основополагающей работы, заложившей основы теории сложности вычислений	США	PhD по математике, Калифорнийский технологический институт, 1955
	Ричард Э. **Стернс** (Richard E. Stearns) (5.7.1936)		США	PhD по математике, Принстонский университет, 1961
1994	Эдуард А. **Фейген-баум** (Edward A. Feigenbaum) (20.1.1936)	За новаторство в разработке и создании крупномасштабных систем искусственного интеллекта, демонстрирующее практическую важность и потенциальное коммерческое влияние технологии искусственного интеллекта	США	PhD по электротехнике, Университет Карнеги-Меллона, 1960
	Д.Р (Радж) **Редди** (D.R (Raj) Reddy) (13.6.1937)		США	PhD по математике, Стэнфордский университет, 1966
1995	Мануэль **Блум** (Manuel Blum) (26.4.1938)	В знак признания его вклада в основы теории сложности вычислений и ее применение в криптографии и проверке программ	США	PhD по математике, Массачусетский технологический институт, 1964

ISSN 2686-679X • RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series, 2022, no. 1

1996	Амир **Пнуэли** (Amir Pnueli) (22.4.1941–2.11.2009)	За фундаментальную работу по внедрению темпоральной логики в вычислительную науку и за выдающийся вклад в верификацию программ и систем	США	PhD по прикладной математике, Научный институт им. Вейцмана, 1967
1997	Дуглас К. **Энгельбарт** (Douglas C. Engelbart) (30.1.1925–2.7.2013)	За вдохновляющее видение будущего интерактивных вычислений и изобретение ключевых технологий, которые позволяют реализовать это видение	США	PhD по электротехнике, Калифорнийский университет (Беркли), 1955
1998	Джеймс Н. **Грей** (James N. Gray) (12.1.1944)	За фундаментальный вклад в исследования баз данных, обработку транзакций и техническое лидерство в реализации систем	США	PhD по компьютерной науке, Калифорнийский университет (Беркли), 1969
1999	Фредерик Ф. **Брукс**, мл. (Frederick Ph. Brooks, Jr.) (19.4.1931)	За выдающийся вклад в развитие компьютерной архитектуры, операционных систем и программной инженерии	США	PhD по прикладной математике/компьютерной науке, Гарвардский университет, 1956
2000	Эндрю Ци-Чжи **Яо** (Andrew Chi-Chih Yao) (24.12.1946)	В знак признания фундаментального вклада в теорию вычислений, включая основанную на сложности теорию генерации псевдослучайных чисел, криптографию и сложность связи	Китай	PhD по физике, Гарвардский университет, 1972, PhD по компьютерной науке, Иллинойский университет, 1975
2001	Оле-Йохан **Даль** (Ole-Johan Dahl) (12.10.1931–29.6.2002) Кристен **Нюгор** (Kristen Nygaard) (27.8.1926–10.8.2002)	За идеи, способствовавшие возникновению объектно-ориентированного программирования, за разработку языков программирования Simula I и Simula 67	Норвегия Норвегия	MS по математике, Университет Осло, 1960 MS по математике, Университет Осло, 1956

ISSN 2686-679X • Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
2002	Леонард М. **Адлеман** (Leonard M. Adleman) (31.12.1945) Рональд Л. **Ривест** (Ronald L. Rivest) (6.5.1947) Ади **Шамир** (Adi Shamir) (6.7.1952)	За гениальный вклад в создание криптографии с открытым ключом, полезной на практике	США США Израиль	PhD по компьютерной науке, Калифорнийский университет (Беркли), 1976 PhD по компьютерной науке, Стэнфордский университет, 1974 PhD по компьютерной науке, Научный институт им. Вейцмана, 1977
2003	Алан К. **Кэй** (Alan C. Kay) (17.5.1940)	За пионерство многих идей, лежащих в основе современных объектно-ориентированных языков программирования, руководство группой, разработавшей Smalltalk, и фундаментальный вклад в развитие персональных компьютеров	США	PhD по электротехнике, Университет штата Юта, 1969
2004	Винтон Г. **Серф** (Vinton G. Cerf) (23.6.1943) Роберт Э. **Кан** (Robert E. Kahn) (23.12.1938)	За новаторскую работу по созданию сетей Интернета, включая разработку и внедрение основных коммуникационных протоколов Интернета TCP/IP, а также за вдохновляющее лидерство в области сетевых технологий	США США	PhD по компьютерной науке, Калифорнийский университет (Лос-Анджелес), 1972 PhD по электротехнике, Принстонский университет, 1964

2005	Петер **Наур** (Peter Naur) (25.10.1928–3.1.2016)	За фундаментальный вклад в разработку языков программирования и введение языка Algol 60, в разработку компиляторов, а также в искусство и практику компьютерного программирования	Дания	PhD по астрономии, Копенгагенский университет, 1957
2006	Фрэнсис **Аллен** (Frances E. Allen (4.8.1932–4.8.2020)	За новаторский вклад в теорию и практику методов оптимизирующих компиляторов, которые заложили основу для современных оптимизирующих компиляторов и автоматического параллельного исполнения	США (первая женщина-лауреат)	MA по математике, Мичиганский университет, 1957
2007	Эдмунд М. **Кларк**, мл. (Edmund M. Clarke, Jr.) (27.7.1945–22.12.2020)	За их роль в развитии проверки моделей (Model-Checking) в высокоэффективную технологию верификации, которая широко применяется в индустрии аппаратного и программного обеспечения	США	PhD по компьютерной науке, Корнельский университет 1976
	Эрнест Аллен **Эмерсон** (Ernest Allen Emerson) (2.6.1954)		США	PhD по прикладной математике, Гарвардский университет, 1981
	Иосиф **Сифакис** (Joseph Sifakis) (26.12.1946)		Греция	State Doctorate по компьютерной науке, Гренобльский университет, 1979
2008	Барбара Дж. **Лисков** (Barbara Jane Liskov) (7.11.1939)	За вклад в практические и теоретические основы проектирования языков программирования и систем, особенно связанных с абстракцией данных, отказоустойчивостью и распределенными вычислениями	США (вторая женщина-лауреат)	PhD по компьютерной науке, Стэнфордский университет, 1968

ISSN 2686-679X • Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1

Продолжение табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
2009	Чарльз П. **Текер** (Charles P. Thacker) (26.2.1943–12.6.2017)	За новаторскую разработку и реализацию первого современного персонального компьютера – Alto в Xerox PARC – и основополагающие изобретения и вклад в развитие локальных вычислительных сетей (включая Ethernet), многопроцессорных рабочих станций, протоколов наблюдения когерентности кэш-памяти и планшетных персональных компьютеров	США	BS по физике Калифорнийский университет, Беркли, 1967
2010	Лесли Г. **Вэлиант** (Leslie G. Valiant) (28.3.1949)	За преобразующий вклад в теорию вычислений, включая теорию вероятностно приблизительно корректного обучения (PAC), сложности перечисления и алгебраических вычислений, а также теорию параллельных и распределенных вычислений	Велико-британия	PhD по компьютерной науке, Уорикский университет, 1974
2011	Джуда **Перл** (Judea Pearl) (4.9.1936)	За фундаментальный вклад в развитие искусственного интеллекта путем разработки исчисления для вероятностных и причинно-следственных рассуждений	США	PhD по электротехнике, Бруклинский политехнический институт, 1965
2012	Шафи **Гольдвас-сер** (Shafi Goldwasser) (14.11.1958)	За преобразовательную работу, заложившую теоретическую основу науки криптографии, в процессе которой были разработаны новые методы эффективной проверки математических доказательств в теории сложности	США (третья женщина-лауреат)	PhD по электротехнике и компьютерной науке, Калифорнийский университет, Беркли, 1984
	Сильвио **Микали** (Silvio Micali) (13.10.1954)		США	PhD по математике, Калифорнийский университет, Беркли, 1982

ISSN 2686-679X • RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series, 2022, no. 1

2013	Лесли **Лэмпорт** (Leslie Lamport) (7.2.1941)	За фундаментальный вклад в теорию и практику распределенных и параллельных систем, в частности за изобретение таких понятий, как причинность и логические часы, безопасность и живучесть, репликация машин состояний и последовательная согласованность	США	PhD по математике, Университет Брандейса, 1972
2014	Майкл **Стоунбрейкер** (Michael Stonebraker) (11.10.1943)	За фундаментальный вклад в развитие концепций и практик, лежащих в основе современных систем баз данных	США	PhD по компьютерной науке и инжинирингу, Мичиганский университет, Энн Арбор, 1971
2015	Б.Уитфилд **Диффи** (B.Whitfield Diffie) (5.6.1944) Мартин Э. **Хеллман** (Martin E. Hellman) (2.10.1945)	За изобретение и популяризацию асимметричной криптографии с открытым ключом, включая ее применение для цифровых подписей, и практического метода обмена криптографическими ключами	США США	BS по математике, Массачусетский технологический институт, 1965 PhD по электротехнике, Стэнфордский университет, 1969
2016	Сэр Тимоти Дж. **Бернерс-Ли** (Sir Timothy J. Berners-Lee) (8.6.1955)	За изобретение Всемирной паутины (WWW), первого веб-браузера, а также фундаментальных протоколов и алгоритмов, позволяющих масштабировать Всемирную паутину	Великобритания	BS по физике, Колледж Королевы Оксфордского университета, 1976

ISSN 2686-679X • Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1

Окончание табл. 1

Год	Лауреат, даты жизни	Формулировка премии	Страна	Ученая степень, место ее получения и год
2017	Джон Л. **Хеннесси** (John L. Hennessy) (22.9.1952)	За систематический новаторский количественный подход к проектированию и оценке компьютерных архитектур, оказавший неизгладимое влияние на микропроцессорную промышленность	США	PhD по компьютерной науке, Университет Стоуни-Брук, 1977
	Дэвид А. **Паттерсон** (David A. Patterson) (16.11.1947)		США	PhD по компьютерной науке, Калифорнийский университет, Лос-Анжелес, 1976
2018	Йошуа **Бенжио** (Yoshua Bengio) (5.3.1964)	За концептуальные и инженерные прорывы, благодаря которым глубокие нейронные сети стали важнейшим компонентом вычислительной техники	Канада	PhD по компьютерной науке, Университет Макгилла, 1991
	Джеффри Э. **Хинтон** (Geoffrey E. Hinton) (6.12.1947)		Канада	PhD по искусственному интеллекту, Эдинбургский университет, 1978
	Ян **Лекун** (Yann LeCun) (8.7.1960)		США	PhD по компьютерной науке, Университет Пьера и Марии Кюри, 1987

ISSN 2686-679X • RSUH/RGGU BULLETIN. "Information Science. Information Security. Mathematics" Series, 2022, no. 1

2019	Эдвин Э. **Катмулл** (Edwin E. Catmull) (31.3.1945) Патрик (Пэт) **Ханрахан** (Patrick M. Hanrahan) (1954)	За фундаментальный вклад в трехмерную компьютерную графику и влияние компьютерно-генерируемых изображений (CGI) в кинематографе и других областях применения	США США	PhD по физике и компьютерной науке, Университет Юты, 1969 PhD по биофизике, Висконсинский университет, 1985
2020	Альфред В. **Ахо** (Alfred Vaino Aho**)** (9.8.1941) Джеффри Д. **Ульльман** (Jeffrey D. Ullman) (22.11.1942)	За фундаментальные алгоритмы и теорию, лежащие в основе реализации языков программирования, а также за обобщение этих и других результатов в своих очень влиятельных книгах, на которых воспитывались целые поколения компьютерщиков	США США	PhD по электротехнике и информатике, Принстонский университет, 1967 PhD по электротехнике, Принстонский университет, 1966
2021	Информация о лауреатах появится весной 2022 г.			

Заключение

За всю историю премиями отмечены ученые по 33 тематическим разделам информатики и вычислительной техники (ИВТ), в которых преобладают искусственный интеллект, языки программирования, сложность компьютерных вычислений, криптография, теория информатики, анализ алгоритмов и компиляторы, что представляется вполне логичным (табл. 2).

Таблица 2

Распределение количества лауреатов
по тематическим разделам ИВТ

Тематический раздел информационных технологий	Количество лауреатов	Годы награждений
Анализ алгоритмов	5	1974, 1986, 1986, 2011, 2013
Архитектура компьютеров	4	1967, 1978, 1999, 2009
Базы данных	4	1973, 1981, 1998, 2014
Верификация аппаратного и программного обеспечения	3	2007, 2007, 2007
Верификация компьютерных программ	2	1972, 1996
Графика компьютерная	3	1988, 2019, 2019
Интерактивные компьютерные вычисления	1	1997
Искусственный интеллект	8	1969, 1971, 1975, 1975, 1994, 1994, 2010, 2011
Комбинаторные алгоритмы	1	1985
Коммуникации Интернета	2	2004, 2004
Компиляторы	5	1966, 1987, 2006, 2020, 2020
Компьютерная сложность	7	1982, 1993, 1993, 1995, 2010, 2012, 2012
Компьютерное оборудование	1	1967
Компьютерное образование	1	2010
Компьютерные системы	1	1990
Конечные автоматы	2	1976, 1976

Окончание табл. 2

Тематический раздел информационных технологий	Количество лауреатов	Годы награждений
Корректирование ошибочных кодов	1	1968
Криптография	7	1995, 2000, 2002, 2002, 2002, 2012, 2012
Надежные конструкции систем	2	1991, 2013
Образование компьютерное	1	1967
Обработка списков	2	1975, 1975
Объектно-ориентированное программирование	2	2001, 2001
Операционные системы	4	1983, 1983, 1999, 2008
Параллельные компьютерные вычисления	1	2010
Персональные компьютеры	3	1992, 2003, 2009
Программирование	3	1966, 1972, 1974
Программное обеспечение	2	1978, 2014
Разработка программного обеспечения	1	1999
Структуры данных	2	1986, 1986
Теория компьютерной науки (информатики)	6	1976, 1976, 1991, 1993, 2000, 2010
Численные методы	1	1968
Численный анализ	2	1970, 1989
Языки программирования	8	1979, 1980, 1984, 1991, 2003, 2005, 2008, 2013
Итого:	98	

Несовпадение количества лауреатов (74) и их распределения по тематикам объясняется тем, что некоторые лауреаты сделали выдающиеся работы в двух областях.

Награды в основном получали представители США (57 чел., 77% от общего количества), затем Великобритании (6 чел.), Канады (3 чел.), Норвегии (2 чел.) и по одному человеку – из Греции, Дании, Израиля, Китая, Нидерландов, Швейцарии. Большинство лауреатов получили образование и ученые степени в области общей

и прикладной математики, электротехники, физики и компьютерной науки, а ко времени своих выдающихся достижений работали профессорами компьютерной науки крупнейших университетов мира, занимали престижные должности в самых влиятельных компьютерных корпорациях (IBM., Hewlett-Packard, Microsoft., Sun Microsystems и др.); являются учредителями и руководителями исследовательских всемирно известных организаций. Средний возраст лауреатов к моменту получения премии составляет 58 лет. Особый интерес представляют научные биографии каждого лауреата, но это уже тема следующей статьи.

Благодарности

Автор благодарен профессору В.В. Арутюнову за формулирование идеи написания данной статьи.

Acknowledgments

The author is grateful to Professor V.V. Arutyunov for formulating the idea of writing this article.

Литература

Лекции 1993 – Лекции лауреатов премии Тьюринга за первые двадцать лет: 1966–1985. М.: Мир, 1993.

Наука 2019 – Наука, технологии, общество и Международное Нобелевское движение // Нобелевский конгресс – 12-я Международная встреча-конференция лауреатов Нобелевских премий и нобелистов: труды. Тамбов: МИНЦ «Нобелистика», 2019.

Тютюнник 1975 – *Тютюнник В.М.* Нобелевские премии и лауреаты по химии // Журнал Всесоюзного химического общества им. Д.И. Менделеева. 1975. Т. 20. № 6. С. 603–609.

Тютюнник 1978 – *Тютюнник В.М.* Химики – лауреаты Ленинской премии. М.: Знание, 1978.

Тютюнник, Федотова 1988 – *Тютюнник В.М., Федотова Т.А.* Золотые медали и именные премии Академии наук СССР. Тамбов: Тамбовский филиал МГИК, 1988.

Тютюнник 1991 – *Тютюнник В.М.* Альфред Нобель и Нобелевские премии. Тамбов, ТГИК, 1991.

Тютюнник, Силиванец 2019 – *Тютюнник В.М., Силиванец Е.А.* Наукометрические анализы выдвижения кандидатов на Нобелевские премии. 1. Номинанты и номинаторы на Нобелевскую премию по химии (1901–1910) // История науки и техники. 2019. № 9. С. 3–21.

Тютюнник 2020a – *Тютюнник В.М.* Тенденции и особенности развития современной науки: номинанты и номинаторы на Нобелевские премии по физике и химии // Формирование профессионала в условиях региона. XXI Международная научная конференция. Тамбов: МИНЦ «Нобелистика», 2020. С. 116–163.

Тютюнник 2020b – *Тютюнник В.М.* Нобелевские лауреаты – отечественные и иностранные члены и обладатели наград Российской академии наук // История науки и техники. 2020. № 9. С. 3–26.

Тютюнник, Силиванец 2020a – *Тютюнник В.М., Силиванец Е.А.* Наукометрические анализы выдвижения кандидатов на Нобелевские премии. Номинанты и номинаторы на Нобелевскую премию по физике (1901–1910) // История науки и техники. 2020. № 2. С. 3–22.

Тютюнник, Силиванец 2020b – *Тютюнник В.М., Силиванец Е.А.* Наукометрические анализы выдвижений на Нобелевские премии. 3. Номинанты и номинаторы на Нобелевскую премию по физиологии или медицине (1901–1910) // История науки и техники. 2020. № 4. С. 3–39.

Тютюнник 2021a – *Тютюнник В.М.* Номинирование на Нобелевскую премию по физике в 1911–1950 годах // Инженерная физика. 2021. № 2. С. 10–33.

Тютюнник 2021b – *Тютюнник В.М.* Наукометрические анализы выдвижений кандидатов на Нобелевские премии. 4. Номинанты и номинаторы на Нобелевскую премию по химии (1911–1950) // История науки и техники. 2021. № 2. С. 12–38.

Ходжес 2015 – *Ходжес Э.* Игра в имитацию. М.: АСТ, 2015.

CACM Staff 2014 – *CACM Staff.* ACM's Turing Award prize raised to $1 million // Communications of the ACM. Vol. 57, no. 12, p. 20.

Leavitt 2006 – *Leavitt D.* The Man Who Knew Too Much: Alan Turing and the Invention of the Computer. New York: W.W. Norton, 2006.

References

CACM Staff (2014), "ACM's Turing Award prize raised to $1 million", *Communications of the ACM,* vol. 57, no. 12, p. 20.

Hodges, E. (2015), *Igra v imitatsiyu* [The Simulation Game], AST, Moscow, Russia.

Leavitt, D. (2006), *The Man Who Knew Too Much: Alan Turing and the Invention of the Computer,* W.W. Norton, New York, USA.

Lektsii (1993), *Lektsii laureatov premii T'yuringa za pervye dvadtsat' let: 1966–1985* [Lectures by Turing Award winners for the first twenty years: 1966–1985], Mir, Moscow, Russia.

Nauka (2019), *Nauka, tekhnologii, obschestvo i Mezhdunarodnoe Nobelevskoe dvizhenie* [Science, Technology, Society and the International Nobel Movement], Nobel Congress – Proceedings of the 12th International Meeting-Conference of Nobel Laureates and Nobelists, MINTs "Nobelistika", Tambov, Russia.

Tyutyunnik, V.M. (1975), "Nobel Prizes and laureates in Chemistry", *Zhurnal vsesoyuznogo khimicheskogo obschestva imeni D.I. Mendeleeva,* vol. 20, no. 6, pp. 603–609.

Tyutyunnik, V.M. (1978), *Khimiki – laureaty Leninskoi premii* [Chemists – laureates of the Lenin Prize], Znanie, Moscow, Russia.

Tyutyunnik, V.M. and Fedotova, T.A. (1988), *Zolotye medali i imennye premii Akademii nauk SSSR*, [Gold medals and personal prizes of the USSR Academy of Sciences], Tambov branch of MGIK, Tambov, USSR.

Tyutyunnik, V.M. (1991), *Alfred Nobel i Nobelevskie premii* [Alfred Nobel and the Nobel Prizes], TGIK, Tambov, Russia.

Tyutyunnik, V.M. and Silivanets, E.A. (2019), "Scientometric analyses of the nomination of candidates for Nobel Prizes. 1. Nominees and nominators for the Nobel Prize in Chemistry (1901–1910)", *Istoriya nauki i tekhniki,* no. 9, pp. 3–21.

Tyutyunnik, V.M. (2020a), "Trends and features of the development of modern science. Nominees and nominators for the Nobel Prizes in Physics and Chemistry", *XXI Int. Scientific Conf. "Formation of a professional in the conditions of the region",* Tambov, Russia, pp. 116–163.

Tyutyunnik, V.M. (2020b), "Nobel laureates – Russian and foreign members and the award winners of the Russian Academy of Sciences", *Istoriya nauki i tekhniki,* no. 9, pp. 3–26.

Tyutyunnik, V.M. and Silivanets E.A. (2020a), "Scientometric analyses of the nomination of candidates for Nobel Prizes. Nominees and nominators for the Nobel Prize in Physics (1901–1910)". *Istoriya nauki i tekhniki,* no. 2, pp. 3–22.

Tyutyunnik, V.M. and Silivanets E.A. (2020b), "Scientometric analyses of Nobel Prize nominations. 3. Nominees and nominators for the Nobel Prize in Physiology or Medicine (1901–1910)", *Istoriya nauki i tekhniki,* no. 4, pp. 3–39.

Tyutyunnik, V.M. (2021a), "Nominations for the Nobel Prize in Physics 1911–1950", *Inzhenernaya fizika*, no. 2, pp. 10–33.

Tyutyunnik, V.M. (2021b), "Scientometric analyses of nominations for Nobel Prizes. 4. Nominees and nominators for the Nobel Prize in Chemistry (1911–1950)", *Istoriya nauki i tekhniki*, no. 2, pp. 12–38.

Информация об авторе

Вячеслав М. Тютюнник, доктор технических наук, профессор, Международный Информационный Нобелевский центр (МИНЦ), Тамбов, Россия; 392002, Россия, Тамбов, Первомайская пл., д. 30-6; vmtyutyunnik@gmail.com

Information about the author

Viacheslav M. Tyutyunnik, Dr. of Sci. (Information Science), professor, International Nobel Information Centre (INIC), Tambov, Russia; bld. 30-6, Pervomaiskaya Sq., Tambov, Russia, 392002; vmtyutyunnik@gmail.com

УДК 534
DOI: 10.28995/2686-679X-2022-1-35-45

Исследование звука: удаление шумов

Александр А. Андреев
Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия, andreev.business.mail@gmail.com

Марина С. Шаповалова
Московский государственный технический университет имени Н.Э. Баумана, Москва, Россия, mshapovalova84@gmail.com

Аннотация. В статье представлены алгоритмы для удаления посторонних шумов из аудиодорожки. Рассмотрены особенности различных видов шумов, которые возникают при звукозаписи. В статье учтены особенности архитектуры Conv-TasNet, базирующейся на наложении сверток на чистый сигнал без разложения на частоты. Проводится анализ алгоритма DEMUC, который напрямую генерирует источники из исходного сигнала, минуя промежуточное предсказание масок; частично заимствована архитектура для сегментации изображений U-Net. Также рассматривается алгоритм шумоподавления HiFi-GA, состоящий из трех основных частей: Wavenet, Postnet и GAN. Для создания чистого сигнала на основе зашумленного используется алгоритм WaveNet, который изначально использовался для перевода текстовой информации в речь. Особенность разных версий алгоритма WaveNet для шумоподавления состоит в том, что генерация нового сигнала может происходить как целиком, так и для каждого момента времени. В работе также представлен математический аппарат для реализации алгоритмов Conv-TasNet, DEMUC, а также HiFi-GA, подробно анализируется шумоподавление при записи звука, исследуются различные методы шумоподавления, формулируются преимущества и недостатки каждого из них.

Ключевые слова: обработка звука, технологии шумоподавления, алгоритмы, методы

Для цитирования: Андреев А.А., Шаповалова М.С. Исследование звука: удаление шумов // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 35–45. DOI: 10.28995/2686-679X-2022-1-35-45

Sound research. Noise removal

Alexander A. Andreev
Bauman Moscow State Technical University, Moscow, Russia,
andreev.business.mail@gmail.com

Marina S. Shapovalova
Bauman Moscow State Technical University, Moscow, Russia,
mshapovalova84@gmail.com

Abstract. The article presents algorithms for removing extraneous noise from an audio track. It considers the features of various types of noise that occur during sound recording. The article takes into account the features of the Conv-TasNet architecture, which is based on the imposition of convolutions on a pure signal without frequency separation. There is an analysis of the DEMUC algorithm, which directly generates sources from the original signal, bypassing the intermediate prediction of masks; the architecture for segmentation of images U-Net is partially borrowed. Also the authors consider the HiFi-GA noise reduction algorithm, consisting of three main parts: Wavenet, Postnet and GAN. A clean signal based on a noisy one is created with the WaveNet algorithm that was originally used to translate text information into speech. A feature of different versions of the WaveNet algorithm for noise reduction is that a new signal can be generated both in its entirety and for each time-point. The paper also presents a mathematical apparatus for implementing the Conv-TasNet, DEMUC, and HiFi-GA algorithms, analyzes in detail noise reduction when recording sound, explores various noise reduction methods, and formulates the advantages and disadvantages of each of them.

Keywords: sound processing, noise reduction technologies, algorithms, methods

For citation: Andreev, A.A. and Shapovalova, M.S. (2022), "Sound research. Noise removal", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 35–45, DOI: 10.28995/2686-679X-2022-1-35-45

Введение

Обработка звука – это процесс исследования динамической/статической звуковой дорожки при помощи применения определенного набора линейных и нелинейных алгоритмов с целью получения необходимой информации. Алгоритмы динамической обработки звука работают с потоковыми аудиозаписями при ста-

тической обработке уже готовой звуковой информации. Данный процесс происходит с использованием компьютерных программ и подразумевает достаточно сложную обработку.

Особенности организации подавления шумов

Процесс исследования и обработки звука так или иначе присутствует в различных сферах деятельности. Технологии шумоподавления используются при очистке аудиозаписей от лишних звуковых событий. При монтаже фильмов, музыки, подкастов и прочих медиа зачастую требуется избавляться от лишних звуков. Также может потребоваться общее улучшение качества записи. Для этого необходимы не только удаление посторонних шумов, но и модификация сигнала, чтобы улучшить восприятие записанной речи.

Популярной и сложной задачей является шумоподавление и воспроизведение одновременно с записью речи. Цель такой обработки – маскировка звуков, которые не имеют отношения к произносимой человеком информации и мешают ее восприятию. Чаще всего такое шумоподавление использует принципы «шумовых ворот», но помимо этого применяются методы машинного обучения.

Также областью использования методов шумоподавления является предобработка и чистка звукового сигнала до применения методов автоматического распознавания речи. При такой обработке звука возникает много сложностей, так как сигнал не должен содержать искусственных артефактов речи, иначе такая «чистка» может ухудшить получаемый результат.

В научном сообществе принято разделять шум на три большие категории [Reddy, Gopal, Cutler, Beyrami1, Cheng, Dubey, Matusevych, Aichner, Aazami, Braun, Rana, Srinivasan, Gehrke 2005]: Стационарный, Импульсный и Нестационарный. К первому относится белый шум, ко второму чих, хлопок и скрип, а третью группу делят на две категории: прерывистый (гудки телефона, сигнализация, стук молотка) и колеблющийся (шум вентилятора, шум ветра, двигатель автомобиля).

Виды методов шумоподавления

Самые простые традиционные методы шумоподавления используются, когда заранее неизвестен характер шума и речи. Отсутствие информации также наблюдается при необходимости избавляться от шума в процессе записи звука. В этом случае шумоподавления используются обычные или спектральные пороги – за-

глушаются любые отзвуки, если они не превышают определенного порога по громкости. В основе других традиционных методов лежит моделирование распределения чистой речи или шума. Делается это с помощью нахождения спектральной плотности мощности (громкости) сигнала. Спектральная плотность мощности сигнала – функция, которая описывает возможную мощность в различных диапазонах частоты. В таком случае, имея спектральную плотность мощности шума, можно использовать метод спектрального вычитания (spectral subtraction).

Спектральные мощности различных источников звука отличаются, и порой значительно (рис. 1):

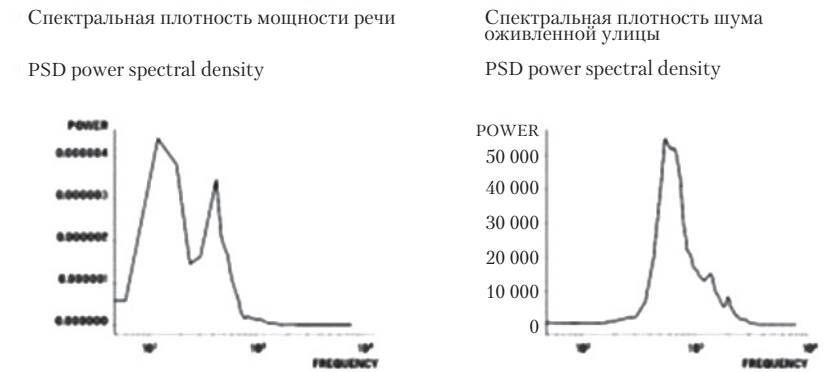


Рис. 1. Пример сравнения спектральных мощностей [Reddy, Gopal, Cutler, Beyrami1, Cheng, Dubey, Matusevych, Aichner, Aazami, Braun, Rana, Srinivasan, Gehrke 2005]

Винеровское оценивание (Wiener filter) используется в качестве одного из традиционных обучаемых способов шумоподавления. Этот подход основан на подборе фильтра, который бы минимизировал разницу между чистым и улучшенным сигналами. Подобно некоторым алгоритмам машинного обучения, при вычислении винеровского фильтра минимизируется метрика Mean Square Error (MSE).

$$H(w) - \frac{P_{ss}(w)}{P_{yy}(w)} = \frac{P_{yy}(w) - P_{dd}(w)}{P_{yy}(w)}, \quad (1)$$

где $P_{yy}(w)$ – спектр чистого сигнала,
$P_{ss}(w)$ – спектр зашумленного сигнала,
$P_{dd}(w)$ – спектр шумного сигнала.

Таким образом, оптимальный винеровский фильтр можно найти в случаях, когда известна «чистая версия» зашумленного сигнала, либо если известен конкретный шум, который надо убрать. Часто после операций по фильтрации шума применяется сглаживание, чтобы избавиться после чистки от артефактов сигнала – «музыкального» шума. Для этого применяются различные фильтры, например Гауссовый фильтр (или размытие по Гауссу [Соловьев 2014]).

В зависимости от способа решения задачи шумоподавления, разграничения спикеров или улучшения сигнала алгоритмы машинного обучения разделяют на две категории: на основе масок и Генеративные и Нейросетевые методы предсказывают маски для каждого спикера/инструмента или чистого сигнала. Эти маски накладываются на оригинальный текст.

Генеративные методы предсказывают новый сигнал для каждого спикера/инструмента или чистый сигнал.

Подходы, которые основаны на маскировании спектрограмм, имеют некоторые недостатки. Например, фаза волны в чистом сигнале может отличаться от фазы волны в зашумленном сигнале. Поэтому даже при вычислении идеальной маски для спектрограммы восстановленная из грязного сигнала фаза может вносить какие-то элементы шума и портить итоговое качество шумоподавления. Еще одним недостатком такой системы является сложность вычисления частотных характеристик сигнала с помощью быстрого преобразования Фурье.

Особенности архитектуры Conv-TasNet

Многие современные подходы шумоподавления часто сравниваются с архитектурой Conv-TasNet [Luo, Mesgarani 2019] как с одной из наиболее устойчивых реализаций. Она основана на наложении 1D сверток на чистый сигнал без разложения на частоты. Предшественник этой архитектуры – TasNet [Luo, Mesgarani 2018] состоит из сверточных энкодера и декодера с некоторыми особенностями: выход энкодера ограничен значениями от нуля до бесконечности $[0, \infty)$; линейный декодер конвертирует выход энкодера в акустическую волну; подобно многим методам-предшественникам на основе спектрограмм, на последнем этапе система приближает взвешивающую функцию (в данном случае LSTM) для каждого момента времени.

Conv-TasNet [van den Oord, Dieleman, Zen, Simonyan, Vinyals, Graves, Kalchbrenner, Senior, Kavukcuoglu 2016] – модификация

алгоритма TasNet, использующая в качестве взвешивающей функции сверточные слои с расширением (dilation). Эта модификация была сделана после того, как свертки с расширением показали себя эффективным алгоритмом при одновременном анализе и генерации данных переменной длины.

Подход для разделения аудио/шумоподавления Conv-TasNet состоит из 3-х компонентов (см. рис. 2): энкодер, разделение, декодер.

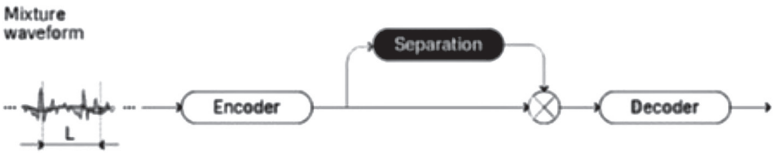


Рис. 2. Подход к разделению аудио
[van den Oord, Dieleman, Zen, Simonyan, Vinyals, Graves, Kalchbrenner, Senior, Kavukcuoglu 2016]

Основной компонент в схеме на рис. 2 – этап разделения. Он решает проблему приближенного исчисления источников, смесь которых мы рассматриваем в качестве «грязных» примеров. Формально предположение о «смешанности» нашего сигнала можно выразить следующим образом:

$$x(t) = \sum_{i=t}^{c} S_i(t), \tag{2}$$

где $x(t)$ – смесь в определенный момент времени;
C – количество источников, несущих вклад в смесь;
$S_1(t) \ldots S_c(t)$ источники в определенный момент времени.

Задача алгоритма машинного обучения – определить источники $S_1(t)$, ..., $S_c(t)$, зная заранее количество источников C и смесь $x(t)$. Разделение в алгоритме происходит не сразу, а только после извлечения признаков из сигнала с помощью «1D блоков» (1-D Conv, рис. 3), он имеет особую структуру (рис. 4) [Luo, Mesgarani 2019].

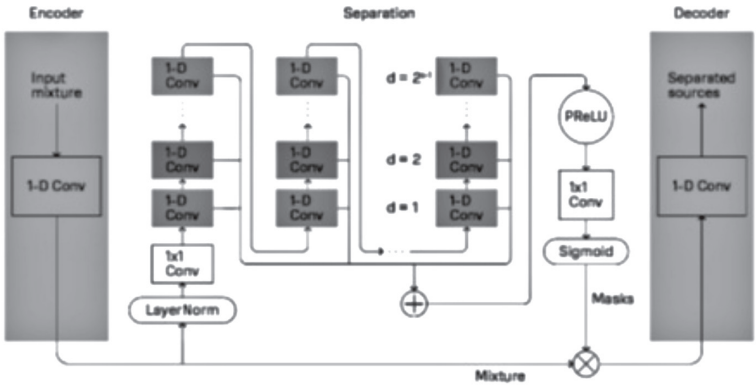


Рис. 3. Преобразование сигнала смеси
в набор отдельных источников

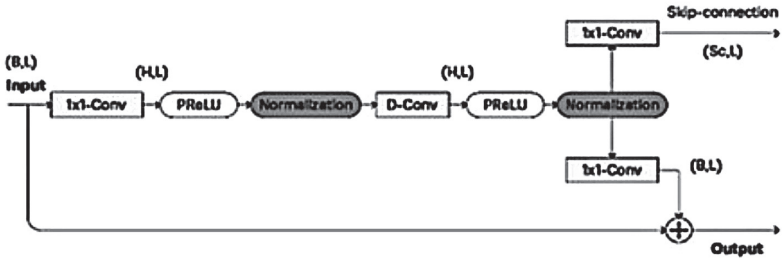


Рис. 4. Структура 1-D Conv

Особенности алгоритма DEMUCS

Алгоритм DEMUCS [Defossez, Synnaeve, Adi 2020] или глубокое извлечение музыкальных источников (Deep Extractor for Music Sources) используется для задач разделения источников в сигнале и шумоподавления; он напрямую генерирует источники из исходного сигнала, минуя промежуточное предсказание масок. Создатели алгоритма исходили из архитектуры для сегментации изображений U-Net. В отличие от обычного автокодировщика слои между собой связаны «соединениями быстрого доступа», в результате итоговый сигнал не ухудшается после сжатия (рис. 5).

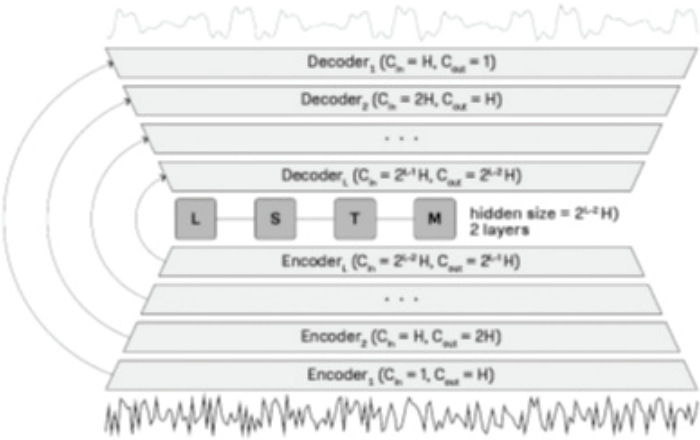


Рис. 5. Структура U-Net для шумоподавления

В качестве «бутылочного горлышка» в DEMUCS применен однонаправленный LSTM слой. Это позволяет эффективно использовать алгоритм для анализа потоковых данных.

В качестве функции потерь при шумоподавлении достаточно использовать L1 Loss между предсказанной записью и эталонной, но для улучшения сходимости также используют STFT Loss разного масштаба, который является суммой двух функций потерь – сходимости (spectral convergence) и амплитуд (magnitude):

$$L_{STFT}(y,\hat{y}) = L_{sc}(y,\hat{y}) + L_{mag}(y,\hat{y}) \tag{3}$$

$$L_{sc}(y,\hat{y}) = \frac{\|\,|STFT(y)| - |STFT(\hat{y})|\,\|_F}{\|STFT(y)\|_F} \tag{4}$$

$$L_{mag}(y,\hat{y}) = \frac{1}{T}\|log|STFT(y)| - log|STFT(\hat{y})|\|_1 \tag{5}$$

где y и $\hat{y}$ – эталонный сигнал и предсказанный сигнал соответственно;
T – длина сигнала;
$\|\cdot\|F$ – норма Фробениуса, а $\|\cdot\|1$ – L1 «норма» (абсолютная ошибка).

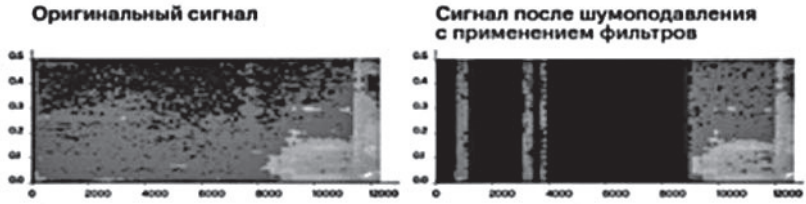


Рис. 6. Результат шумоподавления HiFi-GAN

Данный метод [Su, Jin, Finkelstein 2020] основывается на генерации. В отличие от предшественников, генеративно-состязательная сеть высокой точности (High Fidelity Generative Adversarial Network) хорошо справляется с генерацией аудио подобно студийной записи без артефактов искусственной генерации.

Алгоритм шумоподавления HiFi-GAN состоит из трех основных частей (см. рис. 6): Wavenet, Postnet и GAN. За генерацию чистого сигнала на основе зашумленного отвечает блок WaveNet, этот алгоритм изначально успешно использовался для синтеза речи (текст → аудио). При модификации задачи для анализа аудио эта архитектура также показала себя эффективной. Особенность WaveNet для шумоподавления в том, что генерация нового сигнала происходит для всей записи целиком, а не для каждого момента времени t_n, как это делается в исходном алгоритме WaveNet. Это позволяет улучшать скорость генерации за счет параллелизации процессов, которые могут выполняться одновременно. После генерации WaveNet сигнал проходит через несколько сверточных слоев, этот этап называется Postnet. Он нужен, чтобы исправлять и уточнять грубое и приближенное предсказание WaveNet. Кроме Postnet, регулирующее действие дополнительно оказывают четыре разных дискриминатора, которые обучены отделять чистые оригинальные записи от сгенерированных. Каждый дискриминатор принимает выход Postnet в разном формате.

Заключение

Алгоритмы шумоподавления активно развиваются из-за их необходимости в ежедневном использовании. И поэтому, скорее всего, в скором времени появятся совершенно новые технологии, основанные на иных процессах и структурах, которые позволят совершать данную работу, затрачивая меньший объем ресурсов.

Литература

Соловьев 2014 – *Соловьев С.А.* Решение разреженных систем линейных уравнений методом Гаусса с использованием техники аппроксимации матрицами малого ранга // Вычислительные методы и программирование. 2014. Т. 15. № 3. С. 441–460.

Defossez, Synnaeve, Adi 2020 – *Defossez A., Synnaeve G., Adi Y.* Real time speech enhancement in the waveform domain [Электронный ресурс]. URL: https://arxiv.org/pdf/2006.12847.pdf (дата обращения 15 января 2022).

Luo, Mesgarani 2018 – *Luo Y., Mesgarani N.* Dual-Signal Transformation TASNET: time-domain audio separation network for real-time, single-channel speech separation [Электронный ресурс]. URL: https://arxiv.org/pdf/1711.00541.pdf (дата обращения 13 января 2022).

Luo, Mesgarani 2019 – *Luo Y., Mesgarani N.* Conv-TasNet: surpassing ideal time-frequency magnitude masking for speech separation [Электронный ресурс]. URL: https://arxiv.org/pdf/1809.07454.pdf (дата обращения 14 января 2022).

Reddy, Gopal, Cutler, Beyrami1, Cheng, Dubey, Matusevych, Aichner, Aazami, Braun, Rana, Srinivasan, Gehrke 2005 – *Reddy C.K.A, Gopal V., Cutler R., Beyrami1 E., Cheng R., Dubey H., Matusevych S., Aichner R., Aazami A., Braun S., Rana P., Srinivasan S., Gehrke J.* Deep Noise Suppression Challenge: Datasets, Subjective Testing Framework, and Challenge Results [Электронный ресурс]. URL: https://arxiv.org/pdf/2005.13981.pdf (дата обращения 15 декабря 2021).

Su, Jin, Finkelstein 2020 – *Su J., Jin Z., Finkelstein A.* HiFi-GAN: high-fidelity denoising and dereverberation based on speech deep features in adversarial networks [Электронный ресурс]. URL: https://arxiv.org/pdf/2006.05694.pdf (дата обращения 15 января 2022).

Van den Oord, Dieleman, Zen, Simonyan, Vinyals, Graves, Kalchbrenner, Senior, Kavukcuoglu 2016 – *van den Oord A., Dieleman S., Zen H., Simonyan K., Vinyals O., Graves A., Kalchbrenner N., Senior A., Kavukcuoglu K.* WAVENET: a generative model for raw audio [Электронный ресурс]. URL: https://arxiv.org/pdf/1609.03499.pdf (дата обращения 13 января 2022).

References

Defossez, A., Synnaeve, G. and Adi, Y. (2020), “Real time speech enhancement in the waveform domain”, [Online], available at: https://arxiv.org/pdf/2006.12847.pdf (Accessed 15 January 2022).

Luo, Y. and Mesgarani, N. (2018), “Dual-Signal Transformation TASNET: time-domain audio separation network for real-time, single-channel speech separation”, [Online], available at: https://arxiv.org/pdf/1711.00541.pdf (Accessed 13 January 2022).

Luo, Y. and Mesgarani, N. (2019), “Conv-TasNet: surpassing ideal time-frequency magnitude masking for speech separation”, [Online], available at: https://arxiv.org/pdf/1809.07454.pdf (Accessed 14 January 2022).

Reddy, C.K.A, Gopal, V., Cutler, R., Beyrami1, E., Cheng, R., Dubey, H., Matusevych, S., Aichner, R., Aazami, A., Braun, S., Rana, P., Srinivasan, S. and Gehrke, J. (2005), "Deep noise suppression challenge: datasets, subjective testing framework, and challenge results", [Online], available at: https://arxiv.org/pdf/2005.13981.pdf (Accessed 14 December 2021).

Solov'ev, S.A. (2014), "Solving of the linear equations sparse systems by the Gauss method using the technique of approximation by low-rank matrices", *Vychislitelnye metody I programmirovanie*, vol. 15, no. 3, pp. 441–460.

Su, J., Jin, Z. and Finkelstein, A. (2020), "HiFi-GAN: high-fidelity denoising and dereverberation based on speech deep features in adversarial networks", [Online], available at: https://arxiv.org/pdf/2006.05694.pdf (Accessed 15 January 2022).

Van den Oord, A., Dieleman, S., Zen, H., Simonyan, K., Vinyals, O., Graves, A., Kalchbrenner, N., Senior, A. and Kavukcuoglu, K. (2016), "WAVENET: a generative model for raw audio", [Online], available at: https://arxiv.org/pdf/1609.03499.pdf (Accessed 13 January 2022).

Информация об авторах

Александр А. Андреев, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 1105005, Россия, Москва, 2-я Бауманская ул., д. 5; andreev.business.mail@gmail.com

Марина С. Шаповалова, кандидат педагогических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; mshapovalova84@gmail.com

Information about the authors

Alexander A. Andreev, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005 ; andreev.business.mail@gmail.com

Marina S. Shapovalova, Cand. of Sci. (Education), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Bauman Str., Moscow, Russia, 105005; mshapovalova84@gmail.com

УДК: 004.93
DOI: 10.28995/2686-679X-2022-1-46-62

Метод обнаружения посторонних объектов на взлетно-посадочной полосе по видеопотоку

Никита Е. Шоркин
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, shorkin.nikita29@yandex.ru

Кирилл Л. Тассов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, ktassov@policesoft.ru

Аннотация. Рассмотрена задача обнаружения посторонних объектов на взлетно-посадочной полосе. Существующие автоматизированные системы, решающие эту задачу, базируются на оптико-электронных (камерах) и радиолокационных датчиках (радарах). Однако в этих системах камеры используются только для визуального подтверждения и редко применяются непосредственно для проведения детектирования. Использование видеоинформации для обнаружения объектов позволит повысить степень автоматизации подобных систем. В статье предложен метод обнаружения посторонних объектов по видеопотоку, основанный на пороговой сегментации. Метод работает с данными со статических камер и может применяться как в системах только с камерами, так и в комплексных системах в качестве оптической составляющей. Разработанный метод осуществляет обработку набора подряд идущих кадров видеопотока для проведения обнаружения. Обнаружение объектов осуществляется в два этапа. На первом этапе используется вычитание фона по модели в виде смеси гауссовых распределений. На втором применяется адаптивная пороговая сегментация. Проведено исследование применимости разработанного метода на основании экспериментальных данных. Получены зависимости показателей качества обнаружения объектов от значений параметров метода. Достоинствами предложенного подхода являются высокая скорость обнаружения объектов, высокая точность определения положения объекта в кадре, адаптивность порога сегментации, а также возможность гибкой настройки чувствительности детектирования.

Ключевые слова: посторонние объекты на ВПП, обнаружение объектов по видеопотоку, компьютерное зрение, сегментация изображений

Для цитирования: Шоркин Н.Е., Тассов К.Л. Метод обнаружения посторонних объектов на взлетно-посадочной полосе по видеопотоку // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 46–62. DOI: 10.28995/2686-679X-2022-1-46-62

Method for detecting foreign objects on the runway by video stream

Nikita E. Shorkin
Bauman Moscow State Technical University, Moscow, Russia,
shorkin.nikita29@yandex.ru

Kirill L. Tassov
Bauman Moscow State Technical University, Moscow, Russia,
ktassov@policesoft.ru

Abstract. The article considers a problem of detecting foreign objects on the runway. Existing automated systems that solve that issue are based on cameras and radar sensors. However, in those systems, cameras are used only for visual confirmation and are rarely used directly to perform detection. The use of video information for object detection will increase the degree of automation of such systems. The article proposes a method for detecting foreign objects in a video stream based on threshold segmentation. The method works with data from static cameras and can be used both in systems with only cameras and in complex systems as an optical component. The developed method processes a set of consecutive frames of the video stream to perform detection. Object detection is performed in two stages. At the first stage, background subtraction based on Gaussian mixture model is used. At the second stage, adaptive threshold segmentation is applied. The applicability of the developed method was investigated on the basis of experimental data. The dependences of the quality indicators of object detection on the method parameters were obtained. The advantages of the proposed approach are high speed of object detection, high accuracy of object positioning in the frame, adaptivity of segmentation threshold, as well as flexible adjustment of detection sensitivity.

Keywords: foreign objects on the runway, object detection by video stream, computer vision, image segmentation

For citation: Shorkin, N.E. and Tassov, K.L. (2022), "Method for detecting foreign objects on the runway by video stream", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 46–62, DOI: 10.28995/2686-679X-2022-1-46-62

Введение

Обеспечение безопасности движения самолета по взлетно-посадочной полосе (ВПП) является одной из важнейших задач организации работы аэропорта и воздушного движения. Одним из источников опасности для самолета на земле является наличие мусора на ВПП:

– детали самолетов;
– инструменты, оставленные сотрудниками аэропорта;
– мусор, нанесенный ветром;
– крупные рептилии, птицы;
– хищники, привлеченные останками птиц.

Финансовые потери авиационной промышленности, связанные с нарушениями безопасности ВПП, оцениваются в 4 млрд долларов в год [AERO 2001].

В настоящее время большинство аэропортов решают проблему обнаружения мусора периодическим патрулированием ВПП сотрудниками на служебном транспорте, но такой подход имеет достаточно много ограничений [European Commission CORDIS 2018], в частности при плохих погодных условиях, в темное время суток, а также из-за человеческого фактора.

С развитием технологий стали появляться автоматизированные системы обнаружения мусора на полосе, однако подобными системами, отвечающими современным стандартам, оснащено лишь малое количество наиболее крупных аэропортов.

Указанные системы строятся на оптико-электронных и радиолокационных датчиках (радарах). Радары могут обнаруживать даже малоразмерные объекты с высокой степенью точности в сложных погодных условиях, но при этом не гарантируется правильность обнаружения, что при ложном срабатывании влечет за собой дополнительные расходы и задержки в работе аэропорта. Кроме того, радар дает очень мало информации о самом объекте. Поэтому системы дополняются одной или несколькими видеокамерами, которые наводятся на места возможного расположения посторонних объектов, чтобы по видеоинформации можно было избежать «ложной тревоги». При этом использование исключительно камер требует применения сложных алгоритмов обнаружения.

Подавляющее большинство рассматриваемых систем используют радары для детектирования, а камеры – только для визуального подтверждения [U.S. Federal Aviation Administration 2009]. Существенный недостаток радаров заключается в их негативном влиянии на другие технические средства аэропорта. Этот факт не позволяет осуществлять постоянный мониторинг состояния ВПП.

Расширение роли камер позволяет непрерывно сканировать полосу и использовать полученную видеоинформацию, например, для классификации обнаруженных объектов.

В данной статье предложен метод обнаружения опасных объектов по видеопотоку и реализующие его алгоритмы. Метод может применяться как в системах только с камерами, так и в комплексных системах в качестве оптической составляющей. Однако у него есть ряд ограничений: камера – только статическая, погода – бесснежная, освещенность – не менее 100 лк, линейные размеры объектов на кадрах – не менее 4 пикселей. Кроме того, подразумевается, что в поле зрения камеры находится только ВПП.

Описание предлагаемого метода

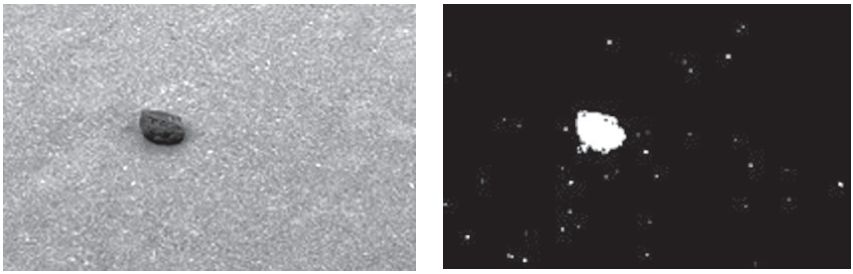
Разработанный метод осуществляет обработку набора подряд идущих кадров видеопотока для проведения обнаружения. Каждый кадр набора подается на вход двухэтапного детектора. На первом этапе по модели фона в виде смеси гауссовых распределений происходит выделение фрагментов кадра, на которых могут содержаться посторонние объекты. Второй этап заключается в сегментации полученных фрагментов с помощью адаптивной пороговой сегментации.

Таким образом, процесс обработки кадров для обнаружения посторонних объектов на ВПП можно представить в виде следующей последовательности действий:

1) выделение набора кадров из видеопотока для проведения детектирования;
2) выделение фрагментов на кадре, в которых, возможно, находятся посторонние объекты;
3) детектирование посторонних объектов в выделенных областях кадра;
4) обнаружение объектов по бинарным маскам, полученным в результате обработки кадров набора.

Определение областей кадра с возможным расположением объектов

Смесь гауссовых распределений предполагает представление каждого пикселя модели в виде взвешенного набора нормальных распределений [KaewTraKulPong, Bowden 2001]. Распределения разделяются на задающие фон и задающие посторонние объекты.



а) *б)*

Рис. 1. Обработка кадра по модели фона:
а) исходный кадр; *б)* отфильтрованная маска

Перед использованием такую модель необходимо сформировать, т. е. задать для каждого пикселя веса компонент смеси и параметры распределений. Эту процедуру можно проводить различными способами [Dempster, Rubin, Laird 1977] [Stauffer, Grimson 1999].

Для каждого пикселя обрабатываемого кадра определяется распределение, к которому относится пиксель, из соответствующей этому пикселю смеси гауссиан. На основании этого производится классификация пикселя на фоновые и пиксели объекта. Если распределение не было найдено, то пиксель классифицируется как пиксель объекта.

Далее осуществляется обновление элемента фона в соответствии с моделью. При этом параметры гауссиан обновляются только в том случае, если для пикселя было найдено определяющее его распределение, иначе обновляются только веса в смеси.

По результатам классификации всех пикселей обрабатываемого кадра строится бинарная маска, в которой единичные пиксели обозначают пиксели объекта, а нулевые – пиксели фона.

Поскольку полученная бинарная маска будет содержать различные шумы, не представляющие интереса, ее необходимо обработать фильтром. Оставшиеся пиксели объектов группируются в прямоугольные области (рис. 2). По этим областям выделяются фрагменты исходного кадра, которые поступают на дальнейшую обработку.

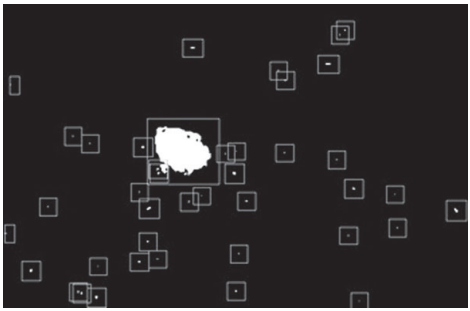


Рис. 2. Выделенные прямоугольные области

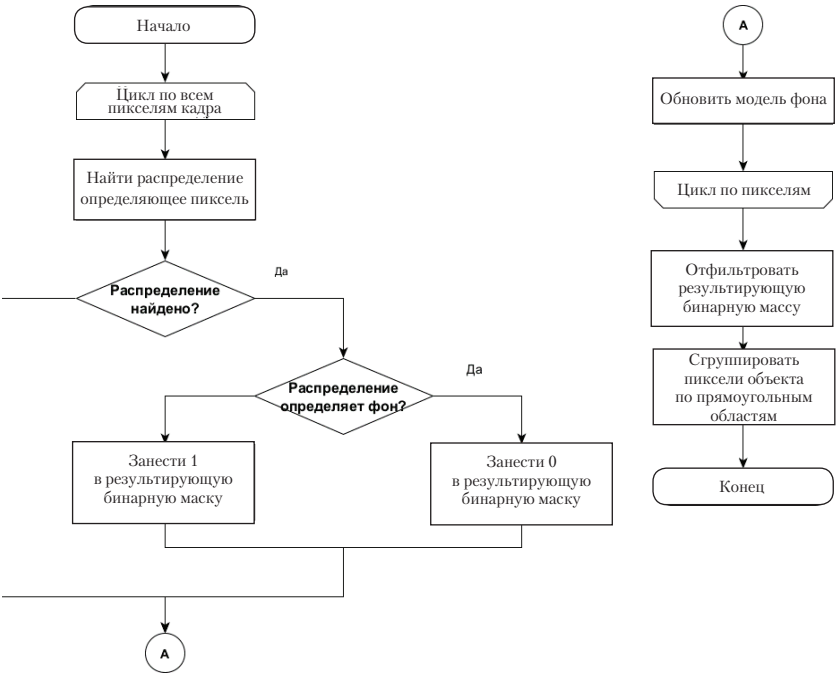


Рис. 3. Схема алгоритма выделения областей кадра с возможным расположением объектов

Общая схема выделения областей кадра, в которых может находиться посторонний объект, представлена на рис. 3.

Модель фона в виде смеси нормальных распределений не гарантирует обязательного обнаружения объекта в выделенных областях кадра, так как она при всей сложности остается подвержена влиянию резких изменений освещения, а также не избавляет от попадания в результат шумов и помех. Поэтому статистическая модель фона применяется только для предварительного определения областей кадра с возможным наличием в них посторонних объектов.

Выделение посторонних объектов на фрагментах кадра

Выделенные на предыдущем этапе фрагменты переводятся в полутоновый цветовой режим. Это обусловлено тем, что пороговая сегментация, как правило, сводится к сегментации именно полутоновых изображений [Гонсалес, Вудс 2012]. Кроме того, такой переход сокращает количество вычислений, поскольку для каждого пикселя нужно будет рассчитать только один порог для одной компоненты цвета (интенсивности), а также избавляет от необходимости принимать решение в ситуации, когда часть компонент цвета будет определена как фоновая, а другая часть – как принадлежащая объекту.

Для каждого пикселя по его локальной окрестности (размеры которой являются параметром метода) вычисляется порог по формуле (1). Этот адаптивный порог используется для классификации пикселя как фонового или принадлежащего объекту по разнице его яркости со средней яркостью в локальной окрестности (2) [Тропченко А.А., Тропченко А.Ю. 2015].

$$T_{xy} = \begin{cases} \beta\left(\frac{2}{3}f_{min} + \frac{1}{3}f_{xy}\right), & \Delta f_{max} \geq \Delta f_{min} \\ \beta\left(\frac{1}{3}f_{min} + \frac{2}{3}f_{xy}\right), & \Delta f_{max} < \Delta f_{min} \end{cases} \quad (1)$$

$$g(x,y) = \begin{cases} 1, & \text{если} Z_r - f_{xy} > T_{xy} \\ 0, & \text{если} Z_r - f_{xy} \leq T_{xy}\,, \end{cases} \quad (2)$$

где β – коэффициент регуляризации;
f_{min} и f_{max} – соответственно минимальное и максимальное значения яркостей в локальной окрестности рассматриваемого пикселя;

f_{xy} – яркость текущего обрабатываемого пикселя;

Δf_{max} и Δf_{min} – модули разности соответственно f_{max} и f_{min} и значения f_{xy};

Z_r – средняя яркость пикселей в локальной окрестности рассматриваемого пикселя.

В результате по каждому фрагменту кадра будет получена бинарная маска, которая определяет наличие постороннего объекта в этом фрагменте. Полученные бинарные изображения подвергаются обработке фильтром для устранения шумовых эффектов.

Далее маски фрагментов объединяются в общую бинарную маску кадра, которая вместе с масками других кадров набора подвергается дальнейшей обработке.

Схема алгоритма обнаружения объектов на фрагментах кадра дана на рис. 4.

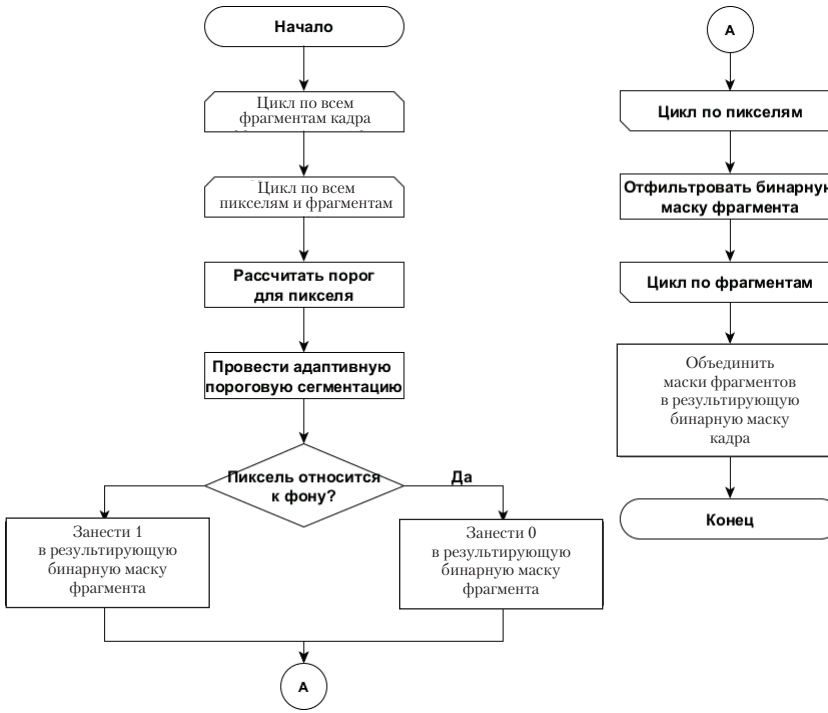


Рис. 4. Схема обнаружения объектов на фрагментах кадра

Обнаружение объектов по нескольким бинарным маскам

Информация со всех бинарных масок всех кадров обрабатываемого набора собирается в общую результирующую маску по следующему принципу. Если пиксель классифицируется как пиксель объекта на большинстве кадров набора, то в результате он заносится как пиксель объекта, в противном случае – как пиксель фона. Полученная таким образом общая бинарная маска определяет обнаруженные объекты. По ней осуществляется построение охватывающих рамок (рис. 5).

а)

б)

Рис. 5. Результаты обнаружения:
а) кадр видеопотока с заданной областью интереса;
б) результат работы метода

Результаты экспериментов

Разработанный метод был программно реализован для исследования его применимости. В качестве критериев оценки выбраны вероятности верного и ложного обнаружений, рассчитываемые по формулам (3) и (4) соответственно.

$$p = \frac{k}{k_0}, \tag{3}$$

где k – количество правильно обнаруженных объектов;
k_0 – общее число объектов.

$$p_f = \frac{1}{n}\sum_{i=1}^{n}\frac{k_{fi}}{k_{0i}}, \quad (4)$$

где k_{fi} – число ложных обнаружений при i-м детектировании;

k_{0i} – общее число обнаружений при i-м детектировании.

Также одной из целей проведения экспериментов была оценка влияния параметров метода на результат обнаружения. Метод имеет четыре основных параметра:

– количество кадров для инициализации модели фона;
– вес фона в модели;
– коэффициент регуляризации;
– размер квадратной локальной окрестности.

Количество кадров, используемых для детектирования объектов, было зафиксировано и равно 15.

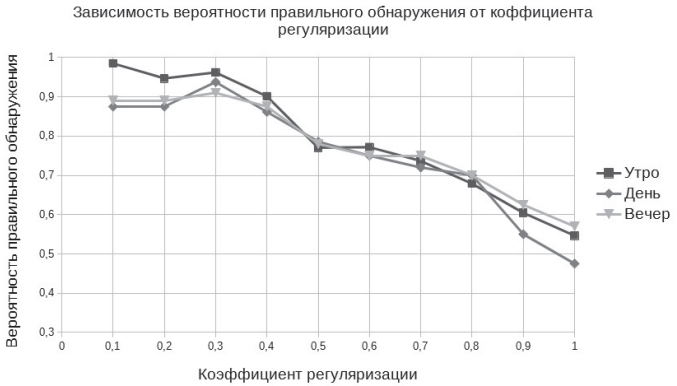
Исходные данные для исследования составили три группы из 200–250 фрагментов видео, снятых в разных временных условиях – по одному набору в разное время суток (утро, день, вечер) без осадков. Способ появления объектов в кадре не фиксировался ввиду его малой значимости для проводимого исследования.

Рис. 6. Пример кадра

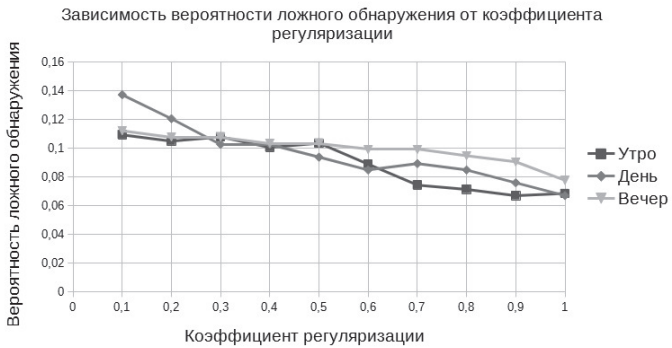
Все кадры были сняты в ходе проведения экспериментов на аэродроме Орловка совместно со специалистами МАНС (концерн «Международные аэронавигационные системы») с использованием PTZ камеры AXIS Q8685-LE (разрешение видео 1920 × 1080 пикселей, 30-кратное оптическое увеличение). В кадрах присутствовал участок ВПП и прилегающая территория (рис. 6). При проведении исследования для кадров задавалась область интереса, содержащая только ВПП. Детектирование проводилось в пределах этой области.

Для имитации мусора на ВПП было выделено 6 типов объектов:
– металлические предметы;
– пластмассовые предметы;
– предметы из резины;
– обломки покрытия ВПП;
– инструменты;
– оборудование ВПП.

По результатам исследования были получены зависимости критериев оценки качества обнаружения от значений параметров. Графики зависимостей представлены на рис. 7–10.



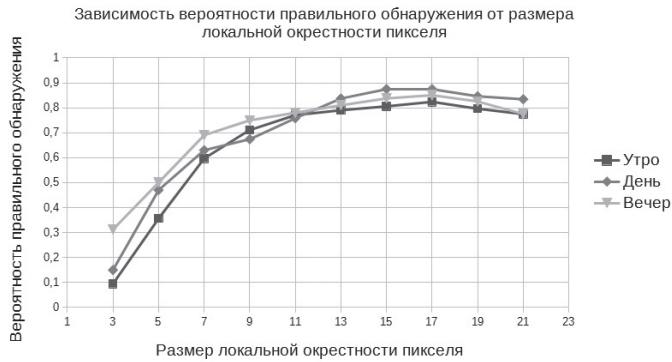
а)



б)

Рис. 7. Зависимость критериев от коэффициента регуляризации:
а) вероятность верного обнаружения;
б) вероятность ложного обнаружения

Коэффициент регуляризации прямо влияет на чувствительность обнаружения по адаптивному порогу сегментации. Полученные зависимости (рис. 7) подтверждают, что увеличение коэффициента ведет к снижению чувствительности и соответственно уменьшению вероятности верного детектирования объекта, одновременно уменьшая количество ложных срабатываний. Приоритетными являются высокие показатели верного обнаружения, поскольку наличие ложно-положительных срабатываний метода не повлечет за собой негативных последствий в отличие от пропуска объектов. В связи с этим оптимальные значения коэффициента регуляризации – 0.1–0.3.

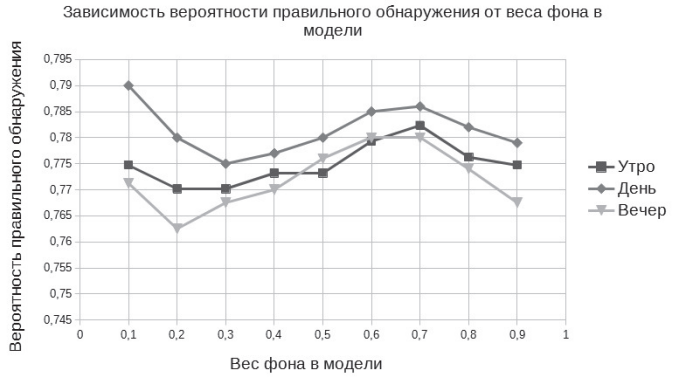


а)

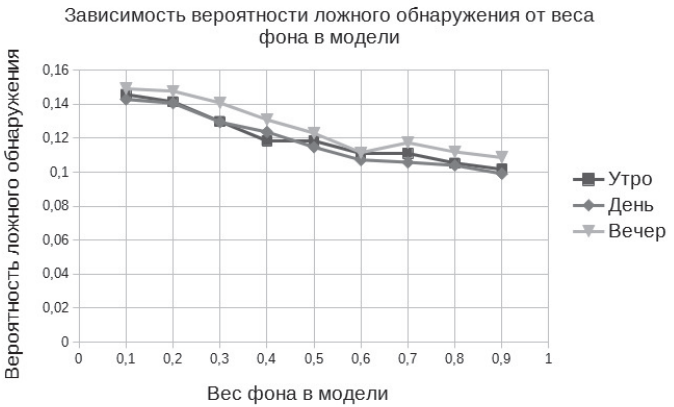
б)

Рис. 8. Зависимость критериев от размера локальной окрестности:
а) вероятность верного обнаружения;
б) вероятность ложного обнаружения

На представленном графике (рис. 8а) отчетливо заметна область, в которой вероятность верного обнаружения достигает максимальных значений. Она соответствует диапазону значений параметра 15–17 пикселей. При дальнейшем увеличении локальной окрестности качество обнаружения падает, поскольку в этом случае на расчет адаптивного порога влияет большее количество шумов.



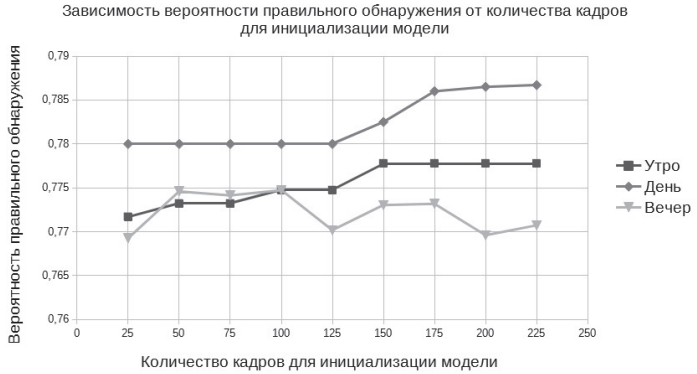
а)



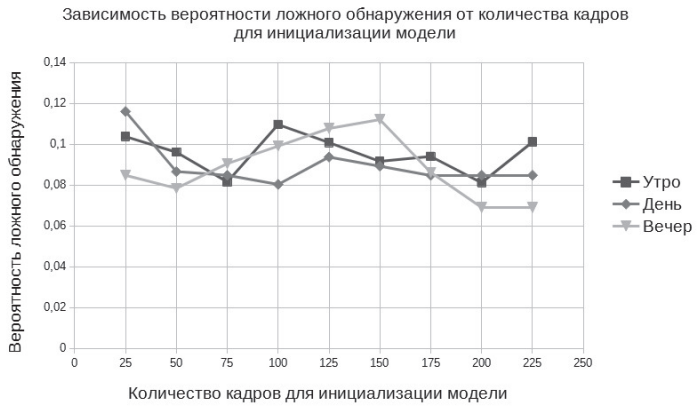
б)

Рис. 9. Зависимость критериев от веса фона в модели:
а) вероятность верного обнаружения;
б) вероятность ложного обнаружения

Исходя из результатов экспериментов, представленных на рис. 9, выделяется диапазон оптимальных значений исследуемого параметра – 0.6–0.7. При меньших значениях веса фона в модели с большей вероятностью происходят ложные детектирования, а при больших – снижается показатель корректных обнаружений.



а)



б)

Рис. 10. Зависимость критериев от количества кадров:
для инициализации модели
а) вероятность верного обнаружения;
б) вероятность ложного обнаружения

При исследовании влияния количества кадров, используемых для инициализации модели фона, на качество детектирования четкую закономерность выявить не удалось. В связи с этим целесообразно выбирать небольшие значения параметра, чтобы минимизировать время инициализации модели фона.

По итогам проведенного исследования определены оптимальные значения параметров метода для исследуемых временных условий: коэффициент регуляризации – 0,1–0,3; размер локальной окрестности – 13–17; суммарный вес фона в модели – 0,6–0,7; количество кадров для инициализации модели – 50–75. При этом показатели качества метода составляют: вероятность верного обнаружения – 85–90%, вероятность ложного обнаружения – 9–10%.

Основное влияние на работу метода оказывают параметры адаптивной пороговой сегментации – размер локальной окрестности для вычисления порога и коэффициент регуляризации.

К достоинствам разработанного метода можно отнести высокую скорость обнаружения объектов даже при реализации на одном процессоре и высокую точность определения положения объекта в кадре, а также возможность гибкой настройки чувствительности детектирования.

Заключение

Предложен метод обнаружения посторонних предметов на ВПП по видеопотоку, основанный на комбинировании статистической модели фона и адаптивной пороговой сегментации. Метод осуществляет обработку информации со статических камер и может применяться как в системах только с камерами, так и в комплексных системах в качестве оптической составляющей. Перед началом работы необходимо сформировать модель фона по набору кадров с ВПП без объектов.

Выбранные алгоритмы обеспечивают высокую скорость детектирования и детальную настройку чувствительности обнаружения.

По результатам экспериментов, проведенных на аэродроме Орловка, определены оптимальные значения параметров метода, позволяющие достичь высоких показателей качества обнаружения.

Литература

Гонсалес, Вудс 2012 – *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. М.: Техносфера, 2012.

Тропченко А.А., Тропченко А.Ю. 2015 – *Тропченко А.А., Тропченко А.Ю.* Методы вторичной обработки и распознавания изображений. СПб.: Университет ИТМО, 2015.

AERO 2001 – Foreign Object Debris and Damage Prevention [Электронный ресурс]. URL: https://www.boeing.com/commercial/aeromagazine/aero_01/textonly/s01txt.html (дата обращения 28 ноября 2020).

Dempster, Rubin, Laird 1977 – *Dempster A.P., Rubin D.B., Laird N.M.* Maximum Likelihood from Incomplete Data via the EM Algorithm // Journal of the Royal Statistical Society. Series B (Methodological). 1977. Vol. 39, no. 1. P. 1–38.

European Commission CORDIS 2018 – Advanced System for Foreign Object Debris and Bird-Aircraft Strike Avoidance [Электронный ресурс] // European Commission CORDIS 2018. URL: https://cordis.europa.eu/project/id/816435 (дата обращения 28 ноября 2020).

KaewTraKulPong, Bowden 2001 – *KaewTraKulPong P., Bowden R.* An improved adaptive background mixture model for real-time tracking with shadow detection [Электронный ресурс] // Proceedings of the 2nd European Workshop on Advanced Video Based Surveillance Systems, 2001. URL: https://www.researchgate.net/publication/2557021_An_Improved_Adaptive_Background_Mixture_Model_for_Realtime_Tracking_with_Shadow_Detection (дата обращения 28 ноября 2020).

Stauffer, Grimson 1999 – *Stauffer C., Grimson W.E.L.* Adaptive background mixture models for real-time tracking [Электронный ресурс] // Proceedings of the 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1999. URL: https://ieeexplore.ieee.org/document/784637 (дата обращения 28 ноября 2020).

U.S. Federal Aviation Administration 2009 – Airport Foreign Object Debris (FOD) Detection Equipment [Электронный ресурс]. URL: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_150_5220-24.pdf (дата обращения 28 ноября 2020).

References

AERO (2001), “Foreign Object Debris and Damage Prevention”, [Online], available at: https://www.boeing.com/commercial/aeromagazine/aero_01/textonly/s01txt.html (Accessed 28 November 2020).

Dempster, A.P., Rubin, D.B. and Laird, N.M. (1977), “Maximum Likelihood from Incomplete Data via the EM Algorithm”, *Journal of the Royal Statistical Society. Series B (Methodological)*, vol. 39, no. 1, pp. 1–38.

European Commission CORDIS (2018), "Advanced System for Foreign Object Debris and Bird-Aircraft Strike Avoidance", *European Commission CORDIS*, [Online], available at: https://cordis.europa.eu/project/id/816435 (Accessed 28 November 2020).

Gonzalez, R. and Woods, R. (2012), *Tsifrovaya obrabotka izobrazhenii* [Digital image processing], Tekhnosfera, Moscow, Russia.

KaewTraKulPong, P. and Bowden, R. (2001), "An improved adaptive background mixture model for real-time tracking with shadow detection", *Proceedings of the 2nd European Workshop on Advanced Video Based Surveillance Systems*, [Online], available at: https://www.researchgate.net/publication/2557021_An_Improved_Adaptive_Background_Mixture_Model_for_Realtime_Tracking_with_Shadow_Detection (Accessed 28 November 2020).

Stauffer, C. and Grimson, W.E.L., (1999), "Adaptive background mixture models for real-time tracking", *Proceedings of the 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, [Online], available at: https://ieeexplore.ieee.org/document/784637 (Accessed 28 November 2020).

Tropchenko A.A. and Tropchenko A.Yu. (2009), *Metody vtorichnoi obrabotki i raspoznavaniya izobrazhenii* [Image post-processing and image recognition methods], Saint-Petersburg State University of Information Technologies Mechanics and Optics, Saint-Petersburg, Russia.

U.S. Federal Aviation Administration (2009), "Airport Foreign Object Debris (FOD) Detection Equipment", [Online], available at: https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_150_5220-24.pdf (Accessed 28 November 2020).

Информация об авторах

Никита Е. Шоркин, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; shorkin.nikita29@yandex.ru

Кирилл Л. Тассов, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; ktassov@policesoft.ru

Information about the authors

Nikita E. Shorkin, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; shorkin.nikita29@yandex.ru

Kirill L. Tassov, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; ktassov@policesoft.ru

УДК 004.056
DOI: 10.28995/2686-679X-2022-1-63-82

Применение генетических алгоритмов в криптографии

Иван Е. Чернов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, chernov-ivan.1997@yandex.ru

Андрей В. Куров
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, avkur7@mail.ru

Аннотация. В настоящее время при разработке компьютерных технологий, обеспечивающих информационную безопасность и защиту информации, широкое применение находят криптографические методы защиты. Основными задачами в криптографии являются разработка новых способов шифрования, сложных для вскрытия, и существующих шифров. Для решения этой задачи, относящейся к классу NP-полных, в последние годы применяются алгоритмы, основанные на природных системах. К ним относятся генетические алгоритмы (ГА), эволюционные методы, алгоритмы роевого интеллекта. В моделях и алгоритмах эволюционных вычислений ключевым элементом является построение начальной модели и правил, по которым она может изменяться (эволюционировать). В течение последних лет были предложены разнообразные схемы эволюционных вычислений, в том числе генетический алгоритм, генетическое программирование, эволюционное программирование, эволюционные стратегии. В работе рассматриваются существующие методы криптографии, базовые понятия и методы современной криптографии, понятие генетического алгоритма, универсальной хеш-функции, а также метод визуализации хеша и построенный на нем генетический алгоритм хеширования. Был реализован генетический алгоритм на языке Golang, модифицированный под текущую задачу нахождения оптимальной хеш-функции. Приводится подробное описание каждого этапа выполнения алгоритма. Также в рамках данной работы было проведено исследование, демонстрирующее работу самого генетического алгоритма и генетического алгоритма хеширования,

оценивающее сходимость генетического алгоритма в зависимости от входных данных, и определяющее возможное направление дальнейших исследований.

Ключевые слова: генетический алгоритм, муравьиный алгоритм, универсальная хеш-функция, цикл

Для цитирования: Чернов И.Е., Куров А.В. Применение генетических алгоритмов в криптографии // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 63–82. DOI: 10.28995/2686-679X-2022-1-63-82

Application of genetic algorithms in cryptography

Ivan E. Chernov
Bauman Moscow State Technical University, Moscow, Russia,
chernov-ivan.1997@yandex.ru

Andrey V. Kurov
Bauman Moscow State Technical University, Moscow, Russia,
avkur7@mail.ru

Abstract. Currently in the development of computer technologies that ensure information security and information protection, cryptographic methods of protection are widely used. The main tasks in cryptography are the development of new encryption features, difficult to break and repetitive ciphers. To solve that problem, falling into the class of NP-complete ones, algorithms based on natural principles have been used in recent years. These include genetic algorithms (GA), evolutionary methods, swarm intelligence algorithms. In models and algorithms of evolutionary computations, the construction of basic models and rules is implemented, according to which it can change (evolve). In recent years, evolutionary computing schemes have been proposed, including the genetic algorithm, genetic programming, evolutionary programming, and evolutionary strategies. The paper discusses the existing cryptography methods, basic concepts and methods of modern cryptography, the notion of a genetic algorithm, a universal hash function, as well as a hash detection method and a genetic hashing algorithm built on it. A genetic algorithm was implemented in the Golang language, modified for the current problem of finding the optimal hash functions. A detailed description of each stage of the algorithm execution is given. Also, within the framework of the research, a study of the function of the genetic algorithm itself and the genetic hashing algorithm was carried out, evaluating the convergence of the genetic algorithm depending on the input data, and evaluating the possible direction of further research.

Keywords: genetic algorithm, ant algorithm, universal hash function, cycle

For citation: Chernov, I.E. and Kurov, A.V. (2022), “Application of genetic algorithms in cryptography”, *RSUH/RGGU Bulletin. “Information Science. Information Security. Mathematics” Series,* no. 1, pp. 63–82, DOI: 10.28995/2686-679X-2022-1-63-82

Введение

Информация – это один из столпов, на котором стоит современное общество. В эпоху Всемирной паутины доступ к информации стал легким и быстрым как для одного человека, так и для крупной корпорации. Но развитие легкости и скорости доступа к данным в компьютерных сетях неизбежно привело к глобальной проблеме – необходимости обеспечивать безопасность информации. При этом основной задачей является защита

1) информации от неавторизованного доступа и ее изменения,
2) сетей и сервисов от неавторизованного доступа,
3) от сетевых атак (DoS-атак, сканирования портов, атак-вторжений).

При разработке информационных технологий, обеспечивающих конфиденциальность и целостность информации, широко применяются методы криптографии, предполагающие создание новых способов шифрования и дешифрования таким образом, чтобы снизить возможность взлома до минимума. В последнее время для решения поставленных задач стали применяться различные виды алгоритмов.

Биоинспирированные и генетические алгоритмы

Биоинспирированные алгоритмы – это алгоритмы оптимизации, основанные на элементах живой природы для моделирования каких-либо явлений и поиска наиболее эффективных решений [Марков, Цирлов 2015]. К ним относятся:

1. Эволюционные методы.
2. Методы «роевого» интеллекта.
3. Методы, имитирующие физические процессы.

В моделях и алгоритмах эволюционных вычислений ключевым элементом является построение начальных моделей и правил, в соответствии с которыми они могут выполняться.

Генетические алгоритмы (ГА) [Goyat 2012] представляют собой стохастические и эвристические оптимизационные методы, предложенные Холландом, они основываются на идее эволюции с помощью естественного отбора, выдвинутой Дарвином. Работа этих алгоритмов аналогична природному естественному отбору, в них используются такие же методы оптимизации, как и в естественной эволюции, а именно наследование, отбор, скрещивание и мутации.

Стандартные операторы генетических алгоритмов:

1. Селекция – осуществляет отбор хромосом в соответствии со значениями их функции приспособленности. Из самых популярных операторов селекции можно выделить турнир и рулетку.

2. Скрещивание – осуществляет обмен частями хромосом между хромосомами в популяции. Может быть одноточечным и многоточечным.

3. Мутация – случайно изменяет части хромосом.

Псевдокод генетического алгоритма в его традиционной форме [Штовба 2003].

```
НАЧАЛО /* генетический алгоритм */
    Создать начальную популяцию
    Оценить приспособленность каждой особи
    останов := FALSE
    ПОКА НЕ останов ВЫПОЛНЯТЬ
    НАЧАЛО /* создать популяцию нового поколения */
        ПОВТОРИТЬ (размер_популяции/2) РАЗ
        НАЧАЛО /* цикл воспроизводства */
        Выбрать две особи с высокой приспособленностью из
        предыдущего поколения для скрещивания
        Скрестить выбранные особи и получить двух потомков
        Оценить приспособленности потомков
        Поместить потомков в новое поколение
      КОНЕЦ
      ЕСЛИ популяция сошлась ТО останов := TRUE
    КОНЕЦ
КОНЕЦ
```

ГА относят к области мягких вычислений [Naik P., Naik G. 2014]. Термин «мягкие вычисления» введен Лотфи Заде в 1994 году. Это понятие объединяет такие области, как нечеткая логика, нейронные сети, вероятностные рассуждения, сети доверия и эволюционные алгоритмы, которые дополняют друг друга и используются в различных комбинациях или самостоятельно для создания гибридных интеллектуальных систем.

Отличительной особенностью применения генетического алгоритма в криптографии является возможность непосредственного

указания самого метода шифрования и дешифрования как целевой функции для расчета пригодности ключа, полученного путем реализации генетических операций. Сам процесс определения ключа при использовании ГА при этом зависит больше от используемого метода, задача которого – обеспечить разнообразие генерации ключей, чем от сложности шифрующих преобразований. Это говорит об актуальности исследования применения генетических алгоритмов к решению задач криптоанализа.

Как и любой эвристический алгоритм, ГА содержит в себе серьезный недостаток [Perrig, Song 1999]: он не дает гарантии нахождения единственного правильного решения для данной задачи. Любое найденное решение считается хорошим только в сравнении с другими решениями, найденными алгоритмом. Поэтому полученное решение можно считать оптимальным, но не самым лучшим, приблизиться к этому решению можно, только запустив алгоритм многократно, и среди вариантов, которые выдает ГА, выбрать самый лучший. Кроме того, единственного правильного решения для задачи может и вовсе не быть. Вследствие этого необходимо указать ГА критерий останова – условие, после которого ГА остановит свою работу. Это может быть ограничение времени выполнения алгоритма, ограничение числа прогонов или ненахождение алгоритмом особей, лучше предыдущих, в течение определенного числа поколений.

В противовес такому недостатку генетического алгоритма, как «слепой» поиск, в качестве его альтернативы представляет интерес метод роевого интеллекта, называемый муравьиным алгоритмом.

Муравьиный алгоритм – алгоритм оптимизации, имитирующий самоорганизацию муравьиной колонии. Данный алгоритм представляет собой вероятностную жадную эвристику, где вероятности увеличиваются исходя из информации о качестве решения, полученной от предыдущих решений.

Основной идеей муравьиного алгоритма является моделирование поведения муравьев, связанного с их способностью быстро находить кратчайший путь от муравейника к источнику пищи и адаптироваться к изменяющимся условиям, находя новый кратчайший путь. При своем движении муравей метит путь феромоном, и эта информация используется другими муравьями для выбора пути. Это элементарное правило поведения и определяет способность муравьев находить новый путь, если старый оказывается недоступным.

Данный алгоритм преимущественно используется для таких задач, как задача коммивояжера и другие задачи поиска маршрута на графах.

Обобщенный вид муравьиного алгоритма выглядит следующим образом.

Пока (условия выхода не выполнены)

1. Создаем муравьев
2. Ищем решения
3. Обновляем феромон

Рассмотрим каждый шаг более подробно.

Шаг 1. Создаем муравьев: определяем стартовую точку, откуда муравей начинает путь. Стартовая точка определяется условием задачи. Также задаем начальный уровень феромона для гарантии ненулевого значения вероятности перехода в следующую вершину.

Шаг 2. Ищем решения: вероятность перехода из вершины I в вершину j рассчитывается по следующей формуле

$$\begin{cases} P_{ij,k}(t) = \dfrac{\left[\tau_{ij}(t)\right]^{\alpha} \cdot \left[\eta_{ij}\right]^{\beta}}{\sum\limits_{l \in J_{i,k}} \left[\tau_{il}(t)\right]^{\alpha} \cdot \left[\eta_{il}\right]^{\beta}}, \text{ если } j \in J_{i,k}, \\ P_{ij,k}(t) = 0, \text{ если } j \notin J_{i,k}, \end{cases} \quad (1)$$

где $\tau_{ij}(\tau)$ – уровень феромона;

η_{ij} – эвристическое расстояние;

α, β – константные параметры.

Необходимо найти компромисс между этими величинами, он находится экспериментально.

Шаг 3. Обновляем феромон:

$$\tau_{ij}(t+1) = (1-p) \cdot \tau_{ij}(t) + \Delta\tau_{ij}(t), \quad (2)$$

где p – интенсивность испарения.

Большим недостатком муравьиного алгоритма является высокая, по сравнению с генетическим алгоритмом, сложность настройки параметров. Для муравьиного алгоритма параметры можно подобрать только экспериментально. Кроме того, в связи с тем что муравьиный алгоритм опирается на память всей колонии вместо памяти только о предыдущем поколении (как в ГА), он требует больших вычислительных ресурсов и проигрывает в скорости работы генетическому алгоритму.

На основе приведенных выше достоинств и недостатков можно сделать вывод, что муравьиный алгоритм – не лучшее решение для задач криптографии, поэтому далее будет рассматриваться только генетический алгоритм.

Универсальные хеш-функции

Хеш-функция – функция преобразования данных произвольного размера в битовую строку заранее определенного размера. Само преобразование с помощью хеш-функции называется хешированием. Данный метод применяется для таких задач, как сохранение паролей в системах защиты в виде хеш-кода и создание электронной подписи.

В более подробном описании хеш-функция [Журкович 2018] – это сопоставление целых чисел, называемых ключами, находящихся в некотором диапазоне [0, M-1], к целым числам в [0, N-1] (называемых N сегментами), известных как хеш. Множество H таких хеш-функций называется универсальным, если для каждой пары целых чисел j и k в диапазоне [0, M-1] и для каждой хеш-функции h, выбранной из множества H случайным образом, выполняется условие (2):

$$\Pr(h(j) = h(k)) \leq \frac{1}{N}, \tag{3}$$

где Pr (E) – вероятность события E.

Полезность данного набора хеш-функций выходит из низкого ожидаемого количества конфликтов между хеш-кодом j и ключами, уже находящимися в хеш-таблице. При использовании любой функции из множества H ожидаемое количество конфликтов будет принимать значение не выше, чем текущий коэффициент нагрузки таблицы, а именно $\frac{n}{N}$, где n – количество хеш-ключей.

Рассмотрим набор хеш-функций следующего вида (3):

$$h_{a,b}(k) = ((ak + b) \bmod p) \bmod N, \tag{4}$$

где p – простое число, $M \leqslant p < 2M$;
a, b – пара целых чисел, полученных случайным образом;
$0 < a < p$, $0 \leqslant b < p$.

Применение генетического алгоритма к универсальной хеш-функции

Рассмотрим элементы генетического алгоритма для выявления оптимальных значений a и b.

1. Хромосома. Так как a и b являются 32-битными целыми числами, хромосома для ГА будет выглядеть как одномерный массив из 64 бит, объединяющий a и b.

2. Популяция. Популяция представляет из себя двумерный массив хромосом P x 64, где P – размер популяции.

3. p_Array. Данный массив содержит простые числа p для каждой пары a и b. Размер массива равен размеру популяции соответственно.

4. Хеш-код. Представляет из себя массив, содержащий произвольное распределение ключей, которые необходимо хешировать.

5. Фитнес-функция. Задача алгоритма – создать хеш-функцию с минимальным количеством коллизий и гарантией заполнения практически всех сегментов, обеспечивая коэффициент нагрузки, близкий к единице. Каждая комбинация a, b и p, обозначенная хромосомой, порождает хеш-функцию. Далее эта хеш-функция применяется ко всем ключам, подлежащим хешированию, и полученные значения анализируются на наличие коллизий и количество заполненных сегментов. Приспособленность каждой хромосомы зависит от коэффициента нагрузки и коллизий и рассчитывается следующим образом:

$$Fitness = \frac{n_f}{n_c + 1}, \quad (5)$$

где n_f – количество заполненных сегментов;
n_c – число коллизий с использованием комбинации a и b в хеш-функции.

Основные шаги алгоритма

Шаг 1. Сжатие произвольного распределения ключей, подлежащих хешированию, в диапазон [0, M-1] путем вычитания из каждого ключа минимального значения ключа в распределении. Таким образом:

$$M = (maxkey - minkey) + 1.$$

Шаг 2. Получение всех возможных значений, соответствующих p:

$$M \leqslant p < 2M.$$

Шаг 3. Генерация начальной популяции. Каждая хромосома создается случайным выбором p из возможных значений. Далее для a и b случайным образом назначается 64-битный шаблон так, чтобы выполнялись условия:

$$0 < a < p,$$
$$0 \leqslant b < p.$$

Затем значение p сохраняется в p_Array с индексом, равным индексу хромосомы.

Шаг 4. Подсчет приспособленности каждой хромосомы путем построения хеш-функции из (4), используя пару a и b хромосомы, а также соответствующее ей значение p. Данная хеш-функция применяется ко всем ключам, которые необходимо захешировать. С помощью (5) производится расчет приспособленности.

Шаг 5. Реализация кроссовера только на той хромосоме, которая содержит a и b. Если вновь созданная хромосома имеет значения a и b, не удовлетворяющие условиям $0 < a < p$, $0 \leqslant b < p$, то значение p переназначается путем поиска такого p из p_Array, чтобы данные условия были выполнены. При этом берется первое попавшееся значение. Если p найдено, то оно назначается в p_Array для текущих a и b. В противном случае кроссовер аннулируется.

Шаг 6. В случае мутации применяется тот же алгоритм действий для коррекции p (см. шаг 5).

Шаг 7. Замена популяции созданным множеством.

Шаг 8. Повторять шаг 4 – шаг 7 для желаемого количества популяций. Лучший индивидуум, получившийся в результате, и будет желаемой хеш-функцией.

Результаты работы алгоритма

Для проведения исследований был реализован генетический алгоритм на языке Golang, модифицированный под текущую задачу нахождения оптимальной хеш-функции, представленный в листинге 1.

Листинг 1

```
package main
import (“fmt”; “math”; “math/rand”; “sort”)

type UnitSort []IUnit
func (us UnitSort) Len() int { return len(us) }
func (us UnitSort) Less(i, j int) bool { return (us)[i].GetFitness() > (us)[j].
GetFitness()}
func (us UnitSort) Swap(i, j int) { (us)[i], (us)[j] = (us)[j], (us)[i] }
type IUnit interface {GetCromosomes() []int; SetCromosomes([]int);
```

```
GetFitness() float64; SetFitness(fitness float64)}
type BaseUnit struct { cromo []int; fitness float64 }
func (bi *BaseUnit) GetCromosomes() []int { return bi.cromo }
func (bi *BaseUnit) SetCromosomes(cromo []int) { bi.cromo = cromo }
func (bi *BaseUnit) GetFitness() float64 { return bi.fitness }
func (bi *BaseUnit) SetFitness(fitness float64) { bi.fitness = fitness }

func main() {
 sel := Panmixia{}
 ga := GenAlgo{
   MaxIteration: 4, Generator: &Generator{20},
    Crossover: &UniformCrossover{Probability: 0.5, ProbabilityFunc: rand.
Float64},
    Mutate:    &OneDotMutatation{Probability: 0.5, ProbabilityFunc: rand.
Float64}, Schema: &Truncation{},
   Fitness: func(unit IUnit) float64 {
    cr := unit.GetCromosomes(); fitness := 0.0; x := 0; y := 0
     for i := 0; i < len(cr)/2; i++ { x += cr[i] }; for i := len(cr) / 2; i < len(cr);
i++ { y += cr[i] }
    fitness = math.Cos(float64(x)) + math.Cos(float64(y)); return fitness
   }, Select: &sel,
 }
 ga.OnBegin = func() { fmt.Print(ga.Populaion[0]) }
 ga.Init(20); ga.Simulation()
}

// ICrossover Operator Interface The Cross() function takes two parent
units and returns two descendant units
//Speed determines how many descendant units will be created
type ICrossover interface { Cross(A, B IUnit) (C, D IUnit); GetSpeed()
float64 }

// UniformCrossover Uniform Crossover. Probability determines the
probability that the gene of the first parent
// unit will be selected. F. e. if x < Probability, unit A gene is selected,
otherwise unit B gene is selected
// ProbabilityFunc sets the distribution of a random variable, so it can be
changed to fit your needs
type UniformCrossover struct { Probability float64; ProbabilityFunc func()
float64 }

func (uc *UniformCrossover) GetSpeed() float64 { return uc.Probability }
```

```
func (uc *UniformCrossover) Cross(A, B IUnit) (C, D IUnit) {
  parentA := A.GetCromosomes(); parentB := B.GetCromosomes(); var CA,
CB []int
  for i := 0; i < len(parentA); i++ {
    pA := uc.ProbabilityFunc(); pB := uc.ProbabilityFunc()
      if pA < uc.Probability { CA = append(CA, parentA[i]) } else { CA =
append(CA, parentB[i]) }
      if pB < uc.Probability { CB = append(CB, parentB[i]) } else { CB =
append(CB, parentA[i]) }
  }
  childA := BaseUnit{}; childB := BaseUnit{}; childA.SetCromosomes(CA);
childB.SetCromosomes(CB)
  return &childA, &childB
}

// IGenerator Generator Interface. Generator is used to form null generation
type IGenerator interface { Generate() []int }

// Generator Base Generator. Generator is used to form null generation.
Creates units with fixed-length
// chromosomes, each gene is either one or zero. Length depends on Len
type Generator struct { Len int }

func (g *Generator) Generate() []int {
            var cromo []int; for i := 0; i < g.Len; i++ { j := rand.Intn(2); cromo =
append(cromo, j) }; return cromo
}

// GenAlgo The main structure of the library. reproduction and population
are
separated for some selection schema
type GenAlgo struct {
  pSize       int // pSize is the size of a null population
  Populaion    []IUnit // population[] is current population
   reproduction []IUnit // reproduction[] is population of descendants and
mutants
   totalFitness float64 // totalFitness is sum of fitness of both parents and
descendants and mutants
  iteration    int // iteration is current population number
  MaxIteration int // maxIteration is max iteration that could be reached
  Generator IGenerator // Generator is chosen IGenerator implementation
  Select    ISelector // Select is chosen ISelect implementation
  Crossover ICrossover // Crossover is chosen ICrossover implementation
  Mutate    IMutate // Mutate is chosen IMutator implementation
```

```
 Schema    ISchema // Schema for create population
  Fitness func(IUnit) float64 //Fitness fitness operator (is function that determines unit's fitness)
 OnBegin func() //OnBegin what is done at the beginning of each iteration
 OnEnd func() //OnEnd what is done at the end of each iteration
}

func (ga *GenAlgo) nullPopulation() {
 ga.iteration = 0; var population []IUnit
 for i := 0; i < ga.pSize; i++ {
p:=BaseUnit{};cromo:=ga.Generator.Generate();p.SetCromosomes(cromo);
f := ga.Fitness(&p)
  p.SetFitness(f); ga.totalFitness += f; population = append(population, &p)
 }
 ga.Populaion = population
}

func (ga *GenAlgo) Init(populationSize int) { ga.pSize = populationSize; ga.nullPopulation() }
func (ga *GenAlgo) ExitOn() bool { return ga.MaxIteration == ga.iteration }

func (ga *GenAlgo) NextGeneration() {
 ga.iteration += 1; var repro []IUnit; N := int(float64(ga.pSize) * ga.Crossover.GetSpeed())
 for i := 0; i <= N; i += 2 {
  A, B := ga.Select.Mater(ga.Populaion); C, D := ga.Crossover.Cross(A, B)
      C.SetFitness(ga.Fitness(C)); D.SetFitness(ga.Fitness(D)); repro = append(repro, C, D)
 }; M := int(float64(ga.pSize) * ga.Mutate.GetSpeed())
 for i := 0; i <= M; i += 2 {
      A := ga.Select.Mutator(ga.Populaion); B := ga.Select.Mutator(ga.Populaion)
  C := ga.Mutate.Mutate(A); D := ga.Mutate.Mutate(B)
      C.SetFitness(ga.Fitness(C)); D.SetFitness(ga.Fitness(D)); repro = append(repro, C, D)
 }
 ga.reproduction = repro
}

func (ga *GenAlgo) Simulation() {
 for !ga.ExitOn() {
  if ga.OnBegin != nil { ga.OnBegin() }
    ga.NextGeneration(); ga.Populaion = ga.Schema.Create(ga.Populaion, ga.reproduction)
```

```
    if ga.OnEnd != nil { ga.OnEnd() }
  }
}

type IMutate interface { Mutate(individuals IUnit) (mutant IUnit);
GetSpeed() float64 }

type OneDotMutatation struct { Probability float64; ProbabilityFunc func()
float64 }
func (odm *OneDotMutatation) Mutate(parent IUnit) (child IUnit) {
    cromo := parent.GetCromosomes(); r := rand.Intn(len(cromo)); n :=
cromo[r]
  if n == 0 { n++; cromo[r] = n } else { cromo[r] = 0 }
  child = &BaseUnit{}; child.SetCromosomes(cromo); return child
}
func (odm *OneDotMutatation) GetSpeed() float64 { return odm.
Probability }

// ISchema Interface for new Generation selection Schema
type ISchema interface { Create(parents, child []IUnit) (generation []IUnit)
}

type Truncation struct{}
func (t *Truncation) Create(parents, child []IUnit) (generation []IUnit) {
   size := len(parents); var all []IUnit; all = append(all, parents...); all =
append(all, child...)
  sort.Sort(UnitSort(all)); all = all[:size]; return all
}

type ISelector interface { Mater([]IUnit) (A, B IUnit); Mutator([]IUnit)
(A IUnit) }

type Panmixia struct{}
func (s *Panmixia) Mater(population []IUnit) (A, B IUnit) {
   size := len(population); i := rand.Intn(size); j := rand.Intn(size); return
population[i], population[j]
}
func (s *Panmixia) Mutator(population []IUnit) (A IUnit) {
  size := len(population); i := rand.Intn(size); return population[i]
}
```

Программа выполнялась несколько раз с различными входными распределениями. Распределения включали целые числа, полученные случайным образом с использованием однородной случайной величины в диапазоне (0, 1), умноженной на требуемый диапазон. Полученный результат округлялся до целого числа. Из-за случайного характера входных распределений внутри них возникали коллизии при генерации. Результаты расчетов приведены в табл. 1.

Численность популяции была зафиксирована на уровне 50, число поколений равнялось 30, вероятность мутации – 0.01, вероятность кроссовера – 0.8.

Таблица 1

№	Диапазон ввода	Кроссовер	Мутация	n	N	Число исходных коллизий	n_c	n_f	p	a	b
1	0-10	Одноточ.	Многоточ	10	10	0	0	10	11	3	2
2	0-500	Одноточ.	Многоточ	10	11	1	4	6	701	67	452
3	0-600	Одноточ.	Многоточ	20	23	2	2	18	1013	626	635
4	0-100	Одноточ.	Одноточ.	100	100	0	0	100	179	109	114
5	0-50000	Одноточ.	Многоточ	100	101	8	21	79	98869	54339	35059
6	0-1000	Одноточ.	Многоточ	500	499	0	1	499	1823	747	5811
7	0-50000	Одноточ.	Многоточ	500	499	37	108	392	69313	46631	9950
8	$5*10^4$-$6*10^4$	Одноточ.	Многоточ	10000	10000	0	0	10000	14153	9347	517
9	$2*10^4$-$5*10^4$	Одноточ.	Многоточ	10000	10000	0	0	10000	57203	25869	37769
10	0-50000	Одноточ.	Многоточ.	10000	10000	911	2397	6692	79063	33068	31178

По результатам работы алгоритма при заданных условиях можно сделать следующие выводы:

1. Во всех случаях множественные мутации давали лучший результат при меньшем числе поколений по сравнению с одно- или двухточечными мутациями. Это происходит потому, что ГА удается различить объекты, закодированные в одной хромосоме. Также было обнаружено, что во всех случаях наилучшим образом показывает себя одноточечный кроссовер.

2. Сходимость алгоритма при данном подходе была в пределах 7–8 поколений в худшем случае.

3. Для каждого входного распределения, где все ключи являются уникальными, количество ключей равно количеству сегментов, а диапазон значений (при рассмотрении в виде [0, M-1]) совпадает с [0, N-1], ГА создает хеш-функцию, дающую нулевые коллизии, то есть, наилучшую. В тех случаях, когда входные распределения

имели исходные коллизии, развитая ГА хеш-функция не могла уменьшить их число вследствие повторяющихся ключей во входном распределении.

4. В некоторых случаях, когда диапазон распределения был большим и не совпадал с [0, N-1], было обнаружено большое количество коллизий. Но оно значительно уменьшилось при изменении N на простое число, ближайшее к N (например, если N изначально равно 500, то изменение значения N на 499 привело к лучшему результату).

Визуализация хеша

Визуализация хеша [Требухин 2017] – это метод, в котором изображения генерируются с использованием бинарных деревьев. Каждый из узлов дерева представляет собой математическую операцию, назначенную случайным образом. Набор операций представляет из себя сложение, вычитание, умножение, деление, а каждый лист узла – случайное число. Дерево строится, и полученное значение присваивается пикселю.

Алгоритм визуализации хеша должен обладать следующими свойствами:

1. Фиксированное выделение памяти.
2. Простота вычислений.
3. Низкая стоимость алгоритма.

Требования к получаемому изображению:

1. Отсутствие постоянного цвета на изображении.
2. Отсутствие правильных форм на изображении (линии, круги, квадраты и т.д).
3. Изображение должно быть трудным для словесного описания людьми.

Генетический алгоритм хеширования

Объединение метода визуализации хеша и генетического алгоритма называется генетическим алгоритмом хеширования. Учитывая порядок выполнения генетического алгоритма, описанный выше, основные шаги генетического алгоритма хеширования можно описать следующим образом:

Шаг 1. Инициализация в ГА числа хромосом и поколений, минимальной и максимальной длины дерева.

Шаг 2. Генерация количества хромосом, которое было указано в шаге 1.

Шаг 3. Построение дерева:

а. Создание ряда узлов исходя из минимального и максимального размера дерева.

б. Назначение случайным образом операции каждому созданному узлу.

в. В случае, если узел является листом – присвоить ему значение, являющееся координатой по оси X или Y, либо значением цвета в модели RGB.

Шаг 4. Проведение следующих операций над поколением:

а. Оценка приспособленности для каждой хромосомы.

б. Селекция пары хромосом при помощи рулетки. При этом хромосомы с более высокой приспособленностью имеют более высокую вероятность быть выбранными. Кроссовер выполняется переключением одного дочернего элемента от каждого корня на другой.

Шаг 5. После того как число поколений достигло максимального значения, выбирается хромосома с наивысшей приспособленностью.

Каждой хромосоме присваивается свое значение приспособленности, рассчитываемое на основе алгоритма, шаги которого рассмотрены далее:

Шаг 1. Из каждой хромосомы (дерева) генерируется изображение в соответствии с цветовой моделью RGB.

Шаг 2. Для этого изображения вычисляется преобразование Фурье, которое создает новое изображение.

Шаг 3. Из полученного изображения создаются два новых изображения: изображение, представляющее оттенок, и изображение, представляющее интенсивность.

Шаг 4. Данные изображения масштабируются и преобразуются в двоичные.

Шаг 5. Для расчета общей приспособленности необходимо получить значение субподготовки для изображений оттенка и интенсивности. Данные субзначения вычисляются путем нахождения радиуса белой области каждого изображения. Радиус рассчитывается следующим образом:

а. Находится центральная точка изображения. В данном исследовании размер изображения 256×256, а координаты центра будут равны 128 и 128.

б. Предполагается, что радиус изначально равен 128/2 или 64.

в. Выбираются 100 точек на окружности четверти круга этого радиуса.

г. Если в данной области белых точек больше, чем черных (белых точек больше 50), то круг с этим радиусом является белой областью изображения. Следовательно, добавляются 32 (64/2) к радиусу; радиус белой области становится 96. Если белых точек окажется меньше на круге радиусом 64, то он находится вне белой области и из 64 вычитается 32; радиус становится 32.

д. Повторяются пункты В и Г в получившейся области, при этом добавляются к новому радиусу или вычитаются из него значения (32, 16, 8, 4, 2, 1). Так находится реальный радиус белой области на изображении.

Уравнение (6) дает окончательную протестированную функцию для расчета значения приспособленности:

$$Fitness = \begin{cases} 0 & , radius < 30\% \\ \dfrac{\left(\frac{1}{0.47-0.24}\right) * (r - 0.24 * maxR)}{127} & , 30\% < radius < 60\% \\ 100 & , 60\% < radius < 70\% \\ \dfrac{\left(\frac{1a}{1.3-0.55}\right) * (1.3 * maxR - r)}{127} & , 70\% < radius < 128\% \end{cases} \quad (6)$$

Рассмотрим пример: реальный радиус белой области равен 77. Начинаем с radius = 64.

Тест 1: пройден, добавляем 32, radius = 96

Тест 2: не пройден, вычитаем 16, radius = 80

Тест 3: не пройден, вычитаем 8, radius = 72

Тест 4: пройден, добавляем 4, radius = 76

Тест 5: пройден, добавляем 2, radius = 78

Тест 6: не пройден, вычитаем 1, radius = 77

Пример изображения и два его преобразования даны на рис. 1, где левое преобразование Фурье отклоняется, а правое принимается. Такие изображения обладают высокой степенью безопасности [Saleh, Eddeen, Saadeh 2014], а потому подходят для скрытия информации.

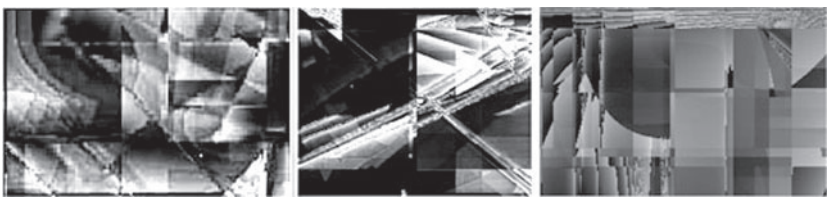


Рис. 1. Результаты генетического алгоритма хеширования со значениями приспособленности 8, 16, 32

На рис. 2 показаны некоторые изображения, созданные с помощью генетического алгоритма хеширования с использованием функции (6) расчета значения приспособленности. Значения приспособленности 27, 83 и 100 соответственно.

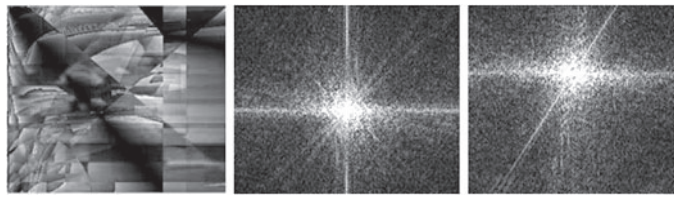


Рис. 2. Результаты генетического алгоритма хеширования со значениями приспособленности 4, 2, 1

Помимо этого, сложность генетического алгоритма хеширования равна O (Log(n)), что меньше, чем сложность обычного алгоритма визуализации хеша $O(n^2)$. Из этого следует его более высокая производительность. Также установлено, что изображения, полученные с помощью генетического алгоритма хеширования, по сравнению с обычным алгоритмом визуализации хеша, более надежны, ибо они сложнее и менее регулярны. С другой стороны, итоговое количество коллизий в обоих алгоритмах различается незначительно, следовательно, коллизии зависят от характера и конструкции хеш-функций.

Заключение

Данная работа демонстрирует, каким образом генетический алгоритм может быть применен в криптографии для шифрования и дешифрования данных. Генетические алгоритмы хорошо себя зарекомендовали и удачно применялись в различных научных статьях для решения задач [Safdari, Joshi 2009]. Использование генетического алгоритма для хеш-функций позволяет получить метод шифрования данных, крайне сложный для взлома, особенно учитывая влияние на него фактора случайности. С помощью проведенного исследования были сделаны выводы о закономерности между входными данными алгоритма и его сходимостью.

Приведенный метод перспективен для использования в криптографии тем, что при своей защищенности он очень производителен.

Литература

Журкович 2018 – *Журкович Я.* Генетические алгоритмы // Center of Scientific Cooperation “Interactive plus”. 2018. № 1. С. 121–130.

Марков, Цирлов 2015 – *Марков А.С., Цирлов В.Л.* Основы криптографии: подготовка к cissp // Вопросы кибербезопасности. 2015. № 1. С. 60–72.

Требухин 2017 – *Требухин А.В.* Методы решения оптимизационных задач с использованием биоинспирированных алгоритмов // Молодой исследователь Дона. 2017. № 1. С. 15–18.

Штовба 2003 – *Штовба С.Д.* Муравьиные алгоритмы // Exponenta Pro. Математика в приложениях. 2003. № 4. С. 70–75.

Goyat 2012 – *Goyat S.* Cryptography Using Genetic Algorithms (GAs) // IOSR Journal of Computer Engineering. 2012. № 1. P. 6–8.

Naik P., Naik G. 2014 – *Naik P., Naik G.* Asymmetric Key Encryption using Genetic Algorithm // International Journal of Latest Trends in Engineering and Technology. 2014. № 3. P. 118–128.

Perrig, Song 1999 – *Perrig A., Song D.* Hash Visualization: A New Technique to Improve Real World Security [Электронный ресурс]. URL: https://netsec.ethz.ch/publications/papers/validation.pdf (дата обращения 21 января 2022)

Safdari, Joshi 2009 – *Safdari M., Joshi R.* Evolving Universal Hash Functions using Genetic Algorithms // International Conference on Future Computer and Communication. 2009. № 3. P. 46–51.

Saleh, Eddeen, Saadeh 2014 – *Saleh E., Eddeen L.N., Saadeh D.* Genetic hashing algorithm [Электронный ресурс]. URL: https://www.researchgate.net/profile/Lubna-Nasir-Eddeen/publication/261596594_Genetic_Hash_Algorithm/links/54eae6600cf25ba91c83f5f3/Genetic-Hash-Algorithm.pdf (дата обращения 20 января 2021).

References

Goyat, S. (2012), “Cryptography Using Genetic Algorithms (GAs)”, *IOSR Journal of Computer Engineering*, no. 1, pp. 6–8.

Markov, A.S. and Tsirlov, V.L. (2015), “Fundamentals of cryptography. Preparing for cissp”, *Voprosy kiberbezopasnosti*, no. 1, pp. 60–72.

Naik, P. and Naik, G. (2014), “Asymmetric Key Encryption using Genetic Algorithm”, *International Journal of Latest Trends in Engineering and Technology*, no. 3, pp. 118–128.

Perrig, A. and Song, D. (1999), “Hash Visualization: A New Technique to Improve Real World Security”, [Online], available at: https://netsec.ethz.ch/publications/papers/validation.pdf (Accessed at 21 January 2022).

Safdari, M. and Joshi, R. (2009), “Evolving Universal Hash Functions using Genetic Algorithms”, *International Conference on Future Computer and Communication*, no. 3, pp. 46–51.

Saleh, E., Eddeen, L.N. and Saadeh, D. (2014), "Genetic hashing algorithm", [Online], available at: https://www.researchgate.net/profile/Lubna-Nasir-Eddeen/publication/261596594_Genetic_Hash_Algorithm/links/54eae6600cf25ba91c83f5f3/Genetic-Hash-Algorithm.pdf (Accessed at 21 January 2022).

Shtovba, S.D. (2003), "Ant algorithms", *Exponenta Pro. Matematika v prilozheniah*, no. 4, pp. 70–75.

Trebukhin, A.V. (2017), "Methods for solving optimization problems using bioinspired algorithms", *Molodoi issledovatel Dona*, no. 1, pp. 15–18.

Zhurkovich, Y. (2018), "Genetic algorithms", *Center of Scientific Cooperation "Interactive plus"*, no. 1, pp. 121–130.

Информация об авторах

Иван Е. Чернов, студент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; chernov-ivan.1997@yandex.ru

Андрей В. Куров, кандидат технических наук, доцент, Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5; avkur7@mail.ru

Information about the authors

Ivan E. Chernov, student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; chernov-ivan.1997@yandex.ru

Andrey V. Kurov, Cand. of Sci. (Computer Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya str., Moscow, Russia, 105005; avkur7@mail.ru

УДК 512
DOI: 10.28995/2686-679X-2022-1-83-97

Алгебраические уравнения в унитарном пространстве и кратчайшее алгебраическое доказательство основной теоремы алгебры

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

Аннотация. Статья посвящена изложению некоторых результатов, полученных при изучении алгебраических уравнений с комплексными коэффициентами от комплексного переменного в унитарном пространстве. В ортонормальном базисе введены два вектора, которые названы вектором корня и вектором коэффициентов алгебраического полинома. С помощью этих векторов алгебраический полином представлен как их скалярное произведение в ортонормальном базисе. Сформулирован и доказан критерий линейной независимости векторов корней в совокупности. Сформулирована и доказана теорема о том, что максимальное число простых корней алгебраического полинома на единицу меньше размерности унитарного пространства. Получено обобщение теоремы Виета и выведены новые формулы, связывающие коэффициенты алгебраического полинома с его корнями. Рассмотрен общий случай алгебраического полинома, когда некоторые его коэффициенты могут быть равны нулю. Введены две ортогональные системы векторов из комбинаций коэффициентов алгебраического полинома и изучены их свойства. Дано кратчайшее алгебраическое доказательство основной теоремы алгебры среди известных доказательств, не выходящее за рамки понятий алгебры полиномов и использующее скалярное произведение векторов в унитарном пространстве, а также одно свойство двуместного предиката из математической логики. Результаты работы могут быть использованы и в учебном процессе в курсе алгебры.

Ключевые слова: алгебраический полином, унитарное пространство, базис, вектор, линейная независимость, линейная зависимость, скалярное произведение, векторное произведение, определитель Вандермонда, формулы Виета, обобщение, ортогональность, разложение, основная теорема алгебры

Для цитирования: Галканов А.Г. Алгебраические уравнения в унитарном пространстве и кратчайшее алгебраическое доказательство основной теоремы алгебры // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 83–97. DOI: 10.28995/2686-679X-2022-1-83-97

Algebraic equations in unitary space and shortest algebraic proof of the fundamental theorem of algebra

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

Abstract. The article deals with the presentation of some results obtained in the study of algebraic equations with complex coefficients from a complex variable in a unitary space. In the orthonormal basis, two vectors are introduced, which are called the vector of root and the vector of coefficients of an algebraic polynomial. With the help of these vectors, an algebraic polynomial is represented as a scalar product of them in an orthonormal basis. The criterion of linear independence of a set of root vectors is formulated and proved. A Theorem is formulated and proved that the maximum number of simple roots of an algebraic polynomial is one less than the dimension of a unitary space. A generalization of Vieta's Theorem is obtained and new formulas connecting the coefficients of an algebraic polynomial with its roots are derived. The general case of an algebraic polynomial is considered, when some of its coefficients may be equal to zero. Two orthogonal vector systems from combinations of coefficients of an algebraic polynomial are introduced. Their properties have been studied. The shortest algebraic proof of the fundamental Theorem of algebra among the known proofs is given, which does not go beyond the concepts of the algebra of polynomials and uses the scalar product of vectors in a unitary space, as well as one property of a two-place predicate from mathematical logic. The results of this work can also be used in the educational process in the algebra course.

Keywords: algebraic polynomial, unitary space, basis, vectors, linear independence, linear dependence, scalar product, vector product, Vandermonde determinant, Vieta formulas, generalization, orthogonality, decomposition, fundamental theorem of algebra

For citation: Galkanov, A.G. (2022), "Algebraic equations in unitary space and shortest algebraic proof of the fundamental theorem of algebra", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 83–97, DOI: 10.28995/2686-679X-2022-1-83-97

Пусть U^{n+1} – унитарное пространство размерности $n+1$, $B=\{\vec{e}_1, \vec{e}_2, \vec{e}_3,..., \vec{e}_{n+1}\}$ – ортонормированный базис в U^{n+1}. Если в базисе B ввести два вектора $\vec{C}=(c_0, c_1, c_2,..., c_n)\in U^{n+1}$ и $\vec{Z}=(1, z, z^2,..., z^n)\in U^{n+1}$, то в этом базисе всякий алгебраический полином $P_n(z)$ с комплексными коэффициентами от комплексного переменного z можно представить в виде скалярного произведения векторов $\vec{Z}$ и $\vec{\vec{C}}$:

$$P_n(z)=c_0+c_1z+c_2z^2+...+c_nz^n=1\cdot\bar{\bar{c}}_0+z\cdot\bar{\bar{c}}_1+z^2\bar{\bar{c}}_2+...+z^n\cdot\bar{\bar{c}}_n=\left(\vec{Z}, \vec{\vec{C}}\right),$$

где $\vec{\vec{C}}$ – вектор, комплексно-сопряженный вектору $\vec{C}$: $\vec{\vec{C}}=(\bar{c}_0, \bar{c}_1, \bar{c}_2,..., \bar{c}_n)$, т.е. если $c_k=a_k+ib_k$, то $\bar{c}_k=a_k-ib_k$, $k\in N=\{1, 2...., n\}$. $\vec{C}$ назовём вектором коэффициентов, $\vec{Z}$ – вектором корня.

Алгебраическое уравнение степени не выше n ($n \geqslant 1$)

$$P_n(z) = c_0 + c_1z + c_2z^2 + ... + c_nz^n = 0, c_n \neq 0 \qquad (1)$$

будем рассматривать в унитарном пространстве U^{n+1}. Набору комплексных чисел $z_1, z_2, ..., z_n$ сопоставим векторы

$$\overrightarrow{Z_k} = (1, z_k, z_k^2, ..., z_k^n) \in U^{n+1}.$$

Теорема 1. Условие $\forall i, j\in N\ (i \neq j)\ [z_i \neq z_j]$ необходимо и достаточно для линейной независимости векторов $\overrightarrow{Z_1}$, $\overrightarrow{Z_2}$,..., $\overrightarrow{Z_n}$, где $i, j\in N$.

Доказательство. Достаточность. Пусть $\forall i, j\in N\ (i \neq j)\ [z_i \neq z_j]$. Рассмотрим векторное произведение векторов $\overrightarrow{Z_1}$, $\overrightarrow{Z_2}$,..., $\overrightarrow{Z_n}$ в базисе B:

$$\vec{V}=\left[\vec{Z_1},\vec{Z_2},...,\vec{Z_n}\right]=\begin{vmatrix}\vec{e}_1 & \vec{e}_2 & \vec{e}_3 \dots \vec{e}_n & \vec{e}_{n+1}\\ 1 & z_1 & z_1^2 \dots z_1^{n-1} & z_1^n\\ 1 & z_2 & z_2^2 \dots z_2^{n-1} & z_2^n\\ \dots & \dots & \dots & \dots\\ 1 & z_n & z_n^2 \dots z_n^{n-1} & z_n^n\end{vmatrix}.$$

Если этот определитель разложить по элементам первой строки, то $\vec{V}=A_{11}\vec{e}_1+A_{12}\vec{e}_2+A_{13}\vec{e}_3...+A_{1n+1}\vec{e}_{n+1}$, где A_{11}, A_{12}, A_{13},..., A_{1n} – алгебраические дополнения элементов первой строки, причем определитель, полученный после вычеркивания элементов первой строки и последнего столбца определителя вектора $\vec{V}$, т. е.

$$\Delta=(-1)^{1+n}\begin{vmatrix}1 & z_1 & z_1^2 & \dots & z_1^{n-1}\\ 1 & z_2 & z_2^2 & \dots & z_2^{n-1}\\ \dots & \dots & \dots & \dots & \dots\\ 1 & z_n & z_n^2 & \dots & z_n^{n-1}\end{vmatrix}=(-1)^{1+n}W\left(z_1,z_2,...,z_n\right)=(-1)^{1+n}\prod\nolimits_{1\le j<i\le n}\left(z_i-z_j\right)$$

с точностью до знака есть определитель Вандермонда, который обладает следующим свойством:

$$\prod\nolimits_{1\le j<i\le n}\left(z_i-z_j\right)\neq 0\Leftrightarrow\forall i,j\in N(i\neq j)\left[z_i\neq z_j\right].$$

Тогда $\vec{V}\neq\vec{\Theta}$, и по свойству векторного произведения векторы $\vec{Z_1}$, $\vec{Z_2}$,..., $\vec{Z_n}$ линейно независимы, где $\vec{\Theta}$ – нуль вектор.

Необходимость. Пусть векторы $\vec{Z_1}$, $\vec{Z_2}$,..., $\vec{Z_n}$ линейно независимы, Допустим, что $\exists i,j\in N(i\neq j)\left[z_i=z_j\right]$. Тогда по свойству определителя $\vec{V}=\vec{\Theta}$, следовательно, векторы $\vec{Z_1}$, $\vec{Z_2}$,..., $\vec{Z_n}$ линейно зависимы, что противоречит условию.

Теорема 2. Максимальное число простых корней полинома $P_n(z)$ на единицу меньше размерности унитарного пространства U^{n+1}.

Доказательство. Предположим, что максимальное число простых корней полинома $P_n(z)$ равно $n - 1$ или $n + 1$.

Случай 1. Максимальное число простых корней полинома $P_n(z)$ равно $n - 1$, т. е.

$$P_n(z_h) = 0 \left(h = \overline{1,\ n-1}\right) \Leftrightarrow \begin{cases} c_0 + z_1 c_1 + z_1^2 c_2 + \ldots + z_1^n c_n = 0, \\ c_0 + z_2 c_1 + z_2^2 c_2 + \ldots + z_2^n c_n = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ c_0 + z_{n-1} c_1 + z_{n-1}^2 c_2 + \ldots + z_{n-1}^n c_n = 0, \end{cases} -$$

система однородных линейных алгебраических уравнений относительно неизвестных $c_0, c_1, c_2, \ldots, c_n$. Она имеет тривиальное решение и бесконечное множество нетривиальных решений, поскольку ранг матрицы ее коэффициентов меньше числа неизвестных. Это значит, что полином $P_n(z) = 0$ или он не определен (его коэффициенты неоднозначны).

Случай 2. Максимальное число простых корней полинома $P_n(z)$ равно $n + 1$.

Каждому простому корню $z_1, z_2, \ldots, z_n, z_{n+1}$ полинома $P_n(z)$ сопоставим вектор

$\overrightarrow{Z_h} = \left(1,\ z_h,\ z_h^2, \ldots,\ z_h^n\right),\ h = \overline{1,\ n+1}.$ Так как

1) векторы $\overrightarrow{Z_1},\ \overrightarrow{Z_2}, \ldots,\ \overrightarrow{Z_h},\ \overrightarrow{Z_{h+1}}$ линейно независимы по теореме 1,

2) $P_n(z_h) = \left(\overrightarrow{Z_h},\ \overrightarrow{\overrightarrow{C}}\right) = 0,$

то в пространстве U^{n+1} существуют $n + 2$ линейно независимых векторов $\overrightarrow{C},\ \overrightarrow{Z_1},\ \overrightarrow{Z_2}, \ldots,\ \overrightarrow{Z_h},\ \overrightarrow{Z_{h+1}}$, что противоречит размерности пространства U^{n+1}.

Примечание 1. Теорему 2 можно было бы доказать с применением теоремы Безу. Однако здесь предпочтение дано альтернативному методу.

В следующей теореме $P_n(z)$ будем считать приведенным полиномом ($c_n = 1$).

Теорема 3 (обобщенная теорема Виета). Для того чтобы комплексные числа $z_1, z_2, ..., z_n$ были простыми корнями полинома $P_n(z)$, необходимо и достаточно, чтобы коэффициенты $P_n(z)$ определялись следующими формулами:

$$c_0 = \frac{\Delta_{11}}{\Delta},\ c_1 = \frac{\Delta_{12}}{\Delta},\ c_2 = \frac{\Delta_{13}}{\Delta},\ldots,\ c_{n-1} = \frac{\Delta_{1n}}{\Delta}, \tag{2}$$

где $$\Delta_{11} = \begin{vmatrix} -z_1^n & z_1 & z_1^2 & \ldots & z_1^{n-1} \\ -z_2^n & z_2 & z_2^2 & \ldots & z_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -z_n^n & z_n & z_n^2 & \ldots & z_n^{n-1} \end{vmatrix}, \quad \Delta_{12} = \begin{vmatrix} 1 & -z_1^n & z_1^2 & \ldots & z_1^{n-1} \\ 1 & -z_2^n & z_2^2 & \ldots & z_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & -z_n^n & z_n^2 & \ldots & z_n^{n-1} \end{vmatrix},$$

$$\Delta_{13} = \begin{vmatrix} 1 & z_1 & -z_1^n & \ldots & z_1^{n-1} \\ 1 & z_2 & -z_2^n & \ldots & z_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & z_n & -z_1^n & \ldots & z_1^{n-1} \end{vmatrix}, \ldots,$$

$$\Delta_{1n} = \begin{vmatrix} 1 & z_1 & z_1^2 & \ldots & -z_1^n \\ 1 & z_2 & z_2^2 & \ldots & -z_2^n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & z_n & z_n^2 & \ldots & -z_1^n \end{vmatrix}, \quad \Delta = \begin{vmatrix} 1 & z_1 & z_1^2 & \ldots & z_1^{n-1} \\ 1 & z_2 & z_2^2 & \ldots & z_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & z_n & z_n^2 & \ldots & z_n^{n-1} \end{vmatrix} \neq 0.$$

Доказательство. Необходимость. Пусть $z_1, z_2, ..., z_n$ – простые корни $P_n(z)$, где $\forall i, j \in N(i \neq j)\left[z_i \neq z_j\right]$. Тогда $\forall k \in N\left[P_n(z_k) = 0\right]$, из чего имеем систему линейных алгебраических уравнений относительно $c_0, c_1, c_2, ..., c_{n-1}$:

$$\begin{cases} c_0 + z_1 c_1 + z_1^2 c_2 + \ldots + z_1^{n-1} c_{n-1} = -z_1^n, \\ c_0 + z_2 c_1 + z_2^2 c_2 + \ldots + z_2^{n-1} c_{n-1} = -z_2^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ c_0 + z_n c_1 + z_n^2 c_2 + \ldots + z_n^{n-1} c_{n-1} = -z_n^n. \end{cases} \tag{3}$$

Определитель Δ при неизвестных c_0, c_1, c_2, ..., c_{n-1} системы (3) есть определитель Вандермонда и $\Delta \neq 0$. Поэтому система (3) имеет единственное решение, т. е. для коэффициентов c_0, c_1, c_2, ..., c_{n-1} справедливы формулы (2).

Достаточность. Пусть справедливы формулы (2), где z_1, z_2, ..., z_n – любые заданные нетривиальные различные комплексные числа. Это значит, что c_0, c_1, c_2, ..., c_{n-1} – единственное решение системы линейных алгебраических уравнений (3). Тогда

$$\begin{cases} c_0 + z_1 c_1 + z_1^2 c_2 + \ldots + z_1^{n-1} c_{n-1} + z_1^n = 0 \Leftrightarrow P_n(z_1) = 0, \\ c_0 + z_2 c_1 + z_2^2 c_2 + \ldots + z_2^{n-1} c_{n-1} + z_2^n = 0 \Leftrightarrow P_n(z_2) = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ c_0 + z_n c_1 + z_n^2 c_2 + \ldots + z_n^{n-1} c_{n-1} + z_n^n = 0 \Leftrightarrow P_n(z_n) = 0. \end{cases}$$

Следовательно, z_1, z_2, ..., z_n – простые корни полинома $P_n(z)$.

Примечание 2. Известная теорема Виета выражает необходимое условие того, чтобы числа z_1, z_2, ..., z_n, были простыми корнями полинома $P_n(z)$ и доказывается с применением теоремы Безу [1], так что теорема Виета является частным случаем теоремы 3. В то же время теорема 3 дает новый алгоритм нахождения коэффициентов полинома $P_n(z)$.

Пример. $P_n(z) = P_3(z) = c_0 + c_1 z + c_2 z^2 + z^3$. Найдем определители системы (3)

$$\Delta_{11} = \begin{vmatrix} -z_1^3 & z_1 & z_1^2 \\ -z_2^3 & z_2 & z_2^2 \\ -z_3^3 & z_n & z_n^2 \end{vmatrix}, \quad \Delta_{12} = \begin{vmatrix} 1 & -z_1^3 & z_1^2 \\ 1 & -z_2^3 & z_2^2 \\ 1 & -z_3^3 & z_n^2 \end{vmatrix}, \quad \Delta_{13} = \begin{vmatrix} 1 & z_1 & -z_1^3 \\ 1 & z_2 & -z_2^3 \\ 1 & z_3 & -z_3^3 \end{vmatrix},$$

$$\Delta = \begin{vmatrix} 1 & z_1 & z_1^2 \\ 1 & z_2 & z_2^2 \\ 1 & z_3 & z_3^2 \end{vmatrix} \neq 0$$

и из (2) находим $c_0 = -z_1z_2z_3$, $c_1 = -z_1z_2 + z_1z_3 + z_2z_3$, $c_2 = -(z_1 + z_2 + z_3)$ – формулы Виета. Как и следовало ожидать, формулы (2) в силу единственности коэффициентов полинома $P_n(z)$ лишь по форме отличаются от формул Виета.

Пусть $P_n(z)$ – полином, некоторые коэффициенты которого могут быть равны нулю. Поэтому $P_n(z)$ запишем в виде без нулевых слагаемых:

$$P_{qm}(z) = c_0 + c_1z^{q1} + c_2z^{q2} + \ldots + c_mz^{qm}, \qquad (4)$$

где $q_1, q_2, \ldots, qm, m \in N$ – показатели степеней ($q_1 < q_2 < ... < q_m$),

$c_0, c_1, ..., c_m$ – отличные от нуля коэффициенты (4).

Примеры:

1) для полинома $(1-i) + (2 + 3i)\,z$: $c_0 = 1 - i$, $c_1 = 2 + 3i$, $q_1 = 1$, $P_1(z) = (1 - i) + (2 + 3i)\,z$;
2) для полинома $i + z^2$: $c_0 = i$, $c_1 = 1$, $q_1 = 2$, $P_2(z) = i + z^2$;
3) для полинома $4 + (5 + 3i)z^6 + (2-i)z^{18}$: $c_0 = 4$, $c_1 = 5 + 3i$, $c_2 = 2-i$, $q_1 = 6$, $q_2 = 18$, $P_{18}(z) = 4 + (5 + 3i)z^6 + (2 - i)z^{18}$.

Если же все коэффициенты полинома $P_n(z)$ отличны от нуля, то в (4) $m = n$, $q_k = k$, $k = 1, 2, ..., n$, т. е. получим полином (1).

Применительно к полиному (4) векторы $\vec{C}$, $\vec{Z}$ запишутся в виде $\vec{C} = (c_0, c_1, c_2, ..., c_m) \in U^{m+1}$, $Z = (1, z^{q_1}, z^{q_2}, ..., z^{q_m}) \in U^{m+1}$, а полином $P_{q_m}(z)$ – в виде $P_{q_m}(z) = \left(\vec{Z}, \vec{C}\right)$. В базисе B построим векторы

$$\overrightarrow{G_1} = \left(1, -c_0/c_1, 0, ..., 0\right), \ \overrightarrow{G_2} = \left(1, 0, -c_0/c_2, ..., 0\right), ...,$$
$$\overrightarrow{G_m} = \left(1, 0, 0, ..., -c_0/c_m\right). \qquad (5)$$

и

$$\overrightarrow{H_1} = \left(0, -\overline{c_0/c_1}, 0, ..., 0\right), \ \overrightarrow{H_2} = \left(0, 0, -\overline{c_0/c_2}, ..., 0\right), ...,$$
$$\overrightarrow{H_m} = \left(0, 0, 0, ..., -\overline{c_0/c_m}\right).$$

Так, если $m=1,$ то (5) состоит из одного вектора $\overrightarrow{G_1}=\left(1,\,-c_0/c_1\right).$ Если $m=2,$ то в (5) входят следующие векторы $\overrightarrow{G_1}=\left(1,\,-c_0/c_1,\,0\right),$ $\overrightarrow{G_2}=\left(1,\,0,\,-c_0/c_2\right).$ При m = 3 (5) состоит из векторов $\overrightarrow{G_1}=\left(1,\,-c_0/c_1,\,0,\,0\right),$ $\overrightarrow{G_2}=\left(1,\,0,\,-c_0/c_2,\,0\right),$ $\overrightarrow{G_3}=\left(1,\,0,\,0,\,-c_0/c_3\right).$ И т.д.

Пусть $M=\{1,\,2,...,\,m\}.$ Свойства векторов $\vec{C},\ \vec{Z},\ \overrightarrow{G_l},\ \overrightarrow{H_l},\ l\in M.$

1^0. Ортогональность $\overrightarrow{G_l},\ \overrightarrow{H_l}$: $\left(\overrightarrow{G_i},\,\overrightarrow{H_j}\right)=\begin{cases}\left(c_0/c_i\right)^2, & \text{если } i=j,\\ 0, & \text{если } i\neq j\end{cases}$

где $i,\,j\in M.$

2^0. Векторы $\overrightarrow{G_1},\,\overrightarrow{G_2},...,\,\overrightarrow{G_m}$ линейно независимы.

Доказательство. Пусть $\lambda_1\overrightarrow{G_1}+\lambda_2\overrightarrow{G_2}+...+\lambda_m\overrightarrow{G_m}=\overrightarrow{\Theta},\ \ \lambda_k\in\mathbb{C},$ $k\in M.$ Равенство

$\lambda_1\overrightarrow{G_1}+\lambda_2\overrightarrow{G_2}+...+\lambda_m\overrightarrow{G_m}=\overrightarrow{\Theta}$ равносильно системе

$$\lambda_1+\lambda_2+...+\lambda_m=0\wedge\left(-\frac{a_0}{a_1}\lambda_1=0\right)\wedge\left(-\frac{a_0}{a_2}\lambda_2=0\right)\wedge\left(-\frac{a_0}{a_m}\lambda_m=0\right),$$

из чего следуют равенства $\lambda_1=\lambda_2=...=\lambda_m=0,$ что по определению означает линейную независимость векторов $\overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m}.$

3^0. Каждый вектор $\overrightarrow{G_k}\ (k\in M)$ ортогонален вектору $\overrightarrow{\overrightarrow{C}}$: $\forall k\in M\left[\left(\overrightarrow{G_k},\,\overrightarrow{\overrightarrow{C}}\right)=0\right].$

Доказательство,

$$\left(\overrightarrow{G_1},\,\overrightarrow{\overrightarrow{C}}\right)=1\cdot a_0-\frac{a_0}{a_1}\cdot a_1=0,$$

$$\left(\overrightarrow{G_k},\,\overrightarrow{\overrightarrow{C}}\right)=1\cdot a_0-\frac{a_0}{a_2}\cdot a_2=0,...,$$

$$\left(\overrightarrow{G_m},\,\overrightarrow{\overrightarrow{C}}\right)=1\cdot a_0-\frac{a_0}{a_m}\cdot a_m=0.$$

4^0. Векторы $\overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m},\ \overrightarrow{C}$ линейно независимы.

Доказательство. Согласно свойству 2^0, векторы $\overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m}$ линейно независимы, а по свойству 3^0 вектор $\overrightarrow{C}$ ортогонален каждому вектору $\overrightarrow{G_k},\ k \in M$. Следовательно, векторы $\overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m},\ \overrightarrow{C}$ линейно независимы.

5^0.

$$\forall \overrightarrow{C} \in U^{m+1}\ \exists \overrightarrow{Z_*} \in U^{m+1}\left[\textit{векторы } \overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m},\ \overrightarrow{Z_*} \textit{ линейно зависимы}\right].$$

Доказательство. Допустим, что доказываемое утверждение ложно. Тогда его отрицание

$$\exists \overrightarrow{C} \in U^{m+1}\ \forall \overrightarrow{Z_*} \in U^{m+1}\left[\textit{векторы } \overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m},\ \overrightarrow{Z_*} \textit{ линейно независимы}\right] \tag{6}$$

должно быть истинным. Из бесконечного множества векторов $\overrightarrow{Z_*}$, удовлетворяющих допущению (6), возьмем $\overrightarrow{Z_1}$ и $\overrightarrow{Z_2}$: $\overrightarrow{Z_1} = \left(1,\ z_1^{q_1},...,\ z_1^{q_m}\right),\ \overrightarrow{Z_2} = \left(1,\ z_2^{q_1},...,\ z_2^{q_m}\right)$, где $z_1 \neq 0,\ z_2 \neq 0,\ z_1 \neq z_2$.

Тогда, согласно допущению (6), векторы $\overrightarrow{G_1},\ \overrightarrow{G_2},...,\ \overrightarrow{G_m},\ \overrightarrow{Z_1},\ \overrightarrow{Z_2}$ линейно независимы, что противоречит размерности пространства U^{n+1}.

Следствие из 5^0.

$$\forall \overrightarrow{C} \in U^{m+1}\ \exists \overrightarrow{Z_*} \in U^{m+1}\left[\overrightarrow{Z_*} = \lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_i \overrightarrow{G_i} + ... + \lambda_m \overrightarrow{G_m}\right],$$

По свойству 1^0 имеем

$$\left(\overrightarrow{Z_*},\ \overrightarrow{H_j}\right) = \left(\lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_i \overrightarrow{G_i} + ... + \lambda_m \overrightarrow{G_m},\ \overrightarrow{H_j}\right)\Big|_{j \in M},$$

откуда формулы для коэффициентов разложения

$$\lambda_1 = -\frac{c_1}{c_0} z_*^{q_1},\ \lambda_2 = -\frac{c_2}{c_0} z_*^{q_2},...,\ \lambda_i = -\frac{c_i}{c_0} z_*^{q_i},...,\ \lambda_m = -\frac{c_m}{c_0} z_*^{q_m}. \tag{7}$$

Теорема 4. Комплексное число z_* есть корень полинома $P_{q_m}(z)$ тогда и только тогда, когда $\overrightarrow{Z_*} = \lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_m \overrightarrow{G_m}$.

Доказательство. Достаточность. Пусть

$$\overrightarrow{Z_*} = \lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_m \overrightarrow{G_m}.$$

$$P_{q_m}(z_*) = \left(\overrightarrow{Z_*}, \overrightarrow{\overrightarrow{C}}\right) = \left(\lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_m \overrightarrow{G_m}, \overrightarrow{\overrightarrow{C}}\right) =$$

$$= \lambda_1 \left(\overrightarrow{G_1}, \overrightarrow{\overrightarrow{C}}\right) + \lambda_2 \left(\overrightarrow{G_2}, \overrightarrow{\overrightarrow{C}}\right) + ... + \lambda_m \left(\overrightarrow{G_m}, \overrightarrow{\overrightarrow{C}}\right) \overset{3^0}{=} 0.$$

Необходимость. Пусть $P_{q_m}(z_*) = 0$. Тогда $\left(\overrightarrow{Z_*}, \overrightarrow{\overrightarrow{C}}\right) = 0$. По свойству 4^0 множество $m+1$ векторов $\overrightarrow{G_1}$, $\overrightarrow{G_2}$,..., $\overrightarrow{G_m}$, $\overrightarrow{\overrightarrow{C}}$ линейно независимо, т.е. их можно взять за базис. При этом разложение $\overrightarrow{Z_*} = \lambda_0 \overrightarrow{\overrightarrow{C}} + \lambda_1 \overrightarrow{G_1} + \lambda_2 \overrightarrow{G_2} + ... + \lambda_m \overrightarrow{G_m}$, из чего $0 = \left(\overrightarrow{Z_*}, \overrightarrow{\overrightarrow{C}}\right) \overset{3^0}{=} \lambda_0 \left(\overrightarrow{\overrightarrow{C}}, \overrightarrow{\overrightarrow{C}}\right)$, откуда $\lambda_0 = 0$.

Покажем, что $\lambda_1 + \lambda_2 + ... + \lambda_m = 1$. С учетом (7) из равенства $P_{qm}(z_*) = 0$ имеем:

$$0 = P_{qm}(z_*) = c_0 + c_1 z_*^{q_1} + c_2 z_*^{q_2} + ... + c_m z_*^{q_m} =$$
$$= c_0 - c_0\lambda_1 - c_0\lambda_2 + ... - c_0\lambda_m \Rightarrow \lambda_1 + \lambda_2 + ... + \lambda_m = 1.$$

Кратчайшее алгебраическое доказательство основной теоремы алгебры

Основная теорема алгебры о существовании хотя бы одного корня алгебраического уравнения (1) «является одним из крупных достижений всей математики и находит применения в самых различных областях науки» [Курош 1968].

Основная теорема исследовалась и доказывалась в трудах А. Жирара, Р. Декарта, К. Маклорена, Л. Эйлера, Ж. Даламбера,

П. Лапласа, Ж. Лагранжа, К. Гаусса и др. [Тихомиров, Успенский 1997]. Однако во всех ее доказательствах применяются методы классического анализа. Так, доказательство основной теоремы, построенное в [Курош 1968], состоит из следующих этапов.

1. Полином (1) объявляется функцией комплексного переменного z.

2. Доказывается непрерывность $P_n(z)$ на всей комплексной плоскости.

3. Доказывается формула Тейлора, дающая разложение $P_n(z+h)$ по степеням h.

4. Доказывается лемма о модуле старшего члена.

5. Доказывается лемма о возрастании модуля многочлена.

6. Доказывается лемма Даламбера.

7. Применяется теорема Вейерштрасса о существовании в замкнутом круге точки минимума для действительной функции комплексного переменного.

Поэтому основная теорема не является чисто алгебраической и изложение ее доказательства занимает 18 страниц [Курош 1968].

В [Тихомиров, Успенский 1997] изложены десять доказательств основной теоремы, из которых десятое авторами названо алгебраическим. В [Błaszczyk 2015] дано доказательство основной теоремы, названное автором абсолютно алгебраическим доказательством: «В нашем доказательстве мы не используем ни понятие непрерывной функции, ни ссылаемся на какую-либо теорему реального и комплексного анализа. Вместо этого мы применяем методы современной алгебры: мы расширяем поле действительных чисел на неархимедово поле гиперреальностей с помощью конструкции ультрапроизведения и исследуем некоторые связи между подкольцом ограниченных гиперреальностей, его максимальным идеалом бесконечно малых и действительными числами». Однако понятие «абсолютно алгебраическое доказательство» так и не определено.

Ниже будет дано кратчайшее алгебраическое доказательство основной теоремы алгебры среди известных доказательств, не выходящее за рамки понятий алгебры полиномов и использующее скалярное произведение векторов в унитарном пространстве, а также одно свойство двуместного предиката из математической логики.

Пусть $f(x, y)$ – двуместный предикат. Имеет место утверждение [Шапорев 2005]:

$$\exists x \in X \, \forall y \in Y \, [f(x, y)] \Rightarrow \forall y \in Y \, \exists x \in X \, [f(x, y)]. \qquad (8)$$

Приведем очевидный факт: любое комплексное число z является корнем хотя бы одного полинома

$$\forall \vec{Z} \in U^{n+1} \ \exists \vec{C} \in U^{n+1} \left[\left(Z, \vec{\vec{C}} \right) = 0 \right]. \tag{9}$$

Теорема 5 (основная теорема алгебры). У всякого полинома $P_n(z)$ существует хотя бы один корень: $\forall \vec{C} \in U^{n+1} \ \exists \vec{Z} \in U^{n+1} \left[\left(\vec{Z}, \vec{\vec{C}} \right) = 0 \right]$.

Доказательство. Допустим, что доказываемое утверждение ложно:

$$\forall \vec{C} \in U^{n+1} \ \exists \vec{Z} \in U^{n+1} \left[\left(\vec{Z}, \vec{\vec{C}} \right) = 0 \right] = \mathit{false}. \tag{10}$$

Тогда отрицание (10) должно быть истинным:

$$\exists C \in U^{n+1} \ \forall Z \in U^{n+1} \left[\left(Z, \overline{C} \right) \neq 0 \right] = \mathit{true}. \tag{11}$$

Используя (8) и (11), получим

$$\exists \vec{C} \in U^{n+1} \ \forall \vec{Z} \in U^{n+1} \left[\left(\vec{Z}, \vec{\vec{C}} \right) \neq 0 \right] \Rightarrow \ \forall \vec{Z} \in U^{n+1} \ \exists \vec{C} \in U^{n+1} \left[\left(\vec{Z}, \vec{\vec{C}} \right) \neq 0 \right]. \tag{12}$$

Однако полученное утверждение в (12) противоречит (9).

Заключение

1. Показано, что изучение алгебраических уравнений в унитарном пространстве с привлечением скалярного произведения и векторного произведения $n + 1$ векторов корней и коэффициентов алгебраического полинома может рассматриваться как альтернативный метод исследования алгебраических уравнений.

2. Установлена связь между размерностью унитарного пространства и максимальным числом простых корней алгебраического уравнения.

3. Получено обобщение теоремы Виета и выведены новые формулы для коэффициентов полинома как решение системы линейных алгебраических уравнений, основным определителем которой оказался определитель Вандермонда. На примере показано, что на самом деле эти новые формулы лишь по форме отличаются от формул Виета для коэффициентов полинома.

4. Рассмотрен наиболее общий случай алгебраического полинома, когда все коэффициенты алгебраического полинома отличны от нуля и когда некоторые его коэффициенты могут быть равны нулю. Для этого случая построены две совокупности взаимно ортогональных векторов, применение которых привело к возможности разложения вектора корня.

5. Дано кратчайшее алгебраическое доказательство основной теоремы алгебры, не выходящее за рамки понятий алгебры полиномов.

Литература

Курош 1968 – *Курош А.Г.* Курс высшей алгебры. М.: Наука, 1968.

Тихомиров, Успенский 1997 – *Тихомиров В.М., Успенский В.В.* Десять доказательств основной теоремы алгебры // Математическое просвещение. 1997. Вып. 1. С. 50–70.

Шапорев 2005 – *Шапорев С.Д.* Математическая логика. СПб.: БХВ – Петербург, 2005.

Błaszczyk 2015 – *Błaszczyk P.A.* Purely Algebraic Proof of the Fundamental Theorem of Algebra [Электронный ресурс]. URL: https://arxiv.org/abs/1504.05609 (дата обращения 10 января 2022).

References

Błaszczyk, P.A. (2015), “Purely Algebraic Proof of the Fundamental Theorem of Algebra”, [Online], available at: https://arxiv.org/abs/1504.05609 (accessed at 10 January 2022).

Kurosh, A.G. (1968), *Kurs vysshey algebry* [Higher algebra course], Nauka, Moscow, USSR.

Shaporev, S.D. (2005), *Matematicheskaya logika* [Mathematical logic], BKHV – Peterburg, Saint-Petersburg, Russia.

Tikhomirov, V.M. and Uspenskiy, V.V. (1997), “Ten proofs of the fundamental theorem of algebra”, *Matematicheskoye prosveshcheniye*, iss. 1, pp. 50–70.

Информация об авторе

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

Information about the author

Allaberdi G. Galkanov, Cand. of Sci. (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 629.7:51
DOI: 10.28995/2686-679X-2022-1-98-119

Вопросы математического моделирования процессов роботизации аэродромно-технического и инженерно-авиационного обеспечения авиационных подразделений Росгвардии

Сергей В. Андреенко
Центральная объединенная база хранения ресурсов Министерства внутренних дел Российской Федерации, Балашиха, Московская обл., Россия, andreenko.sergej@yandex.ru

Дмитрий А. Митюшин
Российский государственный гуманитарный университет, Москва, Россия, dalexx@inbox.ru

Андрей М. Сапунов
Главное управление авиации Росгвардии, Москва, Россия, sapunov.am@mail.ru

Аннотация. Вопросы роботизации в настоящее время становятся все более и более актуальными. Особенно это касается силовых структур, где вопросам роботизации уделяют самое пристальное внимание. В статье приводится общий подход к решению задачи роботизации ряда функций, связанных с процессами аэродромно-технического обеспечения авиационных формирований Федеральной службы войск национальной гвардии Российской Федерации на примере авиационного подразделения. Дан анализ существующей технической составляющей подразделений аэродромно-технического и инженерно-авиационного обеспечения авиационных формирований и формулируются предложения по их переоснащению робототехническими комплексами. При этом не имеет значения отношение авиационного подразделения к военной авиации или к авиации специального назначения. Приводятся задачи, решаемые в процессе аэродромно-технического обеспечения, независимо от вида базирования аэродромов, и потенциальная возможность роботизации данных процессов. Разработан проект математической модели совместного применения различных по степени подвижности наземных робототехнических комплексов при взаимодействии друг с другом на аэродромах Росгвардии и на аэродромах совместного базирования. Математическая модель учитывает ограничения, как сформированные в нормативных правовых документах

функционирования государственной авиации и авиации Росгвардии, так и связанные с особенностями функционирования авиационной техники и техники аэродромного технического обеспечения.

Ключевые слова: мобильный робототехнический комплекс, робот, Росгвардия, войска национальной гвардии, авиация, аэродромно-техническое обеспечение, инженерно-авиационное обеспечение, математическая модель, матрица

Для цитирования: Андреенко С.В., Митюшин Д.А., Сапунов А.М. Вопросы математического моделирования процессов роботизации аэродромно-технического и инженерно-авиационного обеспечения авиационных подразделений Росгвардии // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 98–119. DOI: 10.28995/2686-679X-2022-1-98-119

Mathematical modeling issues of robotization processes of the airfield technical support and engineering-aviation support for Rosgvardiya's (National Guard of Russian Federation) aviation units

Sergey V. Andreenko
Central unified resource storage base
Ministry of Internal Affairs of the Russian Federation,
Balashikha, Moscow region, Russia, andreenko.sergej@yandex.ru

Dmitry A. Mityushin
Russian State University for the Humanities, Moscow, Russia,
dalexx@inbox.ru

Andrey M. Sapunov
General Aviation Authority of National Guard of Russia,
Moscow, Russia, sapunov.am@mail.ru

Abstract. The issues of robotization are currently becoming more and more relevant. It is especially true for the law enforcement agencies, where robotization issues are given the closest attention. The article provides a general approach to solving the issue of robotization of a number of functions related to the processes of the airfield technical support for aviation formations of the Federal Service of the National Guard Troops of the Russian Federation using the example of an aviation unit.

It analyzes the existing technical component of the divisions of aerodrome-technical and engineering-aviation support of aviation formations and

formulates the proposals for their re-equipment with robotic complexes. At the same time, the relation of the aviation unit to military aviation or to special-purpose aviation does not matter. The authors outline tasks solved in the process of aerodrome technical support, regardless of the type of aerodrome basing, and the potential possibility for robotization of those processes. A draft mathematical model has been developed for the joint use of ground-based robotic systems with different degrees of mobility when interacting with each other at the airfields of the Russian Guard and at joint-based airfields. The mathematical model takes into account the limitations, both those formed in the regulatory legal documents for the functioning of state aviation and the aviation of the National Guard, and those associated with the specifics of the functioning of aviation equipment and equipment for airfield technical support.

Keywords: mobile robotic system, robot, National Guard of the Russian Federation (Rosgvardiya), National Guard troops, aviation, airfield technical support, engineering-aviation support, mathematical model, matrix

For citation: Andreenko, S.V., Mityushin, D.A. and Sapunov, A.M. (2022), "Mathematical modeling issues of robotization processes of the airfield technical support and engineering-aviation support for Rosgvardiya's (National Guard of Russian Federation) aviation units", *RSUH/RGGU Bulletin. "Informatics. Information security. Mathematics"* Series, no. 1, pp. 98–119, DOI: 10.28995/2686-679X-2022-1-98-119

Введение

Согласно классификации[1], в настоящее время авиация Росгвардии относится к государственной авиации, и так сложилось, что на текущий момент Росгвардия имеет в своем составе:

- государственную военную авиацию (авиация бывших внутренних войск МВД России);
- государственную авиацию специального назначения (бывшие подразделения авиации органов внутренних дел Российской Федерации).

Одними из основных показателей, определяющих эффективность применения государственной авиации, являются различные виды обеспечений, включая инженерно-авиационное обеспечение (далее – ИАО) и аэродромно-техническое обеспечение (далее – АТО).

Определим данные термины.

[1] Ст. 22 Воздушного кодекса Российской Федерации от 19.03.1997 № 60-ФЗ (ред. от 08.06.2020) (с изм. и доп., вступ. в силу с 01.01.2021).

Согласно Федеральным авиационным правилам [Сазонов 2006] «Инженерно-авиационное обеспечение государственной авиации» (далее – ФАП ИАО), под *инженерно-авиационным обеспечением* понимается комплекс мероприятий, осуществляемых инженерно-авиационной службой авиации (далее – ИАС) в целях поддержания авиационной техники (далее – АТ) в постоянной исправности и готовности к применению и достижению высокой эффективности ее применения в ходе боевых действий (выполнения специальных задач) и боевой подготовки авиации Вооруженных Сил и авиации федеральных органов исполнительной власти и организаций, в ведении которых имеется государственная авиация. ИАО составляет основу технического обеспечения государственной авиации.

Аэродромно-техническое обеспечение – комплекс мероприятий по обеспечению полетов авиационных частей, подразделений и отдельных летательных аппаратов; вид материально-технического обеспечения[2].

АТО включает:

- подготовку аэродромов (посадочных площадок), аэродромных сооружений и средств наземного обеспечения полетов, содержание их в постоянной эксплуатационной готовности;
- обеспечение самолетов (вертолетов) авиационными средствами поражения, горючим, средствами электропитания и др.;
- оказание технической помощи потерпевшим аварию или совершившим вынужденную посадку в районе аэродрома самолетам (вертолетам) и их эвакуацию.

Вопросы применения робототехнических комплексов, предназначенных для автоматизации и роботизации процессов ИАО и АТО авиационных формирований Росгвардии, практически не рассматривались ни внутренними войсками МВД России (ныне переданными в состав Росгвардии), ни Центром авиации МВД России, ни Управлением по обеспечению деятельности подразделений специального назначения и авиации МВД России (также в настоящее время в составе Росгвардии). Основное внимание уделялось и уделяется развитию наземных робототехнических комплексов (далее – НРТК) военного назначения (а именно, боевые НРТК), включая НРТК специального назначения (различные виды разведки, разминирование, радиоэлектронная борьба и прочее). В то же

[2] Аэродромно-техническое обеспечение. Энциклопедия Минобороны России [Электронный ресурс]. URL: http://encyclopedia.mil.ru/encyclopedia/dictionary/ details.htm?id=3095%40morfDictionary (дата обращения 14 октября 2021).

время рассматривались лишь вопросы роботизации обеспечения тыловой деятельности, таких как роботизация операционно-хозяйственной деятельности баз (складов) системы материально-технического снабжения МВД России, однако вопросам роботизации ИАО и АТО в рамках функционирования авиационных формирований как МВД России, так и в настоящее время Росгвардии внимания уделено не было.

Постановка задачи

Предлагается на примере авиационного подразделения Росгвардии определить задачи и порядок работ, выполняемых в ходе ИАО и АТО полетов авиации, а также потенциально возможных к выполнению НРТК обеспечивающего назначения в интересах подразделений аэродромного обслуживания авиационных формирований Росгвардии (частей, отдельных авиационных эскадрилий и авиаотрядов) и предложить математическую модель функционирования НРТК для решения указанных задач.

Виды аэродромов и их основные элементы

Военные аэродромы классифицируются по ряду признаков. Рассмотрим классификацию по техническим характеристикам взлетно-посадочной полосы (далее – ВПП) и оборудованию средствами радиотехнического обеспечения (далее – РТО) полетов [Поздняков, Каргапольцев, Губарев 2015]. По данному признаку военные аэродромы разделяют на аэродромы 1-го, 2-го, 3-го класса и посадочные площадки.

– *аэродромы 1-го класса* предназначены для базирования частей дальней военно-транспортной авиации и авиации военно-морского флота. На этих аэродромах оборудованы одна-две ВПП длиной не менее 2500 *м* и шириной 48...50 *м* каждая грузоподъемностью 60...100 *т*;
– *аэродромы 2-го класса* предназначены для базирования одной-двух авиационных частей фронтовой, военно-транспортной авиации или авиации противовоздушной обороны. Они имеют ВПП длиной не менее 1800 *м*, шириной 32...40 *м* и грузоподъемностью 30...60 *т*;
– *аэродромы 3-го класса* предназначены для базирования авиационных частей фронтовой и армейской авиации и имеют

ВПП длиной не менее 1200 *м*, шириной 32 *м* и грузоподъемностью до 30 *т*;

– *посадочные площадки* служат для кратковременного использования их самолетами весом до 10 *т*, а также самолетами вертикального взлета и посадки и вертолетами. Посадочные площадки имеют небольшие размеры (длина ВПП 300...800 *м*, ширина до 30 *м*) и, как правило, не оборудуются постоянными сооружениями.

Под термином *грузоподъемность аэродрома* понимается максимальный полетный вес самолета (вертолета, заходящего на посадку «по-самолетному»), который может выдержать покрытие аэродрома при его посадке.

Также необходимо выделить *аэродромы совместного базирования*, на которых базируются авиационные формирования государственной авиации различной ведомственной принадлежности, а также экспериментальной и гражданской авиации.

Основными элементами аэродрома являются *летное поле* и *служебно-техническая зона*. На летном поле располагаются *летная полоса*, рулежные дорожки, места стоянки воздушных судов (далее – ВС) – самолетов (вертолетов), площадки для дежурного подразделения, технические позиции, места для обслуживания воздушных судов, пункты управления полетами, стартово-командные пункты, некоторые средства связи и радиосветотехнического обеспечения, а также ряд других объектов.

Служебно-техническая зона (территория) включает ряд сооружений и оборудование, которые обеспечивают техническое обслуживание и ремонт самолетов (вертолетов), хранение горюче-смазочных мероприятий, боеприпасов, авиационно-технического имущества, эксплуатацию и ремонт летного поля, защиту личного состава и техники от средств поражения.

Рассмотрим элементы летного поля [Поздняков, Каргапольцев, Губарев 2015].

Летная полоса включает *взлетно-посадочную полосу*, предназначенную для разбега при взлете и пробега после посадки ВС, а также боковые и концевые полосы безопасности. Полосы безопасности предназначены для обеспечения безопасности на случай возможного выкатывания ВС за пределы ВПП. К торцам ВПП примыкают полосы воздушных подходов, обеспечивающие безопасность при наборе высоты после взлета и при снижении во время захода на посадку. Для остановки ВС в случаях отказа тормозных систем или при прерванном взлете в конце ВПП могут оборудоваться специальные тормозные установки (сетевые и тросовые).

Рулежные дорожки (далее – РД) предназначены для руления и буксирования ВС на взлет или на места стоянок после посадки. Их классифицируют на:

- основные (магистральные) РД, соединяющие концы ВПП между собой и располагающиеся вдоль боковых полос безопасности;
- соединительные РД, соединяющие основные РД с полосой в местах окончания пробега ВС (средняя часть ВПП) для быстрого их схода с полосы;
- вспомогательные РД, соединяющие основные РД с местами стоянок ВС и отдельными частями служебно-технической зоны.

Места стоянки (далее – МС) *ВС* – специально подготовленные и оборудованные для обслуживания ВС участки летного поля.

Для предстартового обслуживания ВС, размещения дежурных вблизи концов летной полосы должны располагаться стартовые площадки. Для защиты ВС и средств их обеспечения от огневого воздействия противника на аэродроме должны оборудоваться специальные укрытия (насыпные обвалования, железобетонные укрытия различных конструкций).

На рис. 1 приведена типовая схема аэродрома, на рис. 2...6 – реальный аэродром авиабазы ВВС США Эдвардс (*Edwards Air Force Base*), Калифорния, снятый с высоты 5,42 *км*. На снимках можно увидеть многие из указанных выше элементов летного поля: две ВПП, рулежные дорожки, подъездные пути и даже самолеты на МС.

Рис. 1. Типовая схема аэродрома
(СССР / Российская Федерация)

Рис. 2. Снимок авиабазы ВВС США Эдвардс с инфраструктурой, полученный из приложения Google Earth

Рис. 3. Снимок аэродрома авиабазы ВВС США Эдвардс, полученный из приложения Google Earth

Рис. 4. Снимок летно-испытательного комплекса Бирк авиабазы ВВС США Эдвардс, полученный из приложения Google Earth

Рис. 5. Снимок центра летных исследований НАСА им. Нила А. Армстронга с аэронавигационной разметкой авиабазы ВВС США Эдвардс, полученный из приложения Google Earth

Рис. 6. Снимок музея авиатехники авиабазы ВВС США Эдвардс, полученный из приложения Google Earth

Условия функционирования НРТК

Условия, или среда, где НРТК предстоит выполнять задачу, может быть двух категорий – недетерминированная (неорганизованная, неопределенная) и детерминированная (организованная, определенная) [Батанов, Грицынин, Муркин 2001].

К детерминированным средам относят среды, спроектированные и созданные человеком. В таких средах уже заранее обеспечена высокая степень организации, либо требуемая степень организации может быть достигнута при сравнительно небольших затратах. Для НРТК это означает, что робот априори «знает» точное распо-

ложение всех объектов в районе выполнения задачи. Пример такой среды для НРТК – рельсовая трасса на складе, в цехе. Также к детерминированным средам можно отнести среды, которые можно организовать требуемым образом, хотя и ценой значительных затрат. Авторы [Батанов, Грицынин, Муркин 2001] называют такие среды не полностью организованными. Назовем их условно детерминированными. В этих средах могут иметь место незначительные отклонения от эталона. Примеры – полевые склады боеприпасов, горюче-смазочных материалов, технологические позиции, отчасти стартовые позиции и т. д.

Недетерминированные среды – это среды, которые практически невозможно организовать требуемым образом. В большинстве случаев в таких средах обстановка меняется достаточно часто. Либо это среды заранее неизвестные ни роботам, ни обслуживающему персоналу. Примеры – природные среды, места ведения боевых действий, места техногенных и природных аварий, в том числе разрушенные детерминированные среды (например, после авиаудара по аэродрому противником), а также применительно к ИАО и АТО среда, где производится погрузка/разгрузка материально-технических средств с ВС или их техническое обслуживание (поскольку при проведении указанных форм авиационного обеспечения места базирования после посадки ВС, в зависимости от сложившейся оперативной обстановки, могут меняться) и т. д.

Согласно п. 652 ФАП-275[3], движение личного состава и техники по аэродрому допускается только по установленным маршрутам и с установленной скоростью. Таким образом, НРТК будут функционировать в условно детерминированной среде. Однако в случае огневого удара по аэродрому, техногенных или природных аварий и катастроф на аэродроме следует понимать, что среда может стать недетерминированной.

Также необходимо отметить, что НРТК должны функционировать как в условиях мирного времени, так и в особых условиях (при возникновении чрезвычайных ситуаций, в условиях локальных конфликтов, при проведении контртеррористических операций, в условиях ведения боевых действий, в том числе широкомасштабных).

Рассмотрим задачи АТО и ИАО, которые можно возложить на НРТК, в том числе с учетом отдаленной перспективы.

---

[3]Приказ Министра обороны РФ от 24 сентября 2004 г. № 275 «Об утверждении Федеральных авиационных правил производства полетов государственной авиации» [Электронный ресурс] // Информационно-правовой портал ГАРАНТ.РУ. URL: https://base.garant.ru/187535/ (дата обращения 14 октября 2021).

Задачи, решаемые робототехническими комплексами в ходе АТО и ИАО

Достаточно часто задачи АТО и ИАО, приведенные в федеральных авиационных правилах, носят общий характер, например, предварительная подготовка воздушного судна к полету включает[4]:

– контрольный осмотр;
– устранение выявленных при осмотре неисправностей.

В день проведения предварительной подготовки кроме подготовки ВС могут выполняться:

– периодические работы в соответствии с регламентом технического обслуживания;
– целевые осмотры и проверки;
– подготовка авиационных средств поражения и съемных агрегатов вооружения;
– замена агрегатов, выработавших ресурс;
– работы по содержанию в исправном состоянии инструмента и закрепленных за подразделением (ВС) средств наземного обслуживания специального применения и средств контроля;
– перекрестные осмотры ВС для проведения посменных полетов;
– устранение неисправностей;
– работы по уходу за авиационными средствами поражения первого боекомплекта и съемными агрегатами вооружения;
– контрольные осмотры авиационной техники руководящим инженерно-техническим составом;
– работы по уходу за специальными автомобилями подразделения, защитными укрытиями и сооружениями;
– тренажи с летным и инженерно-техническим составом;
– оформление эксплуатационной документации;
– другие работы на авиационной технике;
– контроль готовности авиационной техники и инженерно-технического состава к полетам.

Как видно, с точки зрения использования НРТК, данные задачи недостаточно конкретны. Попробуем конкретизировать задачи НРТК при проведении мероприятий АТО и ИАО. При этом в качестве среды функционирования используем склады горюче-смазочных материалов, боеприпасов, авиационно-технического имущества и элементы летного поля. Математическая мо-

[4] Приложение к приказу Министра обороны РФ № 275 от 24 сентября 2004 г. Пункт 127 [Электронный ресурс] // Информационно-правовой портал ГАРАНТ.РУ.

дель роботизации складов описана в [Андреенко 2018, Андреенко 2020]. При этом автор рассматривает базу хранения ресурсов с использованием трех видов робототехнических комплексов – стационарных, ограниченно подвижных и мобильных НРТК. В нашем случае подобные комплексы возможны на крупных авиабазах, но на полевых, оперативных аэродромах могут применяться только мобильные НРТК.

Таким образом, для обеспечения решения задач АТО и ИАО, на НРТК могут быть возложены (в ряде случаев при наличии на борту НРТК специального оборудования) следующие задачи:

- очистка аэродрома при сильных снегопадах;
- очистка покрытия ВПП, РД, аэронавигационных огней от снега, мусора, бетонной крошки и пр.;
- полив аэродрома от пыли, при запуске авиационных двигателей в жару (в частности газовочных площадок), охлаждение шасси, участие в заправке топливом, горюче-смазочными материалами, водой объектов, ВС и автотехники;
- скашивание травы;
- контрольный осмотр ВПП и РД;
- сбор антиобледенительной жидкости с поверхности аэродрома;
- участие в мелком ремонте покрытий ВПП, РД;
- восстановление маркировки на покрытиях аэродрома;
- антиобледенительная обработка и помывка ВС;
- доставка к ВС горюче-смазочных материалов, спецжидкостей и спецгазов, электрического и гидравлического оборудования, т. е. частичное выполнение функций топливо-, масло- и газозаправщиков, моторных подогревателей и кондиционеров, передвижных источников электропитания, гидравлических установок, аккумуляторных батарей, различных грузов;
- доставка к ВС и размещение на его борту авиационных средств поражения (авиабомб, управляемых и неуправляемых ракет, боеприпасов к стрелковому и артиллерийскому вооружению);
- проведение погрузочно-разгрузочных работ на военно-транспортных ВС;
- перемещение и укладка иных грузов в пределах аэродрома;
- охрана периметра аэродрома;
- другие задачи, потенциально возможные к выполнению НРТК на аэродромах.

Таким образом, речь идет о практической замене специальной аэродромной техники на НРТК. Основные преимущества предложенной замены следующие.

1. Высвобождение неквалифицированного личного состава для выполнения других функций (включая переучивание на операторов НРТК для выполнения ими специальных задач, обязательно требующих присутствия человека).

2. Снижение вероятности поражения личного состава при работе в особых условиях, в случае огневого удара по аэродрому или проведении неприятелем (террористическими организациями) диверсионных действий.

3. Снижение вероятности поражения личного состава при несанкционированной детонации авиационных средств поражения во время работы с ними.

4. Снижение массогабаритных характеристик транспортных средств за счет исключения места расположения водителя с системой жизнеобеспечения (отопление, кондиционер и др.). Снижение массы можно использовать для бронирования важных узлов НРТК, либо повышения грузоподъемности НРТК.

5. Работа в условиях химического, радиоактивного и биологического заражения участков аэродрома.

6. Снижение трудозатрат и ускорение проведения различных операций в рамках ИАО и АТО, требующих применения личного состава.

7. Соответствие как основным направлениям развития робототехники, обозначенным президентом Российской Федерации, так и общим тенденциям ее развития в мире.

Проект математической модели совместного применения на аэродромах НРТК различной степени подвижности

Основываясь на приведенном выше примере (рис. 1), работу НРТК можно представить в трех различных средах, где у каждой среды имеются свои особенности и соответственно потребуется применение различных по степени подвижности НРТК. Такими средами (S_i) будут являться:

1. S_1 – среда для работы мобильных НРТК. Включает в себя применение НРТК на позициях 1...6, 8, 10 (рис. 1) и по периметру аэродрома. Предназначена для работы мобильных НРТК по ИАО и АТО, где примером могут служить *Pan-Robots*, *RoboCV X-Motion NG* или другие аналогичные НРТК. Могут использоваться и комплексы, отличающиеся по конструктивным признакам и принципу работы, например НРТК, сконструированные для подвоза

и установки на борт ВС авиационных средств поражения. Они предназначены для замены существующих средств механизации (рис. 7a, 7b), а также охраны периметра аэродрома разведывательными и боевыми НРТК.

Рис. 7a. НРТК типа Pan-Robots

Рис. 7b. НРТК типа RoboCV X-Motion NG

2. S_2 – среда для работы стационарных НРТК. Включает в себя применение НРТК на границе позиций 5 и 7 (рис. 1). Предназначена для работы стационарных НРТК при проведении погрузочно-разгрузочных работ с материально-техническими средствами (грузами) с мобильных НРТК и автомобильной техники в складские помещения; примером может служить НРТК *Robo-Stow* (или другие отечественные аналоги), представляющий собой стационарный робот-манипулятор (рис. 1).

3. S_3 – среда для работы ограниченно подвижных НРТК. Включает в себя применение НРТК на позиции 7 (рис. 8). Предназначена для работы НРТК при перемещении грузов внутри многоярусного хранилища, примером может служить НРТК *Blastman* (либо другие аналоги), отличие которого от требуемого состоит лишь в длине телескопической колонны, количестве колен и грузоподъемности, так как он предназначен для ведения сварочных и иных работ, не требующих подъема полезной нагрузки большой массы (рис. 9).

Каждая из сред S_1, S_2, S_3 обладает своими характеристиками и должна находиться во взаимосвязи с другими, при этом:

$$\begin{cases} S_1 \cap S_2 \\ S_2 \cap S_3 \\ S_3 \cap S_1 \end{cases}$$

Рис. 8. Робот-манипулятор Robo-Stow

Рис. 9. Ограниченно подвижный мостовой НРТК Blastman

Выразим данную совокупность сред, используя круги Эйлера, в виде множеств, в которых присутствует некоторое множество роботов R, соответствующих по типу конкретной среде (рис. 10).

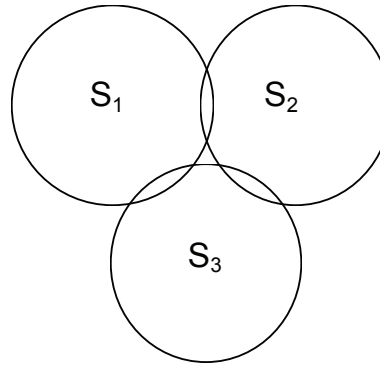


Рис. 10. Совокупность сред (S_1, S_2, S_3) работы мобильных, стационарных и ограниченно подвижных робототехнических комплексов

Соответственно:

$$\left.\begin{array}{l} R_n^{S_1} \in S_1 \\ R_n^{S_2} \in S_2 \\ R_n^{S_3} \in S_3 \end{array}\right\}$$

где n – номер робота в соответствующей среде.

Каждая из описываемых сред S_1, S_2, S_3 имеет свою систему координат (момент времени t на данном этапе несуществен, и до определенного этапа им можно пренебречь), и описать их можно следующим образом (на данном этапе количество НРТК берется из расчета: один основной НРТК и один резервный):

1. S_1 – как двумерную абсолютную систему координат, так как два мобильных робототехнических комплекса в данной среде работают в одной заданной плоскости $S_1 = \{R_1^{S1}, R_2^{S1}\}$.

2. S_2 – как трехмерную абсолютную систему координат для работы в ней двух стационарных робототехнических комплексов. Следовательно, данную среду можно описать аналогично предыдущей: $S_2 = \{R_1^{S2}, R_2^{S2}\}$.

3. S_3 – как трехмерную абсолютную систему координат для работы в ней двух ограниченно подвижных робототехнических комплексов. Соответственно опишем данную среду: $S_3 = \{R_1^{S3}, R_2^{S3}\}$.

Исходя из того, что робототехнические комплексы должны действовать во взаимосвязи друг с другом, получаем: $S_1 = \{R_1^{S1} \cup R_2^{S1}\}$; $S_2 = \{R_1^{S2} \cup R_2^{S2}\}$; $S_3 = \{R_1^{S3} \cup R_2^{S3}\} \Rightarrow$ совокупность указанных сред Z можно выразить в виде расширенной матрицы:

$$Z = \begin{Bmatrix} R_1^{S1} & R_2^{S1} & S_1 \\ R_1^{S2} & R_2^{S2} & S_2 \\ R_1^{S3} & R_2^{S3} & S_3 \end{Bmatrix}$$

В случае организации (постройки) дополнительного (как правило, на аэродромах их несколько) места хранения материально-технических средств (склад, хранилище) встает вопрос о возможности описания перемещения между двумя идентичными совокупностями сред (которые обозначим как Z_1 и Z_2), различного рода материально-технических средств (имущества, грузов). Здесь надо рассмотреть вариант применения транспортировочных мобильных робототехнических комплексов, работающих между хранилищами (складами) в двухмерной системе координат, но необходимое количество мобильных робототехнических комплексов X будет задаваться следующим образом: $X = \{R_{x1}, R_{x2}, \ldots, R_{x12}\}$.

Основываясь на изложенном выше, можно сформулировать первичную модель совместного применения наземных робототехнических комплексов на аэродромах Росгвардии (аэродромах совместного базирования). При этом она должна соответствовать следующим обязательным требованиям (условиям):

1. Должны быть учтены все совокупности систем Z.
2. Должна быть учтена составляющая мобильных робототехнических комплексов X.
3. Z и X должны находиться во взаимосвязи – т. е. все значения Z и X должны присутствовать во всех векторах матрицы (во всех строках и столбцах соответственно).

Тогда описать данную модель M можно в виде квадратной матрицы третьего порядка:

$$M = \begin{Bmatrix} X & Z_2 & Z_1 \\ Z_1 & X & Z_2 \\ Z_2 & Z_1 & X \end{Bmatrix}$$

При необходимости формирования более широкой модели рассмотрим пример, где добавляется еще одна совокупность сред работы НРТК по ИАО и АТО Z (при этом сами среды Z, аналогичные среде S_1, могут быть различны по своей структуре – как по

количеству, так и по составу роботов, что не является препятствием при формировании матричной модели, поскольку это также может быть описано согласно приведенным выше расчетам). То есть для каждой совокупности сред Z (в данном случае Z_3) существует множество сред S с входящим в него подмножеством соответствующих робототехнических комплексов R. В данном случае описать совокупность сред можно следующим образом: $Z_3 = \{S_1^{z3}, S_2^{z3}, \dots, S_n^{z3}\}$, где соответственно каждая среда S будет задаваться аналогично вышеописанному:

$$S_{12}^{x3} = \{R_1^{Sn}, R_2^{Sn}, \dots, S_{12}^{Sn}\}.$$

Тогда описываемую модель можно будет представить в виде квадратной матрицы четвертого порядка:

$$M = \begin{Bmatrix} X & Z_3 & Z_2 & Z_1 \\ Z_1 & X & Z_3 & Z_2 \\ Z_2 & Z_1 & X & Z_3 \\ Z_3 & Z_2 & Z_1 & X \end{Bmatrix}$$

Исходя из изложенного выше, следует, что общую модель совместного применения различных по степени подвижности НРТК на аэродромах Росгвардии (аэродромах совместного базирования) во взаимодействии друг с другом можно представить в виде квадратной матрицы n-го порядка. Однако здесь необходимо уже принимать в расчет временную составляющую t, поскольку без нее все описанное выше будет представлять лишь замкнутую статическую модель.

Требуемую динамическую модель можно представить следующим образом:

$$M(t) = \begin{Bmatrix} \mathbf{X} & Z_n & Z_{n-1} & \cdots & Z_{n-2} & Z_2 & Z_1 \\ Z_1 & \mathbf{X} & Z_n & \cdots & Z_{n-1} & Z_{n-2} & Z_2 \\ Z_2 & Z_1 & \mathbf{X} & \cdots & Z_n & Z_{n-1} & Z_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ Z_{n-2} & Z_2 & Z_1 & \cdots & \mathbf{X} & Z_n & Z_{n-1} \\ Z_{n-1} & Z_{n-2} & Z_2 & \cdots & Z_1 & \mathbf{X} & Z_n \\ Z_n & Z_{n-1} & Z_{n-2} & \cdots & Z_2 & Z_1 & \mathbf{X} \end{Bmatrix}$$

Из приведенного выражения $M(t)$ видно, что достоверность представленных расчетов будет подтверждаться равенством количества транспозиций элементов матрицы по строкам и столбцам с циклической перестановкой π (без повторений) соответствующему количеству размещений $\Lambda\overset{\pi}{\pi}$. То есть $\pi(Z) = \overset{\pi}{\pi}(Z)$ (здесь наличие главной диагонали, состоящей из равнозначных элементов X, в расчет не берется).

Одновременно с этим нормы любой вектор-строки x_n и любого вектор-столбца y_n описанного матричного массива будут соответствовать корню из их скалярного квадрата и будут соответственно равны: $\|x_n\|=\|y_n\|$, т. е. равенство можно выразить через соответствующие тождественные формулы:

$$\sqrt{\sum_{n=1}^{n} x_n^2} \equiv \sqrt{\sum_{n=1}^{n} y_n^2}$$

и

$$\sqrt{\sum_{n=1}^{n} x_n^2 \cdot t_n} \equiv \sqrt{\sum_{n=1}^{n} y_n^2 \cdot t_n}$$

Достоверность приведенного выражения подтверждается транспозицией ее матрицы, при которой свойства модели будут оставаться неизменными:

$$M^{T}(t) = \begin{Bmatrix} X & Z_1 & Z_2 & \cdots & Z_{n-2} & Z_{n-1} & Z_n \\ Z_n & X & Z_1 & \cdots & Z_2 & Z_{n-2} & Z_{n-1} \\ Z_{n-1} & Z_n & X & \cdots & Z_1 & Z_2 & Z_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ Z_{n-2} & Z_{n-1} & Z_n & \cdots & X & Z_1 & Z_2 \\ Z_2 & Z_{n-2} & Z_{n-1} & \cdots & Z_n & X & Z_1 \\ Z_1 & Z_2 & Z_{n-2} & \cdots & Z_{n-1} & Z_n & X \end{Bmatrix}^{T}$$

В целом визуализация представленной модели может иметь вид (рис. 11):

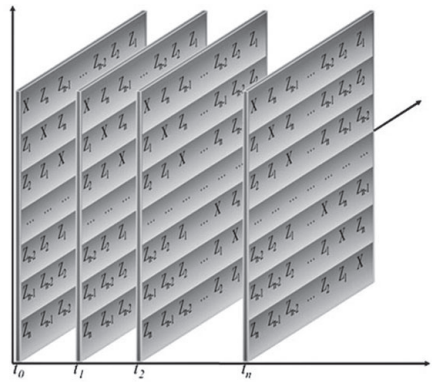


Рис. 11. Пример визуализации
модели совместного применения различных по степени подвижности
наземных робототехнических комплексов на аэродромах Росгвардии
во взаимодействии друг с другом

Выводы

В отношении практической реализации приведенной модели по совершенствованию технической составляющей деятельности инженерно-авиационной службой авиации Росгвардии наиболее целесообразно проведение научно-исследовательских и опытно-конструкторских работ (по линии роботизации АТО и ИАО Росгвардии), в частности, по направлениям:

– разработки робототехнической системы, состоящей из наземных мобильных, ограниченно-подвижных и стационарных робототехнических комплексов;
– научного обоснования экономической целесообразности технического переоснащения ИАС робототехническими средствами.

Также следует отметить, что представленная модель совместного применения различных по степени подвижности НРТК в деятельности ИАС авиации Войск национальной гвардии Российской Федерации во взаимодействии друг с другом может служить базисом при разработке системы управления НРТК в любой детерминированной среде, но данный вопрос требует более детальной проработки и отдельного исследования.

Разработка на базе предложенной обобщенной модели прикладных моделей функционирования НРТК в ходе проведения научно-исследовательских и опытно-конструкторских работ, со-

здание макетных образцов и последующее внедрение результатов НИОКР в процессы АТО и ИАО могут существенно повысить эффективность функционирования инженерно-авиационной службы авиации Федеральной службы войск национальной гвардии Российской Федерации.

Литература

Андреенко 2018 – *Андреенко С.В.* Вопросы роботизации баз хранения ресурсов МВД России // Научно-технический портал МВД России. 2018. № 2 (26). С. 50–59.

Андреенко 2020 – *Андреенко С.В.* Вопросы роботизации баз хранения ресурсов МВД России и их математического моделирования // Взаимодействие вузов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности: Международный круглый стол. Воронеж: Кварта, 2020. С. 122–136.

Батанов, Грицынин, Муркин 2001 – *Батанов А.Ф.*, *Грицынин С.Н.*, *Муркин С.В.* Робототехнические комплексы для обеспечения специальных операций [Электронный ресурс] // Бюро научно-технической информации. URL: http://www.bnti.ru/showart.asp?aid=456&lvl=02.01.02.02 (дата обращения 19 октября 2021).

Поздняков, Каргапольцев, Губарев 2015 – *Поздняков А.В., Каргапольцев А.А., Губарев С.А.* Тактика военно-воздушных сил: Учеб. пособ. [Электронный ресурс]. URL: https://files.mai.ru/site/unit/institute-of-military-science/tvvs/ (дата обращения 19 октября 2021).

Сазонов, Лукин, Матвеев 2006 – *Сазонов Д.В., Лукин А.С., Матвеев А.И.* Инженерно-авиационное обеспечение государственной авиации. Федеральные авиационные правила инженерно-авиационного обеспечения государственной авиации. Ч. 1. Самара: Самарский государственный аэрокосмический университет, 2006.

References

Andreenko, S.V. (2018), “Issues of resources storage base robotization of the MIA RF”, *Scientific and technical portal MIA of Russia*, no. 2 (26), pp. 50–59.

Andreenko, S.V. (2020), “Issues of resources storage base robotization of the Ministry for Internal Affairs of the Russian Federation and their mathematical modeling”, *Int. Round Table “Interaction of universities, scientific organizations and cultural institutions in the field of information protection and security technologies”*, Kvarta, Voronezh, Russia, pp. 122–136.

Batanov, A.F., Gricynin, S.N. and Murkin, S.V. (2001), “Robotic systems for special operations”, *Bureau of Scientific and Technical Information*, [Online], available at

http://www.bnti.ru/showart.asp?aid=456&lvl=02.01.02.02 (Accessed 19 October 2021).

Pozdnyakov, A.V., Kargapoltsev, A.A. and Gubarev, S.A. (2015), *"Taktika voyenno-vozdushnykh sil: Ucheb. posob."* [Air Force tactics: study guide], [Online], available at https://files.mai.ru/site/unit/institute-of-military-science/tvvs/ (Accessed 19 October 2021).

Sazonov, D.V., Lukin, A.S. and Matveev, A.I. (2006), *Inzhenerno-aviatsionnoe obespechenie gosudarstvennoj aviatsii. Federal'nye aviatsionnye pravila inzhenerno-aviatsionnogo obespecheniya gosudarstvennoj aviatsii. Chast 1* [Engineering and aviation support of state aviation. Federal Aviation Rules for Engineering and Aviation Support of State Aviation. Part 1], Samara State Aerospace University, Samara, Russia.

Информация об авторах

Сергей В. Андреенко, Центральная объединенная база хранения ресурсов МВД России, Балашиха, Московская обл., Россия; 143914, Россия, Московская обл., Балашиха, микрорайон Никольско-Архангельский, производственно-складская зона, влад. 1; andreenko.sergej@yandex.ru

Дмитрий А. Митюшин, кандидат технических наук, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; dalexx@inbox.ru

Андрей М. Сапунов, Главное управление авиации Росгвардии, Москва, Россия; 111250, Россия, Москва, ул. Красноказарменная, д. 9; asapunov.am@mail.ru

Information about the authors

Sergey V. Andreenko, Central unified resource storage base of the MIA RF, Balashikha, Moscow region, Russia; est. 1, Production and warehouse area, Nikolsko-Arkhangelskii neighborhood, Balashikha, Moscow region, Russia, 111024; andreenko.sergej@yandex.ru

Dmitry A. Mityushin, Cand. of Sci. (Engineering), Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; dalexx@inbox.ru

Andrey M. Sapunov, Rosgvardiya's General Aviation Authority, Moscow, Russia; bld. 9, Krasnokazarmennaya Str., Moscow, Russia, 111250; sapunov.am@mail.ru

УДК 37.016:519.7
DOI: 10.28995/2686-679X-2022-1-120-136

К вопросу о моделировании методики преподавания дисциплин в педагогике

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

Арслан П. Марданов
Ташкентский государственный технологический университет им. Ислама Каримова, Ташкент, Республика Узбекистан, apardayevich@mail.ru

Нилуфар У. Окбаева
Каршинский государственный университет, Карши, Республика Узбекистан, oqboyeva@internet.ru

Аннотация. Педагогика средней общеобразовательной и высшей школы имеет общую проблему – соотношение языка науки с уровнями абстракций изучаемых объектов, проблем. Если в общеобразовательной школе можно говорить о пропедевтике языка и проблем, то в высшей школе в части моделирования проблем поздно обсуждать необходимые уровни абстракций и способы их описания. В некоторых случаях нахождение общего образовательного (терминологического базового) языка отчасти решает проблему восприятия и обучения подходу к формулировке изучения возникающих при решении задач. На основании примеров из практики преподавания разделов высшей математики и составления моделей курсов с использованием математического моделирования и вычислительных методов для решения изучаемых задач дан опыт вариации моделей обучения в различных образовательных средах. В основу положены работа, пособия, конспекты учебных специальных курсов по высшей математике из трех учебных заведений: ТГТУ им. Ислама Каримова, Государственный университет Карши и РГГУ. В настоящее время степень формализации учебных материалов все больше приобретает высокие уровни абстракции, поэтому студентам (бакалаврам и магистрам) все больше необходим математический язык из разделов вариационного исчисления, символьных методов, топологии и т. д. Сформулировано представление об образовательной системе, построенной на традиционном образовании, и ее соответствии новым требованиям, возникающим в обществе.

Ключевые слова: атомарные понятия, минимальный словарь, электронно-образовательная система, информационно-педагогическая среда, модель педагогическая, лингвистики

Для цитирования: Жаров В.К., Марданов А.П., Окбаева Н.У. К вопросу о моделировании методики преподавания дисциплин в педагогике // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2022. № 1. С. 120–136. DOI: 10.28995/2686-679X-2022-1-120-136

On the issue of modeling the methodology of teaching disciplines in pedagogy

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

Arslan P. Mardanov
Karimov Tashkent State Technical University, Tashkent, Uzbekistan, apardayevich@mail.ru

Nilufar U. Okbayeva
Karshi State University, Karshi, Uzbekistan, oqboyeva@internet.ru

Abstract. The pedagogy of secondary general education and higher education has a common problem – the correlation of the language of science with the levels of abstraction of the objects and problems under study. If in a general education school one can talk about the propaedeutics of language and problems, then in higher education, in terms of modeling problems, it is too late to discuss the necessary levels of abstractions and ways to describe them. In some cases, finding a common educational (terminological base) language partly solves the problem of perception and learning the approach to formulation, studying the problems that arise when solving problems. Based on examples from the practice of teaching sections of higher mathematics and compiling course models using mathematical modeling and computational methods for solving the problems under study, the experience of varying learning models in various educational environments is given. The basis is the work, manuals, abstracts of educational special courses in higher mathematics from three educational institutions: TSTU. Islam Karimov, Karshi State University and RSUH. At present, the degree of formalization of educational materials is increasingly acquiring high levels of abstraction, so students (bachelors

and masters) increasingly need a mathematical language from sections of the calculus of variations, symbolic methods, topology, etc. An idea is formulated about the educational system built on traditional education and its compliance with the new requirements that arise in society.

Keywords: atomic concepts, minimal vocabulary, electronic educational system, information and pedagogical environment, pedagogical model, linguistics

For citation: Zharov, V.K., Mardanov, A.P. and Okbaeva, N.U. (2022), "On the issue of modeling the methodology of teaching disciplines in pedagogy", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series,* no. 1, pp. 120–136, DOI: 10.28995/2686-679X-2022-1-120-136

Введение

Приведем схему-модель целей российской, советской образовательной системы средней общеобразовательной школы. Представим ее крупными «мазками».

Чему должен обучиться ребенок в указанной образовательной системе?	Какие свойства должны развиваться при обучении в школе?
Базовой терминологии	Анализ
Грамотному построению речи	Синтез
Основным логическим операциям, не только с помощью естественнонаучных дисциплин, но прежде всего с помощью родной речи	Обобщение
Иметь представление о предметных задачах учебных дисциплин	Умение вести (поддерживать) учебный, научный дискурс

Предложенную схему назовем схемой традиционного образования. В ней, прежде всего, целью является развитие способностей ребенка и его модальность во взрослой жизни, основанная на умении задавать вопросы, критически мыслить и видеть возможности профессиональной реализации. Также ясно, что предложенная схема противоречит соросовской модели образования-тестирования (навязанной нам в начале двухтысячных годов). Наш опыт преподавания в средней школе и вузе приводит к утверждению: тестирование воспитывает психологический изоляционизм в учениках, а это противоречит этническим установкам людей, традици-

онно живших на территории Российской империи. Из этого вовсе не следует, что мы отрицаем тестирование, но уровень проверки навыков алгоритмического или рецептурного знания никогда не являлся целью российской школы – для этого достаточно обратиться к учебникам А.П. Киселева, Н.Л. Глинки, Ю.В. Ходакова, В.В. Авдеева, В.Г. Короленко, Г.С. Ландсберга и других.

Примеры из современной практики преподавания математики

Первым примером может служить содержание специального курса вообще говоря традиционного для педагогических институтов, но обратим внимание на его окончание. Итак:

Введение
I. Теория пределов числовых последовательностей
  1.1. Последовательность чисел и их предел. Свойства сходящихся последовательностей и операции над ними
  1.3. Монотонные последовательности и их предельные фундаментальные последовательности. Теорема Коши
II. Функция и ее предел в точке и на бесконечности
  2.1. Понятие функции. Функциональные зависимости
  2.2. Элементарные функции
  2.3. Ограниченные функции
  2.4. Предельные свойства функции. Существование предела
  2.5. Сравнение функций
III. Непрерывность и плоская непрерывность функций
  3.1. Понятие непрерывности функции
  3.2. Свойства непрерывных функций
  3.3. Плоская непрерывность функции. Теорема Кантора
  3.4. Компактное множество. Непрерывность на компакте
Использованная литература

Заметим, что в предлагаемой программе для третьего или четвертого курсов будущих учителей математики реанимируются хорошо зарекомендовавшие себя идеи курса математического анализа. Основная идея в постепенном обобщении, переходе к все более высокой степени абстракции вводимых понятий. В этой традиции выдержан весь курс, закрепление же понятий происходит на удачно подобранных заданиях и упражнениях. Кроме этого, обратим внимание, что введение в обиход (пропедевтика) топологиче-

ского языка в лексикон будущих педагогов-математиков позволяет эффективно развивать курсы информационных систем и моделей учебных программ вузов, что вполне полезно будет будущим ученикам этих учителей.

Здесь же приведем еще один пример из практики преподавания в техническом университете. Для этого рассмотрим специальный курс для инженеров-бакалавров и магистров: Преобразование Лапласа как один из способов решения в моделях задач инженерного дела.

Прежде сделаем несколько замечаний. В истории применения математики в инженерном деле пользовались популярностью известные методы решения дифференциальных уравнений, особенно те методы, которые наиболее просто использовали вычислительный аппарат и были «прозрачны» для понимания. У инженеров внимание было направленно на символический (или, как теперь называют, операционный) метод интегрирования линейных дифференциальных уравнений и систем. В конце девятнадцатого века этот метод был усовершенствован американским инженером-электриком Оливером Хэвисайдом (1850–1925). Сначала он был предложен без строгого математического обоснования. Но поразительный успех метода заставил объяснить его с математической точки зрения, что привело к полному оправданию и дальнейшему развитию символических методов.

Применение операционного метода для решения задачи Коши позволяет свести решение дифференциального уравнения для некоторой функции $x(t)$ к решению алгебраического уравнения относительно ее «изображения» – функции $X(p)$. Операции над изображением оказываются более простыми.

Операционный метод хорош своей универсальностью. При решении дифференциальных уравнения и систем операционным методом нет необходимости обращать внимание на такие важные для других методов решения обстоятельства, как:

– составление фундаментальной системы решений и общего решения линейного однородного уравнения, или системы по виду корней характеристического уравнения;
– поиск частного решения линейного неоднородного уравнения по виду правой части с учетом корней характеристического уравнения. Особый выигрыш дает операционный метод при интегрировании систем, характеристические уравнения для которых имеют комплексные или кратные корни.

Еще небольшое замечание. Понятие модели в современной науке стало настолько привычным, что сама потребность выяснения содержания этого понятия почти перестала осознаваться. Мо-

делирование оказалось одним из эффективных, многообразных и универсальных методов научного познания. Это понятие остается одним из наиболее значимых при изучении гносеологических аспектов современной науки. Несмотря на традиционность, понятие модели содержит важные потенции развития, которые при их реализации дают возможность естественного перехода от теоретико-множественных методов научного описания реальных объектов к системным. Поэтому выяснение познавательной роли моделей и моделирования существенно для понимания гносеологических аспектов современной науки и обнаружения в ней неклассических тенденций описания изучаемых объектов.

Следующее замечание. В модели организации такого спецкурса прежде всего учитываются предметные задачи (профессиональные, элементы профессиональных задач), встречавшиеся ранее в обучении по программам физики, электроники, теоретической и технической механики. Весь курс до профессиональных задач состоит из практического и теоретического справочного материала, вводимого с помощью соответствующих задач. Приведем сокращенный пример задачи из [Ляшенко 2018].

...Для мониторинга параметров паровой котельной установки теплоэлектростанции предлагается рассмотреть котельный агрегат как объект с распределенными параметрами. В качестве примера был рассмотрен паровой котел БКЗ-75-39 ГМА.

Паровой котел БКЗ-75-39 ГМА предназначен для получения перегретого пара. Котел барабанный, с естественной циркуляцией, с камерным сжиганием топлива. В котле происходит нагрев воды, ее испарение и перегрев образовавшегося пара. В качестве топлива используется природный газ. Котел предназначен для работы в закрытых помещениях. Паропроизводительность котла 75 т/час, (при реконструкции предусматривается увеличение производительности до 90 т/час), абсолютное давление пара 3,9 МПа и температура 440°С, температура питательной воды 140°С.

Разработка математической модели технологических процессов. Режим течения пароводяной смеси в экранных трубках парогенератора зависит от теплофизических свойств жидкости и пара, расходов отдельных фаз, а также от размеров и положения трубки в пространстве. В вертикальных трубках существуют 4 основных режима течения: пузырьковый, снарядный, кольцевой и эмульсионный. Вследствие постепенного испарения воды в экранных трубах прямоточного парогенератора возможны все режимы двухфазного течения.

Теплообмен в экранных трубках. Значительная часть экранных труб парогенератора находится в пределах топки котла, где темпе-

ратура факела достигает 2000°С. Согласно закону Стефана-Больцмана, описывающему теплообмен путем излучения, тепловой поток между факелом с температурой $\Theta_ф$ и стенкой топки с температурой $\Theta_{ст}$ определяется зависимостью

$$Q_{1-2} = \varepsilon_ф \varepsilon_{ст} C_0 F \left[\left(\frac{\Theta_ф}{100} \right)^4 - \left(\frac{\Theta_{ст}}{100} \right)^4 \right],$$

где $\Theta_{ст}$, $\varepsilon_ф$, $\varepsilon_{ст}$ – приведенные коэффициенты излучения факела и стенки топки соответственно; $C_0 = 5{,}76$ Вт/(м$^2 \cdot K^4$) – коэффициент излучения абсолютно черного тела. Поскольку температура факела значительно выше температуры поверхности нагрева, можно принять, что тепловой поток не зависит от температуры трубок.

Рассмотрим уравнения движения, описывающие течение одно- и двухфазной рабочей среды в экранных трубках парогенератора.

Дифференциальные уравнения однофазного потока. Условия баланса массы, энергии и количества движения для однофазного течения в трубках парогенератора в результате преобразований можно приближенно записать в виде системы нелинейных дифференциальных уравнений в частных производных:

$$\frac{\partial M}{\partial z} = -\frac{\partial \rho}{\partial t};$$

$$\rho \frac{\partial h}{\partial t} + M \frac{\partial h}{\partial z} - \frac{\partial p}{\partial t} - \frac{M}{\rho} \frac{\partial p}{\partial z} = q'_d;$$

$$\frac{\partial M}{dt} + 2\frac{M}{\rho} \frac{\partial M}{\partial z} - \frac{M^2}{\rho^2} \frac{\partial \rho}{\partial z} + \rho g \cos\beta + 10^3 \frac{\partial p}{\partial z} + f \frac{M^2}{\rho} = 0,$$

где $M(z, t) = \rho w$ – массовый расход (w – скорость движения жидкости);
$\rho(z, t) = (p, h)$ – плотность жидкости;
$h(z, t)$ – энтальпия жидкости;
$p(z, t)$ – давление;
$q'_d = \pi d \alpha (\Theta_{in} - \upsilon)$ – внутренний тепловой поток на единицу длины трубки (d – внутренний диаметр трубки);
$\alpha(p, h, M, q)$ – коэффициент теплообмена;
q – тепловой поток на единицу длины трубки;
Θ_{in} – температура внутренней поверхности стенки трубки;
Θ – температура рабочей среды;

υ (p, h) –температура жидкости;
g – ускорение свободного падения;
β – угол между трубкой парогенератора и вертикалью;
f – коэффициент потери давления.

Система уравнений в частных производных гиперболического типа имеет характеристические значения w, $w + c_s$, $w – c_s$, определяющие скорости перемещений вдоль длины трубки, где c_s – скорость звука.

Аналогично были разработаны дифференциальные уравнения для многофазного потока парожидкостной смеси. Парожидкостный поток, перемещающийся в экранной трубке парогенератора, можно считать одномерным. В таком случае система дифференциальных уравнений, описывающих течение пароводяной смеси в экранных трубках парогенератора, принимает следующий вид:

$$\frac{\partial M}{\partial z} = -\frac{\partial \rho}{\partial t};$$

$$\rho \frac{\partial h}{\partial t} + M \frac{\partial h}{\partial t} - \frac{\partial \rho}{\partial t} - \frac{M}{\rho}\frac{\partial \rho}{\partial z} = q_d^{'} - \frac{\partial}{\partial z}\left[M\left(\frac{w_2}{w} - 1\right)(h - h')\right];$$

$$\frac{\partial M}{\partial t} + 2\frac{M}{\rho}\frac{\partial M}{\partial z} - \frac{M^2}{\rho^2}\frac{\partial \rho}{\partial z} + \rho g \cos\beta + 10^3 \frac{\partial p}{\partial z} + f\frac{M^2}{\rho} = 0;$$

$$\frac{w_2}{w} = 1/[c + (1 - c)/S]; \quad S = f(M, p, h),$$

где $(z, t) = (p, h)$ – плотность пароводяной смеси;
h (z, t) – энтальпия пароводяной смеси;
w_2 – скорость движения пара;
w – скорость пароводяной смеси;
h' – энтальпия кипящей воды;
$c = (h - h') / h_{21}$ – массовая доля пара ($h_{21} = h'' - h'$) – тепло испарения;
h'' – энтальпия сухого насыщенного пара;
$(1 - c)$ – массовая доля воды;
$S = w_2 / w_1 = (1 – x)\, c$ – коэффициент скольжения;
$w_1 = (1 – x)\, w / (1 – c)$ – скорость движения воды;
$x = cw_2 / w$ – массовое расходное паросодержание.

Дифференциальные уравнения теплообмена в стенках трубок. Если параметры материала трубки λ, ρ_{Tp} и c_{Tp} с не зависят от температуры, уравнение теплопроводности принимает форму:

$$\frac{\partial \Theta}{\partial t} = a\nabla^2\Theta,$$

где $a = \dfrac{\lambda}{\left(\rho_{Tp} c_{Tp}\right)}$ – коэффициент выравнивания температур;

λ – коэффициент теплопроводности;

ρ_{Tp} и c_{Tp} – плотность и удельная теплоемкость стенки трубки.

В цилиндрической системе координат лапласиан имеет вид

$$\nabla^2\Theta = \frac{1}{r}\frac{\partial}{\partial r}\left(r\frac{\partial \Theta}{\partial r}\right) + \frac{1}{r^2}\frac{\partial^2\Theta}{\partial \varphi^2} + \frac{\partial^2\Theta}{\partial z^2}$$

при граничных условиях:

$$\pi D\lambda\left(\frac{\partial \Theta}{\partial r}\right)_{r=\frac{D}{2}} = q\ ,$$

$$\pi d\lambda\left(\frac{\partial \Theta}{\partial r}\right)_{r=\frac{d}{2}} = \pi d\alpha\left[\Theta_{in} - \vartheta\right] = q_{in},$$

где r – радиальная координата;

φ – угол по периметру трубки;

D, d – внешний и внутренний диаметры трубки парогенератора;

Θ_{in} – температура внутренней поверхности стенки трубки.

В условиях эксплуатации парогенератора градиентом температуры вдоль оси можно пренебречь по сравнению с градиентом вдоль радиуса и периметра трубки.

Приведенные примеры объединяются общей идеей в моделировании методики преподнесения знаний, а именно целеустановкой, т. е. знание не для самого знания, а прежде всего для его приложения. Это становится очевидным, если мы рассмотрим базовую терминологию в примерах, и как она должна совершенствоваться, развиваться в лексиконах студентов, а следовательно, создаваться предпосылки для адаптации к изменяющимся со временем профессиональным тезаурусам. Уточним изложенную идею с помощью языка моделей и тезаурусов.

1. Атомарность понятий в базовой терминологии. Модель развивающегося знания.

Напомним, что до конца шестидесятых годов прошлого века в курсах арифметики и алгебры неполной средней восьмилетней

(семилетней) школы на уроках математики главными вопросами были – «Поставил ли необходимые вопросы к задаче? (О чем эта задача? Перескажи ее суть? Что дано в условии, и что ты должен найти? Сформулируй вопросы, определяющие ход решения задачи? и т. д.) Что же сейчас? Решение задачи будет получено, если начертим таблицу и поставим данные задачи в нужные ячейки (заполним таблицу нужной информацией), или «мы подобную задачу решали», «смотрите внимательнее!». Понятно, что подходы к задачам в том и другом случае отличны или принципиально различны методики. Можно предположить, что такое «размышление», как в последнем случае, относится к начальной ступени обучения школьников, но с появлением ЕГЭ этот подход стал легальным, необходимым для сдачи тестов по ЕГЭ.

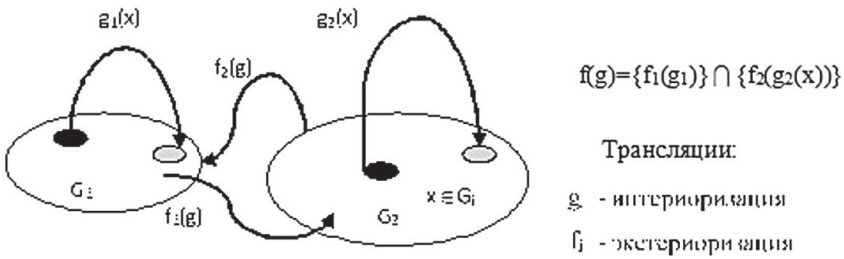
Случился парадокс, в середине шестидесятых педагоги-методисты-математики «уходили» от формального понимания учащимися задачи. Целью педагога было не решение задачи, а ее реальная сущность, если хотите, житейская необходимость. Теперь же пришли к формальным тестам и формальным знаниям, научениям, т. е. замене мышления на тренировку памяти, поисковым задачам. На самом деле тесты не такое уж зло, но в реалиях российского образования они оказались противоречащими традиционному образованию. Модель тестирования, предложенная в КНР, оказалась много эффективнее и полезнее китайскому математическому образованию, нежели наша реализация в период В.М. Филиппова – А.А. Фурсенко. На эту тему один из авторов статьи выступал в 2000 и 2005 годах в МГОПУ на методическом семинаре «Передовые идеи педагогики».

Что же происходит по традиционной схеме обучения математике (первая часть примера)?

Рассмотрим процесс решения задачи пристально. Первая методическая модель направляет школьника на решение «внутренних задач или цепочки задач, построенных на здравом смысле, на понимании задачи». Это значит, что во время интериоризации ему (ученику) необходимо выяснить структуру задачи явно, облачив ее в некоторую речевую форму, представив ее в собственном лексиконе, не в воспроизведенной терминологии. А это уже очень сложная задача, и решению подобных задач нужно учиться. Затем необходимо провести анализ понятой структуры задачи, а уж затем сформулировать вопросы, ведущие к ответам на самостоятельно поставленные вопросы. После чего в классической методике преподавания математики наступал процесс, называемый экстериоризацией, и затем наступал черед процесса коммуникации, который должен оформить результат осмысления задачи [Морковкин, Морковкина

1994] [Давыдов 1972] [Жаров 2003]. Иначе, декодировать данную задачей структуру (формальную конструкцию) в доступный текст, оформленный элементами универсальной, личностной знаковой системой. В такой методике («старой» методике) реакция учащегося конструктивна, т. е. в процессе осмысления задачи возникает и метод ее решения. Итак, вербализуя текст задания в собственном лексиконе (лексиконе, отражающем личностную микросреду), учащийся создает его модель, а занимаясь формулировками вопросов к составляющим частям задачи – уточняет смыслы разбираемых задач и соответствующие модели своего мыслительного опыта, обобщая смыслы, формирует результаты в форме уравнений, приемов упрощений, причинно-следственных выводах.

Изложенное в пункте можно интерпретировать следующим образом (схемой).



Заданы блоки количества информации (по тексту задачи составьте таблицу, вспомните, мы решали подобную задачу), поисковая схема (перебор ячеек памяти, аналоги по признакам конкретной задачи) $g_1(x) \cdot f_i$ – трансляция найденного, проверенного, решенного или похожего на решение во внешнюю контролирующую область (учитель, педагог, книга (решебник, задачник и т. д.)). Итак, методы (способы) изменения (управления) информационной средой личности (потоками информации) в процессе обучения и образуют методику преподавания учебной дисциплины.

Таким образом, взаимное или любое из односторонних влияний лексиконов, а попросту отображений, порождает множество функционалов определенной природы – они линейные, мультипликативные, но без свойства ассоциативности. Последнее свойство вполне очевидно, так как восприятие потока одной и той же порции информации различными субъектами может иметь различные количественные показатели: $I(fgh) \neq I(f)I(gh) \neq I(fg)I(h)$. Поскольку в процессе интериоризации при идеальных условиях, понимая под ними воспроизведение доказательств (математических положений,

аксиоматик или иных математических фактов) для достаточного представления на одном и том же языке информации, количество порции предложенной информации субъектам будет не меньше исходной (за исключением патологических случаев).

Приведем еще один пример. Известно, что в языкознании весьма стойко укрепились понятия «денотат» (denotatum) – обозначаемое (обозначаемый предмет, означающее, по Ф. де Соссюру) и «сигнификат» (significatum) – обозначаемое (содержание языкового знака, означаемое, по Ф. де Соссюру): первое значит значение чего-либо, а второе – содержание понятия, т. е. форма (референтная форма) и содержательная сущность.

Рассмотрим типичный «библиотечный», алгоритмический подход к решению проблемной ситуации. «Задача понимания новой ситуации отчасти состоит в том, чтобы найти в прежнем знании уже существующие схемы, которые могли бы послужить ориентиром для построения новой схемы, соответствующей новой ситуации» [Норман 1985]. Несложно заметить, что «построение новой схемы», как минимум, с точки зрения педагога требует умения «построения», т. е. строить (Из чего строим? Что строим? Строим сразу все здание или постепенно?), навыка «сравнения» (информированности об объектах сравнения, методах и т. д.). Рассуждая – моделируя (априорно или обучено? А может быть, алгоритмично?). Возможно, это был явный лозунг творческой личности (эмоциональный фон), а может быть, пытливый ум? И еще одни фрагмент: «Когда мы стараемся научиться чему-то, мы должны создавать соответствующие новые схемы, которыми можно руководствоваться в действиях» [Norman 1986]. Это очень важный элемент модели обучения математике. К оформлению всей конструктивной модели обучения математике надо указать на некоторые параллели. Во-первых, математика – это язык, на котором говорит наука. Во-вторых, в каждой науке, знании есть своя математика [Лосев 1990]. Следуя этому утверждению [Манин 2008], можно принять математику в качестве раздела лингвистики, со своим алфавитом, грамматикой, синтаксисом, построением семантических связей. Считая, что каждый индивидуум с течением времени овладевает своей знаковой системой, опытом построения связей с окружающей его средой, и понимая, что социум обладает образовательной функцией, можно предположить, что в процессе школьного образования, получения профессиональной квалификации у обучаемого формируется универсальная знаковая система, частью которой является математическая знаковая система со своими правилами вывода. Поэтому предложенная выше схема, вообще говоря, также иллюстрирует процесс развития лексико-

нов, в основании которых лежит универсальная (математическая) знаковая система.

В конструкции мягких моделей [Арнольд 2000] успешно могут быть использованы понятия топологической модели и топологической реляционной системы [Матвеев 2010]. Действительно, на языке топологии поддаются осмыслению и точному описанию семантические базисы (лингвистические тезаурусы), иерархический процесс представления базисных объектов наборами основных признаков с заданными внутренними ассоциативными связями. При таком подходе признаковое пространство наделяется топологической структурой и множеством четких и/или нечетких отношений различной местности. Граф состояний, получаемый при таком подходе, является достаточно точным аналогом ситуации.

В качестве примера вышеизложенного рассмотрим набросок каркаса модели языка обучения. Пусть D = (Q, P, S), где Q есть множество терминов тезауруса, P – множество характеристик, заданных на признаковом пространстве, S – множество нечетких операций и отношений, описывающих, насколько естественен данный объект научному языку определенной области. Тезаурус называется атомарным словарем, если все его элементы уникальны, т. е. не определяются через другие слова любого другого списка. Тезаурус является многоуровневой системой. С помощью одноместной операции присоединения слова одного уровня переводятся в следующий уровень. Многоместные отношения характеризуют словарные гнезда, которые осуществляют ассоциативные связи между различными (не обязательно соседними) уровнями тезауруса. Признаковое пространство наделяется определенной топологией, обусловленной семантическими закономерностями данного тезауруса, ориентированного на заданную часть предметной области. Построение моделей тезаурусов данного класса направлено на постепенное расширение словарного запаса слушателя, на усвоение им ключевых понятий изучаемой теории, глубокое понимание теорем, доказательство которых не должно быть зазубренной цепочкой логических рассуждений [Матвеев 2010, Жаров] [Матвеев 2009]. Заметим, что подобный подход был реализован в конце прошлого века при составлении минимальных словарей, имеющих чрезвычайно важное значение в методике обучения иностранных студентов [Жаров, Матвеев 2009] [Баранова, Жаров 2006]. Важно, чтобы используемые в методике атомарные понятия имели прямое согласование, пересечение с параллельными тематическими планами лекционных и семинарских занятий. Это влияет на скорость освоения изучаемой новой учебной дисциплины, то есть время решения задачи логической адаптации. Напомним, в книге Бертрана

Рассела «Человеческое познание. Его сферы и границы» рассмотрен анализ научных понятий. Утверждается, что слова, употребляемые в той или иной науке, могут быть определены небольшим количеством терминов из числа этих слов. Такой набор начальных слов называется «минимальным словарем» науки, если:

1) каждое иное слово, употребляемое в науке, имеет номинальное определение с помощью слов минимального словаря;
2) ни одно из этих начальных слов не имеет номинального определения с помощью других начальных слов.

Эти понятия, образующие минимальные словари, называют атомарными словами.

Заключение

Вернемся к схеме-модели, данной в начале статьи. Теперь ясно, что к предложенной схеме следует добавить ряд атомарных понятий (слов), объединяющих указанные выше (п. 1) в примерах специальных курсов по математике для бакалавров и для магистров, отраженных в следующем минимальном словаре математики:

Арифметика:
- единица;
- множество;
- сравнение;
- прибавить (сложить);
- знак числа: положительный, отрицательный;
- соответствие.

Элементарная алгебра:
- неизвестная величина;
- уравнение;
- корень уравнения;
- одночлен, многочлен;
- неравенство;
- функция.

Элементарная геометрия.

1. Основные понятия (объекты): точка, прямая и плоскость.

2. Основные понятия (отношения между объектами): принадлежать, находиться между, конгруэнтность (равенство).

Математический анализ:
- бесконечность;
- стремление;
- последовательность;
- предел.

Вспомогательные термины:
- аксиома;
- теорема;
- постулат;
- доказательство;
- рассуждение;
- модель;
- условие, заключение;
- соединять;
- порядок;
- угол;
- непрерывность;
- параллельность, перпендикулярность;
- геометрическое место точек.

Здесь следует заметить, что словарь вспомогательных терминов может быть организован как это сделано у Киселева А.П. или у Шаталова В.Ф.

Во всяком случае, система знаний, организованная по восходящей востребованности в абстрактных понятиях с учетом предметных задач из любой области, позволяет строить общее основание, общий понятийный фундамент ко всей общеобразовательной школе и не только к ней.

Литература

Арнольд 2000 – *Арнольд В.И.* «Жесткие» и «мягкие» модели. М.: МЦНМО, 2000.

Баранова, Жаров 2006 – *Баранова Н.М., Жаров В.К.* Об аподиктических свойствах представления процесса обучения иностранных студентов и онтология содержания предмета учебной дисциплины // Гражданская авиация на современном этапе развития науки, техники и общества. Труды международной научно-технической конференции. М.: МГОУ, 2006. С. 317.

Давыдов 1972 – *Давыдов В.В.* Виды обобщения в обучении (логико-психологические проблемы построения учебных предметов). М.: Педагогика, 1972.

Жаров, Матвеев 2009 – *Жаров В.К., Матвеев О.А.* Методические аспекты описания и моделирования информационной педагогической среды процесса обучения российских и иностранных студентов дисциплинам математического цикла в высших учебных заведениях // Вестник МГОУ. Педагогика. 2009. № 4. С. 103–107.

Жаров 2003 – *Жаров В.К.* О теоретических предпосылках методики использования тезаурусов при обучении иностранных учащихся в техническом университете // Проблемы преподавания РКИ в вузах инженерного профиля. М.: Янус-К, 2003. С. 253–258.

Лосев 1990 – *Лосев А.Ф.* Философия имени. М.: МГУ, 1990.

Ляшенко 2018 – *Ляшенко А.Л.* Математическая модель тепловых процессов парового котла теплоэлектростанции // Известия ЮФУ. Технические науки. 2018. № 5. С. 101–110.

Манин 2008 – *Манин Ю.И.* Математика как метафора. М.: МЦНМО, 2008.

Морковкин, Морковкина 1994 – *Морковкин В.В., Морковкина А.В.* Язык, мышление и сознание et vice versa // Русский язык. 1994. № 1. С. 63–70.

Norman 1985 – *Norman D.* Learning and Memory. San Francisco: W.H. Freeman, 1982.

References

Arnold, V.I. (2000), *"Zhestkie" i "myagkie" modeli* ["Hard" and "soft" models], MTsNMO, Moscow, Russia.

Baranova, N.M. and Zharov, V.K. (2006), "On the apodictic properties of the representation of the process of teaching foreign students and the ontology of the content of the subject of the academic discipline", *Civil aviation at the present stage of development of science, technology and society. Proceedings of the international scientific and technical conference*, Moscow, Russia, p. 317.

Davydov, V.V. (1972), *Vidy obobscheniya v obuchenii (logiko-psihologicheskie problemy postroeniya uchebnykh predmetov)* [Types of generalization in teaching (logical and psychological problems of constructing educational subjects)], Pedagogika, Moscow, Russia.

Liashenko, A.L. (2018), "Mathematical model of thermal processes in a heat-electric power station steam boiler", *Izvestiya SFedU. Engineering Sciences*, no. 5, pp. 101–110.

Losev, A.F. (1990), *Filosofiya imeni* [Philosophy of name], Moscow State University, Moscow, USSR.

Manin, Yu.I. (2008), *Matematika kak metafora* [Mathematics as a metaphor], MTsNMO, Moscow, Russia.

Morkovkin, V.V. and Morkovkina, A.V. (1994), "Language, thought and consciousness et vice versa", *Russkiy yazyk*, no. 1, pp. 63–70.

Norman, D. (1985), *Memory and learning,* W.H. Freeman, San Francisco, USA.

Zharov, V.K. (2003), "On the theoretical prerequisites for the methodology of using thesauri in teaching foreign students at a technical university", *Problems of teaching Russian as a foreign language in engineering universities*, Janus-K, Moscow, Russia, pp. 253–258.

Zharov, V.K. and Matveev, O.A. (2009), "Methodological aspects of describing and modeling the information pedagogical environment of the process of teaching Russian and foreign students the disciplines of the mathematical cycle in higher educational institutions", *Vestnik MGOU. Pedagogika*, no. 4, pp. 103–107.

Информация об авторах

Валентин К. Жаров, доктор педагогических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; valcon@mail.ru

Арслан П. Марданов, Ташкентский государственный технический университет имени И.А. Каримова, Ташкент, Республика Узбекистан; 100174, Республика Узбекистан, Ташкент, ул. Университетская, д. 2; apardayevich@mail.ru

Нилуфар У. Окбаева, Каршинский государственный университет, Карши, Республика Узбекистан; 180103, Республика Узбекистан, Карши, ул. Кучабаг, д. 17; oqboyeva@internet.ru

Information about the authors

Valentin K. Zharov, Dr. of Sci. (Education), professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; valcon@mail.ru

Arslan P. Mardanov, Karimov Tashkent State Technical University, Tashkent, Republic of Uzbekistan; bld. 2, Universitetskaya Str., Tashkent, Republic of Uzbekistan, 100174; apardayevich@mail.ru

Nilufar U. Okbayeva, Karshi State University, Karshi, Republic of Uzbekistan; bld. 17, Kuchabag Str., Karshi, Republic of Uzbekistan, 180103; oqboyeva@internet.ru

Дизайн обложки
Е.В. Амосова

Корректор
О.К. Юрьев

Компьютерная верстка
Н.В. Москвина

Подписано в печать 25.03.2022.
Формат 60×90 1/16.
Уч.-изд. л. 6,5. Усл. печ. л. 8,6.
Тираж 1050 экз. Заказ № 1538

Издательский центр
Российского государственного
гуманитарного университета
125047, Москва, Миусская пл., 6
www.rsuh.ru