

ISSN 2078-9181

DOI 10.15622/sp.#* №

РОССИЙСКАЯ АКАДЕМИЯ НАУК
Отделение нанотехнологий и информационных технологий

САНКТ-ПЕТЕРБУРГСКИЙ
ИНСТИТУТ ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РАН

ТРУДЫ СПИИРАН

proceedings.spiiras.nw.ru



ТОМ 18 № 1



Санкт-Петербург
2019

18+

SPIIRAS PROCEEDINGS

Volume 18 № 1, 2019

Scientific, educational, and interdisciplinary journal primarily specialized
in computer science, automation, and applied mathematics

Trudy SPIIRAN ♦ Founded in 2002 ♦ Труды СПИИРАН

Founder and Publisher

St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences

Editor-in-Chief

R. M. Yusupov, Prof., Dr. Sci., Corr. Member of RAS, St. Petersburg, Russia

Editorial Board Members

A. A. Ashimov ,	Prof., Dr. Sci., Academician of the National Academy of Sciences of the Republic of Kazakhstan, Almaty, Kazakhstan
N. P. Veselkin ,	Prof., Dr. Sci., Academician of RAS, St. Petersburg, Russia
O. Yu. Gusikhin ,	Ph. D., Dearborn, USA
V. Delic ,	Prof., Dr. Sci., Novi Sad, Serbia
A. Dolgui ,	Prof., Dr. Habil., St. Etienne, France
M. Zelezny ,	Assoc. Prof., Ph.D., Plzen, Czech Republic
I. A. Kalyaev ,	Prof., Dr. Sci., Academician of RAS, Taganrog, Russia
A. A. Karpov ,	Assoc. Prof., Dr. Sci., St. Petersburg, Russia
D. A. Ivanov ,	Prof., Dr. Habil., Berlin, Germany
K. P. Markov ,	Assoc. Prof., Ph.D., Aizu, Japan
Yu. A. Merkuriev ,	Prof., Dr. Habil., Academician of the Latvian Academy of Sciences, Riga, Latvia
R. V. Meshcheryakov ,	Prof., Dr. Sci., Tomsk, Russia
N. A. Moldovian ,	Prof., Dr. Sci., St. Petersburg, Russia
V. E. Pavlovskiy ,	Prof., Dr. Sci., Moscow, Russia
A. A. Petrovsky ,	Prof., Dr. Sci., Minsk, Belarus
V. A. Putilov ,	Prof., Dr. Sci., Apatity, Russia
V. K. Pshikhopov ,	Prof., Dr. Sci., Taganrog, Russia
A. L. Ronzhin	(Deputy Editor-in-Chief), Prof., Dr. Sci., St. Petersburg, Russia
A. I. Rudskoi ,	Prof., Dr. Sci., Academician of RAS, St. Petersburg, Russia
H. Samani ,	Assoc. Prof., Ph.D., New Taipei City, Taiwan, Province of China
V. Sgurev ,	Prof., Dr. Sci., Academician of the Bulgarian academy of sciences, Sofia, Bulgaria
V. Skormin ,	Prof., Ph.D., Binghamton, USA
A. V. Smirnov ,	Prof., Dr. Sci., St. Petersburg, Russia
B. Ya. Sovetov ,	Prof., Dr. Sci., Academician of RAE, St. Petersburg, Russia
V. A. Soyfer ,	Prof., Dr. Sci., Academician of RAS, Samara, Russia
B. V. Sokolov ,	Prof., Dr. Sci., St. Petersburg, Russia
L. V. Utkin ,	Prof., Dr. Sci., St. Petersburg, Russia
A. L. Fradkov ,	Prof., Dr. Sci., St. Petersburg, Russia
H. Kaya ,	Assoc. Prof., Ph.D., Tekirdag, Turkey
L. B. Sheremetov ,	Assoc. Prof., Dr. Sci., Mexico, Mexico

Editor: A. I. Motienko

Editor: E. P. Miroshnikova

Technical editor: M. S. Avstriyskaya

Translator: N. V. Kashina

Editorial Board's address

14-th line VO, 39, SPIIRAS, St. Petersburg, 199178, Russia,
e-mail: publ@ias.spb.su, web: <http://www.proceedings.spiiras.nw.ru/>

The journal is indexed in Scopus

© St. Petersburg Institute for Informatics and Automation
of the Russian Academy of Sciences, 2019

ТРУДЫ СПИИРАН

Том 18 № 1, 2019

Научный, научно-образовательный, междисциплинарный журнал с базовой специализацией в области информатики, автоматизации и прикладной математики
Журнал основан в 2002 году

Учредитель и издатель

Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
(СПИИРАН)

Главный редактор

Р. М. Юсупов, чл.-корр. РАН, д-р техн. наук, проф., С-Петербург, РФ

Редакционная коллегия

- А. А. Ашимов**, академик национальной академии наук Республики Казахстан д-р техн. наук, проф., Алматы, Казахстан
Н. П. Веселкин, академик РАН, д-р мед. наук, проф., С.-Петербург, РФ
О. Ю. Гусихин, Ph.D., Диаборн, США
В. Делич, д-р техн. наук, проф., Нови-Сад, Сербия
А. Б. Долгий, Dr. Habil., проф., Сент-Этьен, Франция
М. Железны, Ph.D., доцент, Пльзень, Чешская республика
Д. А. Иванов, д-р экон. наук, проф., Берлин, Германия
И. А. Каляев, академик РАН, д-р техн. наук, профессор, Таганрог, РФ
А. А. Карпов, д-р техн. наук, доцент, С.-Петербург, РФ
К. П. Марков, Ph.D., доцент, Аizu, Япония
Ю. А. Меркурьев, академик Латвийской академии наук, Dr. Habil., проф., Рига, Латвия
Р. В. Мещеряков, д-р техн. наук, профессор, Томск, РФ
Н. А. Молдовян, д-р техн. наук, проф., С.-Петербург, РФ
В. Е. Павловский, д-р физ.-мат. наук, профессор, Москва, РФ
А. А. Петровский, д-р техн. наук, проф., Минск, Беларусь
В. А. Путилов, д-р техн. наук, проф., Апатиты, РФ
В. Х. Пшихопов, д-р техн. наук, профессор, Таганрог, РФ
А. Л. Ронжин (зам. главного редактора), д-р техн. наук, проф., С.-Петербург, РФ
А. И. Рудской, академик РАН, д-р техн. наук, проф., С.-Петербург, РФ
Х. Самани, Ph.D., доцент, Синьбэй, Тайвань, КНР
В. Сгурев, академик Болгарской академии наук, д-р техн. наук, проф., София, Болгария
В. А. Скормин, Ph.D., проф., Бингемптон, США
А. В. Смирнов, д-р техн. наук, проф., С.-Петербург, РФ
Б. Я. Советов, академик РАО, д-р техн. наук, проф., С.-Петербург, РФ
В. А. Соифер, академик РАН, д-р техн. наук, проф., Самара, РФ
Б. В. Соколов, д-р техн. наук, проф., С.-Петербург, РФ
Л. В. Уткин, д-р техн. наук, проф., С.-Петербург, РФ
А. Л. Фрадков, д-р техн. наук, проф., С.-Петербург, РФ
Х. Кайя, Ph.D., доцент, Текирдаг, Турция
Л. Б. Шереметов, д-р техн. наук, Мехико, Мексика

Редактор: А. И. Мотиенко

Выпускающий редактор: Е. П. Мирошникова

Технический редактор: М. С. Австрийская

Переводчик: Н. В. Кашина

Адрес редакции

199178, Санкт-Петербург, 14-я линия, д. 39,
e-mail: publ@iias.spb.su, сайт: <http://www.proceedings.spiiras.nw.ru/>

Журнал индексируется в международной базе данных Scopus

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук»

© Федеральное государственное бюджетное учреждение науки

Санкт-Петербургский институт информатики и автоматизации Российской академии наук, 2019
Разрешается воспроизведение в прессе, а также сообщение в эфир или по кабелю опубликованных в составе печатного периодического издания–журнала «Труды СПИИРАН» статей по текущим экономическим, политическим, социальным и религиозным вопросам с обязательным указанием имени автора статьи и печатного периодического издания–журнала «Труды СПИИРАН»

CONTENTS

R. M. Yusupov TOWARDS THE SEVENTIETH ANNIVERSARY OF RUSSIAN INFORMATICS	5
<i>Artificial Intelligence, Knowledge and Data Engineering</i>	
O.V. Verkholyak, H. Kaya, A.A. Karpov. MODELING SHORT-TERM AND LONG-TERM DEPENDENCIES OF THE SPEECH SIGNAL FOR PARALINGUISTIC EMOTION CLASSIFICATION	30
R.O. Lavrenov, E.A. Magid, F. Matsuno, M.M. Svinin, J. Suthakorn DEVELOPMENT AND IMPLEMENTATION OF SPLINE-BASED PATH PLANNING ALGORITHM IN ROS/GAZEBO ENVIRONMENT	57
<i>Robotics, Automation and Control Systems</i>	
A.S. Gorobtsov, A.E. Andreev, A.E. Markov, A.V. Skorikov, P.S. Tarasov FEATURES OF SOLVING THE INVERSE DYNAMIC METHOD EQUATIONS FOR THE SYNTHESIS OF STABLE WALKING ROBOTS CONTROLLED MOTION	85
V.I. Petrenko, F.B. Tebueva, M.M. Gurchinskiy, V.O. Antonov, A.S. Pavlov PREDICTIVE ASSESSMENT OF OPERATOR'S HAND TRAJECTORY WITH THE COPYING TYPE OF CONTROL FOR SOLUTION OF THE INVERSE DYNAMIC PROBLEM	123
V.I. Chernyshev, L.A. Savin, O.V. Fominova INDIRECT CONTROL OF OSCILLATIONS: ELEMENTS OF THEORY	148
<i>Methods of Information Processing and Control</i>	
K.L. Ovcharenko, I.Yu. Eremeev, K.V. Sazonov, S.S. Semenjuk, A.N. Abakumov. DIFFERENTIAL RANGING METHOD OF DEFINITION LOCATION POSITION OF SATELLITE COMMUNICATION SYSTEM EARTH STATIONS USING REPEATER ON THE UNMANNED AERIAL VEHICLE	176
V.I. Mironov, Y.V. Mironov, I.V. Fominov ENERGETICALLY OPTIMAL CONTROL OF THE CONVERGENCE OF THE SPACECRAFT IN NON-CENTRAL GRAVITATIONAL FIELD OF THE EARTHON THE FAR GUIDANCE STAGE	202
<i>Information Security</i>	
L.K. Babenko, A.V. Trepacheva TOWARDS UNSECURITY OF TWO HOMOMORPHIC ENCRYPTIONS BASED ON RESIDUE SYSTEM	230

СОДЕРЖАНИЕ

Р.М. Юсупов К СЕМИДЕСЯТИЛЕТИЮ ОТЕЧЕСТВЕННОЙ ИНФОРМАТИКИ	5
<i>Искусственный интеллект, инженерия данных и знаний</i>	
О.В. Верхоляк, Х. Кайя, А.А. Карпов. МОДЕЛИРОВАНИЕ КРАТКО- и ДОЛГОВРЕМЕННЫХ ЗАВИСИМОСТЕЙ РЕЧЕВОГО СИГНАЛА ДЛЯ ПАРАЛИНГВИСТИЧЕСКОЙ КЛАССИФИКАЦИИ ЭМОЦИЙ	30
Р.О. Лавренов, Е.А. Магид, Ф. Мацуно, М.М. Свинин, Дж. Сутакорн РАЗРАБОТКА И ИМПЛЕМЕНТАЦИЯ СПЛАЙН-АЛГОРИТМА ПЛАНИРОВАНИЯ ПУТИ В СРЕДЕ ROS/GAZEBO	57
<i>Робототехника, автоматизация и системы управления</i>	
А.С. Горобцов, А.Е. Андреев, А.Е. Марков, А.В. Скорилов, П.С. Тарасов ОСОБЕННОСТИ РЕШЕНИЯ УРАВНЕНИЙ МЕТОДА ОБРАТНОЙ ЗАДАЧИ ДЛЯ СИНТЕЗА УСТОЙЧИВОГО УПРАВЛЯЕМОГО ДВИЖЕНИЯ ШАГАЮЩИХ РОБОТОВ	85
В.И. Петренко, Ф.Б. Тебуева, М.М. Гурчинский, В.О. Антонов, А.С. Павлов ПРОГНОЗНАЯ ОЦЕНКА ТРАЕКТОРИИ РУКИ ОПЕРАТОРА ДЛЯ РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ДИНАМИКИ ПРИ КОПИРУЮЩЕМ УПРАВЛЕНИИ	123
В.И. Чернышев, Л.А. Савин, О.В. Фоминова НЕПРЯМОЕ УПРАВЛЕНИЕ КОЛЕБАНИЯМИ: ЭЛЕМЕНТЫ ТЕОРИИ	148
<i>Методы управления и обработки информации</i>	
К.Л. Овчаренко, И.Ю. Еремеев, К.В. Сазонов, С.С. Семенюк, А.Н. Абакумов. РАЗНОСТНО-ДАЛЬНОМЕРНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ЗЕМНЫХ СТАНЦИЙ СПУТНИКОВЫХ СИСТЕМ СВЯЗИ С ПРИМЕНЕНИЕМ РЕТРАНСЛЯТОРА НА БЕСПИЛОТНОМ ЛЕТАТЕЛЬНОМ АППАРАТЕ	176
В.И. Миронов, Ю.В. Миронов, И.В. Фоминов ЭНЕРГЕТИЧЕСКИ ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ СБЛИЖЕНИЕМ КОСМИЧЕСКИХ АППАРАТОВ В НЕЦЕНТРАЛЬНОМ ГРАВИТАЦИОННОМ ПОЛЕ ЗЕМЛИ НА ЭТАПЕ ДАЛЬНОГО НАВЕДЕНИЯ	202
<i>Информационная безопасность</i>	
Л.К. Бабенко, А.В. Трепачева. О НЕСТОЙКОСТИ ДВУХ СИММЕТРИЧНЫХ ГОМОМОРФНЫХ КРИПТОСИСТЕМ, ОСНОВАННЫХ НА СИСТЕМАХ ОСТАТОЧНЫХ КЛАССОВ	230

Юсупов Р.М. К семидесятилетию отечественной информатики.

Аннотация. Отечественной информатике исполнилось 70 лет. Рожденная в недрах кибернетики, она сегодня является самостоятельной фундаментальной естественно-технической научной дисциплиной с ярко выраженной междисциплинарностью. Информатика определяет научно-методологические основы информатизации и информационного общества и формирует теоретическую базу современных информационных технологий (ИТ). Последние играют существенную роль в развитии экономики и общества в целом. В настоящее время ИТ стали фактически технологиями общего пользования, катализатором развития всех отраслей экономики.

Автор почти пятьдесят лет занимается научно-педагогической деятельностью в сфере информатики и кибернетики (теории и систем управления). В данной статье изложены некоторые его взгляды на развитие информатики и ее взаимоотношения с кибернетикой.

При обсуждении названия и структуры новой науки (информатики) предложено включить в перечень информационных процессов, изучаемых в информатике, процесс защиты информации. Предложен также подход, позволяющий обосновать возможную структуру (перечень научных дисциплин) информатики.

В статье затрагивается проблема отсутствия строгого, устраивающего всех специалистов определения основного объекта информатики — информации. Обсуждается возможность отнесения информации к фундаментальным (базовым) неопределяемым понятиям науки.

Значительное внимание уделяется связи информатики с кибернетикой, утверждается, что информатика зародилась в недрах кибернетики и продолжает тесно взаимодействовать с ней.

Заключительная часть статьи посвящена перспективам развития информатики. Предложено увязывать эти перспективы со следующими тремя факторами: влиянием технонауки, естественной эволюцией информатики и развитием междисциплинарных связей информатики.

Ключевые слова: информация, информатика, кибернетика, информатизация, информационная технология, информационный процесс.

1. Введение. 4 декабря 2018 года отечественной информатике исполнилось 70 лет. В России дата 4 декабря выбрана для празднования Дня информатики неслучайно. 4 декабря 1948 года Государственный комитет при Совете министров СССР по внедрению передовой техники в народное хозяйство зарегистрировал изобретение И. С. Брука и Б. И. Рамеева — цифровую электронную вычислительную машину. Это первый официальный документ, касающийся развития вычислительной техники в стране, которую впоследствии тесно увязывали с информатикой. Термин информатика появился позже, в середине шестидесятых годов прошлого столетия. Идея создания праздника День информатики была высказана журналом *Computer Weekly* в декабре 1998 года.

За истекшие семьдесят лет наша страна вместе со всем миром пережила настоящий информационный бум. В СМИ, в среде специалистов, бизнесменов, политиков и даже обывателей весьма популярными стали понятия информация, информационные технологии, информатизация, информационное общество, информационная безопасность, информационная война и так далее. Резко возросло влияние информатики и информационных технологий на все сферы человеческой деятельности. По сути, информационные технологии начали выполнять роль катализатора развития всех отраслей экономики.

Практически во всех школьных и вузовских учебных планах появились дисциплины по информатике. В университетах начали формироваться кафедры информационного профиля. Была оперативно организована подготовка специалистов по различным направлениям информационных технологий (ИТ).

Передовыми центрами проведения научных исследований в области информатики и ИТ стали наши ведущие университеты страны (МГУ, СПбГУ, НГУ и др.) и академические институты (Вычислительный центр, Институт прикладной математики имени М. В. Келдыша, Институт проблем управления, Институт проблем передачи информации, Институт проблем информатики, Санкт-Петербургский институт информатики и автоматизации и др.).

В 1983 году в структуре АН СССР было создано Отделение информатики, вычислительной техники и автоматизации. Сегодня это подразделение функционирует в виде Отделения нанотехнологий и информационных технологий РАН.

Активное развитие информатики и ИТ способствовало формированию новой стадии в истории развития человечества — информационного общества с цифровой экономикой.

К настоящему времени отечественных работ исторического и методологического характера по информатике издано немного. Известны обзоры [1-3], выполненные под общей редакцией Д. А. Поспелова. Авторы этих обзоров в своих исследованиях исходили из тезиса Д. А. Поспелова: «Совокупность научных направлений, называемых теперь информатикой, именовалась по-разному. Сначала объединяющим названием был термин «кибернетика», затем на роль общего названия той же области исследований стала претендовать «прикладная математика». Поэтому, говоря об истории информатики в бывшем СССР и теперешней России, по сути, надо излагать историю отечественной кибернетики и частично прикладной математики и вычислительной техники».

Общие сведения о развитии информатики и информационных технологий приведены в работе В. И. Левина [4]. В 2007 г. вышло в

свет вузовское учебное пособие [5], в котором предпринята одна из первых попыток осуществить анализ истории информатики и философии информационной реальности. В 2008-2014 годах изданы четыре выпуска истории информатики и кибернетики в Санкт-Петербурге (Ленинграде) [6]. В выпусках содержатся общие сведения о развитии информатики и кибернетики в Санкт-Петербурге, информация о работе отдельных организаций и сведения о деятельности в области информатики и кибернетики выдающихся ученых.

Автор был в свое время свидетелем и в определенной мере участником процесса формирования и развития информатики и ИТ в стране, занимая должности начальника (декана) факультета сбора и обработки информации Военно-космической академии имени А. Ф. Можайского (1976–1989) и директора Санкт-Петербургского института информатики и автоматизации Российской академии наук (1991–2018).

Специфика научной и педагогической деятельности на этих должностях стимулировала и поддерживала заметный интерес автора к проблемам информатики и ИТ, позволила ему приобрести определенный опыт и знания в этих областях.

В данной статье на основе этого «багажа» автор рассматривает некоторые научно-методологические аспекты становления информатики, ее понятийного аппарата, структуры, связи с кибернетикой и перспектив развития.

2. Становление информатики. Термин «Информатика» появился в середине шестидесятых годов практически одновременно в России и во Франции. В 1963 году в журнале «Известия вузов. Электромеханика» (№ 11) была опубликована статья профессора Ф. Е. Темникова «Информатика». В статье была сделана одна из первых попыток очертить границы интегральной науки об информации, состоящей из трех составных частей — теории информационных элементов, теории информационных процессов и теории информационных систем. Но, к сожалению, научная общественность страны не отреагировала серьезно на это событие.

Первоначально под информатикой у нас в стране понимали достаточно узкое научное направление, связанное, прежде всего, с работой с научной и научно-технической информацией, что нашло отражение и в официальных изданиях (справочниках и энциклопедиях). Например, в «Энциклопедии кибернетики» (1974) [7] и в «Словаре по кибернетике» (1979) [8] информатика определена как «научная дисциплина, изучающая

структуру и общие свойства научной информации, а также закономерности всех процессов научной коммуникации».

Указанное «узкое» (библиотечное) понимание информатики сохранилось до наших дней у некоторой части специалистов в основном гуманитарного профиля. Сегодня представители технических и естественных наук вкладывают в это понятие более широкое содержание [9].

Информатика в широком смысле (в дальнейшем речь будет идти в основном о ней) начала активно формироваться как комплекс научных направлений, изучающих процессы и средства сбора, хранения, передачи и обработки и защиты информации, в значительной мере в связи с бурным развитием вычислительной техники и телекоммуникаций.

Так, уже во втором издании Словаря по кибернетике (1989) информатика определяется как наука, изучающая информационные процессы и системы в социальной среде, их роль, методы построения, механизмы воздействия на человеческую практику, усиление этого воздействия с помощью вычислительной техники.

Попытки определить информатику и главный объект исследования — информацию — делаются постоянно. Эта деятельность особенно активизировалась в последние годы. Диапазон подходов и предложений весьма широк. Предлагаются новые наименования обсуждаемого научного направления — информология, информаномия, информатиология, информатистика, инфотроника, информатология, информодинамика и так далее (рисунок 1).

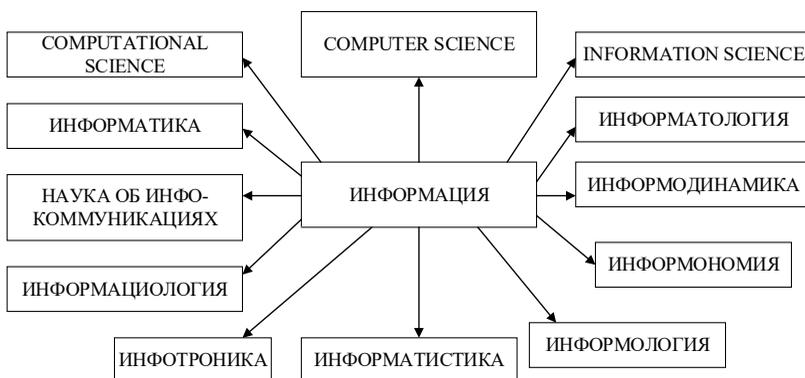


Рис. 1. «Науки» об информации

Пока применительно к рассматриваемой научной дисциплине наиболее прочные позиции сохраняются за терминами информатика и computer science (в англоязычных странах). Приведем некоторые

определения информатики, данные ведущими российскими и зарубежными специалистами в этой области [9].

«Информатика — это название фундаментальной естественной науки, изучающей процессы передачи и обработки информации» (А. П. Ершов).

«Информатика — наука о преобразовании информации, которая базируется на вычислительной технике. Предметом информатики является вычислительная технология как социально-исторический феномен... состав информатики — это три неразрывно и существенно связанные составные части: технические средства, программные и алгоритмические» (А. А. Дородницын).

«Информатика — это некая синтетическая дисциплина, которая включает в себя разработку новой технологии научных исследований и проектирования, основанное на использовании ЭВТ, и несколько крупных научных дисциплин, связанных с проблемой общения с машиной, и наконец, с созданием машины» (Н. Н. Моисеев).

«Информатика — это комплексная научная и технологическая дисциплина, которая изучает, прежде всего, важнейшие аспекты разработки, проектирования, создания, “встраивания” машинных систем обработки данных, а также их воздействия на жизнь общества» (В. С. Михалевич).

«Информатика — наука о проблемах обработки различных видов информации, создании новых высокоэффективных ЭВМ, позволяющая предоставлять человеку широкий спектр различных информационных ресурсов» (Э. А. Якубайтис).

Информатика (наука об инфокоммуникациях) — наука, которая изучает, как приобретается, репрезентируется (представляется), хранится и воспроизводится информация, а также как она передается и используется (Н. А. Кузнецов).

«Информатика — научное направление, являющееся составной частью кибернетики, основные задачи которого заключаются в изучении информационных потребностей общества и разработке путей, средств и методов наиболее рационального их удовлетворения» (В. А. Герасименко).

«Информатика — это наука об осуществляемой преимущественно с помощью автоматических средств целесообразной обработке информации, рассматриваемой как представление знаний и сообщений в технических, экономических и социальных областях» (Французская Академия наук).

«Информатика — это наука, техника и применение машинной обработки, хранения и передачи информации» (М. Брой, Германия).

Анализ этих и других предложений позволяет сформулировать «усредненное» определение информатики как фундаментальной естественно-технической науки о методах и средствах сбора, хранения, передачи, представления и обработки информации.

В последние годы чрезвычайно важное значение приобретает изучение еще одного информационного процесса — процесса защиты информации. Начинают активно развиваться теоретические основы защиты информации и информационной безопасности, разрабатываются технологии, системы и средства защиты, производится подготовка специалистов по нескольким направлениям, таким как организация и технология защиты информации, комплексное обеспечение информационной безопасности автоматизированных систем, компьютерная безопасность и так далее.

Представляется, что теория и практика защиты информации составят в перспективе важнейший раздел информатики. Поэтому автором в свое время было предложено следующее уточненное определение рассматриваемой науки [9]. Информатика — это фундаментальная естественно-техническая наука о методах и средствах сбора, хранения, представления, передачи, обработки и защиты информации. Методы формируют теоретические основы информатики — теория информации, теория алгоритмов, теория информационных процессов, теория обработки сигналов и изображений, теория формальных языков и программирования, теория искусственного интеллекта и так далее. Под средствами следует понимать информационные системы, вычислительную технику, системы связи и передачи данных, информационные технологии.

Кратко прокомментируем приведенное выше определение информатики:

а) Некоторые отечественные и зарубежные специалисты весьма тесно увязывают информатику с вычислительной техникой (ВТ), порой даже сводят ее к теории и практике разработки и использования ВТ. Считаем, что такой подход является не совсем корректным.

Дело в том, что формирование исходных фундаментальных основ и понятий информатики началось еще задолго до появления первых электронных и даже релейных компьютеров. Своим становлением и развитием информатика обязана ряду наук, в том числе математике, логике, лингвистике, теории управления и кибернетике.

Так в математической логике выработаны концепции формальных языков, алгоритмов и исчисления в общем смысле. Более того, такие понятия, как булевские функции и машина Тьюринга оказали прямое влияние на развитие общей архитектуры компьютеров.

Не умаляя роли вычислительной техники в развитии информатики и даже соглашаясь с тем, что вычислительная техника сформировала новый взгляд на информатику, считаем, что нельзя механистически отождествлять информатику с теорией и практикой построения и использования вычислительной техники. Такая попытка делалась и делается рядом авторов до сих пор.

b) В ряде определений информатики в перечне информационных процессов присутствует этап использования информации. Считаем, что в информатике как в фундаментальной науке должны изучаться и разрабатываться методы и средства оперирования с информацией в общем случае безотносительно к областям применения и использования. Вопросы использования и применения информации — это прерогатива других научных дисциплин. Так, проблемы и методы использования информации для решения задач управления объектами различной сложности и различной природы изучается в основном в кибернетике. Информационные процессы в обучении рассматриваются в педагогике и психологии. Медицина использует информацию о здоровье человека и состоянии различных его органов. В метеорологии анализируется информация о состоянии погоды и климата.

В связи с приведенным выше утверждением можно провести аналогию информатики с математикой. В этом отношении весьма показателен пример теории дифференциальных уравнений. Дифференциальные уравнения используются для описания различных процессов во многих (практически во всех) науках, включая гуманитарные и общественные. Но фундаментальные основы теории дифференциальных уравнений, методы их решения, свойства этих решений (устойчивость, сходимости и т.д.) изучаются в рамках математической теории дифференциальных уравнений.

c) Часто поднимается вопрос: каково соотношение «нашей» информатики с «зарубежными» информационными науками? Проведенный анализ показал, что в первом приближении «наша информатика» в ее широком понимании включает разделы, связанные с двумя научными дисциплинами: Computer Science и Information Science [9].

Об этом свидетельствует, в частности, и статья американского специалиста по информатике профессора Горна С. (Gorn S.) «Informatics (computer and Information Science): Its Ideology, Methodology and Sociology» [10], где Computer Science and Information Science рассматриваются как составные части информатики (Informatics).

При рассмотрении информатики как новой отрасли науки, вполне естественным является вопрос: какова структура (перечень разделов) этой науки?

На этот вопрос однозначного ответа пока нет. Информатика как наука еще только формируется. Ее границы четко не очерчены. Она «борется за территории» с кибернетикой, прикладной математикой, теорией связи и с рядом других научных дисциплин. Представляется, что аналогичную ситуацию можно также объяснить «молодостью» информатики, «болезнью ее роста». В определенной степени это можно объяснить и отсутствием соответствующих принципов, критериев, правил, возможно, договоренностей, устраивающих большинство заинтересованных специалистов, позволяющих как-то очертить контуры и структуру информатики. Очевидно, что утверждение является дискуссионным и требует науковедческого обсуждения и обоснования.

Отдельные попытки определить в первом приближении структуру информатики были предприняты в работах ряда отечественных специалистов. Одна из первых попыток структурировать информатику была предпринята, как уже было отмечено, профессором Ф. Е. Темниковым. (см. п. 2). Академик А. А. Дородницын считал, что «...состав информатики — это три неразрывно и существенно связанные составные части: технические средства, программные и алгоритмические» [11].

Профессор Д. А. Поспелов «интегрировал» в информатику теоретическую информатику, искусственный интеллект, информационные системы, информатику в природе, программирование и даже кибернетику [12].

Ряд предложений по структуризации информатики можно найти в работах К. К. Колина [13-15]. В частности, он предлагает представить предметную область информатики в виде матрицы, которая имеет четыре столбца и четыре строки. Столбцы соответствуют основным направлениям дисциплины — техническая, социальная, биологическая и физическая информатика. Строки связаны с уровнями рассмотрения проблем в каждом из этих направлений. К. К. Колин предлагает ввести в рассмотрение четыре следующих уровня: базовые информационные элементы, информационные процессы, информационные системы и фундаментальные основы информатики.

Мы в своих работах [9, 16] предлагаем обосновать содержание информатики с помощью специального структурного представления информатики (рисунок 2), условно названного нами объектно-ориентированным.

Такое представление информатики, по нашему мнению, позволяет решить следующие задачи:

Во-первых, установить логическую связь между основными объектами, изучаемыми в информатике — информацией, информационными процессами, информационными технологиями и информационными системами.

Во-вторых, как-то обосновать (в рамках приведенного подхода) дисциплинарную структуру (перечень научных дисциплин) информатики.



Рис. 2. Объектно-ориентированная структура информатики

Так на рисунке 2 определенные блоки структурной схемы имеют соответствующие номера. К этим номерам «привязаны» группы научных дисциплин, раскрывающие содержание соответствующего блока:

1. – статистическая теория информации
– философские аспекты
– качественная теория информации
– когнитология
– криптография...
2. – теория информационных процессов
3. – теоретические основы вычислительной техники и вычислительных сетей

- теория связи...
- 4. - теория моделирования
- теория языков программирования
- теория алгоритмов
- теория программирования
- искусственный интеллект
- базы данных
- распознавание образов
- теоретические основы защиты информации...
- 5. – теория синтеза организационных структур
- методы управления разработками

В-третьих, определить место информатизации и ее связь с информатикой в целом и информационными технологиями в частности. Информатизация — это социально-экономический и научно-технологический процесс разработки и массового внедрения информационных технологий во все сферы человеческой деятельности для поддержания уровня информированности всех членов общества и его различных институтов (структур), необходимого для кардинального улучшения качества труда и условий жизни людей. Конечной целью информатизации является формирование новой стадии развития — постиндустриальной стадии в форме информационного общества.

3. К определению понятия информации. Хотя информация стала общенаучной категорией, строгого, устраивающего всех специалистов понятия этого феномена до сих пор нет.

Как правило, каждый специалист, «входя» в мир информатики и информационных технологий, стремится дать свое определение информации. Таких определений сегодня существует невообразимое множество.

Так, например, информацией называют:

- любые сведения о каких-либо ранее неизвестных событиях или явлениях;
- содержательное описание объекта или явления;
- результат выбора;
- содержание сигнала, сообщения;
- меру разнообразия;
- отраженное разнообразие;
- сущность, сохраняющуюся при вычислимом изоморфизме;
- сущность, определяющая изменение знаний при получении сообщения;
- уменьшаемую неопределенность;
- меру сложности структур, меру организации;

- результат отражения реальности в сознании человека, представленный на его внутреннем языке;
 - семантику или прагматику синтаксиса языка представления данных;
 - продукт научного познания, средство изучения реальной действительности;
 - основное содержание отображения;
 - бесконечный процесс триединства энергии, движения и массы с различными плотностями кодовых структур бесконечно беспредельной Вселенной;
 - непременную субстанцию живой материи, психики, сознания;
 - результат гомоморфного (т.е. сохраняющего основные соотношения) отображения данной предметной области в некоторые отторжимые от этих элементов сущности — сигналы, характеристики, описания;
 - вечную категорию, содержащуюся во всех без исключения элементах и системах материального мира, проникающую во все «поры» жизни людей и общества;
 - свойства материи, ее атрибут; некую реалию, существующую наряду с материальными вещами или в самих вещах;
 - язык мира как живого целого и так далее.
- Все возможные определения можно условно распределить на четыре группы:
- обычное, широко распространенное «бытовое» понимание информации;
 - понятия, использующие формализованные модели реальных объектов и процессов;
 - подход с позиций теории отражения и познания;
 - подход, учитывающий связь информации со свойствами материи.

Отсутствие единства в определении информации не является препятствием для развития информатики. Такое положение в науке не ново. Так, например, термометр был придуман за много лет до того, как ученые поняли, что именно он измеряет. От первого термометра до общей теории статистических свойств физических систем и основ квантовой физики прошло около трех столетий.

Можно также согласиться с мнением, что термин информация вообще относится к базовым неопределяемым понятиям науки. По этому поводу американский информатик Т. Сарацевич заявил следующее [17]: «Все недовольны тем, что информационная наука не

хочет потрудиться над определением информации. ... На самом же деле ни одна современная наука не имеет определений своих основных феноменов. В биологических науках нет определения жизни, в медицинских — здоровья, в физике — энергии, в электротехнике — электричества, в ньютоновских законах — противодействия. Это просто основные явления, и эта их первичность и служит им определением».

Академик Моисеев в своей книге «Расставание с простотой» [18] по поводу понятия «информация» написал следующее: «Ныне существует обширная наука, именуемая информатикой. Это особая наука — она пронизывает все остальные научные дисциплины. И ей посвящает свои усилия едва ли не половина всего научного персонала (даже не осознавая этого). А феномен этой дисциплины состоит в том, что центральное ее понятие «информация» до сих пор не имеет четкого и общепринятого определения — его используют главным образом на интуитивном уровне <...>, ... я уверен, что строгого и достаточно универсального определения информации не только нет, но и быть не может».

Не в столь категорической форме развивается дискуссия и в связи с рассмотрением проблемы о роли информации в природе и обществе. Основные научные споры в настоящее время концентрируются вокруг двух концепций — атрибутивной и функциональной. «Яблоком раздора» этих концепций является, в сущности, вопрос о наличии информации в неживой природе. Первая концепция рассматривает информацию как атрибут, присущий всем уровням материи, в то время как вторая связывает информацию с самоуправляемыми и самоорганизуемыми системами, сводя порой область бытия информации до человеческого общества.

Так, А. Д. Урсул в работе «Природа информации» [19] считает, что информация является всеобщим свойством материи от простейших неорганических форм до человеческого общества. В то же время академик Н. Н. Моисеев утверждает, что информация связана с человеческим обществом, с задачами управления и принятия решений. Так, в уже указанной книге «Расставание с простотой» он пишет: «Понятие «информация» мне представляется в некотором смысле риторическим <...> необходимость его введения возникает лишь при описании довольно поздних этапов развития материального мира, когда в нем зарождается жизнь, <...> необходимость использования этого термина появляется в нашем описании лишь тогда, когда мы начинаем изучать системы, обладающие целеполаганием, точнее — необходимостью и возможностью выбора нового «желательного» состояния.

То есть тогда, когда мы начинаем изучать объекты, способные к «целенаправленным» действиям ... Во всех остальных случаях, в

том числе и при описании процессов в неживой природе, можно обойтись без использования этого термина — для этого достаточно языка физики и химии».

Мы (автор и его коллеги) в своей информационной деятельности находимся на стороне тех, кто придерживается мнения о том, что неживая природа, конечно, информативна. Информация в объектах неживой природы находится в законсервированном состоянии до момента, пока к объекту не прикоснется рука человека. Без наличия информации в неживой природе трудно представить существование и развитие таких наук, как палеонтология, геология, археология и ряда других наук о неживой природе.

4. Информатика и кибернетика. Информатика все последние семьдесят лет развивалась в условиях активного взаимодействия с другими научными направлениями и дисциплинами. Наиболее «родственные» связи информатика имеет с кибернетикой (общей теорией управления). Это связано с тем, что, во-первых, информатика развивалась в значительной мере в недрах кибернетики, фактически на единой технической базе — вычислительной технике и средствах связи и передачи данных, во-вторых, кибернетика, являясь наукой об общих законах и закономерностях управления и связи, объективно была вынуждена заниматься вопросами использования информации в интересах управления. Так информации и ее использованию уделяется большое внимание в основополагающих работах Н. Винера [20, 21]. Там же вводится понятие «управления с помощью «информативной» обратной связи».

Информационная составляющая пронизывала и некоторые ранние определения кибернетики. Так выступая 19 апреля 1959 г. с докладом на заседании Президиума Академии наук СССР, академик А.И. Берг отмечал, что содержание кибернетики заключается в сборе, переработке и передаче информации с целью улучшения управления для достижения поставленной задачи.

В «Энциклопедии кибернетики» (1974) кибернетика определяется как наука об общих закономерностях получения, хранения, передачи и преобразования информации в сложных управляющих системах.

В свое время были даже предложения рассматривать информатику как кибернетику на современном этапе и ввести в рассмотрение синтезированное научное направление информатика–кибернетика [22].

Сегодня, по нашим представлениям, информатика и кибернетика могут рассматриваться как относительно молодые самостоятельные научные направления, имеющие свои теоретико-

методологические основы, задачи, объекты и предметы исследования. Данное утверждение мы попытались раскрыть с помощью следующей сравнительной таблицы 1.

Таблица 1. Основные понятия кибернетики и информатики

Наука Понятия	Кибернетика	Информатика
Определение науки	Наука об общих законах и закономерностях управления и связи в сложных системах различной природы.	Наука об информации, методах и средствах обработки, хранения, передачи и представления и защиты информации.
Объект исследования	Управление, процессы управления	Информация, информационные процессы
Предмет исследования	Системы и технологии управления	Информационные системы и технологии
Основные понятия	Управление, процессы управления, система управления, обратная связь, модель, информация, технологии управления...	Информация, информационные процессы, системы, технологии, модель...
Основная прикладная задача	Анализ и синтез технологий и систем управления	Создание информационных технологий и информационных систем

Заметим также, что кибернетика и информатика в их современном состоянии могут рассматриваться как отдельные научные направления, развивающиеся, если можно так сказать, в режиме сиамских близнецов. Это качество (сиамские близнецы), которое в таблице 1 условно показано заштрихованной полоской, определяется такими научными дисциплинами, как шенноновская теория информации, теории искусственного интеллекта, распознавание образов, теория моделирования, теоретические основы вычислительной техники и другие, которые разными авторами и разными вузовскими учебными планами причисляются то к кибернетике, то к информатике. В значительной мере это определяется двумя обстоятельствами. Во-первых, относительной молодостью рассматриваемых научных направлений. Во-вторых, превалированием субъективных интересов отдельных педагогических школ и научных авторитетов при определении границ той или иной научной дисциплины.

Характерно, что кибернетика и информатика организационно развивались «под разными знаменами»: Международная федерация по автоматическому управлению (ИФИП) и Международная федерация по обработке информации (ИФИП) соответственно. В Российской академии наук также существовали два тематических отделения: процессов управления и механики и информатики, вычислительной техники и автоматизации.

В последние годы отмечается второй виток сближения кибернетики и информатики. Происходит активное терминологическое и содержательное взаимопроникновение этих научных направлений (рисунок 3).

- информационное управление;
- интеллектуальное управление (ситуационное, нейроуправление, многоагентное, управление на основе эволюционных алгоритмов, основанное на знаниях);
- программная кибернетика и т.д.



Рис. 3. Взаимодействие информатики и кибернетики

Так кибернетическая терминология активно проникает в информатику и вычислительную технику. Сегодня весьма популярными в области ВТ и ИКТ становятся понятия и, соответственно, стратегии адаптивных и проактивных компьютерных систем, адаптивного управления и адаптивного предприятия. Эти стратегии интенсивно развиваются компаниями IBM, Intel Research, Hewlett Packard, Microsoft, Sun и другие. В западной (американской) практике широко

используются термины киберпространства и киберпреступления, которые, по сути, являются аналогами наших информационного пространства и преступления в информационной сфере.

В 2004 г. в Гонконге в рамках 28-й ежегодной Международной конференции по программному обеспечению было проведено необычное мероприятие — Первый семинар по программной кибернетике. Основная идея программной кибернетики — более тесно и формализовано объединить процесс (систему) создания и функционирования программного обеспечения с управлением и дать ответы на ряд вопросов:

- как адаптировать принципы теории управления к программным процессам и системам;
- как формализовать механизмы обратной связи в программных процессах и системах, как ввести в них соответствующие меры;
- как интегрировать программную инженерию с инженерией управления и так далее.

Ответы на эти и другие вопросы позволят, по мнению специалистов, сформировать в программной инженерии (программотехнике) принципиально новую парадигму адаптивного программирования, самоорганизующихся вычислений, реализация которой позволит создать в ПО дополнительные функциональные возможности, позволяющие разработчикам и конечным пользователям гибко реагировать на изменения внешних условий и требований без соответствующего репрограммирования.

В свою очередь методы, технологии и средства, разрабатываемые в недрах инфоакатики, активно внедряются в кибернетику. В связи с этим можно утверждать, что информатика стимулировала развитие таких новых направлений управления, как информационное управление, различных видов интеллектуального управления — ситуационное, нейроуправление, управление, основанное на знаниях, на основе эволюционных алгоритмов, многоагентное управление и так далее (см. рисунок 3).

Теория и системы управления составляют существенную часть кибернетики. Научная карьера автора статьи началась на кафедре автономных систем управления Военно-космической академии имени А. Ф. Можайского в пятидесятых годах прошлого столетия. Впоследствии, занимаясь исследованиями в области информатики и ИТ, автор постоянно интересовался тем, как последние влияют на развитие теории и систем управления. Вывод из этих наблюдений следующий: влияние революционное, фактически все дальнейшее развитие теории и практики управления происходят за счет внедрения в них методов информатики и ИТ.

Информационные технологии позволяют:

- более эффективно реализовать известных принципов и методов управления: оптимального, идентификационного, адаптивного, терминального, координатно-параметрического, с прогнозируемыми моделями, с переменной структурой и так далее;
- создавать принципиально новые концепции и методы управления: интеллектуальное управление (нейроуправление, ситуационное управление, управление на основе правил и автоматов), информационное управление, гисы в системах управления, мобильные технологии в управлении и так далее;
- повысить эффективность проектирования, разработки, создания современных систем управления, возможности управления жизненным циклом сложных управляющих систем, развитие умных производств, роботизированных производств, аддитивных технологий и так далее;
- изменить облик, структуру и состав современных систем управления (интернет-управление, распределенные СУ, сенсорные сети, базы знаний, беспроводные технологии, интеллектуальные роботы, мобильные технологии в управлении и т.д. и т.п.);
- изменить роль и место человека, повысить возможности его эффективного общения с машиной, сформировать интеллектуальное пространство обитания человека (умный дом, умный город и др.) и так далее.

В завершении данного подраздела следует отметить еще одно направление взаимодействия информатики в рамках междисциплинарной отрасли системных знаний. Оно связано с таким направлением теоретических и практических исследований в рассматриваемой отрасли знаний как системология (или общая теория систем).

Взаимодействие информатики с общей теорией систем осуществляется по нескольким направлениям. Первое из этих направлений непосредственно связано с обобщенным описанием объектов и субъектов управления на основе новых формальных подходов, разрабатываемых в современной системологии, к числу которых можно, например, отнести структурно-математический и категорийно-функторный подходы [23]. В этой связи можно также отметить интересные научные результаты, которые были получены к настоящему времени в одном из важнейших направлений исследований системологии, а именно в квалиметрии моделей и полимодельных комплексов (моделеметрии). Данную теорию (моделеметрию) можно широко использовать при построении многокритериального анализа и обоснованном выборе моделей, разрабатываемых и используемых в информатике.

В информатике при решении задач сбора, хранения, передачи, представления, обработки, защиты информации также широко используются методы и алгоритмы декомпозиции (композиции), агрегирования (деагрегирования) и координации, разрабатываемые в общей теории систем применительно к объектам любой природы. С другой стороны, в работе [24] было показано, что подходы, разработанные в современной информатике можно успешно применять при организации процессов управления качеством моделей и полимодельных комплексов, а также при их структурной и параметрической адаптации.

5. О перспективах развития информатики. Перспективы развития информатики свяжем с теми основными тенденциями, которые сегодня развиваются как в науке в целом, так и в недрах самой информатики. Среди этих тенденций выделим следующие три процесса:

1. Формирование нового этапа взаимоотношений науки и технологий.

2. Естественная эволюция информатики.

3. Развитие междисциплинарных связей.

В основу первой тенденции заложена констатация утверждения о том, что целью научной деятельности сегодня является не столько объяснение мира и получение знаний об окружающей нас действительности, так или иначе претендующих на истинность, сколько получение эффекта, который может быть воплощен в пользующийся спросом технологии [25]. Это новое явление современности на Западе получило специальное название — technoscience (технонаука). Наиболее очевидные признаки технонауки — это существенно более глубокая, чем прежде, встроенность научного познания в процесс создания и продвижения новых технологий, неуклонное приближение науки и технологий к человеку, к его непосредственным потребностям.

Английский социолог науки Дж. Займан [26] назвал новую фазу развития науки «постакадемической», подчеркнув, что «это не новый способ производства знания, а новый образ жизни». К числу особенностей этой «постакадемической» науки он отнес повсеместное внедрение «нормы полезности» или эффективности, с помощью которой ожидаемые и предпологаемые открытия заранее оцениваются с коммерческой точки зрения, а «беспользные» науки, вроде астрофизики или археологии, должны доказывать обществу свою «культурную ценность».

Представляется, что инновационный бум, охвативший общество, в значительной мере связан с постакадемической наукой

или технаукой. Сегодня прагматизм по отношению к науке становится основным критерием оценки деятельности ученых и научных коллективов со стороны государства.

Руководство страны требует от науки конкретной отдачи — технологий и продукции, более жестко начинает контролировать расход выделяемых средств, стремится оценивать эффективность научной деятельности с помощью определенных количественных мер — количество публикаций, цитирований, патентов и так далее.

Очевидно, что влияние технауки начинает проявлять себя, в первую очередь, в сфере естественных и технических наук. Касается оно и информатики, связанной с развитием и широким использованием, пожалуй, самых популярных и самых массовых технологий — ИТ.

В частности, за рубежом проблематика теоретических исследований в области информатики в последние годы существенным образом определяется потребностями приложений и непосредственно потребностями рынка информационных средств и технологий. В связи с этим можно отметить активизацию исследований в областях, связанных с компьютерными сетями, в частности повышением их глобальности, производительности, живучести и катастрофоустойчивости, с обработкой распределенной информации и знаний, интеграцией материальных и интеллектуальных ресурсов, защитой информации, дистанционным обучением и так далее.

Чрезвычайно важным является также обстоятельство, связанное с процессом активного и масштабного слияния потребительской электроники (компьютеров, телевизоров, телефонов, игровых приставок и т.д.) с Интернет и другими сетевыми технологиями.

Заметим также, что конкретные программы и планы развитых стран в области информатизации связаны с расширением использования обычными гражданами интернета и современных онлайн-общественных услуг — электронное правительство, электронное здравоохранение, электронная коммерция, электронное обучение, с развитием Интернета вещей.

Отметим, что в процессе проведения исследований в интересах создания соответствующих технологий развиваются такие теоретические разделы информатики, как анализ и извлечение знаний из данных, машинное обучение, многоагентные системы, компьютерное зрение, речевая информатика и обработка информации на естественном языке, управление потоками данных в сетях, новые методы компьютерного моделирования и

супервычислений при решении сложных задач, стеганография и стегаанализ, интеллектуальные сенсорные сети, защита компьютерных сетей, виртуальные организации, интеллектуальное пространство и так далее.

Дальнейшая эволюция информатики как науки связана в значительной мере с развитием понятийного аппарата.

Весьма перспективным в этом отношении, по нашему мнению, может оказаться, в частности, понимание информатики как науки об информации и информационном взаимодействии [27-30].

Взаимодействие — фундаментальная категория, отражающая процессы воздействия различных объектов друг на друга, их взаимную обусловленность, изменение состояния, взаимопереход, а также порождение одних объектов другими. В физике известно силовое (энергетическое), например, гравитационное взаимодействие тел или частиц друг на друга, приводящее к изменению состояния их движения.

Основными особенностями информационного взаимодействия являются:

- ведущая роль здесь принадлежит не энергии или веществу, а информации в различных формах ее проявления;

- информационное взаимодействие не силовое и может осуществляться с помощью очень слабых сигналов;

- при информационном взаимодействии реализуется коммуникативная функция и происходит как закладка смысла в сообщении, так и его постижение при приеме сообщения или более коротко: при информационном взаимодействии главными операциями являются операции со смыслами, образами, эмоциями, а это значит, что передается идеальное;

- идеальные взаимодействия не могут осуществляться при отсутствии памяти у взаимодействующих объектов или более расширительно при отсутствии того, что принято называть элементами сознания (основные свойства психики — это целостность, рефлексивность, спонтанность).

В итоге мы приходим к следующему определению.

Взаимодействие материальных объектов, при котором осуществляется передача (генерация и освоение) идеальных категорий (смыслов, значений, образов, эмоций) будем называть информационным взаимодействием.

В работе [27] информационное взаимодействие определяется как взаимодействие объектов, приводящее к применению знаний хотя бы одного из них.

Структура информационного взаимодействия и проблемы ее становления изложены в работах [9, 28].

Обсуждая перспективы развития информатики, необходимо изучать и процессы взаимодействия этого междисциплинарного научного направления с другими дисциплинами. Приграничные исследования могут давать чрезвычайно интересные результаты.

Известно, что основа каждой науки связана со сбором, обработкой и представлением информации. Это означает, что в ней активно должны использоваться методы и средства, разрабатываемые в информатике. С этим и связана уникальная междисциплинарность информатики. Информационные технологии начинают широко использоваться фактически во всех науках, включая гуманитарные и общественные. В настоящее время активно развиваются биоинформатика, социальная информатика, информационное право, историческая информатика и так далее.

Говоря о связи информатики с наукой в целом (например, рассматривая вопросы информатизации науки), уместно также вспомнить своеобразное определение науки, данное академиком Н. Н. Моисеевым. Он, в частности, отмечал, что наука — это еще один способ накопления, хранения и переработки информации. Научные теории и законы можно рассматривать в качестве специальных средств агрегирования информации и методов, обеспечивающих к ней относительно легкий доступ [31]. Это определение, по сути, позволяет провести некоторую аналогию между наукой и информатикой. В таком контексте науку условно можно рассматривать как макроинформатику, а информатику — как своего рода микронауку. Наука в силу своей природы имеет дело со знаниями. Современные и перспективные интеллектуальные системы, создаваемые в недрах информатики, также оперируют знаниями.

Вышеприведенным сравнением автор еще раз хотел подчеркнуть определенно интегрирующую роль информатики в науке и обществе, роль которой существенно повышается в условиях формирования постиндустриальной стадии развития человечества — информационного общества.

6. Заключение. Рассмотрены научно-методологические аспекты состояния и перспектив развития информатики как фундаментальной науки о методах и средствах сбора, хранения, представления, передачи, обработки и защиты информации.

Каковы альтернативы для дальнейшей эволюции информатики?

Анализ существующих тенденций и соответствующих научных публикаций позволяет выделить три потенциально возможных сценария развития информатики.

Первый сценарий рассмотрен в работе Д. А. Поспелова [12], указанной выше в п. 2. В работе предложено «генеалогическое дерево» информатики с восемью ветвями основных направлений: теоретическая информатика, кибернетика, программирование, искусственный интеллект, информационные системы, вычислительная техника, информация в обществе, информатика в природе. По Д. А. Поспелову взаимодействие (интеграция) информатики и кибернетики должна происходить по циклу — кибернетика породила информатику, последняя поглощает кибернетику. Данная точка зрения для нас является весьма спорной.

Второй возможный сценарий развития информатики связывают с ее возвратом в кибернетику как интегрирующую научную отрасль об управлении и связи.

Представляется, что кибернетика, несмотря на определенную экспансию со стороны информатики, продолжает активно эволюционировать. Достаточно упомянуть о появлении таких «новых кибернетик», как кибернетика второго порядка [32-34], неокибернетика [35-36], кибернетика третьего порядка [37], новая кибернетика [38], кибернетика 2.0 [37] и так далее. Велико и число междисциплинарных кибернетик. К ним, например, можно отнести эволюционную кибернетику [39], геофизическую кибернетику [40], кибернетическую физику [39], космическую кибернетику [41].

Новым этапом развития кибернетики являются также системы c^3 (control + communication + computing) [43] и киберфизические системы [43-45].

Наконец, третий сценарий — это дальнейшее активное развитие информатики как самостоятельной междисциплинарной науки, как теоретической базы для ИТ. Последние уже сегодня имеют надотраслевой характер и являются, как уже было указано, катализатором развития всех отраслей экономики и общества в целом. Важно также отметить, что информация, информатика и ИКТ дали название и способствовали становлению, как уже было отмечено, новой стадии развития человечества — информационного общества, при котором наиболее эффективное и динамичное его развитие возможно на основе максимально полного использования имеющихся информационных ресурсов и средств их обработки, составляющих основу соответствующих информационных пространств. Главным ресурсом ускоренного развития современного информационного общества становятся знания, а главным механизмом развития — цифровая экономика, основанная на знаниях. Основными технологиями цифровой экономики становятся новые информационные и коммуникационные технологии (ИКТ), которые уже фактически

являются технологиями общего назначения также как технологии производства тепла и электроэнергии. Главной компонентой цифрового производства и в целом цифровой экономики станут разнообразные классы киберфизических систем (КФС) и социо-киберфизических систем (СКФС). Их повсеместное внедрение приведет к гораздо большим изменениям, чем появление компьютеров и Интернета. В перспективных КФС наряду с функциями позиционирования, контроля и диагностики также будут реализованы функции автоматического составления отчетов о состоянии соответствующей подсистемы контролируемого оборудования, в том числе данных о всех возникающих неисправностях; об остатке ресурса изнашиваемых деталей; о ресурсе расходных материалов; загрузке оборудования и режиме его эксплуатации. Указанные возможности открывают широчайшие перспективы по автоматизации и интеллектуализации как самого цифрового производства продукции, так и ее обслуживания и эксплуатации во время послепродажного функционирования. В настоящее время мы являемся свидетелями нового этапа промышленной революции, которую в зарубежных странах назвали проектом «Индустрия 4.0». Конкретную реализацию данный проект получает в настоящее время в рамках промышленного Интернета вещей. При этом ключевым элементом предлагаемого электронного обслуживания (e-maintenance) будет являться базирующееся на Веб-технологиях дистанционное администрирование, мониторинг, тестирование, диагностика, прогнозирование состояния эксплуатируемых изделий, реконфигурация их структур, в случае возникновения аварийных и нештатных ситуаций и отсутствии необходимых резервов. Ведущей экономической стратегией многих зарубежных компаний становится стратегия инновационного лидерства, существенно отличающейся от стратегии конкурентной борьбы. Она не связана с поиском последовательных улучшений своих изделий по сравнению с конкурирующими, а направлена на создание абсолютно нового изделия, нового рынка, поиска новых покупателей, пусть даже ценой потери частных старых. Анализ существующих тенденций автоматизации, информатизации и интеллектуализации передовых зарубежных экономик на основе рассматриваемой стратегии инновационного лидерства показывает, что переход к цифровой экономике основных стран мира может быть завершён в ближайшие пять-десять лет и приведет к удвоению их ВВП, а также их технологическому отрыву как в объемах производства, так и в производимых товарах и услугах.

Литература

1. *Поспелов Д.А., Ячов И.Ф.* Очерки истории информатики в России // Научно-издательский центр ОИИГМ СО РАН. 1998. 663 с.

2. *Захаров В.Н., Подловченко Р.И., Фет Я.И.* История информатики в России. Ученые и их школы // М.: Наука 2003. 332 с.
3. *Фет Я.И.* Хрестоматия по истории информатики // Академическое издательство «ГЕО». 2014. 559 с.
4. *Левин В.И.* История информационных технологий // М.: Бином. 2007. 336 с.
5. *Юсупов Р.М., Котенко В.П.* История информатики и философия информационной реальности: учеб. пособие // М.: Акад. проект. 2007. 431 с.
6. *Юсупов Р.М.* История информатики и кибернетики в Санкт-Петербурге // СПб.: Наука. Вып. 2. 2010. 152 с.
7. *Глушков В.М.* Энциклопедия кибернетики // Главная редакция Украинской Советской Энциклопедии. 1974. Т. 2.
8. *Дородицын и др.* Словарь по кибернетике // Главная редакция редакция Украинской Советской Энциклопедии. 1989. 751 с.
9. *Юсупов Р.М., Заболотский В.П.* Концептуальные и научно-методологические основы информатизации // СПб.: Наука. 2009. 542 с.
10. *Gorn S.* Informatics (Computer and information science): Its Ideology, Methodology, and Sociology // Knowledge. 1982. vol. 4. no. 2. pp. 173–198.
11. *Дородицын А.А.* Информатика. Предмет и задачи // М.: Наука. 1986. С. 22–28.
12. *Поспелов Д.А.* Информатика. Энциклопедический словарь для начинающих // М.: Педагогика-Пресс. 1994. С. 348–349.
13. *Колин К.К.* Актуальные философские проблемы информатики. Теоретические основы информатики // М.: КОС*ИНФ. 2009. Т. 2. 222 с.
14. *Колин К.К.* Эволюция информатики // Информационные технологии. 2005. № 1. С. 2–16.
15. *Колин К.К.* Социальная информатика: российская научная школа и перспективные направления исследований // Системы и средства информатики. 2016. Т. 25. Вып. 4. С. 175–193.
16. *Юсупов Р.М.* Наука и национальная безопасность // СПб.: Наука. 2011. 369 с.
17. *Образование, наука и развитие кадрового потенциала. Часть 3 // Информ. бюлл. корп. Microsoft. 2004. Вып. 26.*
18. *Моисеев Н.Н.* Расставание с простотой // М.: Аграф. 1998. 480 с.
19. *Урсул А.Д.* Природа информации // М.: Политиздат. 1968. 288 с.
20. *Винер Н.* Кибернетика или управление и связь в животном и машине // М.: Наука. 1983. С. 344.
21. *Винер Н.* Кибернетика и общество // М.: Издательство иностранной литературы. 1958. 200 с.
22. *Бирюков Б.В.* Кибернетика: прошлое для будущего // М.: Наука. 1981.
23. *Калинин В.Н., Резников Б.А.* Теория ситсем управления (структурно-математический подход) // Л.: ВИКИ. 1978. 417 с.
24. *Микони С.В., Соколов Б.В., Юсупов Р.М.* Квалиметрия моделей и полимодельных комплексов // М.: Наука. 2018. 12 с.
25. *Юдин Б.Г.* Знание как социальный ресурс // Вестник РАН. 2006. Т. 76. № 7.
26. *Займан Д.* Реальная наука // Социология науки: Статьи и рефераты // 2000. СПб. Т. 7.
27. *Кузнецов Н.А.* О развитии фундаментальных исследований по информационному взаимодействию в природе и обществе // Проблемы передачи информации. 1997. Т. 33. № 3. С. 111–112.
28. *Полонников Р.И.* Феномен информации и информационного взаимодействия // СПб.: СПИИРАН. 2001. 171 с.
29. *Колин К.К.* Информационное взаимодействие и понятие информации // М.: МИФИ. Т. 6. С. 26–27.
30. *Иезутов А.Н.* Информатика и философия взаимодействия // СПб.: Эскулап. 1997. 96 с.

31. *Mousses H.H.* Человек и ноосфера // М.: Молодая гвардия. 1990. Т. 351. С. 298.
32. *Mariuyama M.* The second cybernetics: Deviation-amplifying mutual causal processes // *American Scientist*. 1963. Т. 51. С. 164–179.
33. *Von Foerster H.* The Cybernetics of Cybernetics // Minneapolis. 1995. pp. 228.
34. *Mead M.* The Cybernetics of Cybernetics // *Purposive Systems*. New York: Spartan Books. 1968.
35. *Соколов Б.В., Юсупов Р.М.* Неокибернетика в современной структуре системных знаний // *Робототехника и техническая кибернетика*. 2014. № 2. С. 3–11.
36. *Крылов С.М.* Неокибернетика: Алгоритмы, математика эволюции и технологии будущего // М.: Издательство ЛКИ. 2008. 288 с.
37. *Новиков Д.А.* Кибернетика: Навигатор. История кибернетики, современное состояние, перспективы развития // М.: ЛЕНАНД. 2016. 160 с.
38. *Теслер Г.С.* Новая кибернетика // *Логос*. 2004. 404 с.
39. *Редько В.Г.* Эволюционная кибернетика // М.: Наука. 2003. 156 с.
40. *Гаскаров Д.В. и др.* Введение в геофизическую кибернетику и экологический мониторинг // СПб.: ГУВК. 1998. 165 с.
41. *Фрадков А.Л.* Кибернетические системы: от прошлого к будущему // Доклад на Мультиконференции по проблемам управления. 2018.
42. *Калинин В.Н.* Современная космическая кибернетика – методологические основы и направления исследований // *Информация и космос*. 2007. № 3. С. 7–16.
43. *Lee E.A., Seshia S.A.* Introduction to Embedded Systems: A Cyber-Physical Systems Approach // MIT Press. 2017. 585 p.
44. *Müller K.* The New Science of Cybernetics: A Primer // *Journal of Systemics, Cybernetics and Informatics*. 2013. vol. 11. no. 9. pp. 32–46.
45. *Gershenson C., Csermely P.* The Past, Present and Future of Cynemetics and Systems Research // *Systems. Connecting Matter, Life, Culture and Technology*. 2013. vol. 1. no. 3.

Юсупов Рафаэль Мидхатович — д-р техн. наук, профессор, член-корреспондент РАН, заслуженный деятель науки и техники РФ, научный руководитель, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН); президент, НП Национальное общество имитационного моделирования («НОИМ»). Область научных интересов: теория управления, информатика, теоретические основы информатизации и информационного общества, информационная безопасность. Число научных публикаций — более 500. yusupov@iias.spb.su; 14-я линия В.О., 39, Санкт-Петербург; 199178; р.т.: +7 (812) 328-3337.

O.V. VERKHOLYAK, H. KAYA, A.A. KARPOV

MODELING SHORT-TERM AND LONG-TERM DEPENDENCIES OF THE SPEECH SIGNAL FOR PARALINGUISTIC EMOTION CLASSIFICATION*Verkholyak O.V., Kaya H., Karpov A.A. Modeling Short-Term and Long-Term Dependencies of the Speech Signal for Paralinguistic Emotion Classification.*

Abstract. Recently, Speech Emotion Recognition (SER) has become an important research topic of affective computing. It is a difficult problem, where some of the greatest challenges lie in the feature selection and representation tasks. A good feature representation should be able to reflect global trends as well as temporal structure of the signal, since emotions naturally evolve in time; it has become possible with the advent of Recurrent Neural Networks (RNN), which are actively used today for various sequence modeling tasks. This paper proposes a hybrid approach to feature representation, which combines traditionally engineered statistical features with Long Short-Term Memory (LSTM) sequence representation in order to take advantage of both short-term and long-term acoustic characteristics of the signal, therefore capturing not only the general trends but also temporal structure of the signal. The evaluation of the proposed method is done on three publicly available acted emotional speech corpora in three different languages, namely RUSLANA (Russian speech), BUEMODB (Turkish speech) and EMODB (German speech). Compared to the traditional approach, the results of our experiments show an absolute improvement of 2.3% and 2.8% for two out of three databases, and a comparative performance on the third. Therefore, provided enough training data, the proposed method proves effective in modelling emotional content of speech utterances.

Keywords: Speech emotion recognition, computational paralinguistics, affective computing, feature representation, context modelling, artificial neural networks, long short-term memory.

1. Introduction. Automatic emotion recognition has emerged as one of the most important and challenging research topics of affective computing [1, 2], a modern study concerned with recognizing and processing human feelings. Lying at the crossroads of computer and cognitive sciences, this rapidly growing field has gained its popularity due to advent of new trends and technologies that require monitoring of human's psychophysical state with higher level of personalization and adaptation, as well as the ability to simulate empathy for more natural human-computer interaction. The capacity to adapt to user's current emotional state is important because emotions greatly influence people's behavior: they affect communication, health and personal well-being, decision making processes and other important aspects of everyday life. Hence, developing systems that are aware of current user's state will help to incorporate emotional content into human-machine interaction and improve overall user experience.

Some essential issues inherent to the study field of vocal emotions are difficulties of defining emotions, specifying number of existing

emotions, and distinguishing between different emotional states. These questions are important because they define the way investigators approach the study — what emotions to model, what to measure, how to interpret results, etc. In a typical speech research, emotions are defined as “brief and intense reactions to goal-relevant changes in the environment” [3]. Currently, there are two major approaches to modeling the emotional states adopted by researchers — continuous and categorical [1].

Continuous approach assumes that every emotion can be represented as a point in a 2- or 3-dimensional space, where the dimensions represent essential emotion characteristics, such as valence (positive or negative), activation (calm or excited), and even dominance (active or passive). The two- and three- dimensional emotion spaces with some emotion interpretations are shown in Figures 1 and 2, respectively. Categorical approach defines a list of basic emotions, usually from 4 to 7, which can be considered universal: anger, happiness, sadness, surprise, fear and neutral state [4]. Both approaches are actively being exploited in the field; the choice is usually determined by the database of the interest. In this study, we will be using the categorical approach.

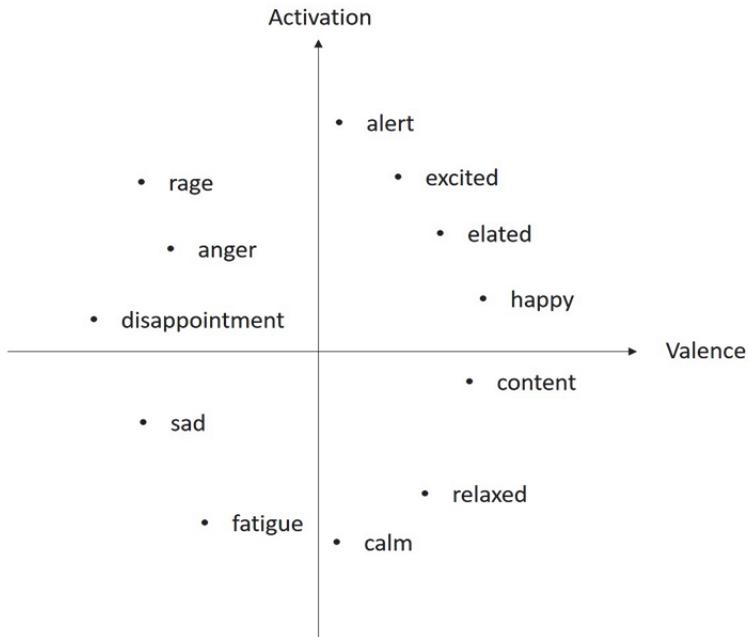


Fig. 1. Two-dimensional approach for emotion modelling by activation and valence dimensions

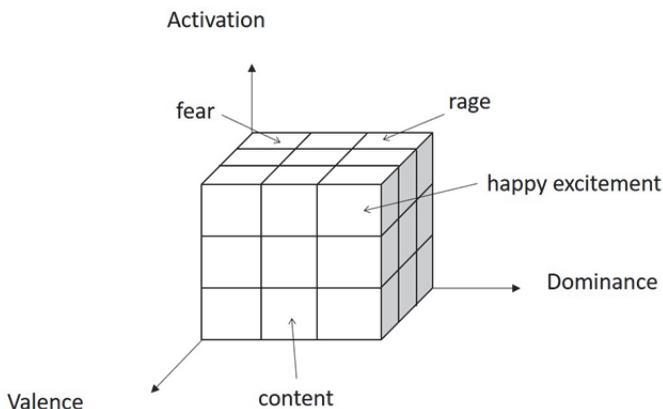


Fig. 2. Three-dimensional space for emotion modelling with some interpretations using activation, valence and dominance dimensions

Practical usage scenarios of emotionally-aware systems are numerous and range from small personalized applications to incorporation into big industries. Personal gadgets, such as smartphones and game consoles, will benefit from collecting data about user's emotional state to adapt their behavior and provide a better user experience; car electronics will monitor driver's stress level and sleepiness to prevent dangerous situations on the roads; banks and call-centers will be able to provide a better quality service; law enforcement agencies may escalate their security measures by automatically spotting suspicious activities. A good example of implementing such technologies on a bigger scale is medical treatment, where there is a need of continuous monitoring of a patient's emotional and psychophysical state, aiding an expert in health examination procedures, as well as better interacting and assisting people struggling to perceive emotions of others — such as children with autism. Involvement of automatic technologies proves beneficial insofar it allows capturing subtle characteristics that may escape from human's eyes and/or ears [2, 5].

Analysis of human emotions is possible from different information channels (modalities). To name a few — voice, face, gestures, postures, eye gaze and other physical measurements, such as electrocardiogram and skin conductance. Integrating several modalities in a single task is the main idea behind multimodal approaches towards emotion recognition. Multiple modalities are complimentary in nature and often bear redundant information. This allows to effectively battle the problem of missing values, where observations from one or several modalities may not be available at a particular time span. However, not all of them are equal in the amount of

information they provide. Voice, among other modalities, provides essential paralinguistic cues that are indicative of speaker's feelings. There are studies, which show that it is easier to read emotions from voice rather than from face [5], probably because people are better at hiding emotions from face, but not from voice [6]. Also, it has been established that face is more reliable conveying the valence of the portrayed emotion, while voice provides a better estimate of its intensity [7]. It means that speech is rather indicative of how calm or excited a person is, although it is not always easy to tell in which way — positive or negative. Thus, considering acoustic features of the signal, angry and happy voices sound similar in that they both carry a high amount of energy, higher fundamental frequency (F0), as well as wider F0 range, upward intonation contours, faster speaking rate and steeper spectral slope [6]. For the reasons described above this work is focused on automatic emotion recognition from speech.

2. Related work. There are several issues that impede the development of speech emotion recognition systems, one of them being absence of understanding what features should be used for classification [8]. Many current state-of-the-art systems use a large amount (on the order of thousands) of presumably relevant features with subsequent dimensionality reduction technique such as Principal Component Analysis (PCA) [9]. Another popular approach is to abandon predefined feature extraction and feed raw signals into a deep neural network, which finds a new feature representation without any hand-crafted engineering [10]. Another big issue, which renders the task of classifying emotions difficult, is the inherent inter-speaker and intra-speaker variability. Inter-speaker variability arises from different people having different age, gender, individual voice quality and characteristics. Intra-speaker variability adds uncertainty even more, for the voice quality of the same person changes with health condition, general mood, social environment, etc.

Cultural differences are another source of ambiguity encountered when modeling emotional states. A lot of debates were spawn around the question whether emotions are universal among people of all ages, genders, cultures and languages [11]. Do these factors define the way emotions are expressed and perceived and if so, how do emotions differ? There are few cross-corpus studies showing results on how well a given model trained on a particular database generalizes to other language databases [12]. Nevertheless, currently there is not enough data to prove or disprove the argument.

Feature extraction is an important step in the overall emotion recognition pipeline. The features can be extracted on two different levels: frame level and utterance level.

On the frame level, a certain amount of features are being extracted from analysis windows of the signal with a predefined frequency, usually

about 100 frames per second. This gives localized characteristics of the signal. To obtain the utterance level features, summarizing functionals are popularly applied to low level descriptors to form global utterance characteristics. Mere extraction of the features from the raw signal may not be enough; to gain a good performance, feature representation learning can be used to build high-level features from low-level features [13, 14]. Utterance-level representation of features was also explored by Kim [15]. Combination of different feature representations has also been explored; for example, Li Yang and Yunxin Zhao proposed to apply a shifting short-time window to extract short-term features and then applied functionals to the resulting sequences to obtain long-term feature representation, following with PCA dimensionality reduction and classification [16]. Dan-Ning Jiang and Lian-Hong Cai made use of temporal features alongside statistical features with GMM and HMM to benefit from both representations [17]. Some authors used combined frame and turn level analysis via HMM and statistical functionals [18].

Various types of classifiers have been used for the task of emotion classification from speech. Some of the desirable characteristics involve ability to work with small sets of data, handling missing values and outliers. As a result of Deep Neural Networks (DNN) becoming more and more powerful [19], various deep architectures, such as convolutional and recurrent NNs are actively being exploited [20-22]. A special type of recurrent neural network (RNN) called Long Short-Term Memory (LSTM) is particularly popular due to its ability to model arbitrarily large temporal sequences [7, 23]. It is an important property for emotion classification since emotions naturally evolve in time and therefore emotionally colored speech signals preserve a temporal structure.

3. Proposed method. General pipeline of a machine learning setup consists of feature extraction, preprocessing and training/testing stage. The baseline methods against which we compare the results consists of a single branch feature representation using predefined INTERSPEECH 2010 feature set (utterance-level functionals extracted via openSMILE toolkit), and a single LSTM Neural Network. The overall baseline pipelines are depicted in Figures 3 and 4. Preprocessing included feature normalization. The classification method was chosen to be logistic regression for the reasons discussed below.

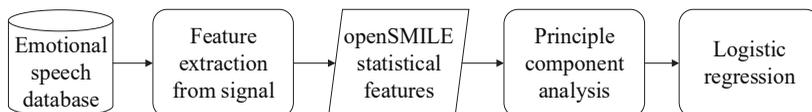


Fig. 3. Baseline method 1: PCA + Logistic Regression

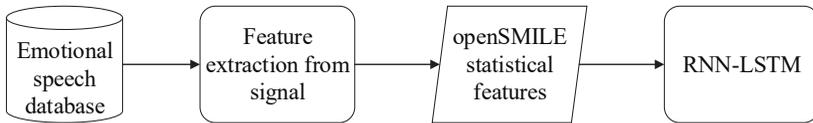


Fig. 4. Baseline method 2: LSTM-RNN

In our work, we propose a novel approach to implement a hybrid feature representation combining two different feature levels to take advantage of both short-time and long-time signal characteristics (Figure 5). The two levels of feature extraction are frame-level and utterance-level. The former corresponds to low level descriptors (LLDs), which are being extracted from every audio frame and form a sequence of feature vectors for every utterance. The length of the sequence depends on the duration of the audio signal and may vary for every utterance. To account for the temporal changes in these features as well as to match the resulting feature vectors of every utterance to have the same size, we let the sequences of LLDs to pass through an LSTM network and set the output of the network from the last frame to be the resulting feature vector describing the given utterance. Because the LSTM network has memory cells that allow accumulating information, the output from the last frame will have accumulated information from all the previous frames.

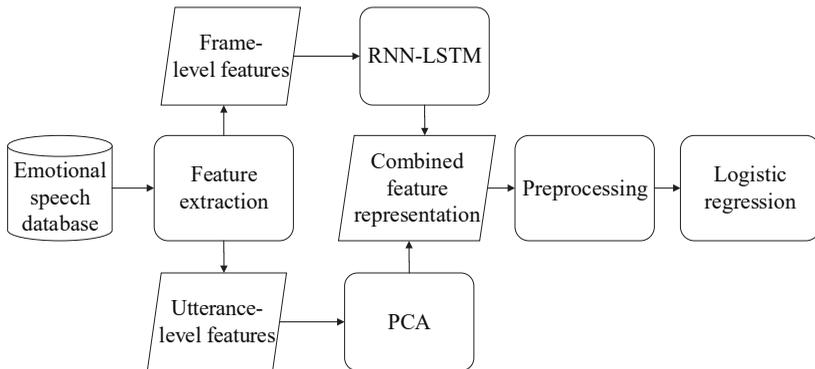


Fig. 5. General scheme of the proposed method

On the other hand, the utterance-level features represent statistical functionals applied to all the LLDs within one utterance and form a feature vector of a fixed size. Because the dimensionality of the resulting feature vector is very high, principal component analysis is used to reduce the number of features as well as to decorrelate them. The resulting two feature representations are concatenated to form a single feature vector, which is further fed into a logistic regression classifier that makes predictions about class labels.

The reason for combining the two different representations is that short-time characteristics (frame level features) together with appropriate modelling techniques allow capturing the temporal structure of the signal, while long-time characteristics (utterance-level features) are capable of expressing general trends [24]. Therefore, by combining the two approaches it is possible to benefit from both temporal dynamics as well as the big picture provided by statistical functionals.

4. Feature extraction and selection. The de-facto standard for feature extraction in the field of affective computing is openSMILE toolkit provided by German company audeERING [25]. There are predefined feature sets that were released during the series of annual INTERSPEECH Computational Paralinguistics Challenge (ComParE) [26-29]. The number of LLD features, as well as the number of applied statistical functionals and the total number of resulting utterance-level features are summarized in Table 1. After experimenting with these feature sets it turned out that the feature set, released in the year 2010, showed a better performance in comparison with other feature sets. The details about the LLDs and functionals in this set are presented in Table 2, the results of the comparison can be seen in Figure 6. Only the most significant number of principal components is shown.

Table 1. openSMILE configuration sets

Configuration set	LLD	Functionals	Total
INTERSPEECH-2009	16	12	384
INTERSPEECH-2010	38	21	1582
INTERSPEECH-2011	60	33	4368
INTERSPEECH-2013	65	54	6373

Table 2. INTERSPEECH 2010 paralinguistics challenge feature set

Low-Level Descriptors	Functionals
PCM loudness	Position maximum/minimum
MFCC [0-14]	Arithmetic mean, Standard deviation
Log Mel Freq. Band [0-7]	Skewness, Kurtosis,
LSP Frequency [0-7]	Linear regression coefficients 1/2
F0 by sub-Harmonic sum	Linear regression error Q/A
F0 envelop	Quartile 1/2/3
Voicing probability	Quartile range 2-1/3-2/3-1
Jitter local	Percentile 1/99
Jitter DDP	Percentile range 99-1
Shimmer local	Up-level time 75/90

Four different feature sets were compared by the accuracy, which was possible to obtain on RUSLANA corpus using particular feature set with the rest classification scheme being equal. The INTERSPEECH 2009 (IS_09) feature set consisted of 384 features, which was considered small enough not to apply any dimensionality reduction techniques. For the rest of the feature sets Principal Component Analysis (PCA) was applied in order to reduce the size of the feature vectors and decorrelate the features. The number of principal components was ranging from 10 to 1000. The INTERSPEECH 2010 feature set comprised 1582 features, INTERSPEECH 2011 feature set — 4368 features and the INTERSPEECH 2013 feature set included 6373 features in total. These features are obtained by applying certain statistical functionals to LLDs extracted on the frame level and represent utterance-level features.

As can be seen from Figure 6, the INTERSPEECH 2010 feature set has shown the best performance in comparison to other available feature sets. Therefore, further research was focused to include only features contained in this set. 38 LLDs were extracted from the audio signal at the frame rate of 100 fps, with the windows of various types and lengths. Hamming window of 25 msec was used for all the features, except the fundamental frequency (F0). The window applied to extract F0 was Gaussian with the length of 60 msec. Moving average filter was applied to all of the characteristics. 21 functionals as well as first order regression coefficients were applied to LLDs. 16 zero features were removed from the set (such as minimum F0 value — always zero). Two other additional features were included — the number of raises and the length of the F0 curve.

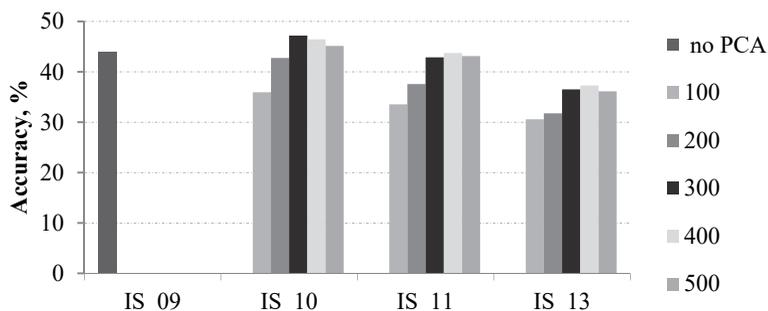


Fig. 6. Comparison of 4 openSMILE feature sets on RUSLANA database using Logistic Regression

PCM loudness is the normalized intensity raised to a power of 0.3. MFCC [0-14] refers to Mel-frequency cepstral coefficients from 0 to 14. Log

Mel Frequency Band [0-7] is the logarithmic power of Mel-frequency bands from 0 to 7 (distributed over a range from 0 to 8 kHz). LSP Frequency [0-7] is the 8-line spectral pair frequencies computed from 8 LPC (Linear Prediction Coding) coefficients. F0 envelop is the envelope of the smoothed fundamental frequency contour. The voicing probability reflects the likelihood that the frame is pitched. Jitter and shimmer are characteristics of voice quality that reflect frequency and amplitude instability, respectively. Jitter local is the frame-to-frame pitch period length deviations. Shimmer local is the frame-to-frame amplitude deviations between pitch periods. Jitter DDP is the differential frame-to-frame jitter (the jitter of the jitter). Some functionals are not applied to every low-level descriptor. For example, minimum, maximum, mean and standard deviation are not applied to voice related LLDs except for fundamental frequency F0.

5. LSTM Recurrent Neural Networks. Recurrent Neural Networks [30] are a special type of Neural Networks that have feedback connections, i.e. the output of an RNN unit is connected to the input of the same unit in order to provide the network ability to the previous activations. This allows to store memory about previous elements of a sequence and make better decisions in future. The general idea of an RNN network with feedback connections is shown below in Figure 7. On the left (a), the figure shows connections of a hidden layer from a Feedforward Neural Network, where the information propagates strictly forward. On the right (b), the same piece of network is shown with added feedback connections to each of the hidden neurons that turns the architecture into a Recurrent Neural Network. The feedback connections may also connect the neurons on the current layer with the previous layers, which allows to build more complex models.

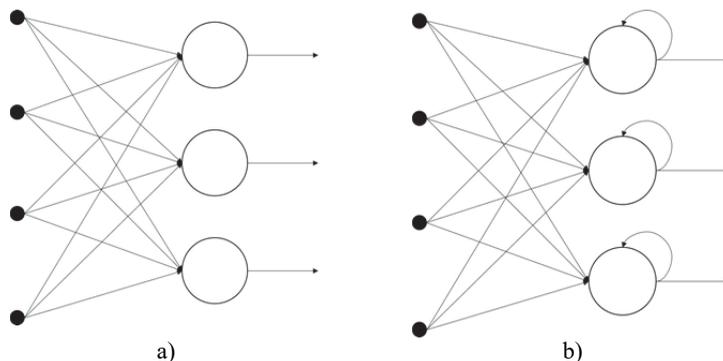


Fig. 7. Recurrent Neural Network structure in comparison with a simple Feedforward Neural Network: a) – feedforward Neural Network; b) – recurrent Neural Network

However, this kind of architecture has several drawbacks, one of which is inability to store sufficiently long context information. Some estimates suggest that the network forgets information after ten steps of iteration. For these reason Recurrent Neural Networks are said to possess short term memory. Vanishing gradients also pose difficulty for applying such networks in practice.

In order to cope with these drawbacks, a special type of cell was invented that can memorize and store an arbitrary amount information in time. It was called Long Short-Term Memory to emphasize that it overcomes the loss of information in RNNs. A typical LSTM cell has the structure depicted in Figure 8. It has an Input Gate i_t , Forget Gate f_t , and Output Gate o_t that regulate the amount of information which is being stored in the cell. The flow of data within the cell also allows to pass through the cell unchanged so that the problem of vanishing gradients is no longer a problem for LSTM. The gates are regulated by equations 1-3, where σ denotes sigmoid function. Each gate has its own weight coefficients W_f , W_i , W_o and biases b_f , b_i , b_o , which are optimized during training. The cell state C_t and output hidden state h_t are given in equations 4-5. The cell state is updated in accordance with the previous cell state and new candidates at the input gate. Output h_t represents a filtered cell state.

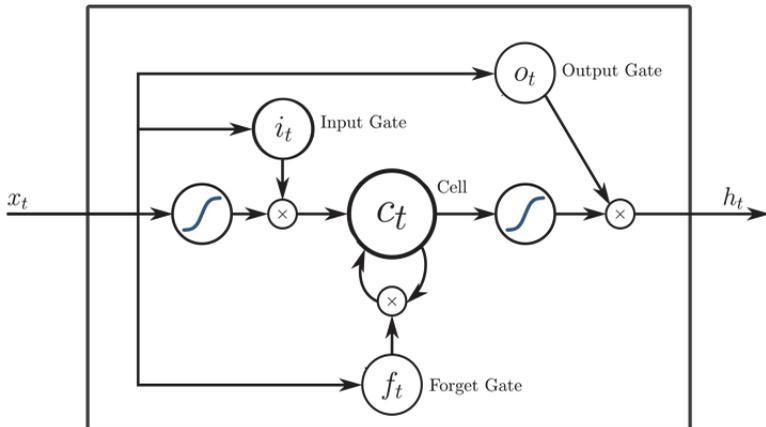


Fig. 8. Structure of a basic LSTM cell [30]

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f), \quad (1)$$

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i), \quad (2)$$

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o), \quad (3)$$

$$C_t = f_t * C_{t-1} + i_t * \tanh(W_c \cdot [h_{t-1}, x_t] + b_c), \quad (4)$$

$$h_t = o_t * \tanh(C_t). \quad (5)$$

Another improvement in LSTM cell structure is the additional peephole connections, which are depicted in Figure 9. Peephole connections are allowing for information to flow directly to the Input, Output and Forget Gates, letting them access to the current cell state.

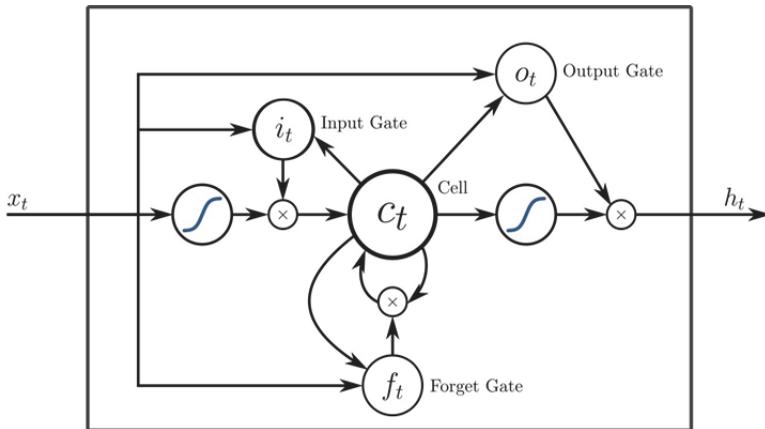


Fig. 9. Structure of an LSTM cell with peephole connections [30]

Different implementations will use some peepholes and not the others. One more variation is to couple forget and input gates. The implication is that the decision on what to store and what to forget are no longer independent and are made jointly, i.e. forgetting happens only when there is new data to put in the memory. Another popular variation on the LSTM cell is the Gated Recurrent Unit (GRU), introduced by Cho et al. [31]. In this particular implementation, the input gate and the forget gate are combined in a single update gate. Cell state and the output hidden state are also merged together. The structure of such unit is simpler than a standard LSTM cell and requires less computation, while providing similar performance.

In an LSTM network, LSTM units replace feedforward neurons. Typically, a hidden layer of LSTM cells would be followed by a fully connected layer, that connects the LSTM layer with the output. The input is represented by a 3-dimensional array, where samples are sequences of

features. Assuming that the number of samples is n , the sequences are of length s and feature vector contains f features, the final topology of the network is depicted in Figure 10.

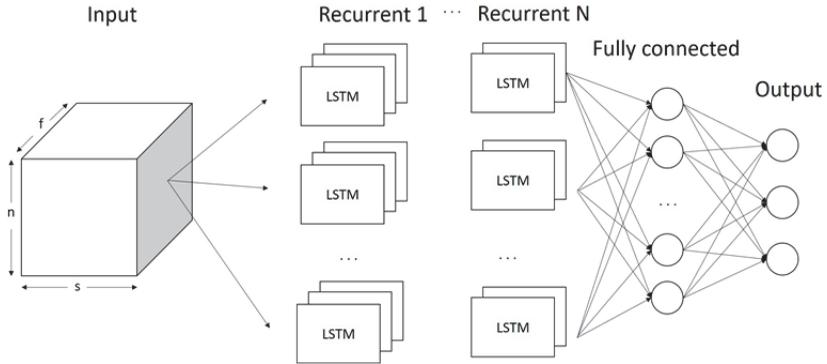


Fig. 10. Topology of an LSTM network: n – number of samples, s – length of the sequence, f – number of features in each observation in the sequence, N – number of recurrent layers used in the network

6. Feature representation using LSTM. In the second branch, frame-level LLD sequences are extracted via openSMILE toolkit in accordance with the feature selection methods described above. These sequences are passed through a unidirectional one-layer RNN-LSTM network with 300 hidden units, one frame at a time. After the last frame has propagated through the network, the output of the network is saved as a feature vector, containing information about temporal structure of the signal. The process of representing an utterance with LSTM unrolled in time is depicted in the Figure 11. The LLD sequence of one particular utterance is denoted as f_0, f_1, \dots, f_d , where d – the number of frames in the utterance. The LSTM network depicted in the diagram is the same network, unrolled in time, to show that only the last output of the LSTM is considered as the feature vector representation for that one utterance.

The training of LSTM network is done as if it performs the function of a classifier — that is, a pair of (feature vector, label) is presented to the network, the weights get updated and the procedure repeats until the network has seen all the samples and the training process converges. Next, the last layer of the network, the softmax layer with the number of units equal to the number of prediction classes, is removed and the output of the network is no longer a probability of belonging to a particular class, but rather a complex 300-dimensional non-linear representation of the input features. The two feature representations are concatenated together to form a single feature vector that is passed to the classification step.

The architecture of the used RNN-LSTM network contains one hidden layer of 128 LSTM units. The initial learning rate is set to 0.001 and is decreased every 100 epochs by the factor of 0.1. The learning process was stopped when the learning curve is not improved for 15 consecutive epochs. Dropout was not applied out of the data size concern: most of the datasets are small in size. L2-regularization was implemented alongside cross-entropy loss function. In all the experiments the optimizer of choice was Adam. Mini-batches of size 250 were used. In all the experiments LSTM implementation was carried out with TensorFlow framework [32].

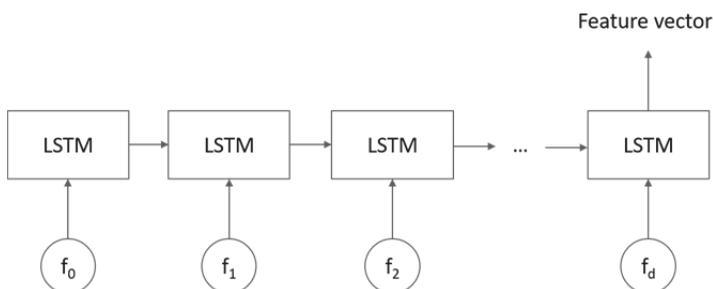


Fig. 11. Feature vector representation via LSTM network. The LLD sequence of one particular utterance is denoted as f_0, f_1, \dots, f_d , where d is the number of frames

7. Feature representation using PCA. The proposed method consists of two different feature representation methods, implemented in parallel, as can be seen in Figure 8. In the first branch, utterance-level functional are computed from LLDs. Statistical functional are known to have more expressive power than LLDs, considering the suprasegmental nature of emotions [24], however they fail to take into account the temporal changes in the signal, which are also of great importance since all emotions evolve in time. The number of possible functionals is very big and it is not clear which ones are more informative than others. They also often have a high correlation. For these reasons and a common problem known as curse of dimensionality [33], PCA is performed to reduce the dimensionality of resulting feature vectors and de-correlate the features.

Mathematically, PCA [34] is defined as an orthogonal linear projection of data to a new coordinate system of the form $\mathbf{T} = \mathbf{X}\mathbf{W}$, where $\mathbf{X} = (x_1, \dots, x_n)^T$ is the data matrix, $\mathbf{W} = (w_1, \dots, w_p)$ is a $p \times p$ weight matrix, whose columns are eigenvectors of $\mathbf{X}^T\mathbf{X}$, and \mathbf{T} is the new PCA representation of the data. The transformation maps each row vector of data $x_{(i)}$ to a new vector of principal component scores $t_{(i)} = (t_1, \dots, t_m)_{(i)}$ given

by $t_{k(i)} = x_{(i)} \cdot \mathbf{w}_{(k)}$ for $i = 1 \dots n, k = 1 \dots m$ with each weight vector \mathbf{w} being a unit vector. The greatest variance happens to lie on the first coordinate, which is also called the first principal component, the second greatest variance – on the second principal component and so on. Principal components are visualized in the directions of greatest variance in Figure 12.

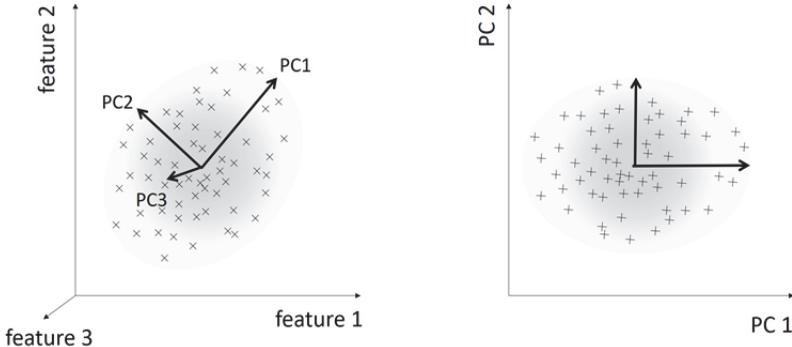


Fig. 12. Illustrations of the Principal Component Analysis: principal components point in the direction of greatest variance

To maximize variance, the first weight vector $\mathbf{w}_{(1)}$ must satisfy the following condition:

$$\mathbf{w}_{(1)} = \arg \max_{\mathbf{w}=1} \{ \mathbf{X} \mathbf{w}^2 \} = \arg \max_{\mathbf{w}=1} \{ \mathbf{w}^T \mathbf{X}^T \mathbf{X} \mathbf{w} \} = \arg \max \left\{ \frac{\mathbf{w}^T \mathbf{X}^T \mathbf{X} \mathbf{w}}{\mathbf{w}^T \mathbf{w}} \right\}. \quad (6)$$

After the $\mathbf{w}_{(1)}$ is found, the first principal component of a data vector $x_{(i)}$ can be found in the transformed coordinates as $t_{1(i)} = x_{(i)} \cdot \mathbf{w}_{(1)}$. The k -th principal component can be found by subtracting from \mathbf{X} the first $k-1$ principal components and then finding the weight vector corresponding to the maximum variance from the new data $\hat{\mathbf{X}}_k$.

$$\hat{\mathbf{X}}_k = \mathbf{X} - \sum_{s=1}^{k-1} \mathbf{X} \mathbf{w}_{(s)} \mathbf{w}_{(s)}^T. \quad (7)$$

8. Classification. A comparative study [35] was conducted on the RUSLANA database to find out the best classification scheme suited for the task. The results of the study are summarized in Figure 13. As can be seen

from the figure, the best prediction accuracy was achieved via Logistic Regression (Log-R) classifier. The second-best approach turned out to be Support Vector Machine (SVM), and the third best — a simple artificial Neural Network (NN) with one hidden layer. Other classifiers, that were used in the comparative study, are: Linear Regression (Lin-R), Naïve Bayes (NB), k-Nearest Neighbours (kNN), and Random Forest (RF).

Linear kernel gave the best result for SVM classification, which proves that with a high number of features non-linear projections don't improve the efficiency of the system. The optimal value for C parameter was chosen empirically. In kNN approach, the best k parameter was also found empirically and was equal to 10 neighboring points. The number of hidden layers in NN varied from 1 to 2, number of neurons in each layer — from 50 to 500. The number of epochs and learning rate ranged from 100 to 500, from 0.1 to 0.0001 respectively. RF parameter was optimized experimentally.

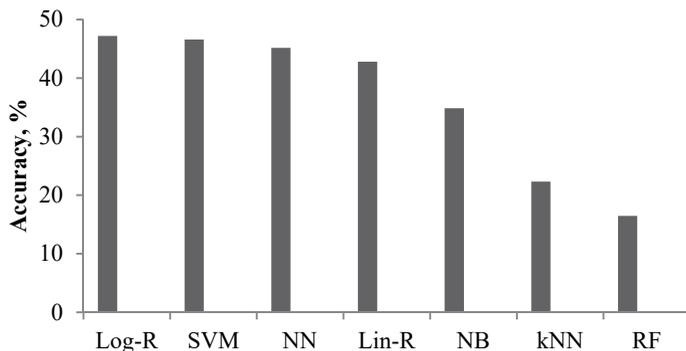


Fig. 13. Classification results of various classifiers applied to RUSLANA

In order to achieve speaker-independent properties of the system we would like to know whether a model trained on a particular set of persons generalizes well to the group of previously unseen voices. To implement this, we need to ensure that all the samples in the validation set are not represented at all in the training set. This is achieved via leave-one-subject-out cross validation strategy, which ensures that the same subject is not represented in both testing and training sets. Hence, the overall experiments are handled as 61-fold subject-independent cross-validation, i.e. the training was implemented on 60 speakers and the testing on the remaining speaker to achieve speaker-independent properties of the system.

9. Logistic Regression. Regression models are used for defining the relationship between one dependent variable and several independent variables. When the dependent variable is in discrete form, the regression turns into a binary classification task. Let us assume that output y_i is a realization of

a random variable Y_i , which takes on one of the two values: 0 and 1 with probabilities π_i and $1-\pi_i$. Such distribution is called a Bernoulli distribution and can be written in the form $\Pr\{Y_i = y_i\} = \pi_i^{y_i} (1-\pi_i)^{1-y_i}$. When building a linear regression an assumption is being made about probabilities π_i having linear dependency on observations: $\pi_i = x_i' \beta = \beta_1 x_{i1} + \beta_2 x_{i2} + \dots + \beta_n x_{in}$, where β is a vector of regression coefficients.

In order to limit the prediction values to the range from 0 to 1, probabilities π_i are transformed to $\frac{\pi_i}{1-\pi_i}$, which reflects the chance of a

particular event happening, which can take on any positive value. After that the transformed values undergo logistic transformation

$\eta_i = \text{logit}(\pi_i) = \log \frac{\pi_i}{1-\pi_i}$. With such representation, when the chance is close

to 0, logit is approaching $-\infty$. From the other side, when the probability is close to 1, both the chance and the logit approach $+\infty$. Therefore, the logit transformation projects probability from the range $\{0, 1\}$ on to the whole rational number space. When the probability is 0.5, the logistic function is 0. Negative numbers correspond to probabilities < 0.5 , and positive numbers correspond to probabilities > 0.5 . This logit transformation is unique and

therefore reversible: $\pi_i = \text{logit}^{-1}(\eta_i) = \frac{e^{\eta_i}}{1+e^{\eta_i}}$. Logistic regression assumes

that probability logit is a linear model: $\text{logit}(\pi_i) = x_i' \beta$. Interestingly enough, logistic regression provided a better performance in comparison to simple feedforward Neural Network, despite having a simpler structure. This phenomenon can be explained by regularization effects.

Regularization can be used in all regression models by adding another term to the loss function, which does not allow for coefficients to grow arbitrarily large, causing model overfitting. Hence, regularization helps to generalize the model and abstract away from the particularities.

There are several underlying assumptions on which the logistic regression models are build. First, it is assumed that there is no linear dependency between regression model factors; second, the variance is assumed to be constant. In practice, it is not always possible to comply with such conditions. Despite of that, logistic regression models are commonly used in practice.

10. Emotional speech corpora. We used 3 open source speech databases to evaluate our proposed method. These corpora are:

RUSLANA [36] (Russian speech), EMODB [37] (German speech), and BUEMO [38] (Turkish speech). The databases were chosen so that they have a similar structure and different languages to see how well the model can be generalized. All of them are well-balanced, i.e. having the same number of samples per each class, acted by non-professional actors, with a predefined set of categorical emotions.

RUSsian LANguage Affective corpus RUSLANA is a Russian language emotional speech database collected at the Department of Phonetics, St. Petersburg State University, Russia, in a sound proof recording studio. It contains audio recordings of 61 subjects (12 male and 49 female), in the age of 16-28 years old, all of whom were university students and native speakers of the standard Russian language. Each speaker pronounced 10 phonetically representative decontextualized sentences, which included all the Russian phonemes and most commonly encountered consonant clusters. Each sentence represented one of the 10 syntactic types, corresponding to distinct intonation contours, which coincide with different intonation contours in Bryzgunova's classification [39] inherent to the Russian language. Every sentence was pronounced with the following six basic emotional states: Neutral (N), Surprise (S), Happiness (H), Anger (A), Sadness (D) and Fear (F). Therefore, there are $61 \text{ speakers} \times 10 \text{ sentences} \times 6 \text{ emotion classes} = 3660$ audio files in total, each ranging in length from 2 to 5 seconds.

RUSLANA was chosen for the training purposes for several reasons. First, it is a well-balanced corpus containing an equal number of emotional utterances in every class; second, the actors are not professional and thus they do not reflect exaggerated intonation and other prosodic characteristics, common to professional performers [40]; third, the corpus construction strategy takes into account peculiarities of the Russian language and therefore provides a useful framework for developing a speech emotion recognition system from Russian speech, research on which until now has been sparse and inconsistent.

A database of German emotional speech (EMODB) was collected at the Department of Technical Acoustics of the Technical University of Berlin, in an anechoic chamber with high-quality recording equipment. Ten non-professional actors (5 male and 5 female) whose age ranged from 21 to 35 years old repeated 10 utterances with the following 7 different emotions: Neutral, Anger, Fear, Joy, Sadness, Disgust and Boredom. The total number of utterances is $10 \text{ speakers} \times 10 \text{ sentences} \times 7 \text{ emotion classes} = 700$ with some additional second versions reaching up to 800 recordings. The utterances of two types (a short sentence and a two phrase sentence) were constructed from everyday life usage.

The speech recordings of the BUEMODB dataset were collected in Bogazici University in Istanbul. There are 121 utterances for each of four emotional classes (Angry, Happy, Neutral and Sad) from 11 amateur theatre

actors (4 male and 7 female) by means of Stanislavskiy effect for generating emotional utterances [41]. The total number of audio files is $11 \text{ speakers} \times 11 \text{ sentences} \times 4 \text{ emotion classes} = 484$. The information about all three databases are summarized in Tables 3 and 4. Table 3 shows general information of how many speakers participated in database collection, what language was used for recording and number of emotion classes. Table 4 shows distribution of number of utterances among the classes.

Table 3. Corpora summary

Corpus	Lang.	Speakers	Females	Classes
EMODB	German	10	5	7
RUSLANA	Russian	61	49	6
BUEMODB	Turkish	11	7	4

Table 4. Corpora class distribution. Classes are abbreviated as follows: N – Neutral, A – Anger, H – happiness, S – Sadness, D – Disgust, F – Fear, B – boredom

Corpus	N	A	H	S	D	F	B	All
EMODB	79	127	71	62	51	69	81	535
RUSLANA	610	610	610	610	610	610	-	3600
BUEMODB	121	121	121	121	-	-	-	484

11. Experimental results and discussion. After experimenting with the number of components used in the PCA analysis we can conclude that for different datasets the optimal number of principal components differs, which may be explained by different data distributions due to varying recording conditions and audio signal quality. This is in consent with the recent study of [42], which showed evidence that the nature of dataset gives an idea to select relevant classifiers. The results are presented in the Table 5.

Table 5. Classification accuracy (%) of logistic regression with various numbers of principal components

PCA #	Classification accuracy (%)		
	EMODB	RUSLANA	BUEMO
10	52.1	31.7	49.4
50	56.3	34.2	52.5
100	48.3	36.9	53.4
200	38.4	43.6	52.8
300	51.1	47.2	55.1
400	52.3	44.9	56.0
500	52.2	44.8	56.2

EMODB showed the best performance at the minimum number of principal components being equal 50, which allowed obtaining classification accuracy of 56.3%. Both RUSLANA and BUEMO datasets required more number of principal components in order to achieve optimal performance. In case of RUSLANA, 300 principal components obtained via PCA resulted in 47.2% classification accuracy. Among other datasets optimal performance on BUEMO was achieved with the highest number of principal components being equal 400. In all the cases the original number of features was reduced more than three times. This indicates that high number of features indeed suffers from curse of dimensionality. The apparent conclusion is that feature decorrelation and dimensionality reductions techniques are an important preprocessing step in emotion classification task.

The baseline classification method, which consisted of single branch openSMILE utterance-level feature extraction, showed maximum classification accuracy of 47.2% on the RUSLANA dataset, 56.3 on the EMODB dataset, and 56.0 on the BUEMO dataset. The second baseline using a single LSTM network gave the worst results, as expected: 40.5% on the RUSLANA dataset, 45.3% on the EMODB dataset, and 39.9% on the BUEMO dataset. The implementation of the single LSTM network alone showed a severe overfitting problem, presumably due to a small size of the dataset.

Implementing the newly proposed method allowed us to obtain a relative improvement over the first baseline (PCA + Logistic regression) 2.3 % in classification accuracy on the RUSLANA corpus and 2.8% on the BUEMO corpus. EMODB, on the contrary, did not show a relative improvement but a comparative performance with the combination of the proposed techniques. The relative improvement over the second baseline was much more prominent 9.0%, 10.8%, 18.9%. The details of the obtained results are summarized in Table 6.

Table 6. Classification accuracy (%) of the baseline and the proposed methods

Modeling method	RUSLANA (6 classes)	EMODB (7 classes)	BUEMO (4 classes)
PCA + Logistic regression	47.2	56.3	56.0
LSTM	40.5	45.3	39.9
Proposed Combination	49.5	56.1	58.8

The number of classes differed from corpus to corpus and therefore the interpretation of the results should be made accordingly. In case of 4

classes (BUEMO), the chance level is 25%, and so the proposed method worked more than twice better than the chance level. In the case of 6 classes (RUSLANA) the chance level is 16.(6)% and so the proposed implementation achieved performance almost 3 times better than the chance level. In case of 7 classes (EMODB), the chance level is at 14.29% giving relative improvement of the proposed approach almost 4 times better than the chance level.

Training an LSTM network on EMODB and BUEMO corpora showed significant overfitting results despite implementing various regularization techniques, such as early stopping and dropout. This can be explained by the small dataset sizes (114 samples per class on average for EMODB, and 121 samples per class for BUEMO). RUSLANA, on the contrary, had 610 samples per class and therefore showed more consistent results on the training. The reader is referred to [43] for more experimental results on the BUEMO corpus.

A sentiment analysis based on automatic text processing can help additionally improving the quality of bimodal speech emotion recognition [44]; automatic speech recognition techniques (e.g. [45, 46]) should be applied for speech-to-text transformation in this case.

12. Conclusions. We have proposed a new method for combining two feature representations for emotion classification from speech: a frame-level representation of low-level descriptors and an utterance-level representation of LLD functionals. The proposed approach is motivated by the need to account for dynamic nature of emotion evolution in time, as well as the trade-off between local LLD features, which give an insight on the temporal changes in signal, and global statistical functionals, which are known to better capture the general trends. Our method was built on traditional application of statistical openSMILE features with PCA dimensionality reduction combined with the recent state-of-the-art LSTM RNN technologies. The optimal number of principal components lies in the range 50 to 400. Principal components less than 50 do not allow adequately modeling the underlying nature of emotions and therefore do not render optimal performance. Principal components more than 400 turn out to possess redundancy and high correlation, which also hinders the effectiveness of classification and shows worse performance in terms of classification accuracy. More features turn out to give worse performance probably due to bigger correlation, redundancy, noise and curse of dimensionality problem.

The experimental results were compared to two different baseline methods. One consisted of a single branch openSMILE utterance-level feature extraction, Principal Component Analysis dimensionality reduction and Logistic Regression classification. The other was based on a single LSTM-

RNN Neural Network trained on utterance-level openSMILE features. The proposed method showed increased classification accuracy compared to the baseline methods, however the results were not consistent across all the datasets. The explanation lies in the different corpus sizes: more samples per class guarantee better performance of the system and less overfitting issue. One of the drawbacks of the proposed method is that it requires a lot of data to be trained. However, with recent advances in cross-corpus analysis it is possible to combine different corpora in order to have more training data and more robust and stable learning process. The method proved effective combining the temporal dynamic changes in frame level features and general trends of utterance-level functionals. Therefore, the direction of future research will be to investigate possible ways of post-processing of the obtained feature representations, scaling and normalization techniques, as well as possibility of conducting cross-corpus analysis in order to upsample the training data.

References

1. Swain M., Routray A., Kabisatpathy P. Databases, features and classifiers for speech emotion recognition: a review. *International Journal of Speech Technology*. 2018. vol. 21. no. 1. pp. 93–120.
2. Mustafa M.B., Yusoof M.A., Don Z.M., Malekzadeh M. Speech emotion recognition research: an analysis of research focus. *International Journal of Speech Technology*. 2018. vol. 21 no. 1. pp. 137–156.
3. Laukka P., Juslin P., Bresin R. A dimensional approach to vocal expression of emotion. *Cognition and Emotion*. 2005. vol. 19 no. 5. pp. 633–653.
4. Nogueira P.A., Rodrigues R., Oliveira E., Nacke L.E. Modelling human emotion in interactive environments: Physiological ensemble and grounded approaches for synthetic agents. *Web Intelligence*. 2015. vol. 13. no. 3. pp. 195–214.
5. Kraus M.W. Voice-only communication enhances empathic accuracy. *American Psychologist*. 2017. vol. 72. no. 7. pp. 644–654.
6. Kreiman J., Sidtis D. Foundations of voice studies: an interdisciplinary approach to voice production and perception. John Wiley & Sons. 2013. 512 p.
7. Wöllmer M. et al. Context-sensitive multimodal emotion recognition from speech and facial expression using bidirectional LSTM modeling. Proc. INTERSPEECH. Japan. 2010. pp. 2362–2365.
8. Anagnostopoulos C.-N., Iliou T., Giannoukos I. Features and classifiers for emotion recognition from speech: a survey from 2000 to 2011. *Artificial Intelligence Review*. 2015. vol. 43 no. 2. pp. 155–177.
9. Shabani S., Norouzi Y. Speech recognition using Principal Components Analysis and Neural Networks. 8th International Conference on Intelligent Systems. 2016. pp. 90–95.
10. Trigeorgis G. et al. Adieu features? end-to-end speech emotion recognition using a deep convolutional recurrent network. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2016. pp. 5200–5204.
11. Kaya H. et al. Emotion, age, and gender classification in children’s speech by humans and machines. *Computer Speech & Language*. 2017. vol. 46. pp. 268–283.
12. Kaya H., Karpov A.A. Efficient and effective strategies for cross-corpus acoustic emotion recognition. *Neurocomputing*. 2018. vol. 275. pp. 1028–1034.
13. Bengio Y., Courville A., Vincent P. Representation learning: A review and new perspectives. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2013. vol. 35. no. 8. pp. 1798–1828.

14. Ghosh S., Laksana E., Morency L.-P., Scherer S. Representation Learning for Speech Emotion Recognition. Proc. INTERSPEECH. 2016. pp. 3603–3607.
15. Kim Y., Provost E.M. Emotion classification via utterance-level dynamics: A pattern-based approach to characterizing affective expressions. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2013. pp. 3677–3681.
16. Li Y., Zhao Y. Recognizing emotions in speech using short-term and long-term features. Fifth International Conference on Spoken Language Processing. 1998. vol. 6. pp. 2255.
17. Jiang D.-N., Cai L.-H. Speech emotion classification with the combination of statistic features and temporal features. ICME. 2004. pp. 1967–1970.
18. Vlasenko B., Schuller B., Wendemuth A., Rigoll G. Combining frame and turn-level information for robust recognition of emotions within speech. Proc. INTERSPEECH. Belgium. 2007. pp. 2249–2252.
19. Sainath T.N., Vinyals O., Senior A., Sak H. Convolutional, long short-term memory, fully connected deep neural networks. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2015. pp. 4580–4584.
20. Mao Q., Dong M., Huang Z., Zhan Y. Learning salient features for speech emotion recognition using convolutional neural networks. *IEEE Transactions on Multimedia*. 2014. vol. 16. no. 8. pp. 2203–2213.
21. Tran D. et al. Learning spatiotemporal features with 3d convolutional networks. Proceedings of the IEEE international conference on computer vision. 2015. pp. 4489–4497.
22. Kim J., Truong K.P., Englebienne G., Evers V. Learning spectro-temporal features with 3D CNNs for speech emotion recognition. Seventh International Conference on Affective Computing and Intelligent Interaction (ACII). 2017. pp. 383–388.
23. Chao L. et al. Long short term memory recurrent neural network based multimodal dimensional emotion recognition. Proceedings of the 5th International Workshop on Audio/Visual Emotion Challenge. 2015. pp. 65–72.
24. Schuller B. et al. The relevance of feature type for the automatic classification of emotional user states: Low level descriptors and functionals. Proc. INTERSPEECH. 2007. pp. 2253–2256.
25. Eyben F., Wöllmer M., Schuller B. Opensmile: the Munich versatile and fast open-source audio feature extractor. Proceedings of the 18th ACM international conference on Multimedia. 2010. pp. 1459–1462.
26. Schuller B., Steidl S., Batliner A. The INTERSPEECH 2009 emotion challenge. Tenth Annual Conference on the International Speech Communication Association INTERSPEECH. 2009. pp. 312–314.
27. Schuller B. et al. The INTERSPEECH 2010 paralinguistic challenge. Proc. INTERSPEECH. 2010. pp. 2794–2797.
28. Schuller B. et al. The INTERSPEECH 2011 speaker state challenge. Proc. INTERSPEECH. 2011. pp. 3201–3204.
29. Schuller B. et al. The INTERSPEECH 2013 computational paralinguistics challenge: social signals, conflict, emotion, autism. Proc. INTERSPEECH. 2013. pp. 148–152.
30. Greff K. et al. LSTM: A search space odyssey. *IEEE Transactions on Neural Networks and Learning Systems*. 2017. vol. 28. no. 10. pp. 2222–2232.
31. Cho K. et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation. arXiv preprint arXiv:1406.1078. 2014.
32. Abadi M. et al. Tensorflow: a system for large-scale machine learning. OSDI. 2016. vol. 16. pp. 265–283.
33. Keogh E., Mueen A. Curse of dimensionality. Encyclopedia of machine learning. Springer. 2011. pp. 257–258.
34. Jolliffe I. Principal component analysis. International encyclopedia of statistical science. Springer. 2011. pp. 1094–1096.

35. Verkholyak O., Karpov A. Combined Feature Representation for Emotion Classification from Russian Speech. International Conference on Artificial Intelligence and Natural Language AINL-2017. Springer CCIS. vol. 789. 2018. pp. 68–73.
36. Makarova V., Petrushin V.A. RUSLANA: A database of Russian emotional utterances. Seventh International Conference on Spoken Language Processing. 2002. pp. 2041–2044.
37. Burkhardt F. et al. A database of German emotional speech. Ninth European Conference on Speech Communication and Technology. 2005. pp. 1517–1521.
38. Meral H.M., Ekenel H.K., Ozsoy A. Analysis of emotion in Turkish. XVII National Conference on Turkish Linguistics. 2003.
39. Bryzgunova, E.A. *Zvuki i intinaciya v russkoy rechi* [Sounds and intonation of Russian Speech]. Moscow: Russkiy yazyk. 1977. 281 p. (In Russ.).
40. Anikin A., Lima C.F. Perceptual and acoustic differences between authentic and acted nonverbal emotional vocalizations. *The Quarterly Journal of Experimental Psychology*. 2017. pp. 1–21.
41. Kaya H., Salah A.A., Gurgun S.F., Ekenel H. Protocol and baseline for experiments on Bogazici University Turkish emotional speech corpus. 22nd Signal Processing and Communications Applications Conference (SIU). 2014. pp. 1698–1701.
42. Koolagudi S.G., Murthy Y.S., Bhaskar S.P. Choice of a classifier, based on properties of a dataset: case study-speech emotion recognition. *International Journal of Speech Technology*. 2018. vol. 21. no. 1. pp. 167–183.
43. Kaya H., Karpov A.A., Salah A.A. Robust acoustic emotion recognition based on cascaded normalization and extreme learning machines. Proc. International Symposium on Neural Networks ISNN-2016. LNCS 9719. 2016. pp. 115–123.
44. Montacié C., Caraty M.J. Vocalic, lexical and prosodic cues for the INTERSPEECH 2018 self-assessed affect challenge. Proc. INTERSPEECH. 2018. pp. 541–545.
45. Besacier L., Barnard E., Karpov A., Schultz T. Automatic speech recognition for under-resourced languages: A survey. *Speech Communication*. 2014. vol. 56. pp. 85–100.
46. Kipyatkova I., Karpov A. A Study of Neural Network Russian Language Models for Automatic Continuous Speech Recognition Systems. *Automation and Remote Control*. 2017. vol. 78. no. 5. pp. 858–867.

Verkholyak Oxana Vladimirovna — Junior Researcher of Speech and Multimodal Interfaces Laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: automatic emotion recognition in speech, affective computing, computational paralinguistics. The number of publications — 9. overkholyak@gmail.com; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-0421, fax: +7(812)328-0421.

Kaya Heysem — Ph.D., Assistant Professor of Computer Engineering Department of Çorlu Faculty of Engineering, Namık Kemal University. Research interests: machine learning, pattern recognition, speech signal processing, emotions in speech. The number of publications — 40. hkaya@nku.edu.tr; Silahtarağa Mahallesi, Üniversite, 1, 59860 Çorlu/Tekirdağ, Turkey, office phone: +902822502346.

Karpov Alexey Anatolyevich — Ph.D., Dr. Sci., Associate Professor, Head of Speech and Multimodal Interfaces Laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: automatic speech recognition, multimodal interfaces, computational paralinguistics. The number of publications — 250. karpov@ias.spb.su; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-0421, fax: +7(812)328-0421.

Acknowledgments. This research is supported by the Russian Science Foundation (project № 18-11-00145).

О.В. ВЕРХОЛЯК, Х. КАЙЯ, А.А. КАРПОВ
**МОДЕЛИРОВАНИЕ КРАТКО- И ДОЛГОВРЕМЕННЫХ
ЗАВИСИМОСТЕЙ РЕЧЕВОГО СИГНАЛА ДЛЯ
ПАРАЛИНГВИСТИЧЕСКОЙ КЛАССИФИКАЦИИ ЭМОЦИЙ**

Верхоляк О.В., Кайя Х., Карпов А.А. Моделирование кратко- и долговременных зависимостей речевого сигнала для паралингвистической классификации эмоций.

Аннотация. Распознавание эмоций в речи стало одним из важных направлений в области аффективных вычислений. Это комплексная задача, трудности которой во многом определяются необходимостью выбора признаков и их оптимального представления. Оптимальное представление признаков должно отражать глобальные характеристики, а также локальную структуру сигнала, поскольку эмоции естественным образом делятся во времени. Подобное представление возможно моделировать с помощью рекуррентных нейронных сетей (РНС — RNN), которые активно используются для различных задач распознавания, предполагающих работу с последовательностями. Предлагается смешанный подход к представлению признаков, который объединяет традиционные статистические признаки с последовательностью значений, полученных на выходе РНС с длинной кратковременной памятью (ДКП — LSTM) и хорошо моделирующих временную структуру сигнала. Таким образом, удастся получить одновременное представление как кратковременных, так и долгосрочных характеристик, позволяющих использовать преимущества обоих подходов к моделированию признаков речевого сигнала. Для экспериментальной проверки предложенного метода была произведена оценка его эффективности на трех различных базах данных эмоционально окрашенной речи, находящихся в свободном доступе: RUSLANA (русская речь), BUEMODB (турецкая речь) и EMOVB (немецкая речь). В сравнении с традиционным подходом результаты наших экспериментов показывают абсолютный прирост в точности распознавания эмоций в 2.3% и 2.8% для двух из вышеупомянутых корпусов, в то время как для третьего корпуса предложенный метод не уступает базовой системе. Следовательно, данный подход можно признать эффективным для моделирования эмоциональной окраски речевых высказываний при условии достаточного количества обучающих данных.

Ключевые слова: распознавание эмоций в речи, компьютерная паралингвистика, аффективные вычисления, представление признаков, моделирование контекста, искусственные нейронные сети, длинная кратковременная память.

Верхоляк Оксана Владимировна — младший научный сотрудник лаборатории речевых и многомодальных интерфейсов, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: автоматическое распознавание эмоций в речи, аффективные вычисления, компьютерная паралингвистика. Число научных публикаций — 9. overkholyak@gmail.com; 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т.: +7(812)328-7081, факс: +7(812)328-7081.

Кайя Хейсем — к-т техн. наук, доцент, Университет Намыка Кемаля (Турция), инженерный факультет Чорлу, Отдел вычислительной техники, Старший преподаватель. Область научных интересов: машинное обучение, распознавание образов, обработка речевых сигналов, эмоции в речи. Число научных публикаций — 40. hkaya@nku.edu.tr; р-н Силахтарага, ул. Университетская 1., 59860 Чорлу, Текирдаг, Турция; р.т.: +902822502346

Карпов Алексей Анатольевич — д-р техн. наук, доцент, заведующий лабораторией речевых и многомодальных интерфейсов, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: автоматическое распознавание речи, многомодальные интерфейсы, компьютерная паралингвистика. Число научных публикаций — 250. karpov@iias.spb.su. 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р. т. +7(812)328-0421, факс +7(812)328-0421.

Поддержка исследований. Работа выполнена при поддержке Российского научного фонда (проект № 18-11-00145).

Литература

1. *Swain M., Routray A., Kabisatpathy P.* Databases, features and classifiers for speech emotion recognition: a review // *International Journal of Speech Technology*. 2018. vol. 21. no. 1. pp. 93–120.
2. *Mustafa M.B., Yusoof M.A., Don Z.M., Malekzadeh M.* Speech emotion recognition research: an analysis of research focus // *International Journal of Speech Technology*. 2018. vol. 21. no. 1. pp. 137–156.
3. *Laukka P., Juslin P., Bresin R.* A dimensional approach to vocal expression of emotion // *Cognition and Emotion*. 2005. vol. 19. no. 5. pp. 633–653.
4. *Nogueira P.A., Rodrigues R., Oliveira E., Nacke L.E.* Modelling human emotion in interactive environments: Physiological ensemble and grounded approaches for synthetic agents // *Web Intelligence*. 2015. vol. 13. no. 3. pp. 195–214.
5. *Kraus M.W.* Voice-only communication enhances empathic accuracy // *American Psychologist*. 2017. vol. 72. no. 7. pp. 644–654.
6. *Kreiman J., Sidtis D.* Foundations of voice studies: an interdisciplinary approach to voice production and perception // *John Wiley & Sons*. 2013. 512 p.
7. *Wöllmer M. et al.* Context-sensitive multimodal emotion recognition from speech and facial expression using bidirectional LSTM modeling // *Proc. INTERSPEECH*. 2010. pp. 2362–2365.
8. *Anagnostopoulos C.-N., Iliou T., Giannoukos I.* Features and classifiers for emotion recognition from speech: a survey from 2000 to 2011 // *Artificial Intelligence Review*. 2015. vol. 43. no. 2. pp. 155–177.
9. *Shabani S., Norouzi Y.* Speech recognition using Principal Components Analysis and Neural Networks // *IEEE 8th International Conference on Intelligent Systems*. 2016. pp. 90–95.
10. *Trigeorgis G. et al.* Adieu features? end-to-end speech emotion recognition using a deep convolutional recurrent network // *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2016. pp. 5200–5204.
11. *Kaya H. et al.* Emotion, age, and gender classification in children’s speech by humans and machines // *Computer Speech & Language*. 2017. vol. 46. pp. 268–283.
12. *Kaya H., Karpov A.A.* Efficient and effective strategies for cross-corpus acoustic emotion recognition // *Neurocomputing*. 2018. vol. 275. pp. 1028–1034.
13. *Bengio Y., Courville A., Vincent P.* Representation learning: A review and new perspectives // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2013. vol. 35. no. 8. pp. 1798–1828.
14. *Ghosh S., Laksana E., Morency L.-P., Scherer S.* Representation Learning for Speech Emotion Recognition // *Proc. INTERSPEECH*. 2016. pp. 3603–3607.
15. *Kim Y., Provost E.M.* Emotion classification via utterance-level dynamics: A pattern-based approach to characterizing affective expressions // *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 2013. pp. 3677–3681.

16. *Li Y., Zhao Y.* Recognizing emotions in speech using short-term and long-term features // Fifth International Conference on Spoken Language Processing. 1998. vol. 6. pp. 2255.
17. *Jiang D.-N., Cai L.-H.* Speech emotion classification with the combination of statistic features and temporal features // ICME. 2004. pp. 1967–1970.
18. *Vlasenko B., Schuller B., Wendemuth A., Rigoll G.* Combining frame and turn-level information for robust recognition of emotions within speech // Proc. INTERSPEECH. 2007. pp. 2249–2252.
19. *Sainath T.N., Vinyals O., Senior A., Sak H.* Convolutional, long short-term memory, fully connected deep neural networks // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2015. pp. 4580–4584.
20. *Mao Q., Dong M., Huang Z., Zhan Y.* Learning salient features for speech emotion recognition using convolutional neural networks // IEEE Transactions on Multimedia. 2014. vol. 16. no. 8. pp. 2203–2213.
21. *Tran D. et al.* Learning spatiotemporal features with 3d convolutional networks // Proceedings of the IEEE international conference on computer vision. 2015. pp. 4489–4497.
22. *Kim J., Truong K.P., Englebienne G., Evers V.* Learning spectro-temporal features with 3D CNNs for speech emotion recognition // Seventh International Conference on Affective Computing and Intelligent Interaction (ACII). 2017. pp. 383–388.
23. *Chao L. et al.* Long short term memory recurrent neural network based multimodal dimensional emotion recognition // Proceedings of the 5th International Workshop on Audio/Visual Emotion Challenge. 2015. pp. 65–72.
24. *Schuller B. et al.* The relevance of feature type for the automatic classification of emotional user states: Low level descriptors and functionals // Proc. INTERSPEECH. 2007. pp. 2253–2256.
25. *Eyben F., Wöllmer M., Schuller B.* Opensmile: the Munich versatile and fast open-source audio feature extractor // Proceedings of the 18th ACM international conference on Multimedia. 2010. pp. 1459–1462.
26. *Schuller B., Steidl S., Batliner A.* The INTERSPEECH 2009 emotion challenge // Tenth Annual Conference on the International Speech Communication Association INTERSPEECH. 2009. pp. 312–314.
27. *Schuller B. et al.* The INTERSPEECH 2010 paralinguistic challenge // Proc. INTERSPEECH. 2010. pp. 2794–2797.
28. *Schuller B. et al.* The INTERSPEECH 2011 speaker state challenge // Proc. INTERSPEECH. 2011. pp. 3201–3204.
29. *Schuller B. et al.* The INTERSPEECH 2013 computational paralinguistics challenge: social signals, conflict, emotion, autism // Proc. INTERSPEECH. 2013. pp. 148–152.
30. *Greff, K. et al.* LSTM: A search space odyssey // IEEE Transactions on Neural Networks and Learning Systems. 2017. vol. 28. no. 10. pp. 2222–2232.
31. *Cho K. et al.* Learning phrase representations using RNN encoder-decoder for statistical machine translation // arXiv preprint arXiv:1406.1078. 2014.
32. *Abadi M. et al.* Tensorflow: a system for large-scale machine learning // OSDI. 2016. vol. 16. pp. 265–283.
33. *Keogh E., Mueen A.* Curse of dimensionality. Encyclopedia of machine learning. Springer. 2011. pp. 257–258.
34. *Jolliffe I.* Principal component analysis. International encyclopedia of statistical science. Springer. 2011. pp. 1094–1096.
35. *Verkholyak O., Karpov A.* Combined Feature Representation for Emotion Classification from Russian Speech // International Conference on Artificial Intelligence and Natural Language AINL-2017. Springer CCIS. vol. 789. 2018. pp. 68–73.

36. *Makarova V., Petrushin V.A.* RUSLANA: A database of Russian emotional utterances // Seventh International Conference on Spoken Language Processing. 2002. pp. 2041–2044.
37. *Burkhardt, F., Paeschke, A., Rolfes, M., Sendlmeier, W.F., et al.* A database of German emotional speech // Ninth European Conference on Speech Communication and Technology. 2005. pp. 1517–152.
38. *Meral H.M., Ekenel H.K., Ozsoy A.* Analysis of emotion in Turkish // XVII National Conference on Turkish Linguistics. 2003.
39. *Брызгунова Е.А.* Звуки и интонация в русской речи // Москва: Русский язык. 1977. 281 с.
40. *Anikin A., Lima C.F.* Perceptual and acoustic differences between authentic and acted nonverbal emotional vocalizations // The Quarterly Journal of Experimental Psychology. 2017. pp. 1–21.
41. *Kaya H., Salah A.A., Gurgen S.F., Ekenel H.* Protocol and baseline for experiments on Bogazici University Turkish emotional speech corpus // 22nd Signal Processing and Communications Applications Conference (SIU). 2014. pp. 1698–1701.
42. *Koolagudi S.G., Murthy Y.S., Bhaskar S.P.* Choice of a classifier, based on properties of a dataset: case study-speech emotion recognition // International Journal of Speech Technology. 2018. vol. 21. no. 1. pp. 167–183.
43. *Kaya H., Karpov A.A., Salah A.A.* Robust acoustic emotion recognition based on cascaded normalization and extreme learning machines // Proc. International Symposium on Neural Networks (ISNN-2016). LNCS 9719. 2016. pp. 115–123.
44. *Montacié C., Caraty M.J.* Vocalic, lexical and prosodic cues for the INTERSPEECH 2018 self-assessed affect challenge // Proc. INTERSPEECH. 2018. pp. 541–545.
45. *Besacier L., Barnard E., Karpov A., Schultz T.* Automatic speech recognition for under-resourced languages: A survey // Speech Communication. 2014. vol. 56. pp. 85–100.
46. *Kipyatkova I., Karpov A.* A Study of Neural Network Russian Language Models for Automatic Continuous Speech Recognition Systems // Automation and Remote Control. 2017. vol. 78. no. 5. pp. 858–867.

Р.О. ЛАВРЕНОВ, Е.А. МАГИД, Ф. МАЦУНО, М.М. СВИНИН, ДЖ. СУТАКОРН
**РАЗРАБОТКА И ИМПЛЕМЕНТАЦИЯ СПЛАЙН-АЛГОРИТМА
ПЛАНИРОВАНИЯ ПУТИ В СРЕДЕ ROS/GAZEBO**

Лавренов Р.О., Магид Е.А., Мацуно Ф., Свинин М.М., Сутакорн Дж. **Разработка и имплементация сплайн-алгоритма планирования пути в среде ROS/Gazebo.**

Аннотация. Планирование пути для автономных мобильных устройств является важной задачей в робототехнике. При планировании пути принято использовать один из двух классических подходов: глобальный, когда карта полностью известна, и локальный, в котором устройство по мере движения обнаруживает препятствия с помощью различных бортовых датчиков. На основе этих двух подходов также создаются алгоритмы, сочетающие в себе сильные стороны глобального и локального планирования.

В ходе предыдущих исследований нами был разработан и реализован в среде Matlab прототип многокритериального сплайн-алгоритма глобального построения маршрута. Алгоритм использует граф Вороного при вычислении первой аппроксимации маршрута для запуска итерационного метода, что позволило находить путь во всех конфигурациях карты при условии существования пути от начальной точки до целевой точки. В ходе итеративного поиска использовалась целевая функция, в которой каждому критерию присваивался его вес в целевой функции. Для реализации критериев в том числе использовался метод потенциальных полей.

В данной статье представлена реализация модифицированного сплайн-алгоритма для применения его на реальных автономных мобильных робототехнических системах. Для этого проводится корректирование уравнений характеристических критериев оптимальности пути. Карта препятствий, представленная в ранней версии алгоритма в виде пересечений кругов, в реальных условиях может быть представлена в виде динамически изменяемой вероятностной карты на основе сетки занятости (OccuancyGrid), а робот уже не представляет из себя геометрическую точку.

Для реализации сплайн-алгоритма и дальнейшего использования его в системах управления реальных мобильных робототехнических устройств исходный код прототипа алгоритма был перенесен из среды Matlab в модуль программного обеспечения, написанный на языке программирования C++. Тестирование быстродействия алгоритма и оптимальность многокритериальной целевой функции проводились в среде ROS/Gazebo, являющимся на сегодняшний день де-факто стандартом программирования и моделирования робототехнических устройств.

Полученный в результате сплайн-алгоритм поиска пути можно интегрировать в системы управления наземных колесных и гусеничных робототехнических устройств, оборудованных лазерным дальномером, а также модифицировать предложенный алгоритм для использования шагающими наземными роботами, беспилотными летающими аппаратами и беспилотными судами. Алгоритм работает в режиме реального времени и параметры влияния критериев на целевую функцию доступны для динамических изменений во время движения мобильного робота.

Ключевые слова: планирование пути, мобильный робот, алгоритм планирования, ROS, Gazebo, сплайн-алгоритм.

1. Введение. Мобильная робототехника постепенно проникает во все сферы нашей жизни. Разнообразные робототехнические системы (РТС) постепенно заменяют людей на тяжелых и опасных

участках работ. Отдельно в этом списке стоят РТС, которых используют при различных техногенных и природных катаклизмах [1]. Благодаря РТС, способным проникать и обследовать опасные для человека зараженные или радиоактивные зоны, могут быть спасены человеческие жизни. В процессе выполнения поставленной задачи автономная или полуавтономная РТС, действующая индивидуально или в составе группы [2], не должна быть уничтожена, повреждена или потеряна вследствие, например, застревания среди препятствий окружающей среды или переворачивания в результате потери равновесия.

Планирование пути автономного РТС, наряду с автономным картографированием и локализацией [3], является важной научной задачей современной робототехники [4]. Основными источниками данных для одновременной локализации и картографирования (англ. simultaneous localization and mapping, SLAM) [5] и дальнейшего планирования пути являются лазерные дальнометры или цифровые камеры [6]. Рассчитываемый маршрут должен быть безопасным для РТС и удовлетворять различным требованиям, включая минимально возможную длину пути, отсутствие резких поворотов и петель, избегание непреодолимых препятствий и столкновений с другими роботами в случае работы в группе [7]. Алгоритм расчета маршрута для РТС должен всегда находить путь, если таковой существует; если путь найти невозможно – алгоритм должен информировать об этом систему управления РТС [8].

Методы планирования пути принято разделять на глобальные и локальные [9]. В первом случае РТС доступна полная карта препятствий окружающей среды, во втором – РТС строит карту по мере своего продвижения к цели, используя бортовые датчики. К классическим глобальным алгоритмам планирования пути относятся все алгоритмы поиска по графу, построенному на основе карты окружающей среды, включая алгоритмы DFS, BFS, оптимальный алгоритм A^* [10] и его частный случай алгоритм Дейкстры, основанный на быстрорастущих случайных деревьях алгоритм RRT [11] и другие.

Для планирования маршрута РТС при выполнении реальных задач чаще всего происходит комбинирование методов: имея первоначальную карту и построив по ней глобальный маршрут, РТС двигается к цели и при этом динамически перестраивает свой путь при обнаружении новых препятствий, используя локальные методы. Такой подход применяется как для наземных РТС, так и для беспилотных летательных аппаратов и беспилотных судов [12]. Примерами классических алгоритмов динамического планирования пути являются модификации алгоритма A^* — алгоритм D^* [13] и его более

распространенная версия D* Lite [14] — и алгоритмы семейства RRT, включая RRT* [15] и RRT^x [16].

Исследование проблемы оптимальности алгоритма планирования маршрута в рамках нашего исследования основано на ранних работах Магида и др. о сплайн-алгоритме для навигации автономной наземной РТС [17]. Прототип алгоритма был разработан в среде Matlab. Результаты тестирования прототипа, наряду с имевшимися изначально упрощениями реальной окружающей среды и препятствий, непригодностью прототипа алгоритма к работе в режиме реального времени, неумением работать с динамическими препятствиями и другими недостатками, показали, что в некоторых случаях алгоритм мог не находить существующий маршрут к целевой точке.

Для усовершенствования оригинального алгоритма было предложено воспользоваться графом Вороного [18]. В новом подходе граф Вороного используется для построения первоначального пути, который служит отправной точкой для итерационного поиска. В отличие от алгоритмов поиска по графу видимости и алгоритмов семейства RRT, которые находят кратчайший путь, граф Вороного позволяет находить наиболее безопасные для РТС маршруты относительно расстояний до препятствий окружающей среды в каждой точке маршрута, что обусловлено принципом построения графа.

Прототип нового алгоритма сначала был разработан и протестирован в среде Matlab [19]. Он гарантировано находил путь во всех случаях за существенно меньшее число итераций, чем оригинальный алгоритм [17]. Кроме того, в ходе исследования были предложены новые дополнительные критерии оценки качества маршрута и изучено их влияние на рассчитываемый путь.

В данной работе описывается реализация модифицированного сплайн-алгоритма для использования на реальных РТС. В ходе реализации был изменен ряд оригинальных уравнений, критериев и оптимизации [17], исходя из реального представления карт и невозможности реалистичного упрощения РТС до геометрической точки. Полученный в результате многокритериальный сплайн-алгоритм можно использовать при автономном планировании пути для систем управления РТС, оборудованных бортовым лазерным дальномером (2D лидаром), а также адаптировать его для использования с бортовыми 2D и 3D камерами.

2. Оригинальный сплайн-алгоритм планирования пути. Оригинальный алгоритм [17] предлагает решение задачи планирования пути для мобильного робота в известной среде, заполненной статическими препятствиями. Препятствия представляются в виде

конечной группы пересекающихся кругов различного диаметра. Каждая группа может содержать один или несколько кругов. Идея такого представления заключается в том, что любой многоугольник можно аппроксимировать конечной группой кругов.

Чтобы гарантировать построение пути, не пересекающего препятствий, отталкивающая потенциальная функция должна обладать высоким значением внутри препятствия и на его границе, и небольшим значением вне препятствия [20]. Таким образом, во время локальной процедуры оптимизации пути, высокое значение потенциальной функции в центре препятствия «выталкивает» все точки пути из препятствия, чтобы минимизировать стоимость пути [21]. Потенциальное поле начинает резко меняться (уменьшаться) на границе препятствия, продолжает уменьшаться с расстоянием, когда точка пути удаляется от границы препятствия, и довольно быстро обращается в ноль еще в непосредственной близости от препятствия. Метод потенциального поля является классическим методом планирования пути РТС, в том числе в динамических условиях [22].

Положение РТС в момент времени t определяется как конфигурация $q(t)=(x(t), y(t))$. Вклад одного круга (где круг является частью препятствия) в общую функцию потенциала отталкивания определяется следующим выражением:

$$U_{rep}(q) = 1 + \tanh(\alpha(\rho - \sqrt{(x(t) - x)^2 + (y(t) - y)^2})), \quad (1)$$

где ρ — радиус круга (препятствия) с центром в точке с координатами (x, y) , а α — эмпирически определяемый параметр, который отвечает за выталкивание пути из границ препятствия. Рисунок 1 демонстрирует пример выбора параметра $\alpha=0.3$ для среды с одним препятствием, которое образовано тремя пересекающимися кругами. Потенциальная функция имеет четко выделяющиеся пики на пересечениях кругов.

Функция топологии $T(q)$, учитывающая все N кругов окружающей среды и их влияние на работа на протяжении всего пути, которая определяется параметрическим выражением на интервале $[0,1]$:

$$T(q) = \sum_{j=0}^{N-1} \int_{t=0}^1 U_{rep}^j(q) \cdot \delta l(t) \cdot dt, \quad (2)$$

где $\delta l(t)$ длина отрезка:

$$\delta l(t) = \sqrt{(x'(t))^2 + (y'(t))^2}. \quad (3)$$

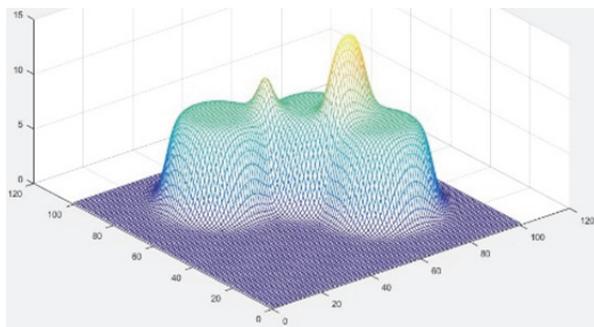


Рис. 1. Пример потенциальной функции для одного препятствия

Функция кривизны пути также определяется параметрическим выражением:

$$R(q) = \sqrt{\int_{t=0}^1 (x''(t))^2 + (y''(t))^2 dt}. \quad (4)$$

Функция, которая учитывает длину пути ($L(q)$), суммирует длины всех сегментов пути:

$$L(q) = \int_{t=0}^1 \delta l(t) \cdot dt. \quad (5)$$

Таким образом, итоговая оценка каждой траектории рассчитывается как сумма трех компонентов:

$$F(q) = \gamma_1 T(q) + \gamma_2 R(q) + \gamma_3 L(q), \quad (6)$$

где $\gamma_{i=1..3}$ — числовые значения влияния каждого компонента на общую стоимость маршрута. В частности, значение влияния потенциального поля $\gamma_{i=1} = \beta/2$, где параметр β эмпирически коррелирует с параметром α из уравнения (1).

Оригинальный сплайн-алгоритм планирования пути работает итеративно. Путь на первой итерации представляет из себя прямую линию между точками старта S и цели T . Сплайн определяется тремя точками: S , T и равноудаленной точкой, лежащей на прямом отрезке, соединяющем точки S и T . Дальнейшие итерации пути используют уравнение (6), и путь оптимизируется с помощью метода Нелдера-Мида (симплекс-метод, [23]). Лучший результат (маршрут) каждой итерации служит начальным значением маршрута для последующей итерации.

Процедура оптимизации работает только с точками пути, которые определяют его сплайн, в то время как оценка стоимости пути учитывает все точки маршрута. Маршрут перестраивается на каждой итерации, используя информацию с предыдущего этапа, увеличивая количество точек сплайна на единицу и корректируя параметры целевой функции стоимости пути. Алгоритм завершается, если количество итераций превышает заданный пользователем предел, или если новая итерация не улучшает предыдущую, но при этом увеличивается порядковая сложность сплайна.

Исходный сплайн-метод позволяет получить гладкий путь без столкновений с препятствиями, если каждое препятствие аппроксимируется одним кругом или линия начальной итерации не проходит через пересечение кругов. Однако, когда препятствия аппроксимированы группой пересекающихся кругов, пересечения образуют локальные максимумы потенциального поля (рисунок 1). Когда в такой среде начальный сплайн проходит через пересечение нескольких кругов, то целевая функция $F(q)$ «выталкивает» сплайн из области пересечения и далее сплайн «застревает» в локальных минимумах, а следующий итерационный сплайн не может «перепрыгнуть» некоторые компоненты препятствия из-за локального характера процесса оптимизации (рисунок 2).

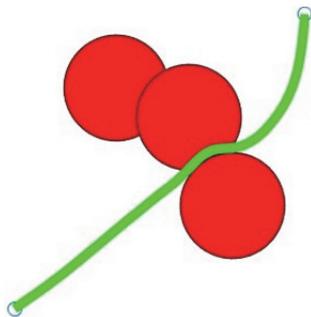


Рис. 2. Пример застревания пути в локальном минимуме потенциальной функции. В результате итеративного процесса путь все еще пересекает препятствия.

Из-за множества пересекающихся кругов, которые генерируют собственные локальные отталкивающие потенциалы, соответствующее глобальное потенциальное поле скрывает узкие проходы между различными препятствиями и позволяет совершить только локальную оптимизацию пути. Таким образом, локальная оптимизация успешно устраняет локальные максимумы, но даже после большого числа

итераций, результирующий путь все еще пересекает препятствия и, следовательно, бесполезен для движения робота.

3. Модифицированный алгоритм поиска пути с использованием графа Вороного. Для создания качественного начального сплайна применяется алгоритм построения графа Вороного [24], что помогает избежать ключевого недостатка оригинального подхода: невозможности выхода из локального минимума функции стоимости пути при неудачном стартовом сплайне независимо от количества последующих итераций алгоритма оптимизации [25]. Для создания графа Вороного требуется предварительно подготовить информацию о препятствиях; данная процедура выполняется в два следующих этапа [24]:

1) Компоновка отдельных препятствий из конечного множества пересекающихся кругов. Данная операция производится итеративно. Осуществляется поиск кругов, связанных пересечением, и такие группы кругов нумеруются как единое препятствие. Когда все круги окружающей среды идентифицированы как составляющие какого-либо препятствия, итеративный поиск завершается. Например, на рисунке 3 показаны четыре препятствия, которые образованы группами кругов, а на рисунке 4 в окружающей среде показаны три препятствия. При построении препятствия каждая пара пересекающихся кругов (i, j) образует одну точку пересечения θ_{ij} в случае граничного касания и пару точек θ_{ij}, θ_{ji} в общем случае пересечения кругов.

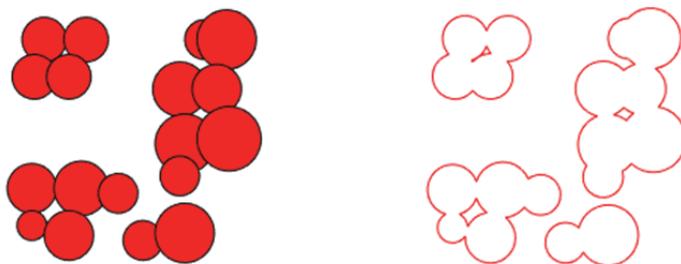


Рис. 3. Среда с препятствиями (слева) и рассчитанные контуры препятствий (справа)

2) Поиск внешних контуров препятствий множества $Obst = \{O_1, O_2, \dots, O_k\}$, где k количество сложносоставных препятствий в окружающей среде. Для этого находят точки пересечения окружностей и из внешних дуг окружностей собираются контуры препятствий. Эта процедура повторяется для каждого препятствия, и по ее завершению

формируется множество контуров. Если размер последнего множества превышает k , это указывает на наличие внутренних контуров. Чтобы избавиться от внутренних контуров, для каждого препятствия O_i вычисляется выпуклая оболочка; если у i -того препятствия имеется несколько контуров, удаляются контуры, которые находятся внутри выпуклой оболочки. К примеру, такая процедура успешно удалила три внутренних контура внутри сложносоставных препятствий среды на рисунке 3. Таким образом, получатся несколько невыпуклых многоугольников, по одному для каждого препятствия из $Obst$.

При построении графа Вороного помимо границ препятствий окружающей среды необходимо добавить внешние границы среды, что позволит находить линии графа, обходящие препятствия с внешней стороны. Для этого рассчитывается квадрат минимального размера со сторонами, параллельными осям глобальной системы координат окружающей среды (англ. axis-aligned bounding box — AABB), и каждая его сторона увеличивается на 40%. Пример такой внешней границы можно увидеть на рисунке 4 (центральное и правое изображения).

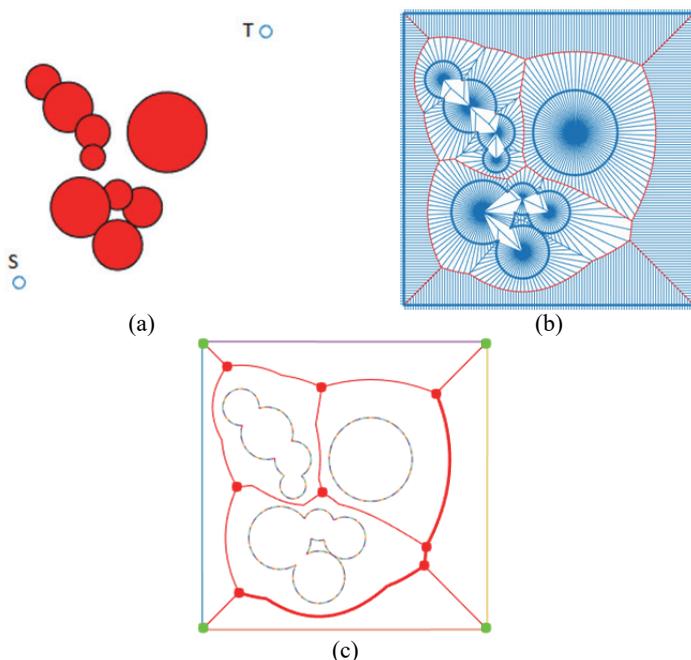


Рис. 4. Среда с препятствиями (а), процедура построения графа Вороного (б), путь на графе Вороного (с)

Далее, имея карту препятствий в виде многоугольников, которые являются приближением контуров препятствий, с использованием классического подхода строится граф Вороного.

1) От границ препятствий и карты с равными промежутками строятся лучи. На рисунке 4b демонстрируется пример построения этих лучей в виде тонких лучей, которые начинаются с границ препятствий и ограничивающей карты и являются перпендикулярами. Толстые линии на рисунке 4b отображают границы препятствий и карты.

2) Вычисляются точки пересечения лучей от разных препятствий. Точки пересечения соединяются отрезками, совокупность которых формируют граф Вороного (тонкие линии на рисунке 4b,c).

После построения графа Вороного, на нем выбираются точки S' и T' ближайšie к начальной позиции S и целевой позиции T , соответственно. Отрезки $[S, S']$ и $[T, T']$ не должны пересекать имеющиеся препятствия окружающей среды. Далее, кратчайший путь между S' и T' находится внутри графа Вороного с использованием алгоритма Дейкстры. На рисунке 4c построенный путь изображен толстыми красными линиями. Любой путь между точками (S, T) на графе Вороного гарантированно не пересекает препятствия и максимально безопасен в отношении расстояния от границ препятствий. Таким образом, он обеспечивает хороший начальный сплайн для исходного сплайн-метода [17].

Далее выбираются начальные точки будущего сплайна, которые надлежащим образом отражают характеристики пути, но при этом позволяют избежать избыточной сложности сплайна. Для этого среди всех точек пути вычисляется минимальный набор точек, последовательное соединение которых образует ломаную линию, не пересекающую препятствия и находящуюся в том же гомотопическом пространстве, что и найденный путь [24]. Найденный набор точек включает точки старта и цели. Данное множество точек используется для построения начального сплайна при запуске сплайн-метода.

Для проверки новый алгоритм был реализован в среде Matlab, и было проведено несколько тысяч симуляций на различных картах препятствий. Особое внимание было уделено случаям, когда оригинальный алгоритм [17] оказывался неудачным и не находил путь, застревая среди препятствий. Так, на рисунке 5 изображена среда, в которой оригинальный сплайн-алгоритм не смог построить маршрут. Граф Вороного предоставляет безопасный путь без столкновений с препятствиями. Следовательно, этот путь гарантирует, что модифицированный сплайн-алгоритм вычислит конечный путь меньшим числом итераций.

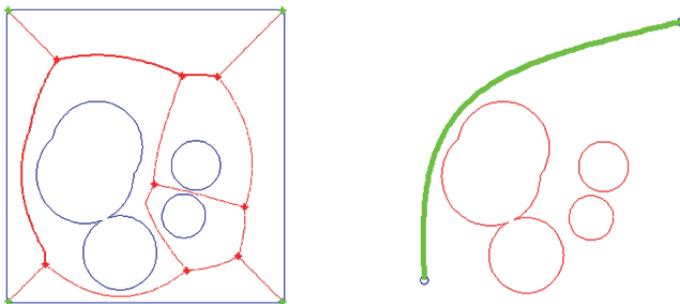


Рис. 5. Путь на графе Вороного (рисунок слева, толстая линия) и результирующий сплайн-путь, найденный итерационным алгоритмом на основе первоначального пути по графу (рисунок справа).

В тестах использовалась целевая функция уравнения (6) со следующим выбором параметров: $\gamma_1 = 1$, $\gamma_2 = 1$, $\gamma_3 = 0.5$. Алгоритм смог успешно рассчитать маршрут во всех случаях, что было естественным следствием применения начального пути, найденного по графу Вороного, в качестве первого сплайна для итерационного алгоритма.

4. Фреймворк ROS и среда симуляции Gazebo.

Робототехническая операционная система ROS (англ. «Robot Operating System») — платформа с открытым исходным кодом для моделирования и программирования РТС, которая на сегодня де-факто является стандартом в программировании РТС. Она предоставляет такие услуги операционной системы, как управление устройствами на низком уровне, аппаратную абстракцию, передачу сообщений между процессами и управление пакетами. Несколько взаимосвязанных процессов, выполняющихся в ROS, могут быть представлены в виде графа, основными элементами которого являются узлы, называемые нодами. Ноды могут принимать и передавать данные от датчиков, приводов, энкодеров и обрабатывать различные сообщения. Программное обеспечение на основе ROS можно разделить на три группы:

1. Языки и независимые от платформы инструменты, используемые для создания и распространения программного обеспечения.

2. Клиентские библиотеки для разработки собственных пакетов, такие как `roscpp`, `rospy` и `roslisp`.

3. Готовые клиентских библиотеки для различных датчиков, роботов и отдельных алгоритмов.

Для моделирования окружения робота с ROS могут применяться симуляторы RViz или Gazebo. Gazebo использует Open

Dynamics Engine как физический движок и объектно-ориентированный графический рендеринг для 3D-рендеринга, имеет бесплатную лицензию для исследователей, предоставляет графический интерфейс пользователя и позволяет описывать динамику роботов на языке программирования Python. Пример созданного окружения и запущенный в нем робот Husky [26] можно увидеть на рисунке 6.



Рис. 6. Робот Husky в симуляторе ROS\Gazebo

Подробные tutorиалы и документация ROS предоставляют шаблоны для реализации собственных пользовательских алгоритмов планирования маршрута. Однако, в ROS в настоящее время реализовано лишь несколько алгоритмов планирования пути автономных РТС [27]. Наиболее распространены алгоритмы, работающие с данными лазерного дальномера. В этих случаях карта окружающей среды является так называемой OccupancyGrid картой — решеткой занятости (рисунок 7). То есть двумерным массивом значений, каждое из которых обозначает наличие препятствия в указанной области. Значения в ячейках могут быть бинарными (0 для пустых ячеек, 1 для занятых препятствием ячеек) или принимать значения в заданном диапазоне, обозначая неровности поверхности и проходимость в указанной области. Значения занятости по умолчанию находятся в диапазоне от 0 до 100. Решетка занятости может быть визуализирована в виде изображения в черно-белом виде с значениями равными 0 для полностью свободных и 100 для абсолютно непроходимых областей. Серые области обозначают неизвестные области карты.

Реализованные в ROS алгоритмы планирования упрощают задачу поиска пути с помощью искусственного программного

расширения найденных на карте препятствий на физический размер робота. Пример таких областей можно увидеть на рисунке 8.



Рис. 7. OccupancyGrid карта, построенная РТС «Сервисила Инженер» при помощи лазерного дальномера Нокучо UTM-30LX-EW LRF

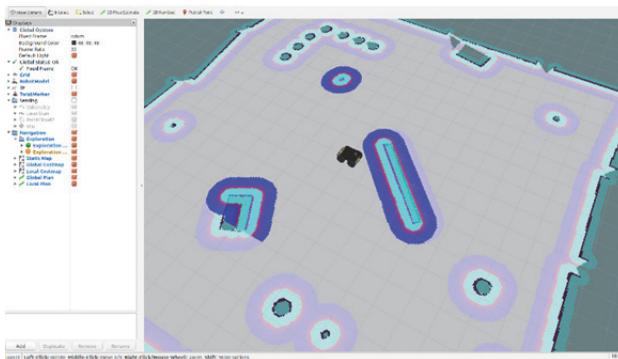


Рис. 8. Робот Husky в симуляторе RViz

Препятствия на рисунке 8 показаны бирюзовым цветом, красным цветом показаны границы препятствий. Синим цветом выделены области вокруг препятствий, которые исключаются из планирования пути, так как считаются опасными ввиду близости к границам препятствий. Окружающая среда, в которой находится РТС, идентична представленной ранее на рисунке 6 среде. При проведении расчетов РТС становится математической точкой. Работа этого процесса в ROS обеспечивается библиотекой Costmap. Данная библиотека является частью стека навигации — набора библиотек, обеспечивающих глобальное и локальное планирование пути,

локализацию, картографирование и вывод робота из состояния застревания [28]. Сплайн-алгоритм будет реализовываться как глобальный алгоритм для стека навигации ROS.

5. Реализация модифицированного сплайн алгоритма в ROS/Gazebo. Основной новизной модифицированного сплайн-алгоритма относительно оригинального алгоритма является использование предварительно рассчитанного графа Вороного по имеющейся карте местности. Проблема реализованного в Matlab первого прототипа нового алгоритма [24, 25] заключается в том, что он не подходит для реального использования системой управления РТС. Если в среде Matlab препятствия представлялись в виде пересечений кругов, реальные карты, получаемые мобильной РТС с помощью лазерного дальномера, представляют из себя ячейки в OccupancyGrid карте с вероятностью выше определенного предела. Двумерные вероятностные сетки занятости являются наиболее распространенным методом представления окружающей среды [29].

Для расчета диаграммы Вороного было решено использовать подход, описанный в работе [30]. Суть его заключается в проходе по всей двумерной карте и нахождение для каждой свободной ячейки расстояния до ближайшей ячейки с препятствием. Для каждой ячейки запоминается индекс ближайшей ячейки с препятствием. Далее, соседние ячейки с препятствиями, имеющие общие точки, объединяются и маркируются как единое препятствие [31]. После этого производится повторный проход по всем индексам карты. Проверяется каждая ячейка — если у нее ближайшее препятствие с номером i , а у ее соседней ячейки ближайшее препятствие с номером, отличным от i , то обе ячейки специальным образом маркируются. После прохода по всей карте совокупность промаркированных ячеек образует граф Вороного; пример карты с выделенными красным цветом маркированными ячейками представлен на рисунке 9. Данный алгоритм так же может быть адаптирован и расширен для применения на 3D карте, если препятствия будут представлены в виде вокселей [32].

Метод расчета графа Вороного на дискретной вероятностной карте для ROS [30] был предварительно реализован в статье [33], где автор применил алгоритм для планирования пути автономного минисудна. Автор использует специальную структуру для различных маркировок каждой ячейки карты, а также для хранения в ней расстояния до препятствий и индексы этих препятствий. После построения графа Вороного, по нему в три этапа осуществляется поиск пути из точки старта в целевую точку в три этапа:

1. Из точки старта S осуществляется поиск кратчайшего пути до ближайшей точки графа S_i

2. Из целевой точки T осуществляется поиск кратчайшего пути до ближайшей точки графа T_1

3. Используя только помеченные как принадлежащие к графу Вороного точки карты, ищется путь от S_1 до T_1

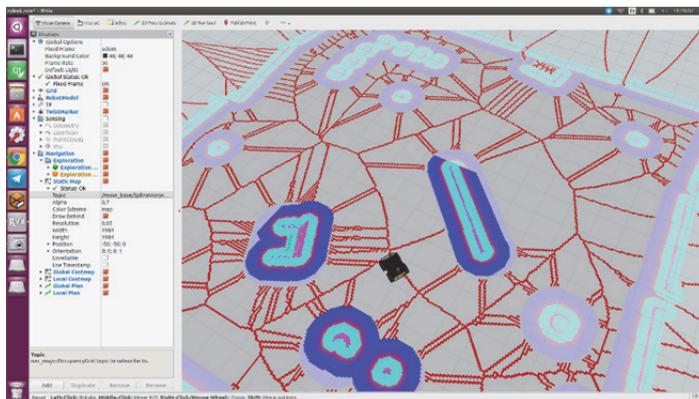


Рис. 9. Пример построенной диаграммы Вороного в симуляторе RViz.

Реализованный и представленный в публикации алгоритм [33] был существенно оптимизирован, что позволило уменьшить среднее время расчета графа Вороного с 8 секунд до 0.5 секунды. Пример результата расчета графа Вороного показан на рисунке 9; расчет и построение диаграммы Вороного в симуляторе RViz заняли менее 1 секунды.

Существенного ускорения расчета графа Вороного удалось добиться благодаря оптимизации используемых алгоритмов и контейнеров. Основным контейнером данных для расчета графа Вороного является динамический массив, каждый элемент которого – очередь индексов ячеек двумерной карты. Так как расстояние до препятствий счетно, в каждой очереди динамического массива хранятся ячейки с одинаковым расстоянием от препятствий. Данный контейнер был оптимизирован таким образом, что он генерируется только в случаях увеличения карты, а непрерывное расположение массива в памяти ускоряет операции с ним. Дополнительно ускорению работы алгоритма способствовало избавление от дублирующих расчетов и избыточных сложных вычислительных операций. Например, в отличие от оригинального подхода, вместо расчета точного расстояния до препятствий хранится квадрат расстояния, что избавляет от многочисленных расчетов корня числа.

После получения с помощью алгоритма Дейкстры пути по графу Вороного, путь преобразовывается в B-сплайн [34] (рисунок 10).

Для хранения сплайна был создан специальный тип данных, хранящий пару переменных типа `boost::math::cubic_b_spline<double>`: параметрические функции $y(t)$ и $x(t)$. Переменная t изменяется от 0 до 1 включительно и указывает на положение РТС на траектории от точки старта ($t=0$) до целевой точки ($t=1$). Функции $x(t)$ и $y(t)$ рассчитывают координаты робота (x, y) на карте в зависимости от положения робота на траектории.

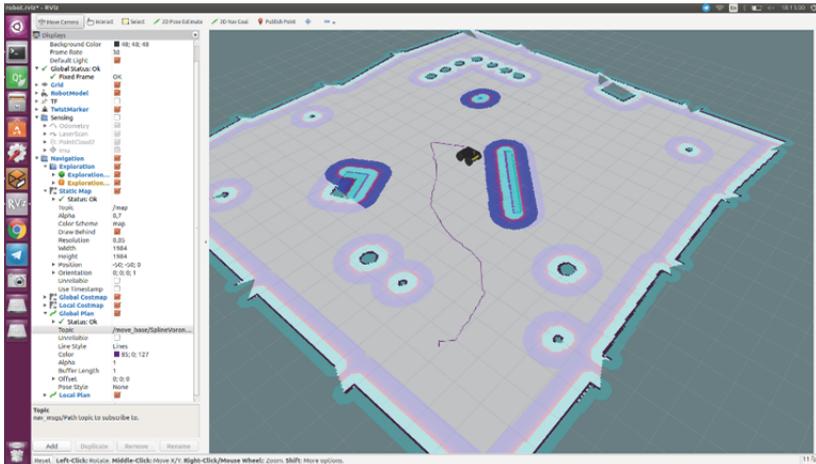


Рис. 10. Путь, рассчитанный по графу Вороного в симуляторе RViz

Чтобы преобразовать найденный путь в В-сплайн, следует задать точность, с которой сплайн будет соответствовать траектории, рассчитываемой по графу Вороного. Для этого путь, представляемый в виде последовательности точек, равномерно делится на N сегментов (первоначальное значение N задано равным 4) и, соответственно, $N+1$ точек: начальная (старт S), конечная (цель T) и $N-1$ промежуточных точек. Эти $N+1$ точек формируют пару сплайнов, задаваемых параметрической функцией с переменной t . Полученный сплайн сравнивается с траекторией, состоящей из ребер графа Вороного, и подсчитывается максимальное отклонение между ними. Если отклонение больше или равно половине ширины робота, то сплайн используется для дальнейшего итерационного поиска. В противном случае, переменная N увеличивается на 1, путь делится на $N+1$ характерных точек, по ним строится сплайн и сравнивается с исходным путем из графа Вороного. Итерационный процесс продолжается до выполнения требования по отклонению.

После расчета пары сплайнов, соответствующих исходному пути в рамках установленной точности, следует итерационный процесс

поиска оптимального сплайн-пути, используя целевую функцию. В начале итерационного процесса подсчитывается значение целевой функции у получившегося сплайна, и он определяется как основной.

N-1 точек промежуточных точек основного сплайна случайным образом перемещаются на небольшое расстояние $\tau \rightarrow 0$ и для получаемого нового сплайна подсчитывается значение целевой функции. Если значение целевой функции получаемого нового сплайн-пути меньше, чем у основного сплайна, он сохраняется и определяется как основной. Далее, у его промежуточные точки случайным образом перемещаются, а новые сплайны сравниваются с ним. Итерационный процесс продолжается до тех пор, пока улучшение результатов расчета стоимости пути (в соответствии с целевой функцией) полученного сплайна не станет меньше выбранного эмпирическим путем порогового значения $\varepsilon=0.1$, а общее количество итераций не превысит 1000 итераций.

Чтобы целевая функция оптимальным образом характеризовала сплайн-путь $q(t)=\{x(t), y(t)\}$, были реализованы три основных критерия оптимальности пути: длина, кривизна и топология. Функция, которая рассчитывает длину пути $L(q)$ аналогично формуле (5), суммирует длины всех сегментов пути. В исходном коде это реализовано с помощью прохода по паре сплайнов с шагом Δ_t , эмпирическим путем установленным $\Delta_t=0.001$. На каждом шаге рассчитывается Δ_x и Δ_y — изменения по осям x и y при изменении параметра t на величину Δ_t . Длина сегмента рассчитывается как корень из суммы их квадратов. Таким образом, длина пути рассчитывается по формуле:

$$L_R(q) = \sum_{t=0, \Delta_t \rightarrow 0}^{1-\Delta_t} \sqrt{((x(t+\Delta_t) - x(t))^2 + (y(t+\Delta_t) - y(t))^2)}. \quad (7)$$

Критерий кривизны пути рассчитывается по уравнению (4) с приближением интеграла по аналогии с уравнением (7), только вместо значения функций сплайнов в точках, в формуле используются производные от функций в этих точках:

$$R_R(q) = \sqrt{\sum_{t=0, \Delta_t \rightarrow 0}^{1-\Delta_t} \frac{((x'(t+\Delta_t) - x'(t))^2 + (y'(t+\Delta_t) - y'(t))^2)}{\Delta_t^2}}. \quad (8)$$

Критерий топологии пути, который в том числе определяет безопасность маршрута относительно удаленности РТС от границ препятствий при движении по данному маршруту, изменяется более кардинально по сравнению с оригинальным алгоритмом [17]. Так как при новом подходе препятствия не представляют из себя пересечения

кругов и количество препятствий может быть достаточно велико, формула расчета критерия топологии пути должна быть адаптирована соответствующим образом. Карту и рассчитанный по ней граф Вороного предоставляют большой набор данных в каждой ячейке карты, включая расстояние до ближайшего препятствия, выраженное в размере ячейки OccupancyGrid карты (который по умолчанию составляет 0.05 метра). Расстояние до препятствий используется в функции расчета потенциального поля. В новых условиях описания препятствий окружающей среды функция потенциала отталкивания (1) в каждой точке пути принимает вид:

$$U_R(t) = 1 - \tanh(\alpha * \text{dist}(t)), \quad (9)$$

где α — это эмпирически определяемый параметр, $\text{dist}(t)$ — минимально расстояние до препятствий в точке t пути. Параметр α отвечает за отталкивание маршрута движения от препятствия. Так как гиперболический тангенс при увеличении аргумента быстро приближается к единице, потенциальное поле быстро ослабевает при отдалении от препятствий. Уменьшение параметра α заставляет робота держаться дальше от препятствий. Эмпирически было получено значение $\alpha=0.1$.

Так как уравнения сплайнов пути являются непрерывными функциями, а расстояния до препятствий дискретны и берутся из карты занятости, то при прохождении по маршруту следует учитывать длину пути, проходящую через каждую ячейку карты. Таким образом, необходимо просуммировать по всем ячейкам карты, которые пересекает путь, произведение потенциала поля в данной ячейке на длину пути, попадающего внутрь данной ячейки. Если путь пересекает N ячеек, то результирующее значение критерия Топологии этого пути будет равно:

$$U_R(q) = \sum_{k=0}^N U_R^k(t) * \delta_q(k), \quad (10)$$

где переменная k обозначает индекс ячейки карты, которую пересекает путь, $\delta_q(k)$ — длина пути, находящегося внутри ячейки k . $U_R^k(t)$ — значение потенциального поля любой точки t пути, которая находится внутри ячейки под номером k .

Итоговая стоимость пути по аналогии с уравнением (6) состоит из суммы трех компонентов:

$$F_R(q) = \gamma_1 T_R(q) + \gamma_2 R_R(q) + \gamma_3 L_R(q). \quad (11)$$

В ходе тестирования алгоритма в среде ROS/Gazebo на роботе Husky [20] эмпирическим образом было установлено, что для достижения паритета критериев, влияние критерия топологии следует существенно увеличить относительно влияния других критериев. После задания веса каждого из критериев в целевой функции: $\gamma_1 = 1$, $\gamma_2 = 1$, $\gamma_3 = 5000$ дальнейшее увеличение веса топологии не изменяет оптимальный путь. Критерий минимального удаления от препятствий регулируется параметром α из функции топологии.

Результаты тестирования алгоритма подтвердили успешность подхода модифицированного сплайн алгоритма. Так, первоначально рассчитанный путь (представлен на рисунке 10) по графу Вороного, который является базой для первого сплайна итеративного алгоритма, является ломаной кривой с множеством резких поворотов. После первых ста итераций (рисунок 11) путь является сплайном, он короче исходного и в нем нет резких изменений пути, для преодоления которых роботу необходимо останавливаться. После 400 итераций (1.3 секунды), итерационный процесс завершился. Рисунок 12 демонстрирует, что в процессе итеративного поиска изгиб траектории в начале пути исчез и длина пути уменьшилась при сохранении безопасного расстояния до препятствий.

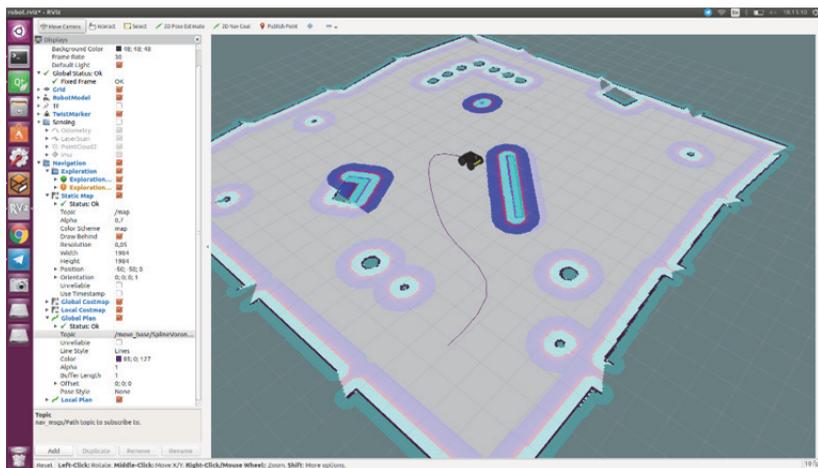


Рис. 11. Маршрут, построенный новым сплайн-алгоритмом за первые 100 итераций. Робот Husky находится на стартовой позиции S

Эксперименты производились на компьютере с процессором Intel Core i7-9700 с 32Гб оперативной памяти. Несколько тысяч симуляционных экспериментов были проведены на двадцати картах

сопоставимых размеров с различными конфигурациями препятствий. Время расчета графа Вороного было стабильным, составляло менее 0.5 секунды и зависело только от сложности карты. Примеры типовой карты показаны на рисунках 8-12, при изменении карты препятствия перемещались и добавлялось от 2 до 10 новых препятствий. Итерационный алгоритм рассчитывал путь в среднем за 2 секунды; время его работы не зависело от конкретной карты, что в первую очередь объясняется сопоставимыми размерами и сложностью использованных в экспериментах карт. Время работы итерационного алгоритма зависело от расстояния между произвольно выбранными стартовой позицией S и целевой позицией T, и сложности участка карты между этими позициями.

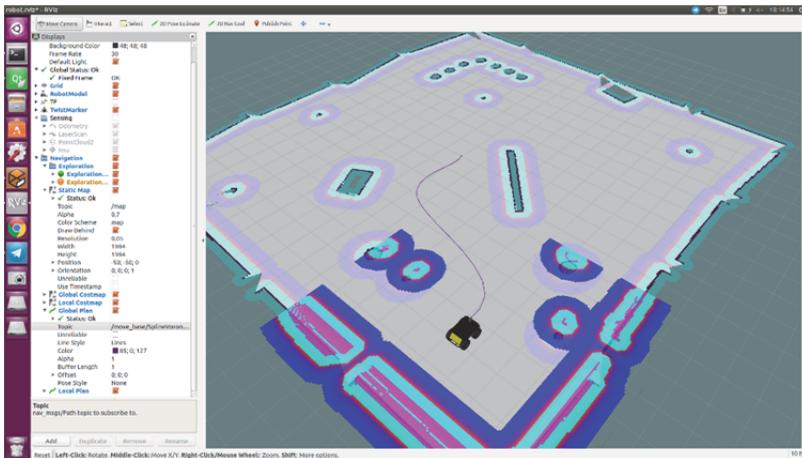


Рис. 12. Маршрут, построенный новым сплайн-алгоритмом за первых 400 итераций. Робот Nusku находится на целевой позиции T

Таблица 1 демонстрирует 15 примеров запуска нового алгоритма на одной и той же карте (рисунок 13) с произвольно выбранными позициями S и T. Время первого расчета траектории больше, чем время расчета последующих, из-за необходимости выделения необходимой для расчетов памяти.

В будущем мы планируем оценить увеличение времени работы алгоритма в случае увеличения размеров и сложности экспериментальных карт на несколько порядков. В настоящее время проводится оптимизация структур данных и алгоритмов, и переход к многопоточному подходу для функций расчета критериев и вычисления графа Вороного. Это позволит существенно ускорить работу алгоритма и

исключит остановки робота (2-3 сек.), необходимые для вычисления нового маршрута при задании новой целевой позиции.

Таблица 1. Время расчета в секундах на одной карте: построение графа Вороного, расчет путь по графу Вороного и последующая оптимизация пути

Номер эксперимента	Время расчета (сек.)		
	Граф Вороного	Путь по графу Вороного	Оптимизация пути
1	0.41	0.03	4.63
2	0.35	0.02	1.81
3	0.34	0.03	2.27
4	0.35	0.02	1.62
5	0.34	0.02	2.28
6	0.34	0.02	1.7
7	0.34	0.02	1.22
8	0.34	0.02	0.82
9	0.35	0.02	0.99
10	0.34	0.02	1.02
11	0.35	0.01	1.12
12	0.34	0.03	1.92
13	0.35	0.01	1.49
14	0.34	0.03	1.38
15	0.35	0.02	1.91

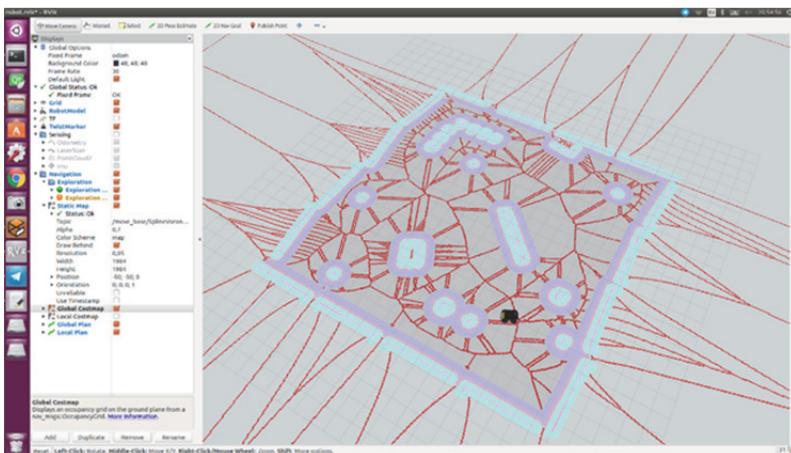


Рис. 13. Карта в симуляторе RViz, использовавшаяся для примеров в таблице 1, и построенная диаграмма Вороного

Также стоит задача интеграции алгоритма в системы управления наземных мобильных РТС лабораторий интеллектуальных

робототехнических систем (ЛИРС) КФУ — гусеничного робота «Сервосила Инженер», колесных «Юниор» и РМВ-2.

Несмотря на то, что алгоритм формально является глобальным и требует наличия статической заранее известной карты, его возможно использовать и в динамически изменяемых условиях, так как он позволяет осуществить перерасчет маршрута движения при локальном изменении карты в режиме реального времени без полного перестроения карты.

8. Заключение. В данной работе описывается модифицированный сплайн-алгоритм планирования пути, а также его реализация для использования в реальных системах управления РТС. В ходе реализации нового алгоритма была проведена адаптация оригинальных формулировок критериев и уравнений, учитывающая реальное представление карт и невозможность аппроксимации РТС геометрической точкой. Полученный в результате многокритериальный сплайн-алгоритм был верифицирован в среде разработки ROS/Gazebo. Данный алгоритм можно использовать для планирования маршрута системой управления любого наземного колесного или гусеничного РТС, оборудованного лазерным дальнометром (лидаром). Алгоритм открыт для использования и редактирования, исходный код находится в репозитории Gitlab [35]. При использовании в целевую функцию оптимизации пути могут быть включены новые критерии или изменен вес уже реализованных критериев.

В разработанный алгоритм будут добавлены новые критерии, которые могут быть полезны при проведении поисково-спасательных операций, при работе автономного РТС в опасных и зараженных территориях. Также целевая функция будет модифицирована для учета опасных точек на карте, которые нужно обходить, или, наоборот, ретрансляторов связи, которые нужно держать в поле зрения как можно дольше.

В качестве дальнейшей работы будет проведено сравнение предложенного алгоритма с типовыми алгоритмами поиска пути, включая A* и RRT*, в симуляционной среде ROS/Gazebo по таким критериям как быстродействие и качество полученного пути. Особое внимание будет уделено комбинированным случаям, когда существующие базовые алгоритмы глобального планирования пути будут использованы при создании стартового сплайна для предложенного в данной работе итеративного сплайн-алгоритма.

Литература

1. *Michael N. et al.* Collaborative mapping of an earthquake damaged building via ground and aerial robots // Journal of Field Robotics. 2012. vol. 29. no. 5. pp. 832–841.

2. *Nagatani K. et al.* Multirobot exploration for search and rescue missions: A report on map building in RoboCupRescue 2009 // *Journal of Field Robotics*. 2011. vol. 28(3). pp. 373–387.
3. *Pshikhovop V., Medvedev M., Krukhmalev V., Shevchenko V.* Base Algorithms of the Direct Adaptive Position-Path Control for Mobile Objects Positioning // *Applied Mechanics and Materials*. 2015. vol. 763. pp. 110–119.
4. *Loevsky I., Shimshoni I.* Reliable and efficient landmark-based localization for mobile robots // *Robotics and Autonomous Systems*. 2010. vol. 58(5). pp. 520–528.
5. *Filipenko M., Afanasyev I.* Comparison of Various SLAM Systems for Mobile Robot in an Indoor Environment // *International Conference on Intelligent Systems*. 2018. 8 p.
6. *Sokolov M., Bulichev O., Afanasyev I.* Analysis of ROS-based Visual and Lidar Odometry for a Teleoperated Crawler-type Robot in indoor environment // *International Conference on Informatics in Control, Automation and Robotics (ICINCO)*. 2017. pp. 316–321.
7. *Wagner G., Choset H.* Subdimensional expansion for multirobot path planning // *Artificial Intelligence*. 2015. vol. 219. pp. 1–24.
8. *Vokhmintsev A., Yakovlev K.* A Real-Time Algorithm for Mobile Robot Mapping Based on Rotation-Invariant Descriptors and Iterative Close Point Algorithm // *International Conference on Analysis of Images, Social Networks and Texts*. 2016. pp. 357–369.
9. *Sullivan J.C.W., Pipe A.G.* Path planning for redundant robot manipulators: a global optimization approach using evolutionary search // *1998 IEEE International Conference on Systems, Man, and Cybernetics*. 1998. vol. 3. pp. 2396–2400
10. *Hart P.E., Nilsson N.J., Raphael B.* A formal basis for the heuristic determination of minimum cost paths // *IEEE transactions on Systems Science and Cybernetics*. 1968. vol. 4. no. 2. pp. 100–107.
11. *LaValle S.M.* Rapidly-exploring random trees: A new tool for path planning // *Iowa State University Ames*. 1998. 4 p.
12. *Яковлев К.С., Макаров Д.А., Баскин Е.С.* Метод автоматического планирования траектории беспилотного летательного аппарата в условиях ограничений на динамику полета // *Искусственный интеллект и принятие решений*. 2014. № 4. С. 3.
13. *Stentz A.* Optimal and efficient path planning for partially-known environments // *International Conference on Robotics and Automation (ICRA)*. 1994. vol. 94. pp. 3310–3317.
14. *Koenig S., Likhachev M.* Fast replanning for navigation in unknown terrain // *IEEE Transactions on Robotics*. 2005. vol. 21. no. 3. pp. 354–363.
15. *Karaman S., Frazzoli E.* Sampling-based algorithms for optimal motion planning // *The International Journal of Robotics Research*. 2011. vol. 30. no. 7. pp. 846–894.
16. *Otte M., Frazzoli E.* RRT X: Real-Time Motion Planning/Replanning for Environments with Unpredictable Obstacles // *Algorithmic Foundations of Robotics XI*. 2015. pp. 461–478.
17. *Magid E., Keren D., Rivlin E., Yavneh I.* Spline-based robot navigation // *2006 IEEE/RSJ International Conference on Intelligent Robots and Systems*. 2006. pp. 2296–2301.
18. *Nagatani K., Iwai Y., Tanaka Y.* Sensor based navigation for carlike mobile robots using Generalized Voronoi Graph // *2001 IEEE/RSJ International Conference on Intelligent Robots and Systems*. 2001. vol. 2. pp. 1017–1022.
19. *Lavrenov R., Matsuno F., Magid E.* Modified Spline-Based Navigation: Guaranteed Safety for Obstacle Avoidance // *International Conference on Interactive Collaborative Robotics*. 2017. pp. 123–133.
20. *Koren Y., Borenstein J.* Potential field methods and their inherent limitations for mobile robot navigation // *1991 IEEE International Conference on Robotics and Automation*. 1991. pp. 1398–1404.

21. *Khatib O.* Real-Time Obstacle Avoidance for Manipulators and Mobile Robots // Autonomous robot vehicles. 1986. pp. 396–404.
22. *Ge S.S., Cui Y.J.* Dynamic motion planning for mobile robots using potential field method // Autonomous robots. 2002. vol. 13. no. 3. pp. 207–222.
23. *Lagarias J.C., Reeds J.A., Wright M.H., Wright P.E.* Convergence properties of the Nelder–Mead simplex method in low dimensions // SIAM Journal on optimization. 1998. vol. 9(1). pp. 112–147.
24. *Лавренов Р.О., Афанасьев И.М., Магид Е.А.* Планирование маршрута для беспилотного наземного робота с учетом множества критериев оптимизации // Третий Всероссийский научно-практический семинар «Беспилотные транспортные средства с элементами искусственного интеллекта». 2016. С. 10–20.
25. *Lavrenov R., Magid E.* Towards heterogeneous robot team path planning: acquisition of multiple routes with a modified spline-based algorithm // MATEC Web of Conferences. 2017. vol. 113. pp. 02015.
26. ROS программная библиотека робота Husky. URL: <http://wiki.ros.org/Robots/Husky> (дата обращения: 11.10.2018).
27. *Zheng K.* ROS Navigation Tuning Guide // arXiv preprint arXiv: 1706.09068. 2017.
28. *Akai N. et al.* Autonomous driving based on accurate localization using multilayer LiDAR and dead reckoning // Intelligent Transportation Systems (ITSC). 2017. pp. 1–6.
29. *Thrun S., Bücken A.* Integrating grid-based and topological maps for mobile robot navigation // Proceedings of the National Conference on Artificial Intelligence. 1996. pp. 944–951.
30. *Lau B., Sprunk C., Burgard W.* Improved updating of Euclidean distance maps and Voronoi diagrams // 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2010. pp. 281–286.
31. *Lau B., Sprunk C., Burgard W.* Efficient grid-based spatial representations for robot navigation in dynamic environments // Robotics and Autonomous Systems. 2013. vol. 61. no. 10. pp. 1116–1130.
32. *Lau B., Sprunk C., Burgard W.* Incremental Updates of Configuration Space Representations for Non-Circular Mobile Robots with 2D 2.5 D or 3D Obstacle Models // ESMR. 2011. pp. 49–54.
33. *Федоренко Р.В., Гуренко Б.В.* Планирование траектории автономного мини-корабля // Инженерный вестник Дона. 2015. Т. 38. № 4-1. 12 с.
34. *Soldea O., Elber S., Rivlin E.* Global curvature analysis and segmentation of volumetric data sets using trivariate B-spline functions // Geometric Modeling and Processing. 2004. pp. 217–226.
35. Реализация сплайн-алгоритма планирования пути. URL: https://gitlab.com/LIRS_Projects/Simulaion-Spline-Voronoi-Planner (дата обращения: 04.10.2018).

Лавренов Роман Олегович — младший научный сотрудник лаборатории интеллектуальных робототехнических систем, ассистент кафедры интеллектуальной робототехники высшей школы информационных технологий и интеллектуальных систем, Казанский (Приволжский) федеральный университет (КФУ). Область научных интересов: алгоритмы планирования пути; алгоритмы локализации и картографирования для автономных робототехнических систем; промышленные роботы-манипуляторы. Число научных публикаций — 24. lavrenov@it.kfu.ru, <https://kpfu.ru/lirs.html>; ул. Кремлевская, 35, Казань, 420008; р.т.: +7(843) 221-3433.

Магид Евгений Аркадьевич — Ph.D., профессор, руководитель лаборатории интеллектуальных робототехнических систем, и.о. заведующего кафедры интеллектуальной робототехники высшей школы информационных технологий и

интеллектуальных систем, Казанский (Приволжский) федеральный университет (КФУ). Область научных интересов: поисково-спасательная робототехника; мобильная робототехника; групповое взаимодействие роботов; планирование маршрута; антропоморфная робототехника; взаимодействие человека и робота; обработка изображений и техническое зрение. Число научных публикаций — 110. magid@it.kfu.ru, <https://kpfu.ru/lirs.html>; ул. Кремлевская, 35, Казань, 420008; р.т.: +7(843) 221-3433.

Мацуно Фумитоши — Ph.D., профессор департамента инженерной механики и науки, Киотский Университет, Япония. Область научных интересов: робототехника; системы управления; поисково-спасательная робототехника. Число научных публикаций – 486. matsuno@me.kyoto-u.ac.jp, ул. Киёдайкацура, 3., Нисикё, Киото, 615-8540, Япония, р.т.: +81-75-383-3593.

Свинин Михаил Михайлович — Ph.D., профессор колледжа информационных наук и инженерии, Университет Ритсумейкан. Область научных интересов: компьютерные науки, математическое моделирование, математические методы в исследованиях. Число научных публикаций — 154. svinin@fc.ritsumei.ac.jp, ул. Нойи Хигаши, 1, Кусацу, Киото, 525-8577, Япония, р.т.: +077-561-3099.

Сутакори Джакрит — Ph.D., профессор департамента биомедицинской инженерии, Университет Махидол. Область научных интересов: медицинская робототехника; поисково-спасательная робототехника; экзоскелеты; мобильная робототехника. Число научных публикаций — 104. jackrit.sut@mahidol.ac.th, ул. 999 Футтамонтон, 4, Салайа, 73170, Таиланд, р.т.: +66 81 913 6220.

Поддержка исследований. Исследование выполнено при финансовой поддержке РФФИ (проект № 19-58-70002).

**R.O. LAVRENOV, E.A. MAGID, F. MATSUNO, M.M. SVININ, J. SUTHAKORN
DEVELOPMENT AND IMPLEMENTATION OF SPLINE-BASED
PATH PLANNING ALGORITHM IN ROS/GAZEBO
ENVIRONMENT**

Lavrenov R.O., Magid E.A., Matsuno F., Svinin M.M., Suthakorn J. **Development and Implementation of Spline-based Path Planning Algorithm in ROS/Gazebo Environment.**

Abstract. Path planning for autonomous mobile robots is an important task within robotics field. It is common to use one of the two classical approaches in path planning: a global approach when an entire map of a working environment is available for a robot or local methods, which require the robot to detect obstacles with a variety of onboard sensors as the robot traverses the environment.

In our previous work, a multi-criteria spline algorithm prototype for a global path construction was developed and tested in Matlab environment. The algorithm used the Voronoi graph for computing an initial path that serves as a starting point of the iterative method. This approach allowed finding a path in all map configurations whenever the path existed. During the iterative search, a cost function with a number of different criteria and associated weights was guiding further path optimization. A potential field method was used to implement some of the criteria.

This paper describes an implementation of a modified spline-based algorithm that could be used with real autonomous mobile robots. Equations of the characteristic criteria of a path optimality were further modified. The obstacle map was previously presented as intersections of a finite number of circles with various radii. However, in real world environments, obstacles' data is a dynamically changing probability map that could be based on an occupancy grid. Moreover, the robot is no longer a geometric point.

To implement the spline algorithm and further use it with real robots, the source code of the Matlab environment prototype was transferred into C++ programming language. The testing of the method and the multi criteria cost function optimality was carried out in ROS/Gazebo environment, which recently has become a standard for programming and modeling robotic devices and algorithms.

The resulting spline-based path planning algorithm could be used on any real robot, which is equipped with a laser rangefinder. The algorithm operates in real time and the influence of the objective function criteria parameters are available for dynamic tuning during a robot motion.

Keywords: path planning, mobile robot, planning algorithm, ROS, Gazebo, spline-based algorithm.

Lavrenov Roman Olegovich — Junior Researcher of Intelligent Robotic Systems Laboratory, lecturer of Intelligent Robotics Department of High School of Information Technology and Intelligent Systems, Kazan Federal University. Research interests: path planning and localization and mapping algorithms for autonomous robots; industrial robot manipulators. The number of publications — 24. lavrenov@it.kfu.ru, <https://kpfu.ru/lirs.html>; 35, Kremlevskaya str., Kazan, 420008, Russia; office phone: +7(843) 221-3433.

Magid Evgeni Arkadievich — Ph.D., Professor, Head of Laboratory of Intelligent Robotic Systems, Head of Department of Intelligent Robotics of High School of Information Technology and Intelligent Systems, Kazan Federal University. Research interests: mobile robotics, group interaction of robots, path planning, anthropomorphic robotics, human-robot interaction, image processing and computer vision. The number of publications — 110. magid@it.kfu.ru, <https://kpfu.ru/lirs.html>; 35, Kremlevskaya st., Kazan, 420008, Russia; office phone: +7(843) 221-3433.

Matsuno Fumitoshi — Ph.D., Full Professor of Mechanical Engineering and Science Department, Kyoto University. Research interests: robotics, control engineering, rescue robotics. The number of publications – 486. matsuno@me.kyoto-u.ac.jp, 3, Kyoudaikaitsura, Nishigyō-ku, Kyoto, 615-8540, Japan; office phone: +81-75-383-3593.

Svinin Mikhail Mikhailovich — Ph.D., Professor of College of Information Science and Engineering, Ritsumeikan University. Research interests: computer science, mathematical modeling and mathematical methods in scientific research. The number of publications – 154. svinin@fc.ritsumei.ac.jp, 1, Noji Higashi, Kusatsu, Kyoto, 525-8577, Japan; office phone: +077-561-3099

Suthakorn Jackrit — Ph.D., Professor of Biomedical Engineering Department, Mahidol University. Research interests: medical robotics, rescue robotics, surgical navigation, exoskeleton, mobile robotics. The number of publications — 104. jackrit.sut@mahidol.ac.th; 4, 999 Phuttamonthon, Salaya, 73170, Thailand; office phone: +66 81 913 6220.

Acknowledgements. This research is supported by RFBR (project No. 19-58-70002).

References

1. Michael N. et al. Collaborative mapping of an earthquake damaged building via ground and aerial robots. *Journal of Field Robotics*. 2012. vol. 29. no. 5. pp. 832–841.
2. Nagatani K. et al. Multirobot exploration for search and rescue missions: A report on map building in RoboCupRescue 2009. *Journal of Field Robotics*. 2011. vol. 28(3). pp. 373–387.
3. Pshikhopov V., Medvedev M., Krukhmalev V., Shevchenko V. Base Algorithms of the Direct Adaptive Position-Path Control for Mobile Objects Positioning. *Applied Mechanics and Materials*. 2015. vol. 763. pp. 110–119.
4. Loevsky I., Shimshoni I. Reliable and efficient landmark-based localization for mobile robots. *Robotics and Autonomous Systems*. 2010. vol. 58(5). pp. 520–528.
5. Filipenko M., Afanasyev I. Comparison of Various SLAM Systems for Mobile Robot in an Indoor Environment. International Conference on Intelligent Systems. 2018. 8 p.
6. Sokolov M., Bulichev O., Afanasyev I. Analysis of ROS-based Visual and Lidar Odometry for a Teleoperated Crawler-type Robot in indoor environment. International Conference on Informatics in Control, Automation and Robotics (ICINCO). 2017. pp. 316–321.
7. Wagner G., Choset H. Subdimensional expansion for multirobot path planning. *Artificial Intelligence*. 2015. vol. 219. pp. 1–24.
8. Vokhmintsev A., Yakovlev K. A Real-Time Algorithm for Mobile Robot Mapping Based on Rotation-Invariant Descriptors and Iterative Close Point Algorithm. International Conference on Analysis of Images, Social Networks and Texts. 2016. pp. 357–369.
9. Sullivan J.C.W., Pipe A.G. Path planning for redundant robot manipulators: a global optimization approach using evolutionary search. 1998 IEEE International Conference on Systems, Man, and Cybernetics. 1998. vol. 3. pp. 2396–2400
10. Hart P.E., Nilsson N.J., Raphael B.A formal basis for the heuristic determination of minimum cost paths. *IEEE transactions on Systems Science and Cybernetics*. 1968. vol. 4. no. 2. pp. 100–107.
11. LaValle S.M. Rapidly-exploring random trees: A new tool for path planning. Iowa State University Ames. 1998. 4 p.
12. Yakovlev K.S., Makarov D.A., Baskin E.S. [The method of automatic planning of the trajectory of an unmanned aerial vehicle under restrictions on flight dynamics].

- Iskusstvennyj intellekt i prinyatie reshenij – Artificial intelligence and decision making* 2014. vol. 4. pp. 3. (In Russ.).
13. Stentz A. Optimal and efficient path planning for partially-known environments. International Conference on Robotics and Automation (ICRA). 1994. vol. 94. pp. 3310–3317.
 14. Koenig S., Likhachev M. Fast replanning for navigation in unknown terrain. *IEEE Transactions on Robotics*. 2005. vol. 21. no. 3. pp. 354–363.
 15. Karaman S., Frazzoli E. Sampling-based algorithms for optimal motion planning. *The International Journal of Robotics Research*. 2011. vol. 30. no. 7. pp. 846–894.
 16. Otte M., Frazzoli E. RRT X: Real-Time Motion Planning/Replanning for Environments with Unpredictable Obstacles. Algorithmic Foundations of Robotics XI. 2015. pp. 461–478.
 17. Magid E., Keren D., Rivlin E., Yavneh I. Spline-based robot navigation. 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems. 2006. pp. 2296–2301.
 18. Nagatani K., Iwai Y., Tanaka Y. Sensor based navigation for carlike mobile robots using Generalized Voronoi Graph. 2001 IEEE/RSJ International Conference on Intelligent Robots and Systems. 2001. vol. 2. pp. 1017–1022.
 19. Lavrenov R., Matsuno F., Magid E. Modified Spline-Based Navigation: Guaranteed Safety for Obstacle Avoidance. International Conference on Interactive Collaborative Robotics. 2017. pp. 123–133.
 20. Koren Y., Borenstein J. Potential field methods and their inherent limitations for mobile robot navigation. 1991 IEEE International Conference on Robotics and Automation. 1991. pp. 1398–1404.
 21. Khatib O. Real-Time Obstacle Avoidance for Manipulators and Mobile Robots. Autonomous robot vehicles. 1986. pp. 396–404.
 22. Ge S.S., Cui Y.J. Dynamic motion planning for mobile robots using potential field method. *Autonomous robots*. 2002. vol. 13. no. 3. pp. 207–222.
 23. Lagarias J.C., Reeds J.A., Wright M.H., Wright P.E. Convergence properties of the Nelder–Mead simplex method in low dimensions. *SIAM Journal on optimization*. 1998. vol. 9(1). pp. 112–147.
 24. Lavrenov R.O., Afanasyev I.M., Magid E.A. [Path planning for an unmanned ground robot based on a variety of optimization criteria]. *Tretij Vserossijskij nauchno-prakticheskij seminar "Bespilotnye transportnye sredstva s ehlementami iskusstvennogo intellekta"* [The third All-Russian Scientific and Practical Seminar "Unpiloted Vehicles with Artificial Intelligence Elements"]. 2016. pp. 10–20. (In Russ.).
 25. Lavrenov R., Magid E. Towards heterogeneous robot team path planning: acquisition of multiple routes with a modified spline-based algorithm. *MATEC Web of Conferences*. 2017. vol. 113. pp. 02015.
 26. ROS programmaya biblioteka robota Husky [ROS program library of Husky robot]. Available at: <http://wiki.ros.org/Robots/Husky>. (accessed: 11.10.2018). (In Russ.).
 27. Zheng K. ROS Navigation Tuning Guide. arXiv preprint arXiv: 1706.09068. 2017.
 28. Akai N. et al. Autonomous driving based on accurate localization using multilayer LiDAR and dead reckoning. *Intelligent Transportation Systems (ITSC)*. 2017. pp. 1–6.
 29. Thrun S., Bücken A. Integrating grid-based and topological maps for mobile robot navigation. Proceedings of the National Conference on Artificial Intelligence. 1996. pp. 944–951.
 30. Lau B., Sprunk C., Burgard W. Improved updating of Euclidean distance maps and Voronoi diagrams. 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). 2010. pp. 281–286.
 31. Lau B., Sprunk C., Burgard W. Efficient grid-based spatial representations for robot navigation in dynamic environments. *Robotics and Autonomous Systems*. 2013. vol. 61. no. 10. pp. 1116–1130.

32. Lau B., Sprunk C., Burgard W. Incremental Updates of Configuration Space Representations for Non-Circular Mobile Robots with 2D 2.5 D or 3D Obstacle Models. ECMR. 2011. pp. 49–54.
33. Fedorenko R.V., Gurenko B.V. [Planning the trajectory of an autonomous mini-ship]. *Inzhenernyj vestnik Dona – Engineering Journal of Don*. 2015. vol. 38. no. 4-1. 12 p. (In Russ.).
34. Soldea O., Elber G., Rivlin E. Global curvature analysis and segmentation of volumetric data sets using trivariate B-spline functions. *Geometric Modeling and Processing*. 2004. pp. 217–226.
35. Realizaciya splajn-algoritma planirovaniya puti [Implementation of the spline algorithm for path planning]. Available at: https://gitlab.com/LIRS_Projects/Simulaion-Spline-Voronoi-Planner (accessed: 04.10.2018).

А.С. ГОРОБЦОВ, А.Е. АНДРЕЕВ, А.Е. МАРКОВ, А.В. СКОРИКОВ,
П.С. ТАРАСОВ

ОСОБЕННОСТИ РЕШЕНИЯ УРАВНЕНИЙ МЕТОДА ОБРАТНОЙ ЗАДАЧИ ДЛЯ СИНТЕЗА УСТОЙЧИВОГО УПРАВЛЯЕМОГО ДВИЖЕНИЯ ШАГАЮЩИХ РОБОТОВ

Горобцов А.С., Андреев А.Е., Марков А.Е., Скориков А.В., Тарасов П.С. Особенности решения уравнений метода обратной задачи для синтеза устойчивого управляемого движения шагающих роботов.

Аннотация. Рассматривается задача синтеза управляемого движения шагающих роботов методом обратной задачи. Уравнения метода обратной задачи представляются с помощью методов динамики связанных систем тел, как уравнения движения свободных тел и уравнения связей. Введены различные группы уравнений связей — для задания походки робота, для выполнения условий устойчивости робота и для согласованного движения заданных звеньев робота. Ключевая особенность уравнений метода обратной задачи в такой постановке состоит в наличии вторых производных координат системы в уравнениях связей, обеспечивающих поддержание роботом вертикального положения. Однозначное решение таких уравнений в общем случае невозможно из-за неопределенности начальных условий для множителей Лагранжа. Рассмотрен приближенный метод решения обратной задачи без учета инерционных составляющих в уравнениях связей, определяющих устойчивость робота. Выписаны уравнения связей, которые определяют согласованное движение отдельных звеньев робота и необходимые для однозначного решения задачи на основе приближенных уравнений. Представлена реализация методов синтеза программного движения в системе управления робота андроида AP600. Выполнено сравнение теоретических и экспериментальных показателей управляемого движения. Установлено, что при достигнутой высокой точности управления следящими приводами относительными движениями звеньев робота с погрешностью несколько процентов, показатели абсолютных движений робота, в частности, углы крена, рыскания и тангажа, отличаются от программных на 30–40%. Показано, что предложенный метод позволяет синтезировать управление роботом в квазистатическом режиме для различных типов движений — вперед, вбок, движение по ступенькам, наклоны и так далее.

Ключевые слова: робототехника, шагающие роботы, управление, антропоморфные роботы, обратная задача, андройды.

1. Введение. Шагающие роботы относятся к развивающемуся классу роботов. Конструкция шагающих роботов обладает избыточными степенями свободы, что отличает их от других мобильных машин, например, колесных, характеризующихся избыточными связями. Избыточные степени свободы робота определяют сложную локомоцию его движений — согласованных взаимных перемещений звеньев робота, обеспечивающих заданное конечное перемещение как всего робота, так и его отдельных частей. Управление локомоцией шагающих роботов является ключевым направлением современных исследований в этой области, которые, в первую очередь, направлены на достижение устойчивого движения как стабильного сохранения вертикального положения. Создание

совершенных методов управления шагающими роботами позволит получить новый класс машин с высокими параметрами по проходимости и универсальности применения, недостижимыми другими существующими транспортными платформами.

В настоящее время как в России, так и за рубежом существует достаточно большое число конструкций андроидов, в которых реализованы некоторые режимы двуногой ходьбы. На рисунке 1 показаны некоторые известные конструкции андроидов.

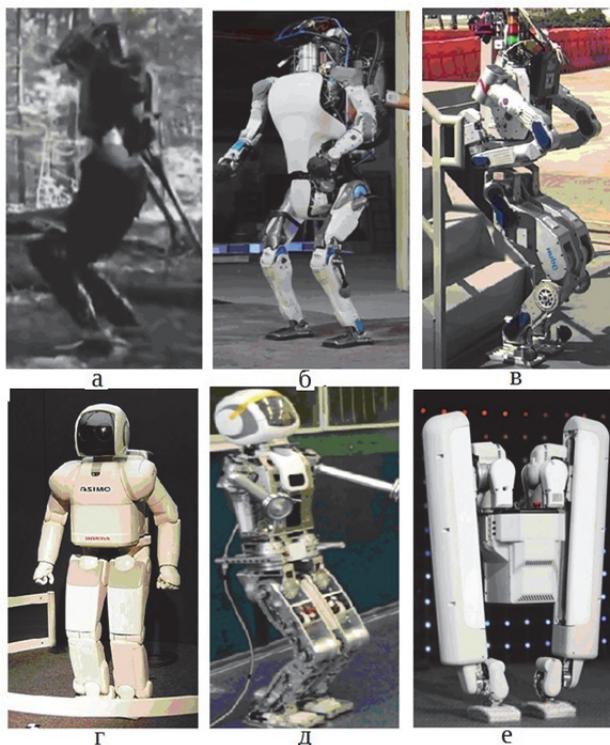


Рис. 1. Некоторые существующие образцы антропоморфных роботов:
 а, б) Boston Dynamics (США); в) Hubo (Республика Корея); г) Honda (Япония);
 д) AP600 (Россия); е) Google X (США)

На данный момент технические характеристики таких роботов позволяют планировать только весьма ограниченные коммерческие применения, например для испытания специальной одежды [1]. Интенсивно ведутся работы в области создания протезов нижних конечностей человека [2-4]. Тем не менее задача синтеза управления

локомоцией шагающих движителей таких роботов остается актуальной. Можно выделить два основных направления решения такой задачи — теоретические методы и методы копирующего управления, основанные, как правило, на использовании движений человека при формировании управляющих воздействий. Второе направление интенсивно развивается, например, в медицине [5], а в области шагающих роботов при разработке экзоскелетов [6].

В работе рассматриваются теоретические методы управления локомоцией роботов — антроидов, для которых вопросы устойчивости наиболее актуальны. Представленные ниже методы могут быть также использованы и для роботов с большим числом ног. Универсальным теоретическим методом синтеза управляемого движения многозвенных механических систем является метод обратной задачи [7, 8], позволяющий определять программные движения системы и ее приводов, реализующие заданный закон перемещения тел в общем случае. Некоторые теоретические аспекты двуногой ходьбы для плоского случая рассмотрены в [9, 10], однако применение таких подходов в методе обратной задачи ограничено расчетными схемами небольшой размерности. Наиболее общий подход может быть получен с помощью методов динамики связанных систем тел [11], для которых к настоящему времени разработаны эффективные численные алгоритмы и которые не накладывают существенных ограничений на размерность и структуру используемой математической модели.

Общее уравнение движения робота как пространственной механической системы можно записать в виде:

$$\begin{cases} M\dot{x} = f(x, \dot{x}, t) + u(t) & (1a) \\ Q_1(x) = 0 & (1b) \end{cases} \quad (1)$$

Здесь x — вектор координат всей системы размерностью $n \times 6$, где n число тел системы, M — матрица инерции, $f(x, \dot{x}, t)$ — вектор позиционных, диссипативных и внешних сил, $Q_1(x)$ — вектор связей размерностью k_1 , описывающих кинематические пары, $u(t)$ — вектор сил (моментов) в приводах, приведенных к координатам тел. При $k_1 = n$ уравнения (1б) называются уравнениями кинематики, они однозначно задают движение механической системы и могут решаться независимо от уравнений (1а). Непосредственное решение уравнений в форме (1) используется редко из-за низкой вычислительной эффективности. В методах динамики систем тел, ориентированных на

численное решение, используется форма представления (1) с множителями Лагранжа и продифференцированными дважды уравнениями связей:

$$\begin{cases} \mathbf{M}\ddot{\mathbf{x}} + \mathbf{D}_1^T \mathbf{p}_1 = \mathbf{f}(\mathbf{x}, \dot{\mathbf{x}}, t) + \mathbf{u}(t) & (2a) \\ \mathbf{D}_1 \ddot{\mathbf{x}} = \mathbf{h}_1(\mathbf{x}, \dot{\mathbf{x}}) & (2б) \end{cases} \quad (2)$$

где \mathbf{D}_1 — матрица коэффициентов уравнений связей размерностью $k_1 \times n$, \mathbf{p}_1 — вектор множителей Лагранжа размерностью k_1 , $\mathbf{h}_1(\mathbf{x}, \dot{\mathbf{x}})$ — вектор правых частей вторых производных уравнений связей. Подробное описание уравнений (2) и особенностей их численного решения можно найти в [11]. Уравнения (2) суть дифференциально-алгебраические уравнения, поскольку включают в себя алгебраические величины — множители Лагранжа. Для решения уравнений (2) в настоящее время существует достаточно большое количество коммерческого и открытого программного обеспечения (ПО) [11]. В функции такого ПО входит автоматическое формирование уравнений движения и связей и их численное интегрирование. В настоящей работе для решения рассматриваемой задачи используется система моделирования динамики систем твердых тел ФРУНД [11].

Уравнения (1)-(2) в механике принято называть уравнениями прямой задачи, в которой находится движение системы по заданным действующим силам. В терминах аналитической механики уравнения (1)-(2) описывают систему с голономными связями. Для нахождения управлений $\mathbf{u}(t)$ в методе обратной задачи сначала ищется программное движение. Для этого действие управляющих сил заменяется дополнительными уравнениями связей. Уравнения (1) применительно к шагающим роботам в этом случае приобретают вид:

$$\begin{cases} \mathbf{M}\ddot{\mathbf{x}} = \mathbf{f}(\mathbf{x}, \dot{\mathbf{x}}, t) & (3a) \\ \mathbf{Q}_1(\mathbf{x}) = \mathbf{0} & (3б) \\ \mathbf{Q}_2(\mathbf{x}) = \mathbf{w}(t) & (3в) \\ \mathbf{Q}_3(\mathbf{x}) = \mathbf{0} & (3г) \\ \mathbf{Q}_4(\mathbf{x}, \ddot{\mathbf{x}}, \mathbf{z}(t)) = \mathbf{0} & (3д) \\ \mathbf{Q}_5(\mathbf{x}, \ddot{\mathbf{x}}, \mathbf{z}(t)) < k_f & (3е) \end{cases} \quad (3)$$

Здесь $\mathbf{Q}_2(\mathbf{x}), \mathbf{Q}_3(\mathbf{x}), \mathbf{Q}_4(\mathbf{x}, \ddot{\mathbf{x}}, \mathbf{z}(t))$ — векторы связей, $\mathbf{Q}_5(\mathbf{x}, \ddot{\mathbf{x}}, \mathbf{z}(t))$ — отношение модулей горизонтальной и вертикальной сил реакций в стопах робота.

Уравнение (3в) размерностью k_2 задает кинематику движения стоп робота и его корпуса. Вектор функция $w(t)$ включает в себя траектории точек левой и правой ног и корпуса.

Уравнение (3г) размерностью k_3 задает вспомогательные связи для исключения избыточных степеней свободы всего робота.

Уравнение (3д) размерностью $k_4 \leq 3$ определяет выполнение условия устойчивости. Условие устойчивости имеет вид [12]:

$$z(t) \in \Gamma, \quad (4)$$

где $z(t)$ — вектор координат точки приложения сил реакций связей в стопах робота, в которой главный момент реакций равен нулю. Такая точка имеет специальное название — точка нулевого момента (ТНМ). Γ — некоторая область на опорной поверхности, нахождение внутри которой обеспечивает устойчивость. В развернутом виде компонента (3д), например, для момента реакции относительно поперечной оси записывается:

$$\sum_{i=1}^n m_i (\ddot{z}_i + g)x_i - \sum_{i=1}^n m_i \ddot{x}_i z_i - \sum_{i=1}^n A_i J_i \dot{\Omega}_i - z_x(t) \sum_{i=1}^n m_i (\ddot{z}_i + g) = 0, \quad (5)$$

где m_i — масса i -го тела, x_i, z_i — продольная и вертикальная координаты центра масс (ц.м.) i -го тела, A_i — матрица перехода из подвижной системы координат i -го тела в неподвижную, J_i — матрица моментов инерции тела, Ω_i — трехмерный вектор угловых скоростей тела в подвижной системе координат, $z_x(t)$ — продольная координата ТНМ. Если считать, что направления координат тел и неподвижной системы координат совпадают, то уравнение (5) соответствует уравнению моментов относительно оси y неподвижной системы координат. Аналогично записывается уравнение моментов относительно оси x , в которое входит поперечная координата ТНМ.

Уравнения связей вида (5) и, следовательно, (3д) качественно отличаются от уравнений связей (3б-3г) — в них входят вторые производные координат системы. Такие уравнения связей называются неголономными.

Скалярное неравенство (3е) задает условие отсутствия скольжения в стопах, которое зависит от коэффициента трения об опорную поверхность k_f . Левая часть этого неравенства представляет

собой отношение главных векторов горизонтальной и вертикальной реакции в стопах. Работы, в которых для шагающих роботов решается обратная задача с учетом отсутствия скольжения в форме неравенства (3е), нам неизвестны. Далее считается, что k_f велико, и неравенство (3е) выполняется.

Приведение системы (3) к виду (2) с помощью множителей Лагранжа и двойного дифференцирования (3б)-(3г) дает:

$$\left\{ \begin{array}{l} M\ddot{x} - D_2^T p_1 - D_2^T p_2 - D_3^T p_3 - D_{41}^T p_4 - D_{42}^T \ddot{p}_4 = f(x, \dot{x}, t) \\ D_1 \ddot{x} = h_1(x, \dot{x}) \\ D_2 \ddot{x} = \ddot{w}(t) \\ D_3 \ddot{x} = h_3(x, \dot{x}) \\ Q_4(x, \ddot{x}, z(t)) = 0 \end{array} \right. , \quad (6)$$

где D_2, D_3 — матрицы коэффициентов связей уравнений (3в) и (3г), D_{41}, D_{42} — матрицы коэффициентов связей уравнения (3д), соответствующие членам с координатами и их вторыми производными, p_2, p_3, p_4 — множители Лагранжа, соответствующие уравнениям (3в)-(3д). Необходимое условие однозначности решения (6) – отсутствие динамических степеней свободы:

$$k_1 + k_2 + k_3 + k_4 = n . \quad (7)$$

Равенство (7) определяет условие отсутствия избыточных степеней свободы у системы. Для получения однозначного решения уравнения (2) такого условия достаточно, однако решение (6) зависит от неопределенных начальных условий для множителей Лагранжа p_4 и их первых производных и, кроме того, условию (4) могут удовлетворять различные функции $z(t)$. Можно утверждать, что система (6) представляет собой особый класс задач, для решения которых точных методов не существует. Ниже будут рассмотрены различные приближенные способы решения (6).

Следует заметить, однако, что (6) имеет точное решение в некоторых частных случаях. Например, если в первую подсистему (6) будет входить уравнение, содержащее только вторую производную одной координаты, то эта вторая производная находится из соответствующей компоненты уравнений 3д. Физически это может соответствовать, например, наличию в механической системе маховика, закрепленного на оси, проходящей через его ц.м.

Технически такое решение малоцелесообразно, но следует отметить, что на практике стабилизация такого типа известна — это балансирование канатоходца с помощью шеста.

Отметим также, что формально для решения обратной задачи и определения программного движения достаточно уравнений кинематики (3б)-(3д) при условии выполнения равенства (7). Тем не менее, численные алгоритмы более эффективны для решения полной системы (6).

Результат решения (6) — программные траектории координат робота, которые можно использовать для нахождения сил в приводах. Например, при использовании пропорционально-дифференциальных регуляторов (ПД регуляторов), величина силы в j -ом приводе:

$$u_j^*(t) = c_j \delta_j + d_j \dot{\delta}_j; j = 1, \dots, n_1. \quad (8)$$

Здесь $u_j^*(t)$ — сила (момент) на выходном звене j -го привода, c_j, d_j — коэффициенты ПД регулятора, δ_j — отклонение между измеренным и программным значениями смещения выходного звена привода, n_1 — количество приводов робота.

Отклонение δ_j равно:

$$\delta_j = \phi_c - \phi_p, \quad (9)$$

где ϕ_c — смещение привода в управляемом движении (измеренное смещение), ϕ_p — программное смещение. Программное смещение получается при решении системы (6). Методом обратной задачи можно найти и непосредственно программные силы в приводах [13]. Вопросы управления по силам в приводах в настоящей работе не рассматриваются. Мы также опускаем вопрос вычисления смещений приводов и приведения сил приводов к соответствующим степеням свободы тел робота, поскольку это легко решается в существующих системах моделирования динамики систем тел с помощью стандартных элементов описания расчетных схем.

2. Возможные методы решения обратной задачи с учетом условий устойчивости. Как уже указывалось, уравнения (6) представляют собой особый класс задач динамики механических систем с неголономными связями. Уравнения неголономных связей содержат еще и неизвестную функцию времени $z(t)$ (три координаты ТНМ), для которой задана только весьма произвольная область

изменения (4). Многозначность решения и отсутствие точных математических методов решения таких задач ведет к использованию различных приближенных подходов.

С точки зрения численного решения системы (6) при заданной $z(t)$, известное на сегодня ПО расчета динамики систем тел не содержит возможностей учета неголономных связей в виде уравнений со вторыми производными в форме (5), хотя принципиальных сложностей для их реализации нет. Общепринято использовать различные редуцированные приближения (5), полученные, например, отбрасыванием членов со вторыми производными. Кроме того, неголономные связи обуславливают неоднозначность решения задачи Коши системы (6) при ненулевых начальных условиях из-за множителей Лагранжа, входящих в уравнения движения тел в виде вторых производных.

Можно отнести все известные методы решения системы (6) к вариационным. Выделяются несколько модификаций этих методов.

1. Прямое решение (численное интегрирование) (6) для заданной функции $z(t)$. Функция $z(t)$ может быть выбрана, например, на основании анализа экспериментальных данных. Если не касаться вопроса начальных условий для соответствующих множителей Лагранжа, то такое решение всегда существует, если оно физически реализуемо. Физическая нереализуемость движения выражается в нарушении геометрических ограничений, определяемых размерами звеньев кинематической схемы робота. Реализуемость движений, очевидно, зависит от числа избыточных степеней свободы робота k_3 (числа дополнительных уравнений связей (3г)). Чем больше избыточных степеней свободы, тем проще избежать геометрических ограничений. Недостаток метода — использование дополнительных уравнений связей, которые, по сути, носят эмпирический характер и формализовать получение которых достаточно сложно. Заметим также, что в скелетах животных число степеней свободы увеличивается за счет составного позвоночника и зачастую наличия специального органа — хвоста.

2. Параметризация компонентов функции $z(t)$. Задача сводится к поиску оптимальных параметров $z(t)$ на некотором временном интервале, минимизирующих величину:

$$\left| Q_4(\mathbf{x}, \dot{\mathbf{x}}, \mathbf{z}(t)) \right|_{\max} \quad t \in t_0, t_1, \quad (10)$$

при этом значения координат и их производных находятся из решения модифицированной системы (6) при выполнении условия (7). В

качестве критерия оптимизации могут использоваться и другие выражения, например, среднеквадратическое отклонение. Широко распространенная модификация системы (6) — упрощение уравнений (5), определяющих выполнение условий устойчивости за счет удержания только составляющих моментов от весов тел. Уравнение (5) принимает вид:

$$\sum_{i=1}^n m_i g x_i - z_X(t) \sum_{i=1}^n m_i g = 0. \quad (11)$$

Система (6) в этом случае записывается:

$$\left\{ \begin{array}{l} M\ddot{x} - D_1^T p_1 - D_2^T p_2 - D_3^T p_3 - D_{41}^T p_4 = f(x, \dot{x}, t) \\ D_1 \ddot{x} = h_1(x, \dot{x}) \\ D_2 \ddot{x} = \ddot{w}(t) \\ D_3 \ddot{x} = h_3(x, \dot{x}) \\ D_{41} \ddot{x} = h_4(\ddot{z}(t)) \end{array} \right. . \quad (12)$$

Решение такой задачи будет соответствовать заданному типу движения корпуса робота и параметров шага, которые определяются функцией $w(t)$. Можно расширить область параметров оптимизации за счет введения в нее параметров шага. Возможно также задание других критериев оптимизации. Однако в любом случае сохраняется главный недостаток такого решения, заключающийся в том, что решение будет соответствовать только одному типу программного движения корпуса робота.

3. Параметризация коэффициентов дополнительных уравнений связей (3г), в предположении, что функция $z(t)$ задана, ее параметры фиксированы, но зависят от $w(t)$. Задача сводится к поиску оптимальной структуры и параметров дополнительных уравнений связей с минимизацией критерия типа (10). Отличие от подхода п.п. 2 в том, что акцент делается на оптимизацию параметров дополнительных уравнений связей. Если в функции $w(t)$ компоненты, определяющие движение стоп, связаны с компонентами, задающими программное движение корпуса, а функция $z(t)$, как уже отмечалось, зависит от $w(t)$, то решение задачи будет удовлетворять различным законам движения корпуса робота.

В существующих системах управления роботами андроидами в основном реализованы различные варианты второго метода. Рассмотрим существующие системы управления роботами андроидами.

3. Существующие подходы к использованию метода обратной задачи в системах управления движением антропоморфных роботов. Управление для существенно неустойчивого режима хронологически было впервые реализовано в одноногом прыгающем роботе [12]. Принцип управления получил название SLIP (Spring Loaded Inverted Pendulum — подпружиненный обратный маятник). В широком круге работ такой подход применяется к управлению двуногими роботами. В [14] представлен способ формирования управления двуногим роботом WL-12R (высота 184 см, масса 127 кг). Можно выделить три части системы управления этого робота — генератор походки, решающий обратную задачу для определения программного движения; планировщик походки, задающий траектории стоп и ТНМ; и блок стабилизирующих обратных связей. Для системы (6) можно провести соответствия с этими частями — генератор походки задается уравнениями связей (3б)-(3д), планировщик походки функциями $w(t)$ и $z(t)$. Блок стабилизирующих обратных связей в системе (6) отсутствует, поскольку эти уравнения описывают только программное движение робота. Приведенная структура системы управления типична для современных шагающих роботов. Планировщик ТНМ робота WL-12R использует уравнения движения в виде связанных точечных масс. Описание генератора походки не приводится. Отмечается [15], что такой робот достигает скорости 38 см/с.

Один из наиболее высокоподвижных из известных антропоморфных роботов — робот ASIMO [16] (высота 120 см, масса 43 кг) обладает максимальной скоростью 3 км/ч. Данный робот самый низкий из представленных на рисунке 1. Подробности алгоритмов системы управления в литературных источниках отсутствуют.

В большинстве существующих в настоящее время систем управления антропоморфными роботами используются упрощенные уравнения динамики и уравнения связей ТНМ (3а, 3д) и точные уравнения связей для кинематической схемы и стоп (3б, 3в). В [17] представлен робот KHR-2 (высота 120 см, масса 56 кг). Планировщик походки, для определения параметров функции $z(t)$, использует решение уравнения обратного маятника. Такое уравнение описывает движение продольной или поперечной координаты ц.м. робота и получается из (5) исключением членов с вертикальными ускорениями и производными от угловых скоростей звеньев робота, а также допущением, что высота ц.м. всех звеньев робота одинакова. Из уравнения перевернутого маятника находится период поперечных или продольных колебаний робота, который затем синхронизируется

с периодом шага, в результате чего с помощью интерполяций получают выражения для функций $w(t)$ и $z(t)$. Функция $w(t)$ входит в уравнение (3в), а $z(t)$ в (3д). Для рассматриваемого робота KHR-2 уравнение (3д) в форме (11) максимально упрощается: оно выражает условие движения только точки одного тела — тазового звена робота, по закону $z(t)$.

Планировщик походки использует три входных параметра — период шага, коэффициент времени опоры на двух ногах, величину поперечного смещения тазового звена. Рассматривается только движение вперед по прямой. Период цикла шага равен 1,9 с. Коэффициент времени опоры для человека равен 10-20 % от периода шага, для робота принималось 5 %. Амплитуда бокового смещения таза 6,4 см при расстоянии между центрами стоп 14 см. Параметры шага рассчитывались для выбранного периода шага. Высота подъема стопы 4 см, длина шага 20 см, форма траектории стопы трапецевидная с интерполяцией тригонометрическими функциями с отсутствием разрывов по скоростям. Форма кривой поперечного смещения таза также интерполировалась тригонометрическими функциями и имела горизонтальные участки для повышения устойчивости. Ходьба начинается из специального начального положения, что, очевидно, связано с тем, что параметры шага определялись для установившегося режима.

Как следует из предыдущего анализа, генератор походки использует упрощенные уравнения, что является одной из причин погрешностей, приводящей к падению робота. Для компенсации таких погрешностей служит блок стабилизирующих обратных связей, в котором можно выделить 3 группы связей — поддержания равновесия, коррекции генератора походки и предикторов падения.

Группа поддержания равновесия включает 4 контура.

Первый контур — демпфирование колебаний при опоре на одну ногу, которое реализовано как дифференциальная обратная связь по угловой скорости крена для привода продольного поворота стопы.

Второй контур — компенсация смещения точки нулевого момента в фазе опоры на одной ноге. Текущие координаты ТНМ получаются из данных датчиков усилий в стопе. Корректирующие величины продольных и поперечных смещений звена таза вычисляются в контуре с обратной связью, в котором используется эмпирическая передаточная функция робота, полученная экспериментально, а передаточная функция обратной связи синтезирована с помощью частотных методов теории автоматического управления.

Третий контур — компенсация непараллельности стопы поверхности при касании за счет ПД регулятора, на вход которого подается момент реакции стопы [18-20].

Четвертый контур — коррекция программного движения стоп, изменяющая фазу их движения в соответствии с фактическим моментом начала опоры каждой стопы.

Группа коррекции генератора походки состоит из двух контуров.

Первый контур — коррекция программного движения звена таза на последующих шагах путем оценки ошибки координат ТНМ на предыдущих шагах.

Второй контур — коррекция положения торса робота в горизонтальной плоскости по эмпирическому алгоритму, используемому в качестве входных параметров измеренные углы крена и тангажа.

Группа предикторов падения содержит два контура.

Первый контур — предсказание позиции наступания. Контур использует статистику движения робота и увеличивает длину выполняемого шага и наклон торса в случае необходимости, что уменьшает вероятность падения вперед.

Второй контур — предсказание падения набок. Контур корректирует угол поперечного наклона оси ступни по предложенному эмпирическому алгоритму.

Генератор походки, используя данные по абсолютным координатам звеньев робота, полученные при решении обратной задачи, вычисляет программные углы поворотов приводов, которые реализуются с помощью ПД регуляторов приводов.

Кроме датчиков положений приводов в обратные связи включены датчики координат ТНМ, углового положения и скорости торса и усилий в ступне. Координаты ТНМ и усилия в ступне подаются в группу поддержания равновесия, а угловые положения, скорости торса и координаты ТНМ в группы коррекции генератора походки и предикторов падения.

Система управления обеспечивала максимальную скорость 22 см/с. Эксперимент также показал, что разница между измеренным и программным положением ТНМ составляет 5-10 см.

В работе [21] для этого же робота приведены экспериментальные данные по параметрам вертикальных реакций в стопах. Динамические выбросы реакций достигают 20-30 % от статических величин в фазе опоры на одной ноге и 40-50 % в фазе опоры на двух ногах. Частота осцилляций реакций около 10 Гц. В [20] для этого же робота используется представление функций координат

ТНМ и стоп в форме полиномов третьего порядка. Разница между измеренным и программным положением ТНМ по сравнению с предыдущим методом интерполяции существенно не изменилась.

В [21] рассматривается метод подбора начальной позы робота, из которой начинается движение. С помощью компьютерного моделирования показано, что правильный выбор начального положения уменьшает время выхода на шагание в стационарном режиме, при этом возмущения по углам качания торса уменьшаются на 50%. Метод прошел апробацию на ряде роботов.

В [18-21] в генераторе походки для представления координат ТНМ и стоп использовались тригонометрические и полиномиальные функции. В работе [22] рассматриваются теоретические возможности использования для этих целей дифференциальных уравнений с дробными производными.

Планировщики походки могут использовать результаты решения прямой задачи с применением данных антропометрических баз [23]. В таких моделях рассматривается расширенный круг движений робота — вставание со стула, поднятие груза и так далее.

Важным контуром обратных связей является контур гашения колебаний при опоре на одну ногу [24], для высоких роботов (выше 120 см) это особенно актуально. В работе рассматриваются контуры гашения угловых колебаний относительно точки опоры ноги в трех плоскостях — продольной, поперечной и горизонтальной. Колебания гасятся за счет введения демпфирования в контуры управления поворотами ног в бедре. Собственные частоты колебаний поднятых ног составляли около 3 Гц.

Робот TORO (рост 174 см, вес 76 кг) [25] содержит в стопах шестикомпонентные датчики сил и моментов для определения координат ТНМ в управляемом движении. Алгоритм управления походкой базируется на методе, названном авторами методом дивергентной компоненты движения (DCM — Divergent Component Motion) [26-34]. Движение ц.м. робота в пространстве происходит вдоль некоторой асимптотически устойчивой траектории, которая и называется дивергентной компонентой движения [25]. Асимптотическая устойчивость траектории обеспечивается тем, что программные координаты ц.м. находятся из системы трех обыкновенных линейных дифференциальных уравнений первого порядка. Сама дивергентная компонента определяется по предлагаемым эмпирическим уравнениям. Метод также апробирован на пространственной одномассовой виртуальной модели.

Еще один метод стабилизации робота — согласованное (compliance) управление [35]. Используется понятие

СОР (Centre Of Pressure) как более широкое, чем ТНМ, поскольку выполнение условий устойчивости для ТНМ не означает, что робот не потеряет устойчивость через несколько шагов. Согласованное управление сводится к тому, что по разнице между измеренными и программными координатами ц.м. и его скоростями вычисляются дополнительные силы, которые пересчитываются в соответствующие корректировочные значения параметров походки. Различные варианты этого метода рассмотрены в [36-40]. В [35] приведены расчетные и экспериментальные данные по эффективности предложенного метода для экспериментального робота высотой 110 см и скоростей движения 5 см/с. Для решения обратной задачи используются значительно редуцированная модель.

Роботы семейства ATLAS имеют систему управления, также построенную на принципе обратного маятника [12]. Роботы могут оснащаться как электрическими, так и электрогидравлическими приводами. Планировщик походки для построения траектории ТНМ использует стратегию так называемой точки захвата (Capture motion) [27]. Стратегия подразумевает определение координат каждого шага из условия возможности остановки робота в данном положении. Использование электрогидравлических приводов высокой удельной мощности позволило в роботах этого семейства реализовать динамическую походку с относительно малым периодом шага. Отличительная черта движения этих роботов — постоянное перешагивание, в том числе при стоянии на месте. Это можно объяснить особенностями функции, описывающей поперечное смещение ТНМ — робот имеет узкую стопу и ТНМ лежит внутри области, ограниченной в поперечном направлении внутренними границами стоп. Такая же особенность походки и у четырехногой шагающей машины этого семейства.

Двуногий робот с поступательными гидравлическими приводами представлен в [41]. Алгоритмы управления основаны на решении линеаризованных уравнений обратного маятника. Экспериментальные данные по параметрам управляемого движения этого робота не приводятся.

Кроме метода обратной задачи для управления шагающими роботами разрабатываются методы, базирующиеся на нейронных сетях, в частности на обучении с подкреплением [36-40]. В работе [42] алгоритмы обучения с подкреплением используются для управления бегом. Существующие нейронные алгоритмы оптимизируют параметры интерполяционных функций сил в приводах робота, а для расчета критериев оптимизации используют решение прямой задачи динамики робота вида (1). Примеры реализации нейронных алгоритмов для

двуногих роботов есть только на виртуальных моделях. Для реальных роботов есть примеры обучения движениям небольшой длительности по времени, например, удар по бейсбольному мячу [43]. В целом недостатки нейронных алгоритмов совпадают с недостатками решения обратной задачи методом п.п. 2.2 — получаемый в результате обучения закон управления соответствует только одному типу движений робота в заданной окружающей обстановке.

Для решения обратной задачи могут использоваться технологии параллельных вычислений [44].

Архитектуры систем управления двуногими и многоногими роботами схожи [39], основные отличия касаются уравнений, описывающих кинематическую схему робота. Структура таких уравнений идентична системе (3).

Наряду с подходами, использующими для описания траекторий ТНМ и точек стоп интерполяции тригонометрическими или полиномиальными функциями, можно выделить методы, где вместо точечных интерполяций используются движения по предельным циклам различных осцилляторов, описываемых нелинейными дифференциальными уравнениями. Применение таких осцилляторов показано в [36] на плоской математической модели андроида. Нелинейные уравнения невысокой размерности также используются для построения регуляторов скорости движения двуногих роботов [27]. Известны работы, в которых для приводов андроидов вместо ПД регуляторов синтезируются оптимальные линейные регуляторы [38].

На основании обзора можно сделать вывод, что большинство существующих систем управления основаны на методе обратной задачи и используют упрощенные математические модели. Наиболее значительные упрощения касаются уравнений, выражающих условия устойчивости робота. По этой причине все рассмотренные системы управления имеют развитые обратные связи, предназначенные для улучшения качества управления. Однако, как следует из обзора, эффективность этих обратных связей нельзя считать удовлетворительной. Невысокая эффективность таких обратных связей, на наш взгляд, вызвана тем, что корректирующие управления являются результатом преобразования звеньями с эмпирическими передаточными функциями и поступают на вход генераторов походки, построенных на упрощенных уравнениях, которые не являются даже линейными приближениями исходных уравнений в текущей точке фазового пространства.

Известные системы управления, как правило, реализуют отдельные режимы движения робота, например, прямолинейное движение вперед по ровной горизонтальной поверхности. С точки

зрения используемой модификации метода обратной задачи, известные системы используют метод, близкий методу п.п. 2.2.

Лучшие результаты по управлению достигнуты для роботов небольшого роста, около 150 см. Все известные шагающие роботы имеют цельную ступню и вызванную этим походку на согнутых в коленях ногах.

4. Предлагаемый метод управления. В данной работе рассматривается разработанная система управления роботом AP600 — рисунок 1, производства ПАО «Андроидная техника». Структура системы управления роботом показана на рисунке 2.

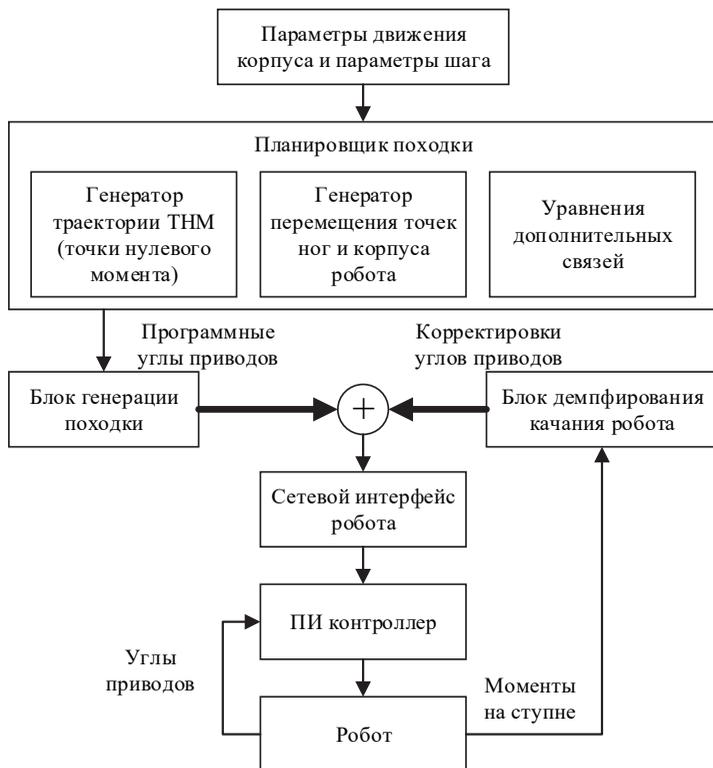


Рис. 2. Структура системы управления роботом

В качестве входных величин системы управления задаются горизонтальные компоненты скорости корпуса робота и параметры шага — максимальная длина, минимальный период, высота подъема, относительные фазы ног. Рассматривается движение робота без поворота относительно вертикальной оси.

Планировщик походки состоит из трех частей, формирующих траектории точек стоп, траектории ТНМ и уравнения дополнительных связей. Трехмерные траектории точек стоп формируются в неподвижной системе координат для одной точки на каждой стопе, лежащей на уровне опорной поверхности в фазе опоры и совпадающей с проекцией центра шарнира стопы. Траектория стопы на одном шаге состоит из четырех участков — подъема, переноса, опускания и опоры. Форма траектории в вертикальной плоскости прямоугольная, на каждом участке кинематические параметры интерполируются тригонометрическими функциями. Для каждого участка вычисляются перемещения, скорости и ускорения. Типичный вид кинематических параметров траектории стопы показан на рисунке 3.

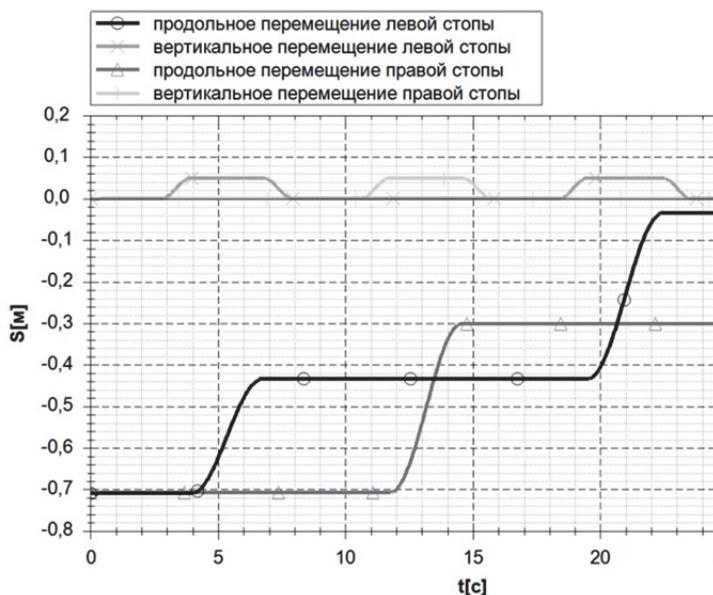


Рис. 3. Программные продольные и вертикальные перемещения стоп робота

Интерполяция тригонометрическими функциями приводит к разрыву скоростей и скачкам ускорений. Из рисунка 4 видно, что в момент начала подъема стопы ускорения скачком принимают максимальные значения. Тем не менее такая интерполяция широко применяется в генераторах походок известных систем управления [17-21]. Как уже отмечалось выше, для исключения таких разрывов и скачков в работах [22, 23, 36-38] рассматривается возможность использования других методов интерполяции — нелинейными

автоколебательными циклами, дифференциальными уравнениями с дробными производными и другие.

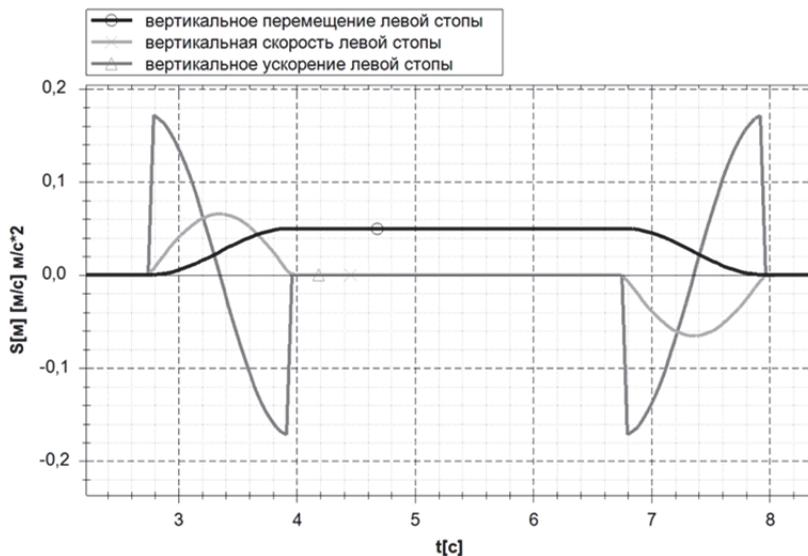


Рис. 4. Программные вертикальные перемещения, скорости и ускорения левой стопы робота

При формировании горизонтальных составляющих траекторий точек стоп используются прогнозируемые значения по соответствующим кинематическим параметрам движения корпуса робота. Движение робота задается по трем точкам корпуса, суммарно по шести направлениям, что однозначно определяет его пространственное положение. Связь траекторий точек стоп с движением корпуса позволяет планировать перемещение стоп при движении робота в любом направлении, повороте и изменении высоты опорной поверхности [13]. Алгоритм изменяет длину шага в зависимости от величины перемещения корпуса, а также позволяет изменять вертикальную координату стопы в зависимости от высоты опорной поверхности, например, при шагании по ступенькам.

Формирование траектории ТНМ робота — компонент функции $z(t)$ выполняется на основании условия (4). Общепринятое условие устойчивости — ТНМ лежит внутри полигона, образованного периметром стоп [17-27]. В рассматриваемой системе управления ТНМ совпадает с центром стопы при опоре на соответствующую ногу или перемещается по прямой, соединяющей

точки центров стоп в фазах опоры на обе стопы. Считается, что цикл шагания состоит из 4 частей — опоры на правой ноге и переноса левой ноги, переноса центра опоры с правой ноги на левую, опоры на левой ноге и переноса правой, переноса центра опоры с левой ноги на правую. Траектория ТНМ интерполируется тригонометрическими функциями. Характерная форма траектории ТНМ для случая с полной остановкой перемещения ТНМ в фазах опоры на одну ногу показана на рисунке 5. Разработанный алгоритм обладает возможностью варьирования амплитудой и временем начала и окончания поперечного смещения ТНМ, допускает наличие постоянной составляющей продольной скорости ТНМ.

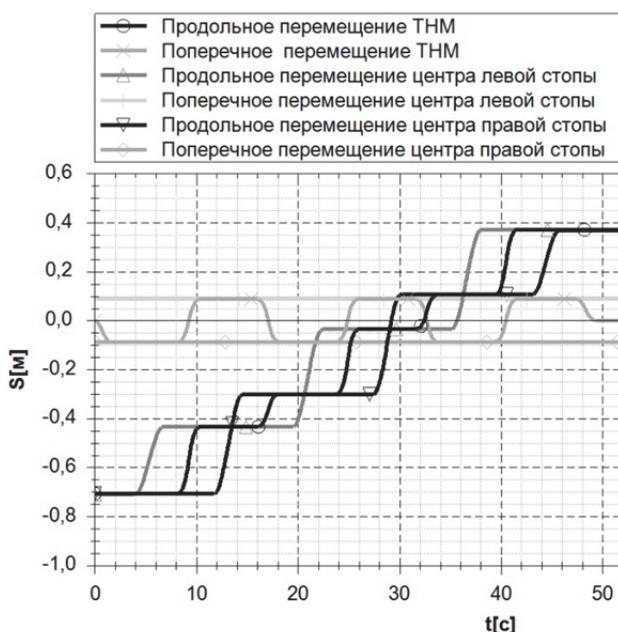


Рис. 5. Программная траектория ТНМ робота

Как отмечалось выше, дополнительные связи служат для задания закономерностей взаимного движения звеньев робота с целью исключения избыточных степеней свободы в роботе и, следовательно, многозначности его возможных движений.

В целом планировщик походки вычисляет для заданного момента времени параметры траекторий точек стоп, корпуса, ТНМ, а также формирует уравнения дополнительных кинематических связей.

Блок обратной задачи по данным планировщика походки вычисляет программные углы приводов робота, решая систему (12). Блок обратной задачи выполнен в системе моделирования динамики систем связанных тел ФРУНД [11, 44], и использует полную динамическую модель робота — рисунок 6.

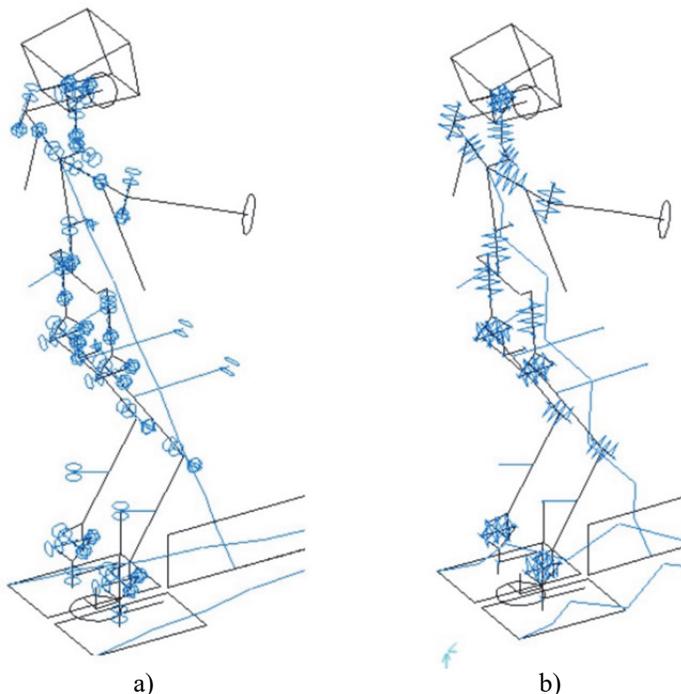


Рис. 6. Схема компьютерной модели андроида, использованной для генерации программного движения: а) кинематическая схема; б) схема приводов

В литературных источниках [1-21] блок обратной задачи зачастую называют блоком обратной кинематики (*inverse kinematics*), хотя задача кинематики для многосвязных пространственных схем имеет больше вычислительных ограничений, чем задача динамики, например, при наличии избыточных связей или степеней свободы. В настоящей работе решается задача динамики, поскольку это позволяет ввести в рассмотрение больше классов структур кинематических цепей. Отметим также, что обратная задача является достаточно сложной математической и вычислительной проблемой, не всегда корректной. В робототехнике для ее решения, как правило, используются специализированные программы, например, SL [21], или

универсальные пакеты динамики систем тел (MBS пакеты). Существуют классы шагающих машин, в которых упрощение решения обратной задачи достигается за счет применения специальных конструктивных схем, например как в шагающих машинах с ортогональными движителями [45].

Программный комплекс ФРУНД позволяет решать уравнения (12) автономно для анализа параметров движения робота или в составе системы управления роботом.

Каждая компонента функции $z(t)$ входит в одно из трех уравнений, выражающих условие устойчивости. Применяются упрощенные уравнения вида (11), которые, в отличие от известных работ, включают в себя все слагаемые с координатами звеньев робота. Физически это соответствует движению ц.м. робота по траектории $z(t)$. Уравнения (11) асимптотически стремятся к (5) при бесконечно малой скорости движения звеньев робота. Режим движения, удовлетворяющий уравнениям (11), можно назвать квазистатическим.

Составляющие $z_x(t)$ и $z_y(t)$, как уже отмечалось, имеют вид, показанный на рисунке 5. Вертикальной координате $z_z(t)$ может назначаться специальная функция, например, огибающая поверхности переменной высоты. При шагании по ровной поверхности вертикальной координате присваивается постоянное значение, подобранное расчетным путем из условия минимального угла сгиба ног в коленном суставе. Известные кинематические схемы роботов содержат стопу, выполненную в виде одного звена, при этом во время шагания плоскость стопы горизонтальна. Такая кинематическая схема позволяет изменять расстояние от ц.м. робота до места опоры стопы в основном за счет сгиба ноги в колене. По этой же причине в позе готовности и во время шагания ноги согнуты в коленях, что также характерно для известных конструкций роботов (рисунок 1). С энергетической точки зрения шагание на согнутых ногах лишает всех преимуществ, свойственных парасагиттальному типу расположения конечностей, характерному для высших животных, в частности млекопитающих. Движения робота с опорой на прямые ноги конструктивно можно добиться двумя путями — введением дополнительных звеньев в торсе или в ступне. Кинематические схемы существующих роботов, как правило, выбраны из условия минимального количества шарниров и приводов, но такое условие определяет возможность шагания только на согнутых ногах.

На рисунке 7 показаны расчетные положения робота в конце шага с разной высотой ц.м., из которых видно, что при высоком расположении ц.м. взаимные повороты звеньев приобретают неприемлемо большие значения. Неразрешимость этой проблемы в рамках существующих кинематических схем привела к появлению кинематических схем роботов без коленного сустава (рисунок 1е).

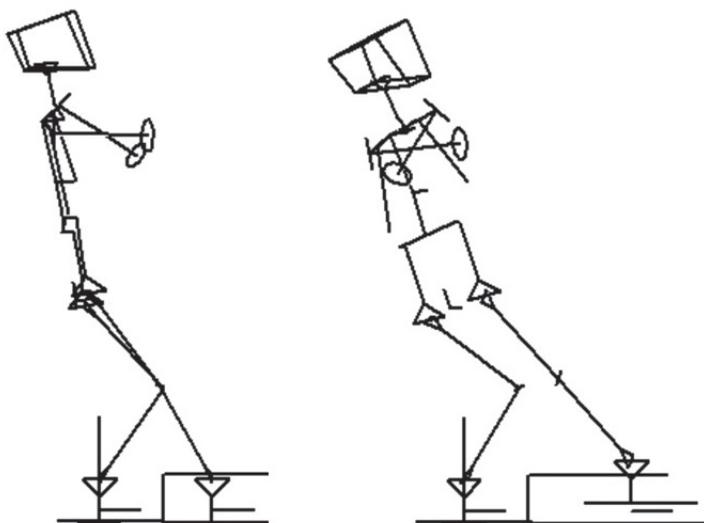


Рис. 7. Расчетные положения робота в конце шага левой ногой, высота ц.м. – 0.57 м. (слева) и 0.61 м. (справа)

Перечислим используемые уравнения дополнительных связей.

Связь между углом продольного наклона торса и продольными углами бедер обеих ног:

$$U_{yk} + k_y U_{yl} + k_y U_{yr} = U_{yp}. \quad (13)$$

Здесь U_{yk} — угол поворота торса робота относительно поперечной оси, U_{yl} — угол поворота левого бедра относительно поперечной оси, U_{yr} — угол поворота правого бедра относительно поперечной оси, U_{yp} — среднее значение угла поворота торса в продольной плоскости, k_y — масштабный коэффициент. За счет этого уравнения достигается изменение среднего значения продольного угла наклона торса (рисунок 8).

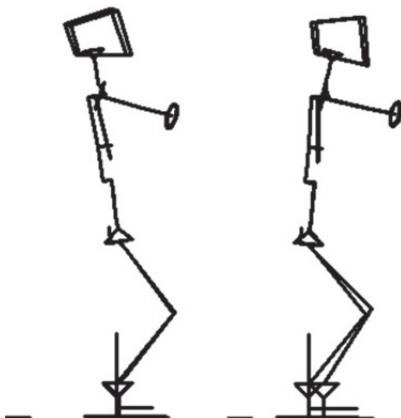


Рис. 8. Изменение продольного наклона корпуса в зависимости от коэффициентов уравнения (13), фаза начальной позы

Связь между углом наклона торса относительно продольной оси и поперечной координатой ц.м. робота:

$$S_{yk} + k_x U_{xk} = 0. \quad (14)$$

Здесь S_{yk} — поперечное смещение ц.м. торса, U_{xk} — угол поворота торса относительно продольной оси, k_x — масштабный коэффициент. Такая связь позволяет изменять размах угла наклона торса в поперечной плоскости – (рисунок 9) и тем самым регулировать диапазон углов приводов. Например, для робота AP600 при походке, показанной слева на рисунке 9, происходит превышение максимальных углов поворота бедер относительно продольной оси, а при другой походке программные углы поворота торса укладываются в конструктивные ограничения — рисунок 9 справа.

Связи, фиксирующие углы поворота стоп в продольной и поперечной плоскости:

$$U_{xsl} = 0,$$

$$U_{ysl} = 0,$$

$$U_{xsr} = 0,$$

$$U_{ysr} = 0.$$

Здесь U_{xsl}, U_{ysl} — углы поворота левой стопы относительно продольной и поперечной осей соответственно, U_{xsr}, U_{ysr} — аналогичные углы поворота правой стопы.

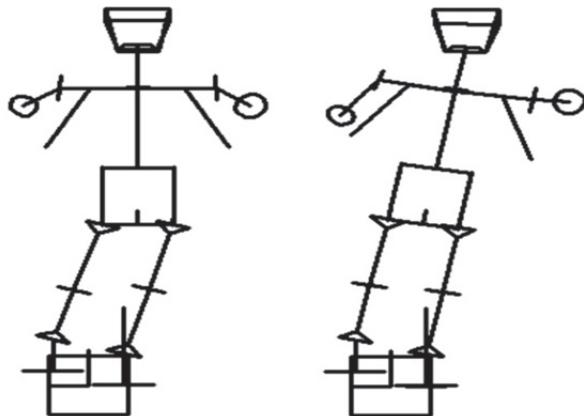


Рис. 9. Изменение поперечного наклона корпуса в зависимости от коэффициентов уравнения (14), фаза опоры на правую ногу

Связи, задающие угловое положение головы относительно продольной и поперечной осей:

$$\begin{aligned} U_{xh} &= 0, \\ U_{yh} &= 0. \end{aligned}$$

Здесь U_{xh}, U_{yh} — углы поворота головы относительно продольной и поперечной осей соответственно

Связи, задающие поперечное расстояние от рук до корпуса:

$$\begin{aligned} S_{yk} - S_{yla} &= S_{ylp}, \\ S_{yk} - S_{yra} &= S_{yrp}. \end{aligned}$$

Здесь S_{yk} — поперечное смещение ц.м. корпуса, S_{yla}, S_{yra} — поперечное смещение ц.м. левой и правой рук, S_{ylp}, S_{yrp} — поперечное расстояние от левой и правой рук до ц.м. корпуса.

Связи, задающие вертикальное расстояние от рук до корпуса:

$$\begin{aligned} S_{zk} - S_{zla} &= S_{zlp}, \\ S_{zk} - S_{zra} &= S_{zrp}. \end{aligned}$$

Здесь S_{zk} — вертикальное смещение ц.м. корпуса, S_{zla}, S_{zra} — вертикальное смещение ц.м. левой и правой рук, S_{zlp}, S_{zrp} — вертикальное расстояние от левой и правой рук до ц.м. корпуса.

Расчетная схема робота, соответствующая его кинематике, содержит 22 тела, то есть 132 степени свободы. После наложения всех связей при расчете обратной задачи система (12) становится статической с нулевым числом степеней свободы, поскольку общее число уравнений связей равно числу степеней свободы свободной системы.

Для работы системы управления необходимо согласование нулевых положений углов приводов, что выполняется на вспомогательной модели робота, которая с помощью дополнительных упругих связей выставляется в положение, соответствующее конструктивным нулевым значениям датчиков углов поворота приводов.

Программно система управления роботом выполнена в виде дополнительных модулей системы моделирования ФРУНД, которая через программу сетевого интерфейса связана с сетью робота.

С помощью представленной системы управления были проведены эксперименты с движением робота AP600 (рисунки 10-12).

Система управления в режиме реального времени решает систему уравнений (12) со скоростью, достаточной для того, чтобы обеспечить частоту подачи сигналов управления 200 Гц (процессор Intel core i7).

Система управления позволяет выполнять различные типы движений: движение вперед и назад (рисунок 10); движение вбок (рисунок 11), движение вперед через ступеньку (рисунок 12). Реализована также возможность выполнения роботом наклонов при стоянии на месте.

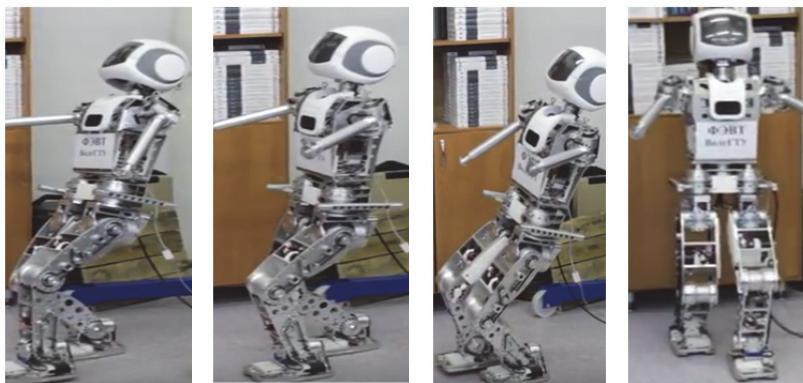


Рис. 10. Движение робота вперед

(URL: frund.vstu.ru/volggtu-robot-android-ar-600-21-marta-2016)

Эксперименты показали возможность длительного шагания робота в таком режиме и достаточно точное воспроизведение программного движения приводов (рисунок 13). Различие по параметрам абсолютного движения значительно больше (рисунки 14-16).

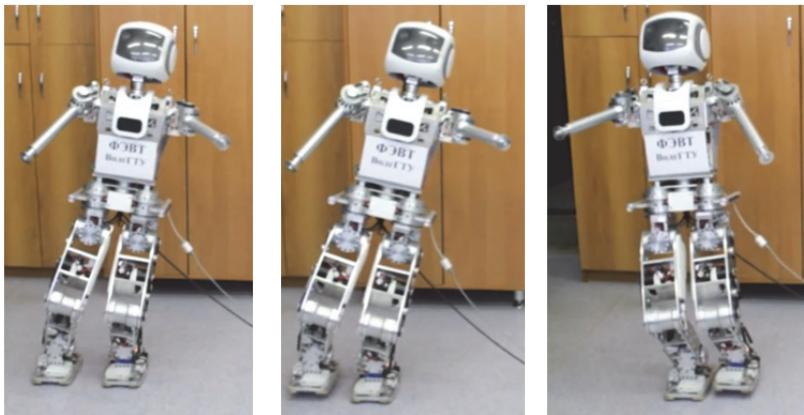


Рис. 11. Движение робота бок
(URL: <http://frund.vstu.ru/volggtu-robot-android-ar-600-22-marta-2016/>)



Рис. 12. Перешагивание робота через препятствие
(URL: frund.vstu.ru/volggtu-robot-android-ar-600-preodolevaet-stupen-16-marta-2016/)

Эксперименты показали возможность длительного шагания робота в таком режиме и достаточно точное воспроизведение программного движения приводов (рисунок 13). Различия по параметрам абсолютного движения значительно больше (рисунки 14–16).

На рисунке 13 показаны программные и измеренные углы поворота привода левого колена. Для ПИ регулятора этого привода коэффициент пропорционального звена составлял 2000, интегрального – 5 (в единицах системы управления приводами робота AP600). Из графиков видно, что максимальная погрешность управления составляла 3–5 %.

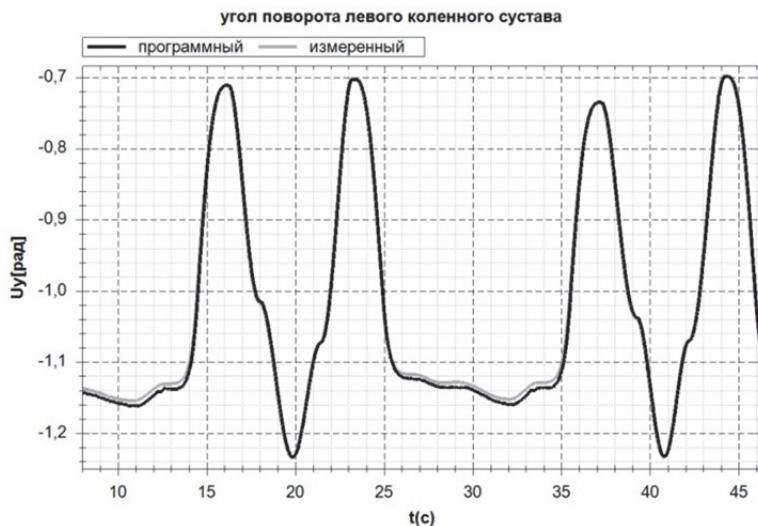


Рис. 13. Угол поворота коленного сустава при ходьбе

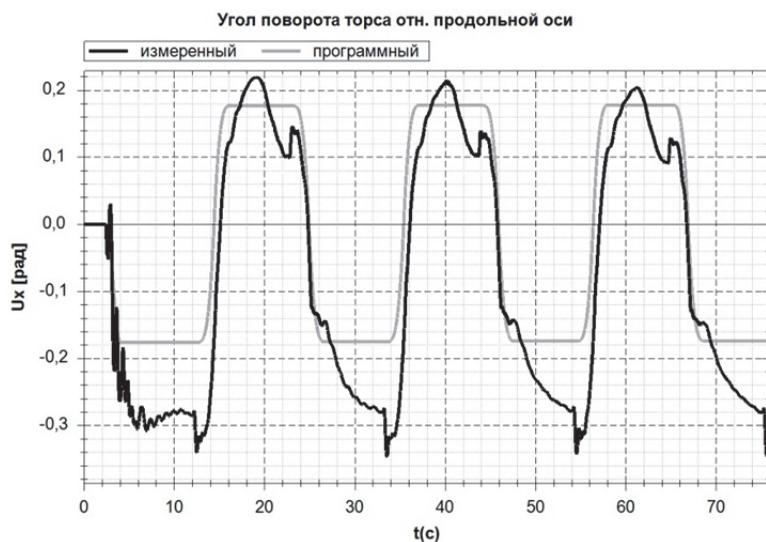


Рис. 14. Угол поворота торса относительно продольной оси

По углам поворота торса, на котором расположен гироскопический блок, погрешность управления значительно больше (рисунки 14-16).

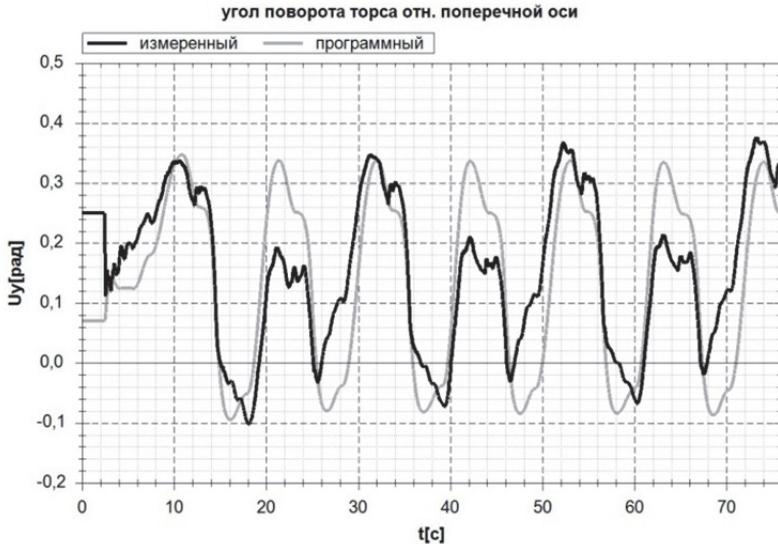


Рис. 15. Угол поворота торса относительно поперечной оси

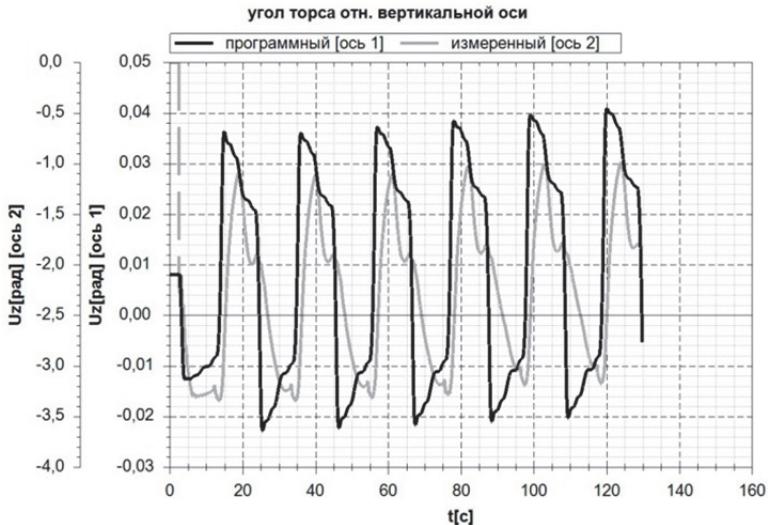


Рис. 16. Угол поворота торса относительно вертикальной оси

Погрешности в абсолютных перемещениях звеньев робота приводят к значительным ударным нагрузкам при постановке стоп (рисунки 17, 18).

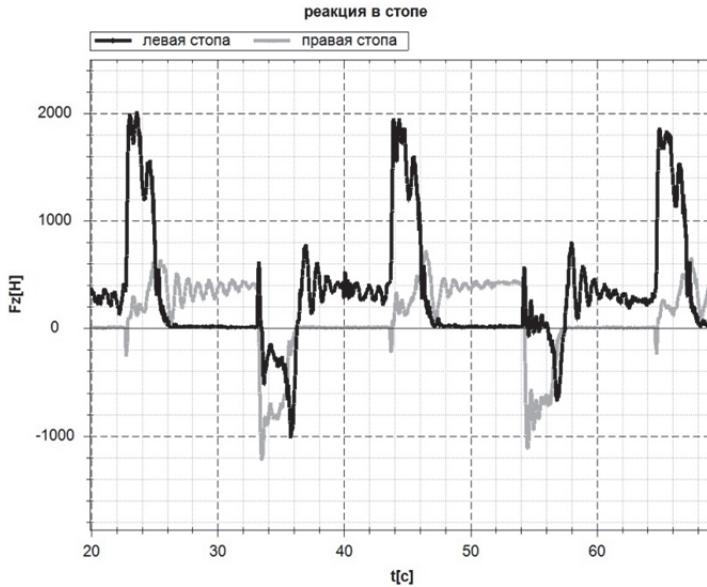


Рис. 17. Силы в стопах, боковые датчики

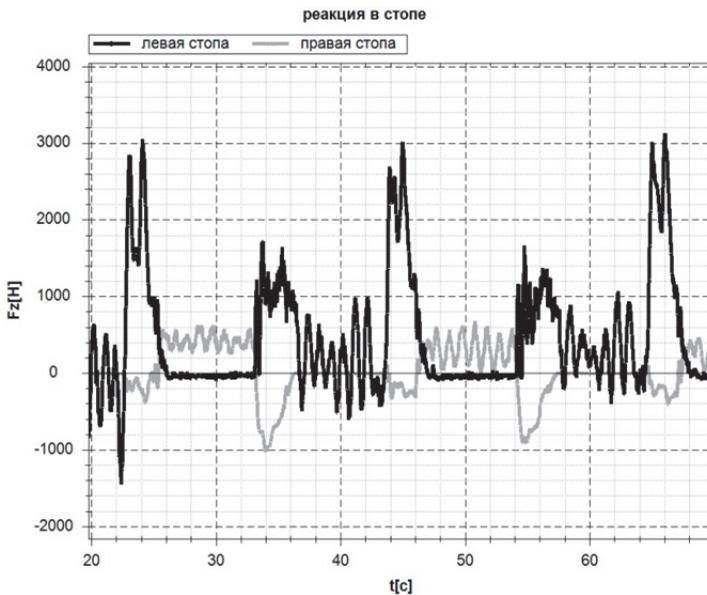


Рис. 18. Силы в стопах, продольные датчики

Робот обладает также низкой собственной частотой качания на стопе – порядка 1 Гц, период которой в 3-10 раз больше, чем у некоторых известных роботов [20, 23, 24]. Введение обратной связи по реакции стопы (контур демпфирования на рисунке 2) не привело к существенному уменьшению таких колебаний.

Увеличение скорости движения в квазистатическом режиме было ограничено силовыми характеристиками приводов – в момент переноса происходило отключение приводов ног из-за ограничений по току.

Значительное расхождение абсолютных углов поворота можно объяснить погрешностями в геометрических и массово инерционных параметрах модели, а также податливостью звеньев робота. К геометрическим параметрам относятся нулевые положения датчиков углов приводов и координаты ц.м. звеньев. В силу конструктивных особенностей робота нулевое положение задается со значительной погрешностью. Массы и моменты инерции звеньев взяты приблизительно из условия достижения полной массы робота.

Достигнутая в экспериментах максимальная устойчивая скорость робота составляла 5 см/с. Такое значение сопоставимо с максимальными скоростями роботов, управление которых базируется на использовании уравнения обратного маятника. Однако предложенное управление применимо к существенно большему количеству типов движений робота, поскольку не связано с обязательной синхронизацией по периоду шага.

5. Заключение. Анализ математических моделей, используемых в методе обратной задачи в существующих системах управления роботами андроидами, показал, что для описания движения ТНМ используются упрощенные уравнения, не учитывающие инерционные составляющие и полную структуру робота, что может быть причиной погрешностей управления.

Сравнение кинематических схем двуногих роботов и методов управления ими установило, что все известные роботы андройды реализуют локомоцию ног, свойственную латеральному типу расположения конечностей, что выражается в походке на присогнутых коленях.

Предложенные алгоритмы планировщика походки на основе связанного формирования кинематических параметров стоп, корпуса и ТНМ робота позволяют реализовать квазистатические режимы движения робота андроида различных типов — вперед, назад, вбок, шагание по ступенькам, наклоны и так далее. Принципы управления на основе использования точных квазистатических уравнений, связывающих координаты ТНМ с координатами звеньев робота, дают

возможность синтезировать значительно более широкий круг движений робота, чем методы на основе уравнения обратного маятника. При этом допускается произвольное движение всех звеньев робота, например, рук, что позволяет планировать выполнение роботом полезных операций. Предложенный подход допускает широкое варьирование параметров шага — высоты и длины, что важно для достижения высокой проходимости шагающих машин как их главного преимущества.

Разработанная система управления является удобным средством экспериментальной доводки аппаратной и программной части робота для улучшения его технических характеристик, а также может быть использована в качестве базовой платформы для двуногого робота с полезными функциональными возможностями как прототипа коммерческого образца.

Литература

1. *Nelson G. et al.* Petman: A humanoid robot for testing chemical protective clothing // Journal of the Robotics Society of Japan. 2012. vol. 30. no. 4. pp. 372–377.
2. *Kim J.Y., Yang U.J.* Mechanical design of powered prosthetic leg and walking pattern generation based on motion capture data // Advanced Robotics. 2015. vol. 29. no. 16. pp. 1061–1079.
3. *Zhao J. et al.* Design of variable-damping control for prosthetic knee based on a simulated biped // 2013 IEEE International Conference on Rehabilitation Robotics (ICORR). 2013. pp. 1–6.
4. *Abdolshah S., Abdolshah M., Tang S.H.* Trajectory Planning and Walking Pattern Generation of Humanoid Robot Motion // International Journal of Robotics and Automation (IAES). 2015. vol. 4. no. 2. pp. 135–142.
5. *Liatsikos E. et al.* Setup of da Vinci System for Kidney Surgery // Laparoscopic and Robot-Assisted Surgery in Urology: Atlas of Standart Procedures. 2011. pp. 32–36.
6. *Лавровский Э.К., Письменная Е.В., Комаро П.А.* Управление ходьбой экзоскелетона нижних конечностей при вязкоупругой связи его с телом человека-оператора // Мехатроника, автоматизация, управление. 2015. Т. 16. № 2. С. 96–100.
7. *Крутько П.Д.* Обратные задачи динамики управляемых систем. Нелинейные модели // М.: Наука. 1988. 328 с.
8. *Vukobratovic M. et al.* Biped locomotion – Dynamics, Stability, Control and Application // Springer-Verlag. 1990. vol. 7. 349 p.
9. *Белецкий В.В.* Двуногая ходьба // М.: Наука. 1984. 286 с.
10. *Формальский А.М.* Перемещение антропоморфных механизмов // М.: Наука. 1984. 368 с.
11. *Горобцов А.С., Карцов С.К., Плетнев А.Е., Поляков Ю.А.* Компьютерные методы построения и исследования математических моделей динамики конструкций автомобилей: монография // М.: Машиностроение. 2011. 462 с.
12. *Raibert M.H.* Legged Robots // Communications of the ACM. 1986. vol. 29. no. 6. pp. 250.
13. *Горобцов А.С.* Синтез параметров управляемого движения многозвенных механических систем произвольной структуры методом обратной задачи // Мехатроника, автоматизация, управление. 2004. № 6. С. 43–50.

14. *Yamaguchi J., Kinoshita N., Takanishi A., Kato I.* Development of a biped walking robot adapting to the human's living floor // Proceedings of the 1996 IEEE International Conference on Robotics & Automation. 1996. pp. 232–239.
15. *Mann G.* Stability Control in an Actively-Balanced Bipedal Robot // Proceedings of the Australian Conference on Robotics and Automation. 2000. pp. 191–195.
16. *Yirose M., Ogawa K.* Honda Humanoid Robot Development // Philosophical transactions of the Royal Society A: Mathematical, physical, and engineering sciences. 2007. pp. 11–19.
17. *Kim J.Y., Park I.W., Oh J.H.* Experimental realization of dynamic walking of the biped humanoid robot KHR-2 using zero moment point feedback and inertial measurement // Advanced Robotics. 2006. vol. 20. no. 6. pp. 707–736.
18. *Kim J.H., Oh J.H.* Realization of dynamic walking for the humanoid robot platform KHR-1 // Advanced Robotics. 2004. vol. 18. no. 7. pp. 749–768.
19. *Kim J.Y., Park I.W., Oh J.H.* Walking Control Algorithm of Biped Humanoid Robot on Uneven and Inclined Floor // Journal of Intelligent & Robotic Systems. 2007. vol. 48. no. 4. pp. 457–484.
20. *Park I.W., Kim J.Y., Oh J.H.* Online Walking Pattern Generation and Its Application to a Biped Humanoid Robot – KHR-3 (HUBO) // Advanced Robotics. 2008. vol. 22. no. 2-3. pp. 159–190.
21. *Kim J.Y., Kim J.H.* Error Analysis and Effective Adjustment of the Walking-Ready Posture for a Biped Humanoid Robot // Advanced Robotics. 2010. vol. 24. pp. 2137–2169.
22. *Pinto C.M.A., Machado J.A.T.* Fractional central pattern generators for bipedal locomotion // Nonlinear Dynamics. 2010. vol. 62. no. 1-2. pp. 27–37.
23. *Di Gironimo G. et al.* Biomechanically-based motion control for a digital human // International Journal on Interactive Design and Manufacturing (IJIDeM). 2012. vol. 6. no. 1. pp. 1–13.
24. *Kim J.Y., Lee J., Oh J.H.* Experimental realization of dynamic walking for a human-riding biped robot, HUBO FX-1 // Advanced Robotics. 2007. vol. 21. no. 3-4. pp. 461–484.
25. *Engelsberger J. et al.* Overview of the torque-controlled humanoid robot TORO // Proceedings of IEEE-RAS International Conference on Humanoid Robots. 2014. pp. 916 – 923.
26. *Engelsberger J., Ott C., Albu-Schaëffer A.* Three-dimensional bipedal walking control using divergent component of motion // Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems. 2013. pp. 2600–2607.
27. *Pratt J., Carff J., Drakunov S., Goswami A.* Capture point: A step toward humanoid push recovery // Proceedings of IEEE-RAS International Conference On Humanoid Robots. 2006. pp. 200–207.
28. *Engelsberger J.* Trajectory generation for continuous leg forces during double support and heel-to-toe shift based on divergent component of motion // Proceedings of IEEE RSJ International Conference on Intelligent Robots and Systems. 2014. pp. 4022–4029.
29. *Khusainov R., Klimchik A., Magid E.* Swing leg trajectory optimization for a humanoid robot locomotion // Proceedings of the 13th International Conference on Informatics in Control, Automation and Robotics (ICINCO). 2016. pp. 130–141.
30. *Khusainov R., Shimchik I., Afanasyev I., Magid E.* Toward a human-like locomotion: modelling dynamically stable locomotion of an anthropomorphic robot in simulink environment // Proceedings of 12th International Conference on Informatics in Control, Automation and Robotics (ICINCO). 2015. pp. 141–148.
31. *Khusainov R., Sagitov A., Afanasyev I., Magid E.* Bipedal robot locomotion modelling with virtual height inverted pendulum and preview control approaches in Simulink

- environment // Journal of Robotics, Networking and Artificial Life. 2016. vol. 3. no 3. pp. 182–187.
32. *Khusainov R., Afanasyev I., Magid E.* Anthropomorphic robot modelling with virtual height inverted pendulum approach in Simulink: step length and period influence on walking stability // International Conference on Artificial Life and Robotics (ICAROB). 2016.
 33. *Liu C., Wang D., Chen Q.* Central pattern generator inspired control for adaptive walking of biped robots // IEEE Trans. Syst. Man Cybern. 2013. pp. 1206–1215.
 34. *Shafiq N., Abdolmaleki A., Lau N., Reis L.P.* Development of an Omnidirectional Walk Engine for Soccer Humanoid Robots // International Journal of Advanced Robotic Systems. 2015. 190 p.
 35. *Zhou C. et al.* Stabilization of bipedal walking based on compliance control // Autonomous Robots. 2016. vol. 40. no. 6. pp. 1041–1057.
 36. *Santos C.P., Alves N., Moreno J.C.* Biped Locomotion Control through a Biomimetic CPG-based Controller // Journal of Intelligent & Robotic Systems. 2017. vol. 85. no. 1. pp. 47–70.
 37. *Kobayashi T. et al.* Adaptive speed controller using swing leg motion for 3-D limit-cycle-based bipedal gait // Nonlinear Dynamics. 2016. vol. 84. no. 4. pp. 2285–2304.
 38. *Dallali H. et al.* On the use of positive feedback for improved torque control // Control Theory Tech. 2015. vol. 13. no. 3. pp. 266–285.
 39. *Sutyasadi P., Parnichkun M.* Gait Tracking Control of Quadruped Robot Using Differential Evolution Based Structure Specified Mixed Sensitivity Robust Control // Journal of Control Science and Engineering. 2016. 18 p.
 40. *Ijspeert A.J.* Central pattern generators for locomotion control in animals and robots: a review // Neural Networks. 2008. vol. 21. no. 4. pp. 642–653.
 41. *Ковальчук А.К., Кулаков Д.Б., Семенов С.Е.* Управление исполнительными системами двуногих шагающих роботов. Теория и алгоритмы // М.: Изд-во МГОУ. 2007. 160 с.
 42. *Duan Y. et al.* Benchmarking Deep Reinforcement Learning for Continuous Control // International Conference on Machine Learning. 2016. pp. 1329–1338.
 43. *Peters J., Schaal S.* Reinforcement learning of motor skills with policy gradients // Neural Networks. 2008. vol. 21. pp. 682–697.
 44. *Горобцов А.С., Климов С.Ю., Гетманский В.В.* Parallel Inverse Dynamics Method for Synthesis of Control Movement of Multidimensional Walking Robot // 2009 IEEE International Conference on Mechatronics and Automation (ICMA 2009). 2009. pp. 3169–3172.
 45. *Брискин Е.С., Вершинина И.П., Малолетов А.В., Шаронов Н.Г.* Об управлении движением шагающей машины со сдвоенными ортогонально-поворотными движителями // Известия РАН. Теория и системы управления. 2014. № 3. С. 168–176.

Горобцов Александр Сергеевич — д-р техн. наук, с.н.с., заведующий кафедрой высшей математики, Волгоградский государственный технический университет (ВолГТУ); главный научный сотрудник, Федеральное государственное бюджетное учреждение науки Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН). Область научных интересов: вычислительная механика, динамика машин, оптимальное управление в механических системах. Число научных публикаций — 200. vm@vstu.ru, www.frund/vstu.ru; пр. им. В.И. Ленина, 28, Волгоград, 400005, РФ; р.т.: +7(8442)24-84-87; факс: +7(8442)24-84-89.

Андреев Андрей Евгеньевич — к-т техн. наук, заведующий кафедрой электронно-вычислительных машин и сетей, Волгоградский государственный технический университет (ВолГТУ). Область научных интересов: высокопроизводительные

вычисления, вычислительная механика, динамика машин, оптимальное управление в механических системах Число научных публикаций – 140. Andan2005@yandex.ru, www.frund/vstu.ru; пр. им. В.И. Ленина, 28, Волгоград, 400005, РФ; р.т.: +7(8442)24-84-94; факс: +7(8442)24-84-89.

Марков Алексей Евгеньевич — магистрант кафедры электронно-вычислительных машин и систем факультета электроники и вычислительной техники, Волгоградский государственный технический университет (ВолгГТУ). Область научных интересов: управление антропоморфными роботами, применение, технология разработки программных комплексов для управления в робототехнике, компьютерное зрение. Число научных публикаций – 9. markovalex95@gmail.com; пр. им. В.И. Ленина, 28, Волгоград, 400005, РФ; р.т.: +7(919)983-0500.

Скориков Андрей Викторович — аспирант кафедры высшая математика факультета электроники и вычислительной техники, Волгоградский государственный технический университет (ВолгГТУ). Область научных интересов: управление антропоморфными роботами, применение, технология разработки программных комплексов для управления в робототехнике. Число научных публикаций — 10. scorpion_energy@mail.ru; пр. им. В.И. Ленина, 28, Волгоград, 400005, РФ; р.т.: +7(927)066-8164.

Тарасов Павел Сергеевич — аспирант кафедры высшая математика факультета электроники и вычислительной техники, Волгоградский государственный технический университет (ВолгГТУ). Область научных интересов: управление антропоморфными роботами, управление многозвенными робототехническими системами, применение, технология разработки программных комплексов для управления в робототехнике. Число научных публикаций — 25. tarasradio@mail.ru; пр. им. В.И. Ленина, 28, Волгоград, 400005, РФ; р.т.: +7(919)989-0240.

A.S. GOROBTSOV, A.E. ANDREEV, A.E. MARKOV, A.V. SKORIKOV,
P.S. TARASOV

**FEATURES OF SOLVING THE INVERSE DYNAMIC METHOD
EQUATIONS FOR THE SYNTHESIS OF STABLE WALKING
ROBOTS CONTROLLED MOTION**

Gorobtsov A.S., Andreev A.E., Markov A.E., Skorikov A.V., Tarasov P.S. **Features of Solving the Inverse Dynamic Method Equations for the Synthesis of Stable Walking Robots Controlled Motion.**

Abstract. The problem of walking robots controlled motion synthesis by the inverse dynamic method is considered. The inverse dynamic method equations are represented by the methods of multibody system dynamics as free bodies motion equations and constraint equations. The variety of constraint equations group are introduced to specify the robot gait, to implement the robot stability conditions and to coordinate specified robot links movement. The key feature of the inverse dynamic method equations in this formulation is the presence of the second derivatives of the system coordinates in the constraint equations expressing the stability conditions that ensure the maintenance of the vertical position by the robot. The determined solution of such equations in general case is impossible due to the uncertainty of the initial conditions for the Lagrange multipliers. An approximate method for solving the inverse dynamic without taking into account the inertial components in the constraint equations that determine the stability of the robot is considered. Constraint equations that determine the coordinate movement of individual robot links and required for unique problem solving based on approximate equations are presented. The implementation of program motion synthesis methods in the control system of the humanoid robot AR-600 is presented. The comparison of theoretical and experimental parameters of controlled motion is performed. It has been established that with the achieved high accuracy of the robot links tracking drives control with an error of several percent, the indicators of the robot's absolute movements, in particular, the angles of roll, yaw and pitch, differ from the programmed by 30-40%. It's shown that proposed method allows to synthesize robot control in quasistatic mode for different movement types such as moving forward, sideways, walking on stairs, inclinations etc.

Keywords: robotics, walking robots, control, humanoid robots, inverse dynamic, androids.

Gorobtsov Aleksander Sergeevich — Ph.D., Dr. Sci., senior researcher, head further mathematics department, Volgograd State Technical University (VSTU); chief researcher, Mechanical Engineering Research Institute of the Russian Academy of Sciences. Research interests: multibody systems dynamics, machinery dynamics, optimal control of mechanical systems. The number of publications – 200. vm@vstu.ru, www.frund/vstu.ru; 28, Lenin avenue, Volgograd, 400005, Russia; office phone: + 7(844)224-84-87, fax: + 7(844)224-84-89.

Andreev Andrey Evgenevich — Ph.D., head of Electronic Computing Machines and Systems Department of Faculty of Electronics and Computer Technology, Volgograd State Technical University (VSTU). Research interests: high performance computation, multibody systems dynamics, machinery dynamics, optimal control of mechanical systems. The number of publications – 140. adan2005@yandex.ru, www.frund/vstu.ru; 28, Lenin avenue, Volgograd, 400005, Russia; office phone: + 7(844)224-84-94, fax: + 7(844)224-84-89.

Markov Aleksey Evgenevich — Master Student of Electronic Computing Machines and Systems Department of Faculty of Electronics and Computer Technology, Volgograd State Technical University (VSTU). Research interests: humanoid robots control, software systems

development technology for control in robotics, computer vision. The number of publications – 9. markovalex95@gmail.com; 28, Lenin avenue, Volgograd, 400005, Russia; office phone: +7(919)983-0500.

Skorikov Andrey Viktorovich — Ph.D. Student of Electronic Computing Machines and Systems Department of Faculty of Electronics and Computer Technology, Volgograd State Technical University (VSTU). Research interests: humanoid robots control, software systems development technology for control in robotics. The number of publications – 10. scorpion_energy@mail.ru; 28, Lenin avenue, Volgograd, 400005, Russia; office phone: +7(927)066-8164.

Tarasov Pavel Sergeevich — Ph.D. Student of Electronic Computing Machines and Systems Department of Faculty of Electronics and Computer Technology, Volgograd State Technical University (VSTU). Research interests: humanoid robots control, multilink robotic systems control, software systems development technology for control in robotics. The number of publications – 25. tarasradio@mail.ru; 28, Lenin avenue, Volgograd, 400005, Russia; office phone: +7(919)989-0240.

References

1. Nelson G. et al. Petman: A humanoid robot for testing chemical protective clothing. *Journal of the Robotics Society of Japan*. 2012. vol. 30. no. 4. pp. 372–377.
2. Kim J.Y., Yang U.J. Mechanical design of powered prosthetic leg and walking pattern generation based on motion capture data. *Advanced Robotics*. 2015. vol. 29. no. 16. pp. 1061–1079.
3. Zhao J. et al. Design of variable-damping control for prosthetic knee based on a simulated biped. 2013 IEEE International Conference on Rehabilitation Robotics (ICORR). 2013. pp. 1–6.
4. Abdolshah S., Abdolshah M., Tang S.H. Trajectory Planning and Walking Pattern Generation of Humanoid Robot Motion. *International Journal of Robotics and Automation (IAES)*. 2015. vol. 4. no. 2. pp. 135–142.
5. Liatsikos E. et al. Setup of da Vinci System for Kidney Surgery. *Laparoscopic and Robot-Assisted Surgery in Urology: Atlas of Standart Procedures*. 2011. pp. 32–36.
6. Lavrovsky E., Pismennaya E., Komaro P. [Walking control of lower limbs exoskeleton with visco-elastic coupling with the body of the human operator]. *Mehatronika, avtomatizacija, upravljenje – Mechatronics, automation, control*. 2015. Issue 16. vol. 2. pp. 96–100. (In Russ.).
7. Krutko P. *Obratnii zadachi dinamiki upravlyayemih sistem* [Inverse dynamics problems of controlled systems]. Moscow: Nauka. 1988. 328 p. (In Russ.).
8. Vukobratovic M. et al. *Biped locomotion – Dynamics, Stability, Control and Application*. Springer-Verlag. 1990. vol. 7. 349 p.
9. Beletsky V. *Dvunogaja hodba* [Biped locomotion]. Moscow: Nauka. 1984. 286 p. (In Russ.).
10. Formalsky A. *Pepemeshhenie antropomorfnyh mekhanizmov* [The movement of anthropomorphic mechanisms]. Moscow: Nauka. 1984. 368 p. (In Russ.).
11. Gorobtsov A., Kartsov S., Pletnev A., Polyakov Ju. *Komp'yuternye metody postroenija i issledovanija matematicheskikh modelej dinamiki konstrukcij avtomobilej* [Computer methods for constructing and investigating mathematical models of vehicle dynamics dynamics]. Moscow: Mashinostroenie. 2011. 462 p. (In Russ.).
12. Raibert M. H. Legged Robots. *Communications of the ACM*. 1986. vol. 29. no. 6. pp. 250.

13. Gorobtsov A. [Controlled motion of multi-link mechanical systems of arbitrary structure by the inverse problem method parameters synthesis]. *Mehatronika, avtomatizacija, upravljenje – Mechatronics, automation, control*. 2004. vol. 6. pp. 45–50. (In Russ.).
14. Yamaguchi J., Kinoshita N., Takanishi A., Kato I. Development of a biped walking robot adapting to the human's living floor. Proceedings of the 1996 IEEE International Conference on Robotics & Automation. 1996. pp. 232–239.
15. Mann G. Stability Control in an Actively-Balanced Bipedal Robot. Proceedings of the Australian Conference on Robotics and Automation. 2000. pp. 191–195.
16. Yirose M., Ogawa K. Honda Humanoid Robot Development. *Philosophical transactions of the Royal Society A: Mathematical, physical, and engineering sciences*. 2007. pp. 11–19.
17. Kim J.Y., Park I.W., Oh J.H. Experimental realization of dynamic walking of the biped humanoid robot KHR-2 using zero moment point feedback and inertial measurement. *Advanced Robotics*. 2006. vol. 20. no. 6. pp. 707–736.
18. Kim J.H., Oh J.H. Realization of dynamic walking for the humanoid robot platform KHR-1. *Advanced Robotics*. 2004. vol. 18. no. 7. pp. 749–768.
19. Kim J.Y., Park I.W., Oh J.H. Walking Control Algorithm of Biped Humanoid Robot on Uneven and Inclined Floor. *Journal of Intelligent & Robotic Systems*. 2007. vol. 48. no. 4. pp. 457–484.
20. Park I.W., Kim J.Y., Oh J.H. Online Walking Pattern Generation and Its Application to a Biped Humanoid Robot – KHR-3 (HUBO). *Advanced Robotics*. 2008. vol. 22. no. 2-3. pp. 159–190.
21. Kim J.Y., Kim J.H. Error Analysis and Effective Adjustment of the Walking-Ready Posture for a Biped Humanoid Robot. *Advanced Robotics*. 2010. vol. 24. pp. 2137–2169.
22. Pinto C.M.A., Machado J.A.T. Fractional central pattern generators for bipedal locomotion. *Nonlinear Dynamics*. 2010. vol. 62. no. 1-2. pp. 27–37.
23. Di Gironimo G. et al. Biomechanically-based motion control for a digital human. *International Journal on Interactive Design and Manufacturing (IJIDeM)*. 2012. vol. 6. no. 1. pp. 1–13.
24. Kim J.Y., Lee J., Oh J.H. Experimental realization of dynamic walking for a human-riding biped robot, HUBO FX-1. *Advanced Robotics*. 2007. vol. 21. no. 3-4. pp. 461–484.
25. Engelsberger J. et al. Overview of the torque-controlled humanoid robot TORO. Proceedings of IEEE-RAS International Conference on Humanoid Robots. 2014. pp. 916 – 923.
26. Engelsberger J., Ott C., Albu-Schaëffer A. Three-dimensional bipedal walking control using divergent component of motion. Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems. 2013. pp. 2600–2607.
27. Pratt J., Carff J., Drakunov S., Goswami A. Capture point: A step toward humanoid push recovery. Proceedings of IEEE-RAS International Conference On Humanoid Robots. 2006. pp. 200–207.
28. Engelsberger J. Trajectory generation for continuous leg forces during double support and heel-to-toe shift based on divergent component of motion. Proceedings of IEEE RSJ International Conference on Intelligent Robots and Systems. 2014. pp. 4022–4029.
29. Khusainov R., Klimchik A., Magid E. Swing leg trajectory optimization for a humanoid robot locomotion. Proceedings of the 13th International Conference on Informatics in Control, Automation and Robotics (ICINCO). 2016. pp. 130–141.
30. Khusainov R., Shimchik I., Afanasyev I., Magid E. Toward a human-like locomotion: modelling dynamically stable locomotion of an anthropomorphic robot in simulink

- environment. Proceedings of 12th International Conference on Informatics in Control, Automation and Robotics (ICINCO). 2015. pp. 141–148.
31. Khusainov R., Sagitov A., Afanasyev I., Magid E. Bipedal robot locomotion modelling with virtual height inverted pendulum and preview control approaches in Simulink environment. *Journal of Robotics, Networking and Artificial Life*. 2016. vol. 3. no 3. pp. 182–187.
 32. Khusainov R., Afanasyev I., Magid E. Anthropomorphic robot modelling with virtual height inverted pendulum approach in Simulink: step length and period influence on walking stability. International Conference on Artificial Life and Robotics (ICAROB). 2016.
 33. Liu C., Wang D., Chen Q. Central pattern generator inspired control for adaptive walking of biped robots. *IEEE Trans. Syst. Man Cybern.* 2013. pp. 1206–1215.
 34. Shafii N., Abdolmaleki A., Lau N., Reis L.P. Development of an Omnidirectional Walk Engine for Soccer Humanoid Robots. *International Journal of Advanced Robotic Systems*. 2015. 190 p.
 35. Zhou C. et al. Stabilization of bipedal walking based on compliance control. *Autonomous Robots*. 2016. vol. 40. no. 6. pp. 1041–1057.
 36. Santos C.P., Alves N., Moreno J.C. Biped Locomotion Control through a Biomimetic CPG-based Controller. *Journal of Intelligent & Robotic Systems*. 2017. vol. 85. no. 1. pp. 47–70.
 37. Kobayashi T. et al. Adaptive speed controller using swing leg motion for 3-D limit-cycle-based bipedal gait. *Nonlinear Dynamics*. 2016. vol. 84. no. 4. pp. 2285–2304.
 38. Dallali H. et al. On the use of positive feedback for improved torque control. *Control Theory Tech.* 2015. vol. 13. no. 3. pp. 266–285.
 39. Sutyasadi P., Parnichkun M. Gait Tracking Control of Quadruped Robot Using Differential Evolution Based Structure Specified Mixed Sensitivity Robust Control. *Journal of Control Science and Engineering*. 2016. 18 p.
 40. Ijspeert A.J. Central pattern generators for locomotion control in animals and robots: a review. *Neural Networks*. 2008. vol. 21. no. 4. pp. 642–653.
 41. Kovalchuk A.K., Kulakov D.B., Semenov S.E. *Upravlenie ispolnitelnymi sistemami dvunogih shagajushchih robotov. Teorija i algoritmy* [Controlling the executive systems of bipedal walking robots. Theory and algorithms]. Moscow: MGOU Pub. 2007. 160 p. (In Russ.).
 42. Duan Y. et al. Benchmarking Deep Reinforcement Learning for Continuous Control. International Conference on Machine Learning. 2016. pp. 1329–1338.
 43. Peters J., Schaal S. Reinforcement learning of motor skills with policy gradients. *Neural Networks*. 2008. vol. 21. pp. 682–697.
 44. Gorobtsov A.S., Klimov S.Ju., Getmanskij V.V. Parallel Inverse Dynamics Method for Synthesis of Control Movement of Multidimensional Walking Robot. 2009 IEEE International Conference on Mechatronics and Automation (IEEE ICMA 2009) 2009. pp. 3169–3172.
 45. Briskin E., Vershina I., Maloletov A., Sharonov N. [On the control of the movement of a walking machine with dual orthogonal-rotary propulsors]. *Izvestija RAN. Teorija i sistemy upravlenija – Proceedings of the Russian Academy of Sciences. Theory and control systems*. 2014. vol. 3. pp. 168–176. (In Russ.).

В.И. ПЕТРЕНКО, Ф.Б. ТЕБУЕВА, М.М. ГУРЧИНСКИЙ,
В.О. АНТОНОВ, А.С. ПАВЛОВ
**ПРОГНОЗНАЯ ОЦЕНКА ТРАЕКТОРИИ РУКИ ОПЕРАТОРА
ДЛЯ РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ДИНАМИКИ ПРИ
КОПИРУЮЩЕМ УПРАВЛЕНИИ**

Петренко В.И., Тебуева Ф.Б., Гурчинский М.М., Антонов В.О., Павлов А.С. **Прогнозная оценка траектории руки оператора для решения обратной задачи динамики при копирующем управлении.**

Аннотация. Одной из важнейших задач современной робототехники является разработка роботов для выполнения рутинных, вредных и опасных видов работ без непосредственного участия человека. Несмотря на активное развитие технологий искусственного интеллекта, на данный момент робототехнические системы не способны заменить человека при решении сложных задач в динамической среде. Наиболее перспективными для применения в ближайшее время являются роботы, реализующие копирующий тип управления, или так называемое виртуальное присутствие оператора. Принцип копирующего управления построен на захвате движения удаленно находящегося оператора и формировании управляющих сигналов для приводов робота. Для управления приводами могут использоваться следящие системы или системы на основе планирования движения. Следящие системы более просты, однако системы на основе планирования движения позволяют добиться большей плавности движения и меньшего износа деталей объекта управления. Для реализации управления на основе планирования движения вводится искусственная задержка между движениями оператора и объекта управления для накопления необходимых данных.

Цель исследования — устранение задержки, возникающей при управлении приводами антропоморфного манипулятора на основе решения обратной задачи динамики при копирующем типе управления в масштабе реального времени. Предлагается использовать для планирования движения не измеренные, а прогнозные значения обобщенных координат руки оператора. На основе измеренных значений обобщенных координат руки оператора формируются временные ряды и выполняется их прогнозирование. Прогнозные значения обобщенных координат используются при планировании траектории движения антропоморфного манипулятора и решении обратной задачи динамики. Прогнозирование осуществляется методом линейной регрессии, имеющим относительно малую вычислительную сложность, что является важным критерием для работы системы в масштабе реального времени.

Разработанный математический аппарат позволяет на основе параметров прогнозирования и максимальных допустимых ускорений движения приводов манипулятора найти теоретическую оценку пределов значений ошибки прогнозирования траектории движения руки оператора при использовании предлагаемого подхода для конкретных задач.

Проведенная программная симуляция в среде Matlab подтвердила адекватность полученной теоретической оценки максимального значения ошибки прогнозирования, а также перспективность предлагаемого подхода для проверки на практике.

Ключевые слова: прогнозирование; обратная задача динамики; захват движения; антропоморфный манипулятор; копирующий тип управления; траектория движения руки оператора; виртуальное присутствие.

1. Введение. Огромный интерес для разработчиков робототехнических комплексов представляют интенсивно

развивающиеся безлюдные технологии. Концепция безлюдных технологий заключается в применении роботов для выполнения рутинных, вредных и опасных видов работ без непосредственного участия человека. Автоматизация является залогом безопасности и высокой эффективности решения поставленных задач [1, 2].

Одним из важнейших направлений, развиваемых в рамках безлюдных технологий, являются антропоморфные роботы. Антропоморфные роботы универсальны, так как с физиологической точки зрения обладают функциональностью, наиболее близкой к человеческой. Подобные роботы предназначены в первую очередь для работы в условиях человекоориентированной среды, например в составе космических миссий [3-6]. Наиболее известными антропоморфными роботами, позволяющими выполнять работы в опасных условиях, являются робот Robonaut 2 [5], и российский робот FEDOR, разрабатываемый для выполнения аварийно-спасательных операций на земле и в космосе [6]. Антропоморфные роботы могут работать в различных режимах управления: автоматическом, супервизорном и копирующем.

Автоматическое управление подразумевает полностью самостоятельные действия робота, то есть автономию при принятии решений. Несмотря на активные исследования в области искусственного интеллекта и разработки автономных роботов [7, 8], роботы пока не способны полностью заменить человека при выполнении сложных задач в динамической среде.

Супервизорное управление подразумевает постановку задачи оператором и ее самостоятельное выполнение роботом [9, 10]. При этом используются методы автоматического управления на уровне исполнения решений [11]. В таком режиме могут решаться только штатные задачи, требующие небольшой адаптации под конкретные условия.

На данном этапе развития науки и техники полностью заменить человека при выполнении сложных задач в динамической среде могут только роботы, реализующие удаленное присутствие оператора путем использования копирующего типа управления. В режиме копирующего управления робот повторяет действия оператора, то есть реализуется технология телеоперации, или так называемого удаленного присутствия [12-16].

В настоящей статье рассматривается частная задача удаленного присутствия — управление приводами антропоморфного манипулятора. Для управления приводами манипулятора при копирующем типе управления применяются два подхода.

Первый подход заключается в использовании следящих систем, в которых значение управляющего сигнала зависит от рассогласования

между целевым значением обобщенной координаты манипулятора и реальным значением, измеренным с помощью соответствующих датчиков [17]. Общие сведения о подобных системах приведены в работах [18-19]. Несмотря на простоту реализации и надежность подобных систем, при больших скоростях движения манипулятора вследствие негладкости его движения возникают различные механические вибрации, снижающие точность управления и увеличивающие износ деталей [20]. Поэтому для выполнения сложных работ в экстремальных условиях, когда необходимо выполнение целевых операций на максимальной скорости, становится актуальной проблема повышения точности копирования и снижения износа деталей манипулятора.

Второй подход заключается в предварительном планировании траектории движения манипулятора и расчете необходимых усилий в приводах манипулятора путем решения обратной задачи динамики на основе точной динамической модели манипулятора. Такой подход применяется в мощных манипуляторах, для которых возникновение механических вибраций вследствие негладкости движения может привести к выходу манипулятора из строя [20]. Различные методы решения обратной задачи динамики для этого случая предложены в [21-25]. В [24] рассматривается решение обратной задачи динамики для избыточных манипуляторов, к которым относятся и антропоморфные. Для ускорения решения обратной задачи динамики используют методы параллельных вычислений [25], требующие дополнительных ресурсов.

Второй подход применим, когда законы движения манипулятора по обобщенным координатам заранее известны. В случае же копирующего типа управления законы изменения обобщенных координат формируются в процессе движения в реальном масштабе времени. В условиях неопределенности траектории движения руки оператора может быть внесена искусственная задержка между движениями оператора и манипулятора, в течение которой происходит накопление измеренных значений обобщенных координат руки оператора. Затем на основе накопленных данных на некотором интервале времени система управления манипулятором может осуществить планирование движения и решение обратной задачи динамики для выполнения плавного и точного движения. При работе в экстремальных условиях на максимальных скоростях задержка, возникающая между движениями оператора и движениями манипулятора, может помешать качественному выполнению целевых операций. Таким образом, оба подхода к управлению приводами манипулятора при реализации удаленного присутствия имеют свои

преимущества и недостатки. В данной статье описывается развитие второго подхода путем использования прогнозной оценки траектории движения руки оператора.

2. Материалы и методы. Рассмотрим прогнозирование траектории движения руки оператора на основе обобщенных координат. Данные координаты могут быть непосредственно измерены с помощью задающего устройства в виде экзоскелета [12, 13] либо получены путем захвата движения узловых точек руки оператора с помощью оптических [27], инерционных [28] или магнитных [29] датчиков с последующим решением обратной задачи кинематики.

Пусть задающим устройством используется кинематическая модель руки оператора с m степенями подвижности. Пример такой модели с $m = 7$ степенями подвижности приведен на рисунке 1.

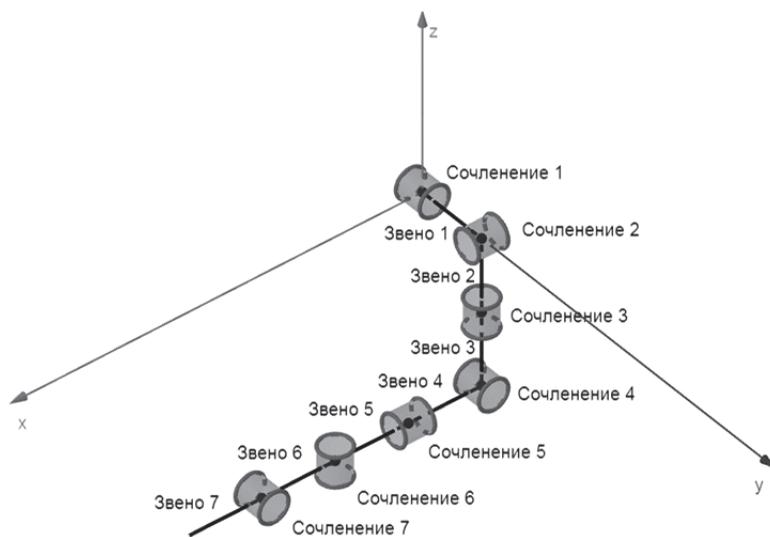


Рис. 1. Кинематическая модель руки оператора с семью степенями подвижности

Входными данными для прогнозирования являются m временных рядов измеренных значений обобщенных координат руки оператора. Для простоты изложения будем рассматривать произвольную обобщенную координату руки оператора. Приводимые рассуждения могут быть распространены на любое число обобщенных координат.

Суть предлагаемого подхода заключается в следующем. Пусть в момент времени t_0 наступает начало очередного цикла планирования

траектории движения руки оператора для решения обратной задачи динамики. Так как планирование траектории согласно предлагаемому подходу выполняется на основе прогнозных значений, длительность каждого подобного цикла планирования равна дальности прогнозирования τ_1 (рисунок 2).

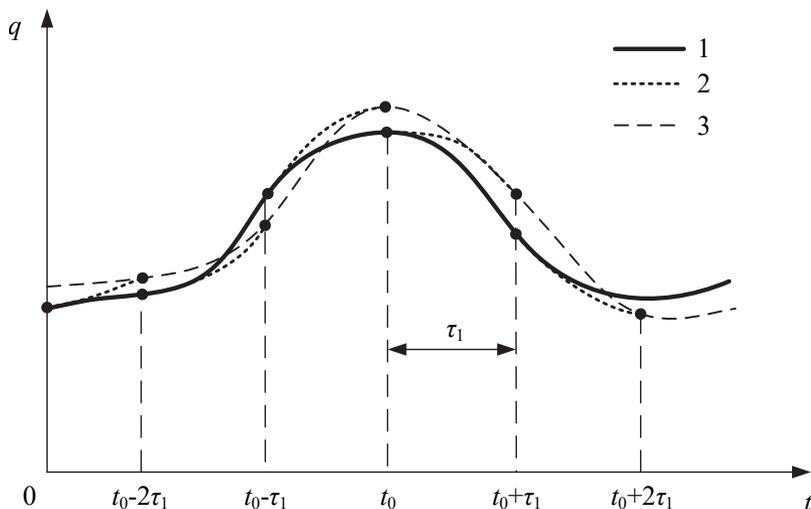


Рис. 2. Траектории движения: 1) руки оператора; 2) прогнозная оценка траектории движения руки оператора; 3) антропоморфного манипулятора

Входными данными является временной ряд $Q = \langle q_i \rangle$ измеренных значений обобщенной координаты q в моменты времени t_i до момента t_0 включительно. Вопросы влияния погрешности измерений на результаты прогнозирования выходят за рамки данной статьи, поэтому будем считать погрешность измерения несущественной. Также известны значения скорости и ускорения обобщенных координат манипулятора в момент t_0 , измеренные с помощью датчиков или найденные косвенным образом (например, с помощью численного дифференцирования / интегрирования). В общем случае текущие значения обобщенных координат манипулятора не совпадают с измеренными значениями обобщенных координат руки оператора, вследствие погрешности следования манипулятора по заданной траектории или ошибки прогнозирования на прошлой итерации для интервала $[t_0 - \tau_1, t_0]$.

Согласно предлагаемому подходу для каждой обобщенной координаты выполняется прогнозирование значений на основе известных элементов временного ряда на дальность прогнозирования τ_1 . Для движения манипулятора выполняется планирование траектории и решение обратной задачи динамики, исходя из условий гладкого перехода из текущей траектории в прогнозную траекторию движения (рисунок 2). Далее осуществляется движение манипулятора на основе решения обратной задачи динамики в течение спрогнозированного интервала времени τ_1 . Затем цикл прогнозирования повторяется.

Временной ряд $Q = \langle q_i \rangle$ является дискретизацией непрерывной функции изменения обобщенной координаты $q(t)$ руки оператора. Поэтому прогнозирование значений обобщенных координат может быть выполнено с использованием трендовых моделей, представляющих собой построение линейной или нелинейной регрессии методом наименьших квадратов.

В статье рассматривается наиболее простой случай — прогнозирование на основе линейной регрессии. При рассмотрении на достаточно малой дальности прогнозирования τ_1 движение руки оператора по обобщенным координатам является практически линейным. В то же время построение линейной регрессии имеет относительно малую временную вычислительную сложность. Поэтому в статье приводится анализ возможности использования линейной регрессии, а также границ ее применимости. Актуальность использования нелинейной регрессии и перечень необходимых для этого дополнительных данных приводятся в разделе «Обсуждение». Для нахождения границ применимости линейной регрессии в качестве способа для прогнозирования в данном разделе проводится теоретическая оценка верхней границы ошибки прогнозирования и далее выполняется проверка полученных выкладок с помощью программной симуляции.

Условимся понимать под ошибкой прогнозирования абсолютную величину разности между прогнозным и реальным значениями обобщенной координаты. Найдем зависимость верхней оценки ошибки прогнозирования Δq_1 от дальности прогнозирования τ_1 . Функция линейной регрессии значений обобщенной координаты руки оператора $q(t)$ может быть найдена с помощью метода наименьших квадратов на основе k последних известных элементов временного ряда Q :

$$\hat{q}(t) = et + f;$$

$$e = \frac{k \sum_{i=1}^k t_i q_i - \sum_{i=1}^k t_i \sum_{i=1}^k q_i}{k \sum_{i=1}^k t_i^2 - \left(\sum_{i=1}^k t_i \right)^2};$$

$$f = \frac{\sum_{i=1}^k q_i - e \sum_{i=1}^k t_i}{k},$$
(1)

где $\hat{q}(t)$ — прогнозные значения рассматриваемой обобщённой координаты; e и f — коэффициенты линейной регрессии.

Очевидно, что значения коэффициентов линейной регрессии e и f зависят от закона изменения обобщённой координаты руки оператора $q(t)$ и периода дискретизации измерений Δt .

Рассмотрим граничный случай, когда $\Delta t \rightarrow 0$, а $k = 2$, то есть когда линия линейной регрессии является касательной к графику зависимости $q(t)$ обобщённых координат руки оператора от времени t .

Чтобы манипулятор мог двигаться синхронно с рукой оператора, значения скорости и ускорения обобщённых координат не должны превышать максимально допустимых значений, которые могут развивать приводы манипулятора. Таким образом, прогнозирование может быть использовано для устранения задержки только в тех случаях, когда при движении руки оператора выполняются следующие условия:

$$q_{\min} \leq q(t) \leq q_{\max};$$
(2)

$$|\dot{q}(t)| \leq v_{\max};$$
(3)

$$|\ddot{q}(t)| \leq a_{\max},$$
(4)

где q_{\min} и q_{\max} — конструктивные ограничения, накладываемые на минимальное и максимальное значение обобщённой координаты, соответственно; v_{\max} — максимальное допустимое значение скорости изменения обобщённой координаты; a_{\max} — максимальное допустимое значение ускорения изменения обобщённой координаты.

Уравнение линейной регрессии, составленное для обобщённой координаты, описывает равномерное движение. Максимальное отклонение прогнозных значений от реальных будет

наблюдаться при движении руки оператора с максимальным ускорением. Для нахождения верхней оценки ошибки прогнозирования в качестве закона изменения рассматриваемой обобщенной координаты может быть выбрано движение с максимальным по абсолютному значению, а значит постоянным ускорением. Такое движение описывается уравнением:

$$q(t) = at^2 + bt + c, \quad (5)$$

где a , b и c — коэффициенты квадратного трехчлена, моделирующего равноускоренное движение.

Для определенности примем, что движение осуществляется с максимальным по абсолютному значению и положительным ускорением. Тогда в момент времени t_0 выполняются следующие условия:

$$\begin{aligned} q(t_0) &= at_0^2 + bt_0 + c = \hat{q}(t_0) = e(t_0)t_0 + f(t_0), \\ \dot{q}(t_0) &= 2at_0 + b = \dot{\hat{q}}(t_0) = e(t_0). \end{aligned} \quad (6)$$

Первое уравнение в (6) следует из условия непрерывности движения руки оператора, второе — из геометрического смысла касательной, которая совпадает с линией регрессии.

В силу того, что ускорение движения руки оператора положительно, график движения является выпуклым вниз и величина ошибки прогнозирования может быть найдена как разность между измеренным значением обобщенной координаты руки оператора и ее прогнозным значением в момент $t_0 + \tau_1$:

$$\begin{aligned} \Delta q_1(t_0, \tau_1) &= q(t_0 + \tau_1) - \hat{q}(t_0 + \tau_1) = \\ &= a(t_0 + \tau_1)^2 + b(t_0 + \tau_1) + c - e(t_0)(t_0 + \tau_1) - f(t_0) = a\tau_1^2, \end{aligned} \quad (7)$$

где $\Delta q_1(t_0, \tau_1)$ — зависимость величины ошибки прогнозирования от момента выполнения прогнозирования t_0 и дальности прогнозирования τ_1 .

Коэффициент a в уравнении (5) может быть найден из условия движения с максимальным ускорением:

$$\begin{aligned} \ddot{q}(t) &= 2a = a_{max}, \\ a &= \frac{a_{max}}{2}. \end{aligned} \quad (8)$$

Таким образом, независимо от конкретной формы графика закона движения руки оператора по рассматриваемой обобщенной координате, величина ошибки прогнозирования для дальности прогнозирования τ_1 будет лежать в диапазоне:

$$\Delta q_1(\tau_1) \in \left[-\frac{a_{\max} \tau_1^2}{2}; \frac{a_{\max} \tau_1^2}{2} \right]. \quad (9)$$

Выражение (9) позволяет теоретически оценить применимость линейной регрессии исходя из величины максимально допустимого ускорения и необходимой дальности прогнозирования для условий конкретной задачи.

Полученная величина погрешности найдена для идеальной касательной, проведенной к графику закона движения в момент выполнения прогнозирования. При работе в реальных условиях данная касательная не может быть найдена точно вследствие погрешностей и дискретности измерений. Найдем верхнюю оценку величины ошибки прогнозирования с учетом того, что линия регрессии, построенная на реальных значениях, не совпадает с касательной, проведенной к закону движения в момент времени t_0 .

Для реализации непрерывности движения наложим на линию регрессии условие ее прохождения через последнюю известную точку временного ряда Q . Аналогично предыдущему идеализированному случаю наибольшая разность между реальным и прогнозным значениями обобщенной координаты будет наблюдаться при движении с максимальным ускорением, описываемым уравнением (5). В таком случае линия регрессии будет лежать между идеализированной касательной, рассмотренной выше, и секущей, проведенной через первую и последнюю точки подмножества элементов временного ряда, участвующих в формировании уравнения регрессии (рисунок 3). Для нахождения верхней оценки ошибки прогнозирования в качестве линии регрессии будем рассматривать ее граничное положение, соответствующее секущей, приведенной на рисунке 3. Данный случай соответствует количеству элементов $k=2$ в выборке для построения регрессии и ненулевому периоду дискретизации измерений $\Delta t \neq 0$.

Уравнение касательной, проведенной к графику закона движения руки оператора в точке t_0 , имеет вид:

$$\begin{aligned}\hat{q}(t_0, t) &= e(t_0)t + f(t_0); \\ e(t_0) &= 2at_0 + b; \\ f(t_0) &= -at_0^2 + c,\end{aligned}\quad (10)$$

где $\hat{q}(t_0, t)$ — линия прогнозных значений, соответствующая касательной, проведенной к графику закона движения в момент времени t_0 ; $e(t_0)$ и $f(t_0)$ — коэффициенты касательной; a , b и c — коэффициенты закона движения в уравнении (5).

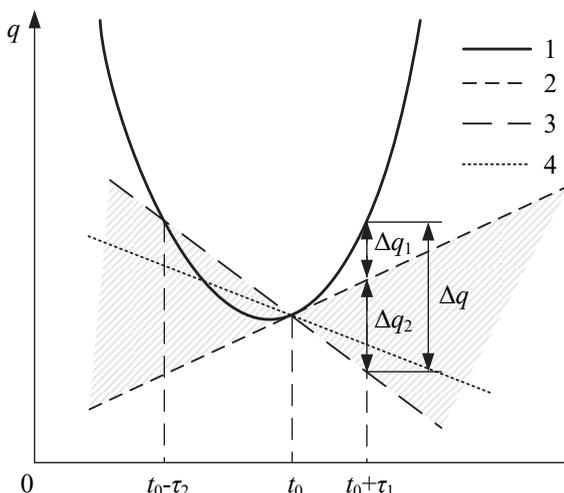


Рис. 3. Область возможного расположения линии регрессии: 1) закон движения руки оператора; 2) касательная к закону движения, проведенная в момент t_0 ; 3) секущая, проведенная через первую и последнюю точку выборки, участвующей в формировании линии регрессии; 4) линия регрессии

Уравнение секущей может быть найдено следующим образом:

$$\begin{aligned}q_s(t_0, \tau_2, t) &= p(t_0, \tau_2)t + l(t_0, \tau_2); \\ p(t_0, \tau_2) &= \frac{q(t_0) - q(t_0 - \tau_2)}{\tau_2} = \frac{2at_0\tau_2 - a\tau_2^2 + b\tau_2}{\tau_2} = 2at_0 - a\tau_2 + b; \\ l(t_0, \tau_2) &= q(t_0) - p(t_0, \tau_2)t_0 = -at_0^2 + a\tau_2 t_0 + c,\end{aligned}\quad (11)$$

где $q_s(t_0, \tau_2, t)$ — уравнение секущей; $p(t_0, \tau_2)$ и $l(t_0, \tau_2)$ — коэффициенты уравнения секущей; τ_2 — длительность интервала

времени между первым и последним измерениями в выборке для построения регрессии (рисунок 3).

Величина разности между прогнозными значениями при прогнозировании с помощью касательной и секущей линий для дальности прогнозирования τ_1 составит:

$$\begin{aligned} \Delta q_2(t_0, \tau_1, \tau_2) &= e(t_0)(t_0 + \tau_1) + f(t_0) - \\ &- p(t_0, \tau_2)(t_0 + \tau_1) + l(t_0, \tau_2) = a\tau_1\tau_2, \end{aligned} \quad (12)$$

где $\Delta q_2(t_0, \tau_1, \tau_2)$ — зависимость величины ошибки прогнозирования от момента выполнения прогнозирования t_0 , дальности прогнозирования τ_1 и длительности интервала времени между первым и последним измерениями в выборке для построения регрессии τ_2 .

Верхняя оценка полного значения ошибки прогнозирования может быть вычислена как сумма ошибок прогнозирования, найденных с помощью формул (7) и (12):

$$\begin{aligned} \Delta q(t_0, \tau_1, \tau_2) &= \Delta q_1(t_0, \tau_1) + \Delta q_2(t_0, \tau_1, \tau_2) = \\ &= a\tau_1^2 + a\tau_1\tau_2 = a(\tau_1^2 + \tau_1\tau_2). \end{aligned} \quad (13)$$

Путем выбора значений параметров a , τ_1 и τ_2 можно добиться компромисса между требуемым ускорением движения и допустимой ошибкой прогнозирования. В разделе «Результаты» показано, что данная оценка завышена и при применении линейной регрессии к реальному движению величина ошибки прогнозирования в разы меньше.

3. Результаты. Для оценки эффективности предложенного подхода к решению обратной задачи динамики с использованием прогнозной оценки траектории движения руки оператора была разработана имитационная модель в среде Matlab/Simulink с применением библиотеки Simscape Multibody. Имитационная модель включает в себя антропоморфный манипулятор с $m = 7$ степенями подвижности и сферический целевой предмет, расположенный за прямоугольным препятствием на краю стола. Манипулятор является моделью руки оператора, необходимой для получения тестовых законов движения по обобщенным координатам. Полученные законы движения используются в качестве входных данных для программной симуляции работы предложенного подхода. Задачей движения является взятие целевого предмета в обход препятствия. Раскадровка движения модели руки оператора приведена на рисунке 4.

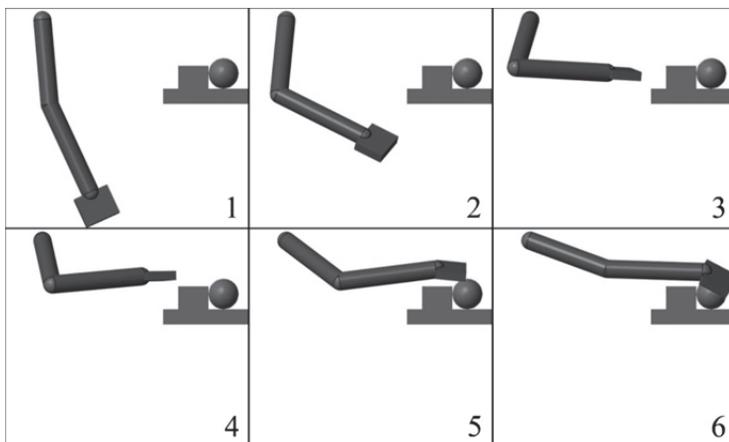


Рис. 4. Раскадровка движения модели руки оператора при выполнении целевой операции

Для получения законов движения руки оператора найдены промежуточные положения, через которые должна пройти рука оператора при выполнении целевой операции. Затем с помощью интерполяции кубическими сплайнами получены законы движения по всем степеням подвижности, представленные на рисунке 5.

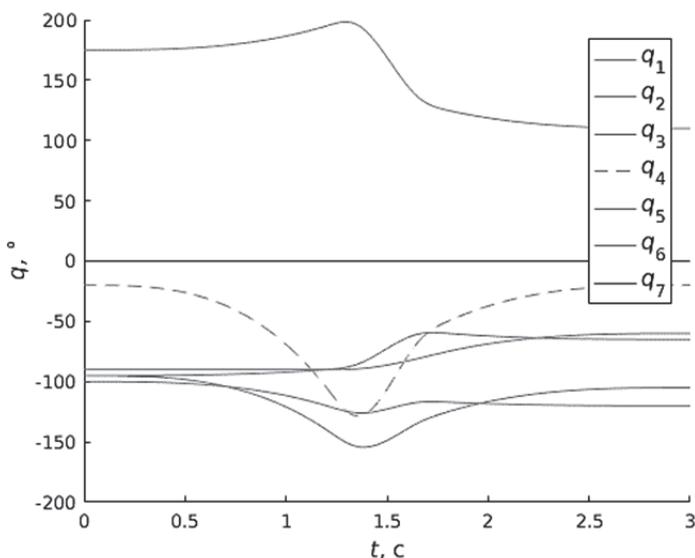


Рис. 5. Законы движения руки оператора по обобщенным координатам

Скорости и ускорения изменения обобщенных координат приведены на рисунках 6 и 7 соответственно.

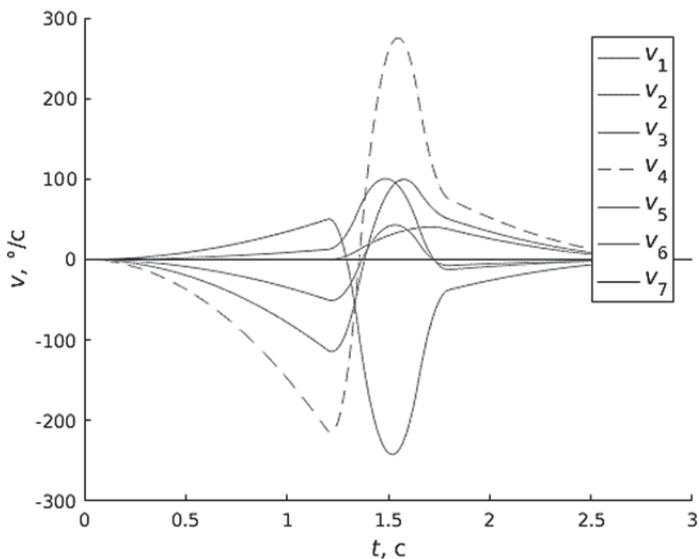


Рис. 6. Скорости изменения обобщенных координат

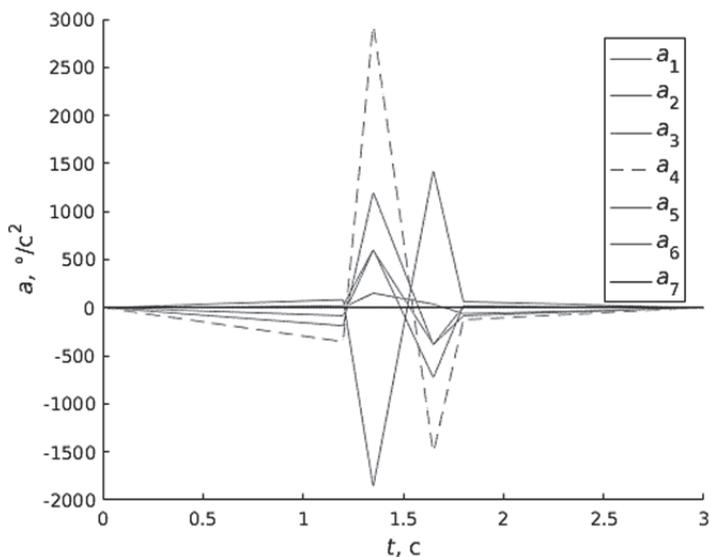


Рис. 7. Ускорения изменения обобщенных координат

В качестве объекта для прогнозирования рассмотрим закон движения по четвертой обобщенной координате (q_4 на рисунке 5) вследствие его наибольшей нелинейности. Как следует из рисунка 7, значение мгновенного ускорения изменения данной координаты максимально.

Исследуем зависимость величины ошибки прогнозирования Δq_1 от дальности прогнозирования τ_1 при использовании идеализированной линейной регрессии, построенной в момент осуществления прогнозирования и являющейся касательной к графику закона движения.

В ходе эксперимента траектория движения была разбита на 1000 промежуточных положений, для каждого из которых выполнено прогнозирование на различную дальность прогнозирования τ_1 . Для каждой дальности прогнозирования было найдено наибольшее значение ошибки прогнозирования. Результаты симуляции и верхняя оценка ошибки прогнозирования, найденная по формуле (7), представлены на рисунке 8. В качестве максимально допустимого ускорения принято максимальное ускорение в течение всего движения $a_{max} = 3,0 \cdot 10^3 \text{ }^\circ / \text{c}^2$. Как видно из рисунка 8, экспериментальное значение погрешности не превышает значения оценки, рассчитанного по формуле (7).

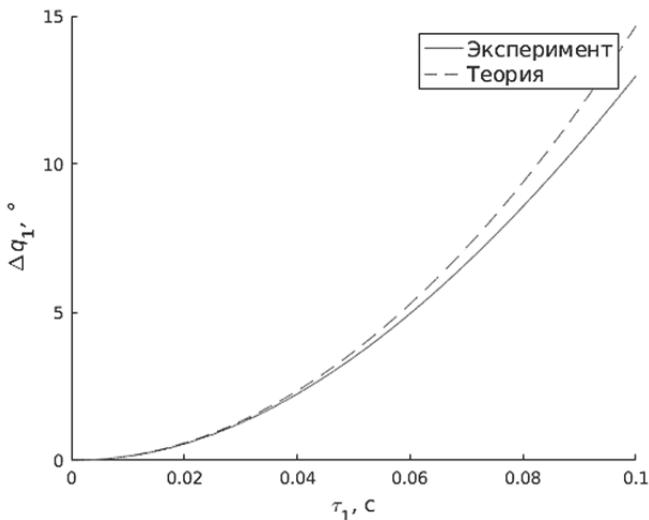


Рис. 8. Зависимость ошибки прогнозирования Δq_1 от дальности прогнозирования τ_1

Для нахождения зависимости величины ошибки Δq_1 от максимального ускорения a_{max} в течение движения выполним масштабирование закона движения по оси времени. При этом увеличатся максимальные значения скорости и ускорения, что приведет к увеличению ошибки прогнозирования. Результаты соответствующей симуляции для дальности прогнозирования $\tau_1 = 0,1c$ приведены на рисунке 9. Как следует из графиков, величина фактической ошибки не превышает величину теоретической оценки.

По аналогии с двумя предыдущими симуляциями исследуем зависимость величины ошибки прогнозирования Δq_2 от длительности временного интервала τ_2 при $a_{max} = 3,0 \cdot 10^3 \text{ } ^\circ / c^2$, и величины максимального ускорения a_{max} при $\tau_1 = 0,1c$ и $\tau_2 = 0,1c$. Результаты соответствующих симуляций приведены на рисунках 10 и 11.

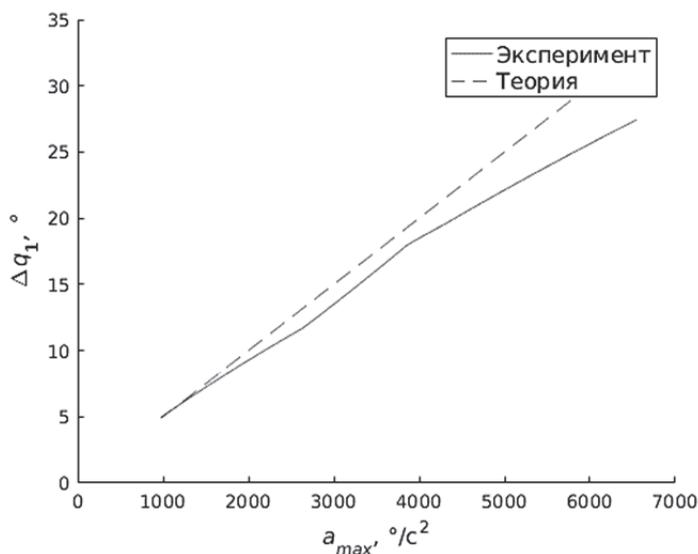


Рис. 9. Зависимость ошибки прогнозирования Δq_1 от величины максимального ускорения a_{max}

По аналогии с двумя предыдущими симуляциями исследуем зависимость величины ошибки прогнозирования Δq_2 от длительности временного интервала τ_2 при $a_{max} = 3,0 \cdot 10^3 \text{ } ^\circ / c^2$, и величины

максимального ускорения a_{max} при $\tau_1 = 0,1c$ и $\tau_2 = 0,1c$. Результаты соответствующих симуляций приведены на рисунках 10 и 11.

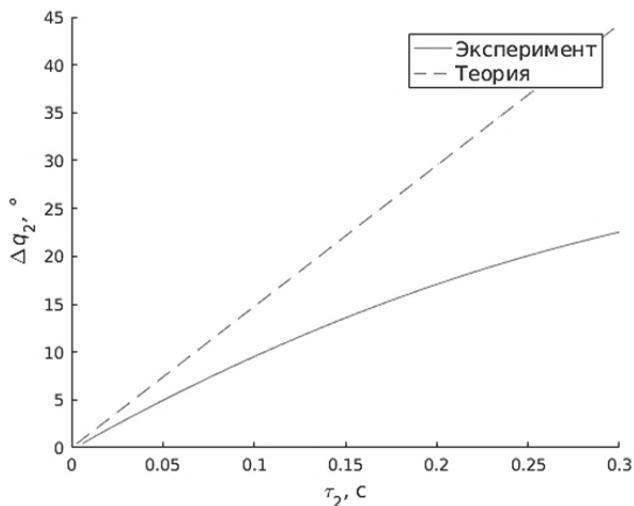


Рис. 10. Зависимость величины ошибки прогнозирования Δq_2 от длительности интервала τ_2

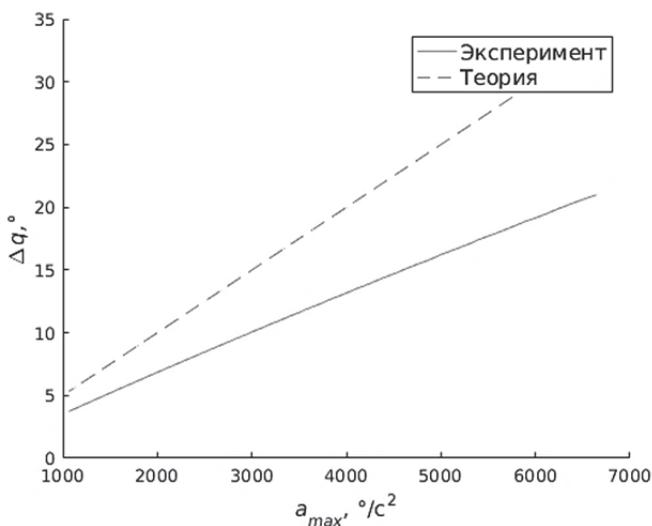


Рис. 11. Зависимость величины ошибки прогнозирования Δq_2 от максимального ускорения a_{max}

Из графиков на рисунках 10 и 11 видно, что реальное значение величины ошибки не превышает теоретической оценки. График изменения величины полной ошибки прогнозирования Δq в течение тестового движения при $a_{max} = 3,0 \cdot 10^3 \text{ }^\circ / \text{c}^2$, $\tau_1 = 0,05 \text{ c}$ и $\tau_2 = 0,1 \text{ c}$ приведен на рисунке 12.

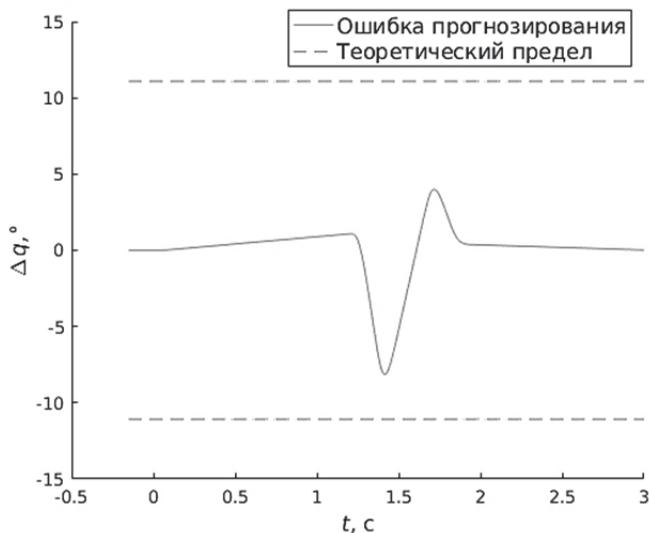


Рис. 12. Изменение величины полной ошибки прогнозирования Δq в течение тестового движения

Как следует из графика на рисунке 12, ошибка прогнозирования максимальна на среднем участке движения и практически отсутствует на начальном и конечном. Таким образом, предложенный подход позволяет получить относительно точную прогнозную оценку на крайних участках движения, то есть при выполнении непосредственно целевых операций. Менее точная оценка получается на среднем участке движения. Требования по точности прогнозирования на данном участке движения могут быть снижены, так как на нем не выполняются целевые операции, а осуществляется только перемещение между областями пространства, в которых выполняются целевые операции.

4. Заключение. Для устранения задержки, возникающей при управлении приводами антропоморфного манипулятора на основе решения обратной задачи динамики при копирующем типе управления в масштабе реального времени, предложено использование прогнозной

оценки обобщенных координат руки оператора вместо их измеренных значений. Законы изменения обобщенных координат являются непрерывными функциями времени, поэтому для выполнения прогнозирования предложено использовать трендовые модели.

Наименьшую вычислительную сложность имеет линейная регрессия, возможность применения которой рассмотрена в данной статье. В ходе выполнения исследования была найдена теоретическая зависимость оценки верхней границы величины ошибки прогнозирования от различных параметров используемого метода прогнозирования и ограничений, накладываемых на движение оператора.

Для подтверждения полученных результатов была выполнена программная симуляция движения руки оператора. Полученные с ее помощью результаты свидетельствуют об эффективности предложенного подхода к решению обратной задачи динамики на основе прогнозной оценки траектории движения руки оператора и адекватности найденной теоретической оценки значения верхнего предела ошибки прогнозирования.

Полученные в ходе симуляции реальные значения ошибки прогнозирования траектории (максимальное значение $4,0^\circ$) для тестового движения руки оператора не превышают максимального теоретического значения $\Delta q = 11,1^\circ$, определяемого формулой (13), что подтверждает ее адекватность. Квадратичный рост теоретической оценки величины ошибки прогнозирования с увеличением дальности прогнозирования позволяет использовать метод линейной регрессии только для краткосрочного прогнозирования.

Исследование величины реальной ошибки прогнозирования с помощью симуляции показало, что при применении линейной регрессии ее значение относительно невелико в начале и в конце тестового движения, и значительно больше в его середине. Так как взаимодействие с объектами окружающего мира выполняется на начальном и конечном участках движения, предложенный подход имеет предпосылки для проверки его применимости на практике.

В данной работе для прогнозирования использована линейная регрессия вследствие ее относительно низкой временной вычислительной сложности, что необходимо для систем реального времени. Особенностью линейной регрессии является ее нечувствительность к природе происхождения входных данных. Анализируемые в статье законы движения руки оператора получены с помощью интерполяции кубическими сплайнами. Таким образом, при прогнозировании с помощью нелинейной регрессии в виде кубического полинома могла быть получена нулевая ошибка прогнозирования, что

было бы несправедливо для работы в реальных условиях. Полученная теоретическая оценка пределов ошибки прогнозирования справедлива для любого движения при условии ограничения максимальных ускорений изменения обобщенных координат.

Для дальнейшего развития предложенного метода решения обратной задачи динамики на основе прогнозных значений необходимо проведение исследований эффективности различных методов прогнозирования на наборе входных данных, полученных с помощью реальных задающих устройств для среднесрочного прогнозирования (дальность которого имеет величину, сравнимую с длительностью отдельного движения оператора).

Литература

1. *Kiyani M.N., Khan M.U.M.* A prototype of search and rescue robot // Proceedings of 2nd International Conference on Robotics and Artificial Intelligence (ICRAI). 2016. pp. 208–213.
2. *de Greeff J. et al.* Persistent Robot-Assisted Disaster Response // Companion of ACM/IEEE International Conference on Human-Robot Interaction. 2018. pp. 99–100.
3. *Сохин И.Г. и др.* Эргономическое исследование дистанционного взаимодействия космонавтов с антропоморфными роботами-помощниками // Робототехника и техническая кибернетика. 2016. № 3(12). С. 18–22.
4. *Богданов А.А., Кутлубаев И.М., Сычков В.Б.* Перспективы создания антропоморфных робототехнических систем для работы в космосе // Пилотируемые полеты в космос. 2012. № 1(3). С. 78–84.
5. *Diffler M.A., Ambrose R.O.* Robonaut: A Robotic Astronaut Assistant // Proceeding of the 6-th International Symposium on Artificial Intelligence and Robotics & Automation in Space: i-SAIRAS. 2001. 8 p.
6. Фёдор (робот). URL: [https://ru.wikipedia.org/wiki/%D0%A4%D1%91%D0%B4%D0%BE%D1%80_\(%D1%80%D0%BE%D0%B1%D0%BE%D1%82\)](https://ru.wikipedia.org/wiki/%D0%A4%D1%91%D0%B4%D0%BE%D1%80_(%D1%80%D0%BE%D0%B1%D0%BE%D1%82)). (дата обращения: 27.07.2018).
7. *Richert A., Müller S., Schröder S., Jeschke S.* Anthropomorphism in social robotics: empirical results on human-robot interaction in hybrid production workplaces // AI and Society. 2018. vol 33. no. 3. pp. 413–424.
8. *Garcia S. et al.* An Architecture for Decentralized, Collaborative, and Autonomous Robots // Proceedings of IEEE International Conference on Software Architecture (ICSA). 2018. pp. 75–84.
9. *Страшинов Е.В., Торгашев М.А.* Супервизорное управление антропоморфными роботами с применением инверсной кинематики // Виртуальное моделирование, прототипирование и промышленный дизайн. Материалы международной научно-практической конференции. 2017. С. 186–190.
10. *Макарычев В.П., Юревич Е.И.* Супервизорное управление космическими манипуляторами // СПб.: Астерион. 2005. 106 с.
11. *Антонов В.О., Гурчинский М.М., Петренко В.И., Тебуева Ф.Б.* Метод планирования оптимальной траектории движения трехзвennого манипулятора в объемном пространстве с препятствием // Вестник Дагестанского государственного технического университета. Технические науки. 2018. № 45(1). С. 98–112.
12. Андроидная Техника, НПО. URL: <http://www.robogeek.ru/companies/androidnaya-tehnika> (дата обращения: 27.07.2018).

13. *Chen C.W., Hong R.M., Wang H.Y.* Design of a Controlled Robotic Arm // Proceedings of 3rd International Conference on Green Technology and Sustainable Development (GTSD). 2016. pp. 22–23.
14. *Ibhar N., Flores W., Leon R.* Design of a low-cost teleoperated robotic arm: Assembly and performance testing // Proceedings of IEEE 37th Central America and Panama Convention (CONCAPAN). 2017. pp. 1–5.
15. *Petrenko V.I. et al.* Calculating rotation angles of the operator's arms based on generalized coordinates of the master device with following anthropomorphic manipulator in real time // International Journal of Mechanical Engineering and Technology. 2018. vol. 9(1). pp. 447–461.
16. *Tan K.K., Putra A.S.* Control System in Servo Drives // Advances in industrial control. 2011. 197 p.
17. *Kazantsev V.P., Dadenkov D.A.* Position-servo drives with finite control // Proceedings of Russian Electrical Engineering. 2015. vol. 86. no. 6. pp. 344–349.
18. *Botan C., Ostafi F.* Optimal control of a servo drive system with variable torque // Proceedings of 21st International Conference on System Theory, Control and Computing (ICSTCC). 2017. pp. 500–505.
19. *Gasparetto A., Boscariol P., Lanzutti A., Vidoni R.* Path Planning and Trajectory Planning Algorithms: A General Overview // Motion and operation planning of robotic systems. 2015. pp. 3–27.
20. *Muller A.* Recursive second-order inverse dynamics for serial manipulators // Proceedings of IEEE International Conference on Robotics and Automation (ICRA). 2017. pp. 2483–2489.
21. *Bajodah A.* Asymptotic robot manipulator generalized inverse dynamics // Nonlinear Dynamics and Systems Theory. 2013. vol. 13. no. 1. pp. 25–46.
22. *Liu T., Gao F., Zhao X., Qi C.* Inverse Dynamics of a 6-DOF Decoupling Manipulator // Proceedings of ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 2014. 9 p.
23. *De La Cruz J.S., Kulic D., Owen W.* Learning inverse dynamics for redundant manipulator control // Proceedings of Autonomous and Intelligent Systems (AIS). 2010. pp. 1–6.
24. *Fijany A., Bejczy A.K.* Parallel computation of manipulator inverse dynamics // Journal of Robotic Systems. 1991. vol. 8. no. 5. pp. 599–635.
25. *Lee C.S.G.* Parallel algorithms and architectures for inverse dynamics computation // Parallel Computation Systems for Robotics. 1992.
26. *Megalingam R.K., Vivek G.V., Bandyopadhyay S., Rahi M.J.* Robotic arm design, development and control for agriculture applications // Proceedings of 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS). 2017. pp. 1–7.
27. *Fang B., Sun F., Liu H., Yao G.* Robotic teleoperation systems using a wearable multimodal fusion device // International Journal of Advanced Robotic Systems. 2017. vol. 14. no. 4. pp. 1–11.
28. *Bluethmann W., Ambrose R., Diffler M., Askew S.* Robonaut: A robot designed to work with humans in space // Autonomous Robots. 2003. vol. 14. no. 2-3. pp. 179–197.

Петренко Вячеслав Иванович — к-т техн. наук, доцент, заведующий кафедрой организации и технологии защиты информации института информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет. Область научных интересов: системы защиты информации, позиционно-траекторные задачи управления антропоморфными манипуляторами, арифметические операции в конечных полях, синтез дискретных последовательностей, системы связи. Число научных публикаций — 241. vip.petrenko@gmail.com, <http://www.ncfu.ru/spisok-sotrudnikov/1041-petrenko-vyacheslav-ivanovich.html>; пр-т Кулакова, 2, Ставрополь, 355029; р.т.: +7(8652)94-42-36.

Тебуева Фариза Биляловна — д-р физ.-мат. наук, доцент, заведующий кафедрой прикладной математики и компьютерной безопасности, института информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет. Область научных интересов: моделирование неопределенностей, анализ и прогнозирование временных рядов, многокритериальные задачи на графах, позиционно-траекторные задачи управления антропоморфными манипуляторами. Число научных публикаций — 102. fariza.teb@gmail.com, <http://www.ncfu.ru/spisok-sotrudnikov/1424-tebueva-fariza-bilyalovna.html>; пр-т Кулакова, 2, Ставрополь, 355029; р.т.: +7(8652)94-41-90.

Гурчинский Михаил Михайлович — аспирант кафедры прикладной математики и компьютерной безопасности института информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет. Область научных интересов: позиционно-траекторные задачи управления антропоморфными манипуляторами. Число научных публикаций — 5. gurmikhail@yandex.ru; пр-т Кулакова, 2, Ставрополь, 355029; р.т.: +7(8652)94-41-90.

Антонов Владимир Олегович — старший преподаватель аспирант кафедры прикладной математики и компьютерной безопасности, института информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет. Область научных интересов: позиционно-траекторные задачи управления антропоморфными манипуляторами. Число научных публикаций — 26. ant.vl.02@gmail.com; пр-т Кулакова, 2, Ставрополь, 355029; р.т.: +7(8652)94-41-90.

Павлов Андрей Сергеевич — аспирант кафедры прикладной математики и компьютерной безопасности института информационных технологий и телекоммуникаций, Северо-Кавказский федеральный университет. Область научных интересов: позиционно-траекторные задачи управления антропоморфными манипуляторами. Число научных публикаций — 6. andrew.pavlov.2015@yandex.ru; пр-т Кулакова, 2, Ставрополь, 355029; р.т.: +7(8652)94-41-90.

Поддержка исследований. Исследование выполнено в рамках реализации научного проекта по теме «Разработка программно-аппаратного комплекса системы управления на основе решения обратной задачи динамики и кинематики» в рамках ФЦП ИР 2014-2020 (уникальный идентификатор RFMEFI57517X0166) при финансовой поддержке Министерства науки и высшего образования Российской Федерации.

V.I. PETRENKO, F.B. TEBUEVA, M.M. GURCHINSKIY, V.O. ANTONOV,
A.S. PAVLOV

PREDICTIVE ASSESSMENT OF OPERATOR'S HAND TRAJECTORY WITH THE COPYING TYPE OF CONTROL FOR SOLUTION OF THE INVERSE DYNAMIC PROBLEM

Petrenko V.I., Tebueva F.B., Gurchinskiy M.M., Antonov V.O., Pavlov A.S. **Predictive Assessment of Operator's Hand Trajectory with the Copying Type of Control for Solution of the Inverse Dynamic Problem.**

Abstract. The most important task of modern robotics is the development of robots to perform the work in potentially dangerous fields which can cause the risk to human health. Currently robotic systems can not become a full replacement for man for solving complex problems in a dynamic environment despite an active development of artificial intelligence technologies.

The robots that implement the copying type of control or the so-called virtual presence of the operator are the most advanced for use in the nearest future. The principle of copying control is based on the motion capture of the remote operator and the formation of control signals for the robot's drives. A tracking system or systems based on movement planning can be used to control the drives. The tracking systems are simpler, but systems based on motion planning allow to achieve more smooth motion and less wear on the parts of the control object. An artificial delay between the movements of the operator and the control object for necessary data collection is used to implement the control-based motion planning.

The aim of research is a reduction of delay, which appears when controlling the anthropomorphic manipulator drives based on the solution of the inverse dynamic problem, when real time copying type of control is used. For motion path planning it is proposed to use forecast values of the generalized coordinates for manipulator. Based on the measured values of the generalized coordinates of the operator's hand, time series are formed and their prediction is performed. Predictive values of generalized coordinates are used in planning the anthropomorphic manipulator trajectory and solving the inverse dynamic problem. Prediction is based on linear regression with relatively low computational complexity, which is an important criterion for the system operation in the real time operation mode. The developed mathematical apparatus, based on prediction parameters and maximum permissible accelerations of the manipulator drives, allows to find a theoretical estimate of error values limits for planning the operator's hand trajectory using the proposed approach for specific tasks. The adequacy of the maximum theoretical value of the prediction error, as well as the prospects of the proposed approach for testing in practice is confirmed by the software simulation in Matlab environment.

Keywords: Prediction, Inverse Dynamic Problem, Motion Capture, Anthropomorphic Manipulator, Copying Type of Control, The Operator's Hand Trajectory, Virtual Presence.

Petrenko Vyacheslav Ivanovich — Ph.D., Associate Professor, Head of the Organization and Technology of Information Security Department of Institute of Information Technologies and Telecommunications, North-Caucasus Federal University. Research interests: Information Security Systems, Position-Trajectory Control of Anthropomorphic Manipulators, Arithmetic Operations in Finite Fields, Synthesis of Discrete Sequences, Communication Systems. The number of publications — 241. vip.petrenko@gmail.com, <http://www.ncfu.ru/spisok-sotrudnikov/1041-petrenko-vyacheslav-ivanovich.html>; 2, pr. Kulakova, Stavropol, 355029, Russia; office phone: +7(8652)94-42-36.

Tebueva Fariza Bilyalovna — Ph.D., Dr. Sci., Associate Professor, Head of the Applied Mathematics and Computer Security Department of Institute of Information Technologies and Telecommunications, North-Caucasus Federal University. Research interests: Modeling of Uncertainties, Analysis and Forecasting of Time Series, Multicriteria Problems on Graphs, Position-Trajectory Control of Anthropomorphic Manipulators. The number of publications — 102. fariza.teb@gmail.com, <http://www.ncfu.ru/spisok-sotrudnikov/1424-tebueva-fariza-bilyalovna.html>; 2, pr. Kulakova, Stavropol, 355029, Russia; office phone: +7(8652)94-41-90.

Gurchinsky Mikhail Mikhailovich — Ph.D. student of Applied Mathematics and Computer Security Department of Institute of Information Technologies and Telecommunications, North-Caucasus Federal University. Research interests: Position-Trajectory Control of Anthropomorphic Manipulators. The number of publications — 5. gurcmikhail@yandex.ru; 2, pr. Kulakova, Stavropol, 355029, Russia; office phone: +7(8652)94-41-90.

Antonov Vladimir Olegovich — Senior Lecturer of the Applied Mathematics and Computer Security Department of Institute of Information Technologies and Telecommunications, North-Caucasus Federal University. Research interests: Position-Trajectory Control of Anthropomorphic Manipulators. The number of publications — 26. ant.vl.02@gmail.com; 2, pr. Kulakova, Stavropol, 355029, Russia; office phone: +7(8652)94-41-90.

Pavlov Andrey Sergeevich — Ph.D. student of Applied Mathematics and Computer Security Department of Institute of Information Technologies and Telecommunications, North-Caucasus Federal University. Research interests: Position-Trajectory Control of Anthropomorphic Manipulators. The number of publications — 6. andrew.pavlov.2015@yandex.ru; 2, pr. Kulakova, Stavropol, 355029, Russia; office phone: +7(8652)94-41-90.

Acknowledgements. This research is supported by the scientific project «Development of the software and hardware system of the control system based on the solution of the inverse problem of dynamics and kinematics» in the Federal Target Program 2014-2020 (unique identifier RFMEFI57517X0166) with the financial support of the Ministry of Science and Higher Education of the Russian Federation.

References

1. Kiyani M.N., Khan M.U.M. A prototype of search and rescue robot. Proceedings of 2nd International Conference on Robotics and Artificial Intelligence (ICRAI). 2016. pp. 208–213.
2. de Greeff J. et al. Persistent Robot-Assisted Disaster Response. Companion of ACM/IEEE International Conference on Human-Robot Interaction. 2018. pp. 99–100.
3. Sohin I.G. et al. [Ergonomic study of remote interaction of astronauts with anthropomorphic helper robots]. *Robototekhnika i tehniceskaja kibernetika – Robotics and technical cybernetics*. 2016. vol. 3(12). pp. 18–22. (In Russ.).
4. Bogdanov A.A., Kutlubaev I.M., Sychkov V.B. [Prospects for the creation of anthropomorphic robotic systems for work in space] *Pilotiruemye poley v kosmos – Manned space flight*. 2012. vol. 1 (3). pp. 78–84. (In Russ.).
5. Diffler M.A., Ambrose R.O. Robonaut: A Robotic Astronaut Assistant. Proceeding of the 6-th International Symposium on Artificial Intelligence and Robotics & Automation in Space: i-SAIRAS. 2001. 8 p.
6. Fedor (robot) [Fedor (robot)]. Available at: [https://ru.wikipedia.org/wiki/%D0%A4%D1%91%D0%B4%D0%BE%D1%80_\(%D1%80%D0%BE%D0%B1%D0%BE%D1%82\)](https://ru.wikipedia.org/wiki/%D0%A4%D1%91%D0%B4%D0%BE%D1%80_(%D1%80%D0%BE%D0%B1%D0%BE%D1%82)). (accessed: 27.07.2018). (In Russ.).

7. Richert A., Müller S., Schröder S., Jeschke S. Anthropomorphism in social robotics: empirical results on human-robot interaction in hybrid production workplaces. *AI and Society*. 2018. vol 33. no. 3. pp. 413–424.
8. Garcia S. et al. An Architecture for Decentralized, Collaborative, and Autonomous Robots. Proceedings of IEEE International Conference on Software Architecture (ICSA). 2018. pp. 75–84.
9. Strashnov E.V., Torgashev M.A. [Supervision control of anthropomorphic robots using inverse kinematics]. *Virtual'noe modelirovanie, prototipirovanie i promyshlennyj dizajn: Materialy IV Mezhdunarodnoj nauchno-prakticheskoj konferencii* [Virtual modeling, prototyping and industrial design: Proceedings of the IV International Scientific and Practical Conference]. 2017. pp. 186–190. (In Russ.).
10. Makarychev V.P., Yurevich E.I. *Supervizornoe upravlenie kosmicheskimi manipulatorami* [Supervisory control of space manipulators]. SPb.: Asterion. 2005. 106 p. (In Russ.).
11. Antonov V.O., Gurchinskij M.M., Petrenko V.I., Tebueva F.B. [The method of planning the optimal trajectory of the three-link manipulator in the volumetric space with an obstacle]. *Vestnik Dagestanskogo gosudarstvennogo tehničeskogo universiteta. Tehničeskije nauki – Bulletin of the Dagestan State Technical University. Technical science*. 2018. vol. 45(1). pp. 98–112. (In Russ.).
12. Androidnaja Tehnika, NPO [Android Technology, NGO]. Available at: <http://www.robo geek.ru/companies/androidnaya-tehnika> (accessed 27.07.2018). (In Russ.).
13. Chen C.W., Hong R.M., Wang H.Y. Design of a Controlled Robotic Arm. Proceedings of 3rd International Conference on Green Technology and Sustainable Development (GTSD). 2016. pp. 22–23.
14. Ibar N., Flores W., Leon R. Design of a low-cost teleoperated robotic arm: Assembly and performance testing. Proceedings of IEEE 37th Central America and Panama Convention (CONCAPAN). 2017. pp. 1–5.
15. Petrenko V.I. et al. Calculating rotation angles of the operator's arms based on generalized coordinates of the master device with following anthropomorphic manipulator in real time. *International Journal of Mechanical Engineering and Technology*. 2018. vol. 9(1). pp. 447–461.
16. Tan K.K., Putra A.S. Control System in Servo Drives. *Advances in industrial control*. 2011. 197 p.
17. Kazantsev V.P., Dadenkov D.A. Position-servo drives with finite control. *Proceedings of Russian Electrical Engineering*. 2015. vol. 86. no. 6. pp. 344–349.
18. Botan C., Ostafi F. Optimal control of a servo drive system with variable torque. Proceedings of 21st International Conference on System Theory, Control and Computing (ICSTCC). 2017. pp. 500–505.
19. Gasparetto A., Boscariol P., Lanzutti A., Vidoni R. Path Planning and Trajectory Planning Algorithms: A General Overview. Motion and operation planning of robotic systems. 2015. pp. 3–27.
20. Muller A. Recursive second-order inverse dynamics for serial manipulators. Proceedings of IEEE International Conference on Robotics and Automation (ICRA). 2017. pp. 2483–2489.
21. Bajodah A. Asymptotic robot manipulator generalized inverse dynamics. *Nonlinear Dynamics and Systems Theory*. 2013. vol. 13. no. 1. pp. 25–46.
22. Liu T., Gao F., Zhao X., Qi C. Inverse Dynamics of a 6-DOF Decoupling Manipulator. Proceedings of ASME 2014 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference. 2014. 9 p.

23. De La Cruz J.S., Kulic D., Owen W. Learning inverse dynamics for redundant manipulator control. *Proceedings of Autonomous and Intelligent Systems (AIS)*. 2010. pp. 1–6.
24. Fijany A., Bejczy A.K. Parallel computation of manipulator inverse dynamics. *Journal of Robotic Systems*. 1991. vol. 8. no. 5. pp. 599–635.
25. Lee C.S.G. Parallel algorithms and architectures for inverse dynamics computation. *Parallel Computation Systems for Robotics*. 1992.
26. Megalingam R.K., Vivek G.V., Bandyopadhyay S., Rahi M.J. Robotic arm design, development and control for agriculture applications. *Proceedings of 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*. 2017. pp. 1–7.
27. Fang B., Sun F., Liu H., Yao G. Robotic teleoperation systems using a wearable multimodal fusion device. *International Journal of Advanced Robotic Systems*. 2017. vol. 14. no. 4. pp 1–11.
28. Bluethmann W., Ambrose R., Diftler M., Askew S. Robonaut: A robot designed to work with humans in space. *Autonomous Robots*. 2003. vol. 14. no. 2-3. pp. 179–197.

В.И. ЧЕРНЫШЕВ, Л.А. САВИН, О.В. ФОМИНОВА
**НЕПРЯМОЕ УПРАВЛЕНИЕ КОЛЕБАНИЯМИ: ЭЛЕМЕНТЫ
ТЕОРИИ**

Чернышев В.И., Савин Л.А., Фомина О.В. **Непрямое управление колебаниями: элементы теории.**

Аннотация. Приводится краткий обзор основных направлений исследований в области управляемых виброзащитных систем. Показано, что виброзащитные системы с непрямым управлением процессами колебаний позволяют с минимальными затратами энергии обеспечить программируемые переключения параметров и структур, при которых диссипативные, восстанавливающие и инерционные силы формируются по принципу активного воздействия. В рамках синтеза непрямого управления получены цепочки новых вспомогательных математических конструкций для нахождения оптимальных синтезирующих функций управления параметрами упругодемпфирующих звеньев, что позволило выделить базовую модель с прерывистым демпфированием и базовую модель с импульсной ловушкой. В результате исследования на основе метода гармонического баланса динамических свойств базовой модели с прерывистым демпфированием получены расчетные формулы для определения параметров компенсационного воздействия и расчета коэффициента динамичности. Установлено, что при оптимальной последовательности переключений демпфирования резонансные явления устраняются, а переходные процессы затухают в пределах одного периода кинематического возмущения. Базовая модель с импульсной ловушкой имитирует предельный вариант прерывистого демпфирования и реализует процесс наложения удерживающих связей, последовательность и длительность которых являются новыми переменными, существенно повышающими управляемость. Причем для непрямого импульсного управления характерен определенный минимум энергозатрат не зависящий от достигаемого эффекта виброзащиты. Регламентированное увеличение продолжительности наложения удерживающей связи в области низких частот и уменьшение этой продолжительности в области высоких частот обеспечивает монотонно-убывающую зависимость для коэффициентов динамичности на всем диапазоне частот. Рассмотрен пример решения оптимизационной задачи управления процессом демпфирования для базовой модели системы виброизоляции. Установлено, что прерывистое демпфирование является необходимым признаком оптимальности системы виброизоляции: демпфер включается в работу при смене знака скорости объекта и выключается из работы при смене знака смещения объекта.

Ключевые слова: колебания, виброзащитные системы, не прямое управление, оптимальное и субоптимальное управление, базовая модель с прерывистым демпфированием, базовая модель с импульсной ловушкой.

1. Введение. Обеспечение нормативных показателей вибрационного состояния в различных зонах виброактивных агрегатов во многом зависит от эффективности используемых для этих целей виброзащитных систем. При этом необходимо учитывать, что динамические свойства данных систем проявляются только во взаимодействии с защищаемым объектом, как части виброактивного агрегата, отражающего специфику его функционирования [1-4].

В настоящее время известны главные причины тех затруднений, которые встречаются на пути создания виброзащитных систем.

Снижение собственной частоты защищаемого объекта дает положительный эффект только при узкополосном спектре кинематического возмущения и отсутствии силового возмущения. Если в реальных условиях работы виброзащитная система воспринимает силовое возмущение, то при мягком подвесе можно наблюдать большие перемещения защищаемого объекта, а также пробои подвески, сопровождаемые ударами об ограничители. С другой стороны, при случайных возмущениях со сплошным спектром не удастся избежать проявления резонансных явлений, а «срезание» резонансных пиков посредством увеличения демпфирования неизбежно ухудшает динамические свойства виброзащитной системы в области высоких частот.

Вполне очевидно, что в классе линейных и пассивных виброзащитных систем преодолеть указанные противоречия невозможно. В связи с этим, активные виброзащитные системы [5, 6], управление в которых непосредственно отождествляется с компенсационным воздействием и характеризуется как прямое управление, а также виброзащитные системы с непрямым управлением [7-11], опосредствовано формирующие компенсационные воздействия за счет существенно-нелинейных проявлений, являются более перспективными.

Для работы активных систем требуются мощные внешние источники энергии, то есть велика энергоемкость процесса управления. По этой причине использование данных систем в роторных агрегатах может оказаться экономически нецелесообразно.

Теоретически, если мощность внешнего источника энергии активной системы неограниченна, то имеем тривиальный случай идеальной виброзащиты, который, однако, не реализуется на практике из-за запаздывания в срабатывании исполнительного механизма и других привносимых факторов, связанных с обработкой и обеспечением разрешающих скоростей потоков информации. Наряду с этим активные системы с ограниченной мощностью внешнего источника энергии, воспроизводящие релейный закон изменения компенсационного воздействия, обходятся дискретными во времени потоками информации, что значительно упрощает схемные решения и элементную базу для реализации данного способа управления.

Активные виброзащитные системы позволяют разрешить отмеченные выше противоречия за счет формируемого компенсационного воздействия, адекватного силовому и кинематическому возмущениям. Вследствие этого активные виброзащитные системы являются эталонными моделями, которые обеспечивают предельные возможности виброзащиты при оптимальном управлении и рассматриваются как прообразы лучших моделей виброзащитных систем с непрямым управлением.

В отличие от прямого управления, которое непосредственно воздействует на защищаемый объект и, по сути, является компенсационным воздействием, не прямое управление воздействует, например, на параметры упругодемпфирующего звена и посредством переключения подсистем или их отдельных структур оказывает опосредствованное влияние на движение защищаемого объекта.

Известны исследования динамических свойств виброзащитных систем с непрямым управлением параметрами демпфирования и жесткости, когда эти параметры изменяются в зависимости от интенсивности колебаний в том или ином диапазоне частот [12, 13]. Результаты данных исследований позволяют определить предельные варианты виброзащиты для способа управления параметрами упругодемпфирующего звена в амплитудно-частотной области. В области низких и резонансных частот коэффициенты динамичности равны единице. В области высоких частот они остаются такими же, как и для линейной виброзащитной системы с нулевым демпфированием. Достичь лучших показателей при таком способе управления параметрами упругодемпфирующего звена невозможно и, следовательно, проблемы виброзащиты остаются нерешенными.

Другой подход к решению проблем виброзащиты в рамках непрямого управления разработал С.В. Елисеев [14, 15]. Он предложил использовать дополнительные (неудерживающие и удерживающие) связи, а также переключать параметры и структуры виброзащитной системы при смене ряда априорных ситуаций, определяемых через компоненты состояния системы. Для этих целей допускается воспроизводить различные нелинейные проявления, которые программируются на основе «элементов памяти», зафиксированных в актуализированных свойствах конструкций подсистем. Математически переключения соответствующих параметров и структур описываются в виде разрывных нелинейностей и отображают режим «включить-выключить» работы исполнительных органов: механизмов преобразования движений, динамических гасителей, корректоров, переключателей. При этом данные виброзащитные системы являются наиболее перспективными, поскольку они позволяют избежать больших и неоправданных энергетических затрат на управление, а при определенных программируемых переключениях параметров и структур не уступают по эффективности активным виброзащитным системам.

Поскольку формально каждый нелинейный эффект представим как результат непрямого управления [16], то вариант непрямого импульсного управления является естественной имитацией разрывной нелинейности. Такой обобщенный подход позволяет теоретически обосновать новый класс виброзащитных систем с непрямым

управлением, а также соответствующие способы переключений их параметров и структур в амплитудно-фазовой области. Определенный подход к решению задач синтеза подобных систем можно найти в математических трудах французских авторов А. Бенсуан и Ж. Лионс [17], а также в прикладных работах по данной тематике [18-21]. Из-за того, что в роторных агрегатах невозможно получить несмещенную текущую информацию для решения задач управления процессами виброзащиты, особое внимание следует уделить методам построения нечетких алгоритмов управления [22] и, в частности, нечетким алгоритмам минимаксной процедуры нахождения непрямого импульсного управления [23].

Анализ известных устройств виброзащитной техники, которые реализуют способ непрямого управления, показал, что они, как правило, не оптимальны и решают частные задачи виброзащиты. Главная причина заключается в том, что в рамках данного научного направления создание обобщающих базовых элементов теории виброзащитных систем с непрямым управлением еще не завершено. По крайней мере, требуется проведение комплексных исследований для решения ряда актуальных проблем виброзащиты.

Тематика первоочередных исследований представлена следующими пятью разделами:

1. Разработка информационного обеспечения непрямого управления – нахождение синтезирующих функций и установление связи оптимальных алгоритмов переключений параметров и отдельных структур с принятым показателем качества.

2. Разработка базовых моделей виброзащитных систем с непрямым управлением, позволяющих формировать диссипативные, восстанавливающие и инерционные силы по принципу активного воздействия, а также осуществлять циклические (рекуперативные) процессы накопления потенциальной и кинетической энергии и возвращение ее в систему с положительным эффектом.

3. Сопоставительный анализ универсальных (не зависящих от частотно-фазовой модуляции) антирезонансных, противоударных и инвариантных свойств базовых моделей.

4. Отработка схемных и конструктивных решений исполнительных органов и в целом мехатронных устройств непрямого управления.

5. Оценка эффективности работы сложных технических систем, в которых используются виброзащитные системы с непрямым управлением.

2. Элементы информационного обеспечения непрямого управления. В рамках синтеза оптимального непрямого управления

решалась задача нахождения оптимальных и субоптимальных синтезирующих функций и соответствующих алгоритмов переключений параметров и отдельных структур виброзащитных системы в соответствии с принятым показателем качества. В качестве научной гипотезы допускалась возможность воспроизведения посредством непрямого управления компенсационных воздействий по принципу активных систем.

Основной характеристикой всякой управляемой виброзащитной системы является ее оптимальность по принятым критериям. Это также ассоциируется с проблемой установления и поддержания режима оптимального управления. Синтез оптимального управления базируется на использовании трех связанных между собой оценочных критериях: 1) показателе качества, устанавливаемого в зависимости от целей функционирования системы во времени; 2) показателе энергоемкости, который определяет минимальное потребление энергии на управление; 3) критерии управляемости. Обеспечение предельно-минимального уровня расхода энергии на управление от внешнего источника соотносится с возможностью системы сохранять управляемость.

Активные виброзащитные системы:

$$\dot{x} = f(x, t) + u \quad (1)$$

являются эталонными моделями. Они реализуют предельные антирезонансные, противоударные и инвариантные свойства при заданных ограничениях на управление ($u \in U$) и принимаемом показателе качества:

$$J(x, u) = \int_0^T F(x, u, t) dt \rightarrow \min. \quad (2)$$

Поскольку управление активных систем напрямую зависит от энергоресурса внешнего источника, то оптимизация показателя качества (2) достигается за счет большого расхода энергии. В рамках системы (1) это противоречие не снимается. Кроме того, прямое действие управления на защищаемый объект предопределяет его «повышенную чувствительность» к области допустимых значений или накладываемых ограничений, — сужение этой области однозначно приводит к ухудшению управляемости.

Естественно, что для системы (1) наиболее экономичным является импульсный режим (вариант прямого импульсного управления). Однако при этом достижение минимума показателя качества (2) возможно только с интегрантом определенного частного вида.

Качественно новые возможности будем иметь при переходе к виброзащитным системам с непрямым управлением:

$$\dot{x} = f(x, u, t) = \alpha(x, t) + \phi(x, u, t); \quad (3)$$

и использовании показателя качества независящего от управления:

$$J(x) = \int_0^T F[x(t)] dt \rightarrow \min. \quad (4)$$

В системах с непрямым управлением компенсационные воздействия определяются функцией $\phi(x, u, t)$. Управление в эту функцию входит как аргумент, то есть в системе (3) управление отождествляется с изменением выделяемого параметра или отдельной структуры. Данные изменения (в том числе и скачкообразные) не связаны с большим расходом энергии и всегда ограничены, то есть при гарантированном малом потреблении энергии на управление оптимизация показателя качества (4) обеспечивается за счет проявления нелинейных свойств системы. При этом формируемое в соответствии с целью управления компенсационное воздействие обеспечивает необходимый перевод системы из заданного начального состояния в заданное конечное состояние, что является косвенным признаком управляемости системы.

С позиции современных представлений системотехники и концепции управления [16], каждое проявление нелинейности формально можно представить как некоторое не прямое управление. Такой подход позволяет использовать общие положения и аппарат теории управления при проведении синтеза и разработке теории нового класса виброзащитных систем с непрямым управлением.

Функциональное уравнение Беллмана [24]:

$$-\frac{\partial V}{\partial t} = \min_{u \in U} \left(\frac{\partial V}{\partial x} \dot{x} + F \right), \quad (5)$$

где $V = \int_t^T F(x, \tau) d\tau$ допускает для циклических (колебательных) процессов следующие цепочки преобразований, приводящие к

соотношениям, которые можно использовать для нахождения синтезирующих функций управления:

$$F[x(t)] \Rightarrow \frac{dF}{dt} \Rightarrow \min_{u \in U} \frac{dF}{dt} = \min_{u \in U} (\nabla F \cdot f), \quad (6)$$

$$\frac{d^2 F[x(t)]}{dt^2} \Rightarrow \min_{u \in U} \frac{d^2 F}{dt^2} = \min_{u \in U} [\nabla G \cdot fd]. \quad (7)$$

Здесь $f^T = (f_1 \dots f_n)$, $fd^T = (f_1 \dots f_n \dot{f}_1 \dots \dot{f}_n)$,
 $\nabla F = \left(\frac{\partial F}{\partial x_1} \dots \frac{\partial F}{\partial x_n} \right)$, $G(x, f) = \nabla F \cdot f \rightarrow \nabla G = \left(\frac{\partial G}{\partial x_1} \dots \frac{\partial G}{\partial x_n} \frac{\partial G}{\partial f_1} \dots \frac{\partial G}{\partial f_n} \right)$.

Первая цепочка преобразований воспроизводит алгоритм получения соотношения (6) для функции $F[x(t)]$, явно не зависящей от времени, а вторая цепочка демонстрирует преобразование этого соотношения в новое соотношение (7), которое также может быть использовано для нахождения синтезирующей функции управления.

Очевидно, что соотношения (6) и (7) гарантируют достижение минимума для конкретных показателей качества типа (4) только тогда, когда произведение $\frac{dF}{dt} \cdot \frac{d^2 F}{dt^2} < 0$. Отсюда получаем объединяющее эти соотношения неравенство:

$$\min_{u \in U} [(\nabla F \cdot f) \cdot (\nabla G \cdot fd)] < 0. \quad (8)$$

Таким образом, получены соотношения, которые связывают компоненты вектора состояния системы и вектора управления и позволяют определить информационное обеспечение непрямого управления для типовых показателей качества и, соответственно, находить синтезирующую функцию непрямого управления.

Поставим следующую оптимизационную задачу. Для динамической системы с управляемым процессом демпфирования:

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -u(x_2 - \dot{y}) - k^2(x_1 - y), \end{aligned} \quad (9)$$

требуется найти оптимальное управление $u \geq 0$, которое минимизирует показатель качества:

$$J = \int_0^T x_1^2 dt. \quad (10)$$

Управление оптимально, если выполняется неравенство (8). В данной задаче:

$$F = x_1^2, \quad \nabla F = (2x_1, 0), \quad G(x, f) = 2x_1 f_1, \quad \nabla G = (2f_1, 0, 2x_1, 0),$$

$$f_1 = x_2, \quad f_2 = -u(x_2 - \dot{y}) - k^2(x_1 - y), \quad \dot{f}_1 = f_2.$$

Отсюда:

$$\nabla F \cdot f = 2x_1 f_1, \quad \nabla G \cdot fd = 2f_1^2 + 2x_1 f_2.$$

С учетом этого имеем:

$$\min_u 2x_1 x_2 \left\{ 2x_2^2 + 2x_1 \left[-u(x_2 - \dot{y}) - k^2(x_1 - y) \right] \right\} < 0,$$

$$\min_u x_2 u(\dot{y} - x_2) < 0, \quad u \rightarrow \text{sign} \left[x_2(x_2 - \dot{y}) \right].$$

Если предположить, что $u = (u_0, 0)$, то оптимальное управление можно представить в виде следующей синтезирующей функции:

$$u = \begin{cases} u_0, & x_2(x_2 - \dot{y}) \geq 0, \\ 0, & \text{иначе.} \end{cases} \quad (11)$$

Как видно, данная синтезирующая функция зависит от компонент состояния системы (абсолютной и относительной скорости защищаемого объекта) и определяет прерывистый процесс демпфирования (прерывистый вариант переключений диссипативных сил). Заметим, что здесь реализован двухступенчатый вариант прерывистого демпфирования. Обобщая данный результат, можно утверждать о целесообразности, например, реализации трехступенчатого варианта прерывистого демпфирования, рассматривая компоненты управления $u = (u_1, u_0, 0)$ как новые переменные, позволяющие оптимизировать процесс демпфирования. Очевидно, что один из данных вариантов непрямого управления процессом прерывистого демпфирования является субоптимальным (почти оптимальным).

Изменим оптимизационную задачу, то есть будем искать оптимальное управление $u \geq 0$, которое минимизирует показатель качества:

$$J = \int_0^T x_2^2 dt. \quad (12)$$

В данном случае используем соотношение (6), которое зависит от управления.

Поскольку

$$F = x_2^2, \quad \nabla F = (0, 2x_2), \quad f_1 = x_2, \quad f_2 = -u(x_2 - \dot{y}) - k^2(x_1 - y),$$

то соотношение (6) запишется в виде:

$$\min_{u \in U} (\nabla F \cdot f) = \min_u 2x_2 \cdot [-u(x_2 - \dot{y}) - k^2(x_1 - y)].$$

Из данного соотношения получим такое же оптимальное управление, как и в предыдущем случае:

$$\min_u x_2 \cdot [-u(x_2 - \dot{y})], \quad u \rightarrow \text{sign}[x_2(x_2 - \dot{y})].$$

Этот результат свидетельствует о том, что оптимальный прерывистый процесс демпфирования в системах виброзащиты данного типа обеспечивается при минимизации показателя качества (4) как с интегрантом $F(x) = x_1^2$, так и с интегрантом $F(x) = x_2^2$.

Особый интерес представляют предельные варианты управления, приводящие к скачкообразному изменению структуры системы (3), когда управление периодически резко возрастает $u \rightarrow \infty$, и варианты, когда управление периодически «исчезает» $u \rightarrow 0$. Последовательное чередование данных управлений определяет так называемое не прямое импульсное управление. Допускаются также следующие последовательности:

$$u_{\min} \leq u \leq u_{\max} \Leftrightarrow u \rightarrow 0 \dots, \quad u \rightarrow \infty \Leftrightarrow u_{\min} \leq u \leq u_{\max} \dots$$

Причем в моменты времени, когда $u_{\min} \leq u \leq u_{\max}$, исходная структура системы (3) не изменяется.

Рассмотрим динамическую систему с так называемой импульсной ловушкой, которая позволяет периодически блокировать

систему посредством резкого увеличения вязкого сопротивления и тем самым реализовать не прямое импульсное управление:

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -[u = (\infty, 0)] \cdot (x_2 - \dot{y}) - 2n(x_2 - \dot{y}) - k^2(x_1 - y), \\ J &= \int_0^T x_2^2 dt \rightarrow \min. \end{aligned} \quad (13)$$

Математическая модель данной системы неотделима от принятого здесь показателя качества (12), по отношению к которому дифференциальные уравнения являются внешними ограничениями, то есть при оптимальной последовательности чередования предельных значений непрямого импульсного управления достигается условный минимум показателя качества (12).

Поскольку при $u \rightarrow \infty$ импульсная ловушка блокирует систему и на соответствующем интервале движения фазовые координаты известны: $x_1 = y$; $x_2 = \dot{y}$, то оптимальную синтезирующую функцию непрямого импульсного управления, по аналогии с предыдущими примерами, можно представить в следующем виде:

$$u = \begin{cases} \infty, & |\dot{y}| \leq \Delta, \\ 0, & \text{иначе.} \end{cases} \quad (14)$$

Здесь использован новый ограничительный параметр Δ , который косвенно определяет длительность интервала движения заблокированной системы. Определение данного параметра связывается с достижением минимума принятого показателя качества. Последнее гарантируется только в том случае, если на интервале свободного движения системы выполняется необходимое условие оптимальности непрямого импульсного управления $x_2(x_2 - \dot{y}) < 0$.

Рассмотренные динамические системы, в контексте известных классификационных построений [23], относятся к базовым моделям виброзащитных систем с непрямым управлением процессом прерывистого и ударного демпфирования.

3. Базовая модель виброзащитной системы с прерывистым демпфированием. Воспользуемся методом гармонического баланса [25] для определения установившихся режимов колебаний базовой модели с прерывистым демпфированием [23]:

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -u(x_2 - \dot{y}) - k^2(x_1 - y), \\ u &= \begin{cases} u_0, & x_2(x_2 - \dot{y}) \geq 0, \\ 0, & \text{иначе.} \end{cases} \end{aligned} \quad (15)$$

Преобразуем базовую модель (15) к безразмерному виду, полагая при этом, что кинематическое возмущение $y = y_0 \sin \omega t$:

$$\begin{aligned} \dot{\xi}_1 &= \xi_2; \\ \dot{\xi}_2 &= -\frac{\varepsilon}{\eta}(\xi_2 - \cos \tau) - \frac{1}{\eta^2}(\xi_1 - \sin \tau), \\ \varepsilon &= \begin{cases} \varepsilon_0, & \xi_2(\xi_2 - \cos \tau) \geq 0, \\ 0, & \text{иначе.} \end{cases} \end{aligned} \quad (16)$$

Здесь приняты следующие безразмерные переменные и параметры:

$\xi_1 = \frac{x_1}{y_0}$, $\xi_2 = \frac{x_2}{y_0 \omega}$, $\dot{\xi}_2 = \frac{\dot{x}_2}{y_0 \omega^2}$ — смещение, скорость и ускорение защищаемого объекта;

$\eta = \frac{\omega}{k}$ — относительная частота; $\tau = \omega t$ — безразмерное время;

$\varepsilon = \frac{u}{k} \left(\varepsilon_0 = \frac{u_0}{k} \right)$ — относительное демпфирование.

Для установившегося режима колебаний системы (в пределах периода $T = 2\pi$) зависимость изменения относительного демпфирования можно записать в виде:

$$\varepsilon = \begin{cases} \varepsilon_0, & \text{если } \tau_1 \leq \tau \leq \tau_2 \text{ или } \tau_3 \leq \tau \leq \tau_4; \\ 0, & \text{если } 0 < \tau < \tau_1, \tau_2 < \tau < \tau_3 \text{ или } \tau_4 < \tau < T; \end{cases} \quad (17)$$

где τ_1 , τ_3 — моменты времени, в которые демпфер включается в работу и $\varepsilon = \varepsilon_0$, τ_2 , τ_4 — моменты времени, в которые демпфер выключается из работы и $\varepsilon = 0$.

Причем $\tau_3 = \tau_1 + \pi$, $\tau_4 = \tau_2 + \pi$ и, соответственно,

$$\xi_2(\tau_1) - \cos \tau_1 = 0, \quad \xi_2(\tau_2) = 0. \quad (18)$$

Для описания установившихся колебаний защищаемого объекта будем использовать усеченные тригонометрические ряды:

$$\xi_1 = \sum_{n=1}^N A_n \cos(n\tau) + B_n \sin(n\tau), \quad \xi_2 = \sum_{n=1}^N n [-A_n \sin(n\tau) + B_n \cos(n\tau)], \quad (19)$$

где N — число членов тригонометрических рядов, A_n, B_n — неизвестные коэффициенты тригонометрических рядов.

Линеаризация диссипативной составляющей производится по следующей схеме:

$$\varepsilon (\xi_2 - \cos \tau) \approx \sum_{n=1}^N R_n \cos(n\tau) + S_n \sin(n\tau), \quad (20)$$

где коэффициенты Фурье:

$$\begin{aligned} R_n(C_n, D_n, \tau_1, \tau_2) &= \\ &= \frac{\varepsilon_0}{\pi} \left\{ \int_{\tau_1}^{\tau_2} \left\{ \sum_{n=1}^N n [-A_n \sin(n\tau) + B_n \cos(n\tau)] - \cos \tau \right\} \cos(n\tau) d\tau + \right. \\ &+ \left. \int_{\tau_1+\pi}^{\tau_2+\pi} \left\{ \sum_{n=1}^N n [-A_n \sin(n\tau) + B_n \cos(n\tau)] - \cos \tau \right\} \cos(n\tau) d\tau \right\}, \end{aligned} \quad (21)$$

$$\begin{aligned} S_n(C_n, D_n, \tau_1, \tau_2) &= \\ &= \frac{\varepsilon_0}{\pi} \left\{ \int_{\tau_1}^{\tau_2} \left\{ \sum_{n=1}^N n [-A_n \sin(n\tau) + B_n \cos(n\tau)] - \cos \tau \right\} \sin(n\tau) d\tau + \right. \\ &+ \left. \int_{\tau_1+\pi}^{\tau_2+\pi} \left\{ \sum_{n=1}^N n [-A_n \sin(n\tau) + B_n \cos(n\tau)] - \cos \tau \right\} \sin(n\tau) d\tau \right\}. \end{aligned} \quad (22)$$

Теперь система дифференциальных уравнений (16) может быть заменена линеаризованной системой уравнений следующего вида:

$$\begin{aligned} \dot{\xi}_1 &= \xi_2; \\ \dot{\xi}_2 &= -\frac{1}{\eta} \left[\sum_{n=1}^N R_n \cos(n\tau) + S_n \sin(n\tau) \right] - \frac{1}{\eta^2} (\xi_1 - \sin \tau). \end{aligned} \quad (23)$$

С учетом соотношений (19), данная система дифференциальных уравнений преобразуется в трансцендентное уравнение:

$$\begin{aligned}
 & -\sum_{n=1}^N n^2 [A_n \cos(n\tau) + B_n \sin(n\tau)] + \frac{1}{\eta} \sum_{n=1}^N [R_n \cos(n\tau) + S_n \sin(n\tau)] + \\
 & + \frac{1}{\eta^2} \sum_{n=1}^N [A_n \cos(n\tau) + B_n \sin(n\tau)] - \frac{1}{\eta^2} \sin \tau = 0.
 \end{aligned}
 \tag{24}$$

После группировки слагаемых трансцендентного уравнения (24) получаем следующую совокупность уравнений:

$$\begin{aligned}
 & A_n \left(-n^2 + \frac{1}{\eta^2} \right) + R_n (A_n, B_n, \tau_1, \tau_2) \frac{1}{\eta} = 0, \\
 & B_n \left(-n^2 + \frac{1}{\eta^2} \right) + S_n (A_n, B_n, \tau_1, \tau_2) \frac{1}{\eta} = \frac{1}{\eta^2}.
 \end{aligned}
 \tag{25}$$

Используем также тригонометрические ряды (19) для преобразования соотношений (18) к следующему виду:

$$\sum_{n=1}^N n [-A_n \sin(n\tau_1) + B_n \cos(n\tau_1)] - \cos(\tau_1) = 0,
 \tag{26}$$

$$\sum_{n=1}^N n [-A_n \sin(n\tau_2) + B_n \cos(n\tau_2)] = 0.
 \tag{27}$$

Совокупность полученных уравнений (25), (26) и (27) является замкнутой относительно неизвестных параметров A_n, B_n, τ_1, τ_2 .

Поскольку установившийся процесс колебаний базовой модели (15) в пределах периода является кососимметричным, то при решении полученной замкнутой системы уравнений следует учитывать только нечетные составляющие, то есть принимать $n = 1, 3, 5, \dots$. Анализ результатов решений системы уравнений (25)-(27) показал, что достаточная для практического использования точность воспроизведения реальных динамических процессов в нелинейной системе данного типа обеспечивается при учете первых трёх (нечётных) слагаемых в разложении (19).

На рисунке 1 приведены выборочные решения системы уравнений (25)-(27) в виде графиков компонент состояния базовой модели, кинематического возмущения и прерывистого демпфирования, коррелированного по знаку с относительной скоростью защищаемого объекта. Из приведенных графиков расчетных зависимостей следует, что на резонансной частоте амплитуды колебаний защищаемого объекта ограничены и не превышают амплитуды колебаний подвижного основания. При этом на опорной относительной частоте $\eta = 1,41$ прерывистый процесс демпфирования обеспечивает снижение амплитуды колебаний защищаемого объекта по сравнению с амплитудой колебаний подвижного основания практически в четыре раза.

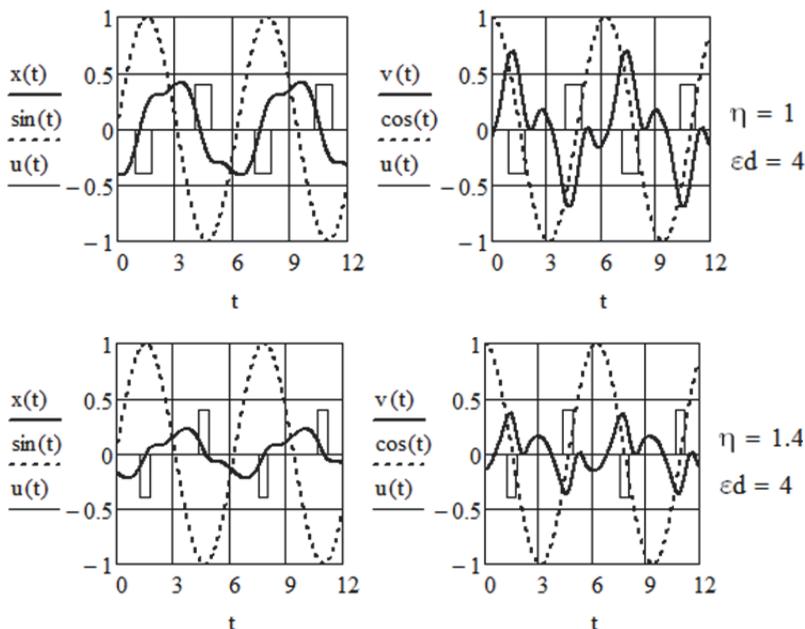


Рис. 1. Графики расчетных зависимостей: базовая модель с прерывистым демпфированием; примечание: $x(t) = \xi_1$; $v(t) = \xi_2$; $u(t) = \epsilon(\tau) \cdot \text{sign}(\xi_2 - \cos \tau)$

Отметим следующую важную особенность оптимального прерывистого демпфирования — в области высоких частот ($\eta > 1,0$) моменты времени выключения демпфера из работы, связанные со сменой знака абсолютной скорости защищаемого объекта, практически совпадают с моментами времени, в которые происходит

смена знака относительного смещения защищаемого объекта. Как следствие, становится возможным реализовать субоптимальный алгоритм непрямого управления процессом демпфирования, при котором демпфер включается в работу при смене знака относительной скорости и выключается из работы при смене знака относительного смещения. Заметим, что для поддержания субоптимального прерывистого процесса демпфирования можно использовать актуализированные свойства собственно системы и тем самым обходиться без электронных средств слежения. При этом следует ожидать, что динамические свойства базовой модели в указанном диапазоне частот установившихся колебаний практически не изменятся.

Приведенные в таблице 1 значения коэффициентов динамичности позволяют сделать следующие выводы о динамических свойствах базовой модели (16). Во-первых, с увеличением относительного демпфирования резонансные пики уменьшаются и смещаются в сторону низких частот. Во-вторых, в области высоких частот значения коэффициентов динамичности монотонно уменьшаются, оставаясь не только меньше единицы, но и меньше значений коэффициентов динамичности линейной системы без демпфирования, определяемых из соотношения:

$$Kd = \frac{1}{|1 - \eta^2|} \quad (\eta > 1,41). \quad (28)$$

Таблица 1. Коэффициенты динамичности

εd	η							
	0,6	0,8	1,0	1,2	1,4	1,6	1,8	2,0
2	1,563	0,989	0,753	0,533	0,374	0,266	0,192	0,144
3	0,942	0,725	0,498	0,344	0,244	0,173	0,139	0,111
4	0,820	0,593	0,413	0,299	0,224	0,171	0,133	0,106
5	0,743	0,558	0,407	0,312	0,234	0,177	0,137	0,108
6	0,723	0,566	0,439	0,345	0,252	0,186	0,152	0,111

Таким образом, доказано, что в рамках объектно-ориентированной методики использования метода гармонического баланса можно с заданной степенью точности воспроизводить установившиеся колебания виброзащитной системы с управляемым демпфером прерывистого действия. При этом соответствующая диссипативная сила, как управляющее воздействие, позволяет устранить резонансные явления и существенно снизить интенсивность колебаний защищаемого объекта.

3. Базовая модель виброзащитной системы с импульсной ловушкой. Рассматривается виброзащитная система, в которой импульсная ловушка позволяет периодически резко увеличивать вязкое сопротивление и тем самым реализует процесс ударного демпфирования колебаний защищаемого объекта. Базовую модель такой виброзащитной системы получим, объединяя (13) и (14):

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -u \cdot (x_2 - \dot{y}) - 2n(x_2 - \dot{y}) - k^2(x_1 - y), \\ u &= \begin{cases} \infty, & |\dot{y}| \leq \Delta, \\ 0, & \text{иначе.} \end{cases} \end{aligned} \quad (29)$$

Предполагается, что в результате срабатывания импульсной ловушки, имитирующей процесс наложения удерживающей связи, можно реализовать оптимальные последовательности программируемых «мгновенных» переводов системы из одного состояния в другое, при которых достигается минимизация принятого показателя качества на траекториях движения системы, состоящих из кусков границ допустимой области и кусков сопряженных экстремалей. Упорядоченная и расширенная последовательность срабатываний импульсной ловушки и их длительности являются новыми переменными, существенно повышающими управляемость системы по сравнению, например, с вариантом пассивных ограничителей. Причем для непрямого импульсного управления характерен определенный минимум энергозатрат, не зависящий от достигаемого эффекта виброзащиты. Это относится и к так называемым скользящим режимам, то есть при повторных срабатываниях импульсной ловушки на кусках траектории движения системы в пределах границ допустимой области.

В пределе, когда $\Delta \rightarrow 0$, базовая модель (29) имитирует периодические процессы ударного демпфирования и имеет качественно новое описание — дифференциальные уравнения движения объекта между соударениями дополняются конечными соотношениями, определяющими начальные условия:

$$\begin{aligned} \dot{x}_1 &= x_2; \\ \dot{x}_2 &= -2n(x_2 - \dot{y}) - k^2(x_1 - y), \quad \text{при } \dot{y}(t_i) \neq 0, \end{aligned} \quad (30)$$

$$x_2^+(t_i) \rightarrow \dot{x}_i^+ = 0, \quad x_1^+(t_i) \rightarrow x_i^+ = x_1^-(t_i) \rightarrow x_i^-, \quad \text{при } \dot{y}(t_i) = 0. \quad (31)$$

Здесь в моменты времени t_i положение объекта фиксируется по отношению подвижного основания и скорость объекта становится равной нулю. Длительность фиксации $\Delta \rightarrow 0$.

Будем искать периодические решения дифференциального уравнения (30) при детерминированном кинематическом возмущении $y(t) = y_0 \cos(\omega t)$.

В начале из решения дифференциального уравнения (30)

$$\xi(\tau) = \exp(-\varepsilon d \cdot \tau / \eta) \cdot [C_1 \cos(\tau / \beta) + C_2 \sin(\tau / \beta)] + Kd \cdot \cos(\tau - \phi) \quad (32)$$

определим постоянные интегрирования C_1 и C_2 , используя соотношения (31) на i -ом интервале движения объекта $\xi(0) = \xi_0$, $\dot{\xi}(0) = 0$.

После несложных преобразований получим:

$$C_1 = \xi_0 - Kd \cdot \cos \phi; \quad C_2 = \gamma \cdot (\xi_0 - Kd \cdot \cos \phi) - Kd \cdot \beta \cdot \sin \phi. \quad (33)$$

В (32) и (33) приняты следующие обозначения безразмерных переменных и параметров:

$$\begin{aligned} \tau &= \omega t; \quad \xi_i(\tau) = x_i(\tau) / y_0; \quad \eta = \omega / k; \quad \varepsilon d = n / k; \\ Kd &= \frac{\sqrt{1 + 4 \cdot \varepsilon d^2 \eta^2}}{\sqrt{(1 - \eta^2)^2 + 4 \cdot \varepsilon d^2 \eta^2}}; \quad \gamma = \frac{\varepsilon d}{\sqrt{1 - \varepsilon d^2}}; \quad \beta = \frac{\eta}{\sqrt{1 - \varepsilon d^2}}; \\ \phi &= \operatorname{arctg} \frac{2 \cdot \varepsilon d \cdot \eta^3}{1 - \eta^2 + 4 \cdot \varepsilon d^2 \eta^2}. \end{aligned}$$

Исходя из того, что для периодического процесса $\xi_i(\pi) = -\xi_0$, выразим ξ_0 через безразмерные параметры базовой модели:

$$\xi_0 = Kp \frac{\exp(-\varepsilon d \cdot \pi / \eta) \cdot \left(\cos \phi \cdot \cos \frac{\pi}{\beta} + \gamma \cdot \cos \phi \cdot \sin \frac{\pi}{\beta} + \beta \cdot \sin \phi \cdot \sin \frac{\pi}{\beta} \right) - \cos(\pi - \phi)}{1 + \exp(-\varepsilon d \cdot \pi / \eta) \cdot \left(\cos \frac{\pi}{\beta} + \gamma \cdot \sin \frac{\pi}{\beta} \right)}. \quad (34)$$

С учетом постоянных интегрирования (33) и начального смещения (34) общее решение (32) описывает движение объекта в пределах полупериода ($0 \leq \tau \leq \pi$) установившихся — периодических колебаний.

Результаты расчетов коэффициентов динамичности по перемещению $Kd_0 = \max|\xi(\tau)|$, произведенных с использованием общего решения (32) и уравнений (33), (34), когда параметр $\Delta = 0$, сведены в таблицу 2. Там же приведены предельные (минимально-достижимые на заданной частоте η) значения коэффициентов динамичности Kd_1 и Kd_2 базовой модели (29) с конечным временем срабатывания импульсной ловушки Δ_1 и Δ_2 соответственно. Эти данные получены в результате моделирования работы базовой модели (29) на ЭВМ.

Для сравнения в двух нижних строках таблицы 2 приведены значения коэффициентов динамичности Kd неуправляемой (пассивной) виброзащитной системы при кинематическом воздействии. В нашем случае — это базовая модель (29) при $u \equiv 0$.

Таблица 2. Результаты расчетов базовой модели с импульсной ловушкой

η	0,6	0,8	1,0	1,2	1,4	1,6	1,8	2,0	εd
Kd_0	1,517	1,952	1,213	0,529	0,388	0,291	0,225	0,180	0,1
	1,459	1,633	1,182	0,674	0,463	0,354	0,288	0,244	0,2
Δ_1	0,70	0,50	0,30	0,20	0,16	0,13	0,11	0,09	0,1
Kd_1	0,885	0,731	0,496	0,279	0,193	0,154	0,133	0,113	
Δ_2	0,80	0,60	0,40	0,20	0,10	0,08	0,06	0,04	0,2
Kd_2	0,944	0,859	0,736	0,573	0,414	0,325	0,268	0,234	
Kd	1,547	2,571	5,099	2,052	1,038	0,659	0,468	0,336	0,1
	1,505	2,180	2,693	1,703	1,031	0,704	0,524	0,412	0,2

Дополнительные результаты проведенных расчетов в виде характерных графиков компонент состояния базовой модели с импульсной ловушкой, имитирующей процесс ударного демпфирования, когда параметр $\Delta = 0$, и процесс наложения удерживающей связи, когда параметр $\Delta \neq 0$, приведены на рисунках 2 и 3.

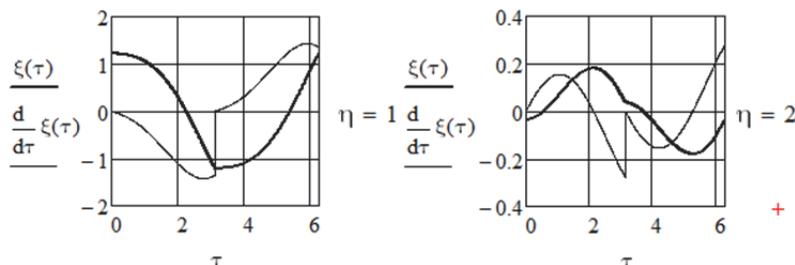


Рис. 2. Графики расчетных зависимостей: имитация ударного демпфирования; примечание: $\varepsilon d = 0,1$; $\Delta = 0$

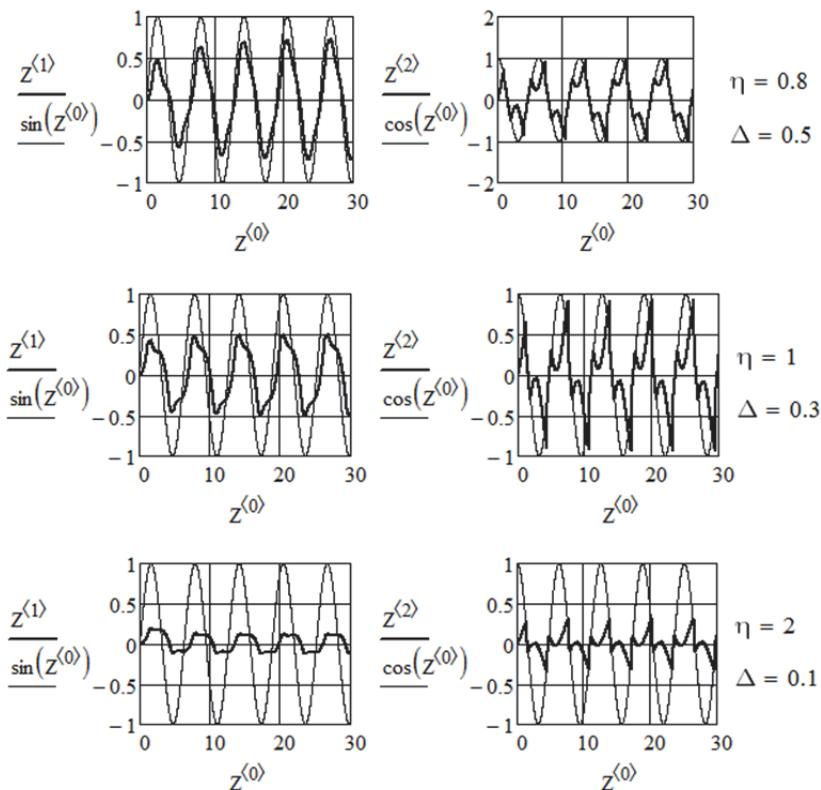


Рис. 3. Графики расчетных зависимостей: имитация наложения удерживающих связей; примечание: $\varepsilon d = 0,1$; $Z^{(0)} = \tau$; $Z^{(1)} = \xi(\tau)$; $Z^{(2)} = \ddot{\xi}(\tau)$

В отличие от неуправляемых виброзащитных систем базовая модель с импульсной ловушкой позволяет существенно снизить уровни колебаний объекта, как в области низких (дорезонансных), так и в области высоких (зарезонансных) частот.

Реализация ударного демпфирования позволяет сместить пиковые значения коэффициентов динамичности в дорезонансную область частот и положительный эффект виброзащиты достигается, если относительная частота $\eta > 1,1$. При этом наблюдается монотонное уменьшение амплитуд колебаний объекта. Показательно, что на характерной частоте кинематического воздействия, когда $\eta \approx 1,41$, амплитуды колебаний объекта уменьшаются более чем в два раза.

В момент срабатывания импульсной ловушки происходит скачкообразное «обнуление» скорости защищаемого объекта. После этого объект совершает «свободное» движение, которое происходит до тех пор, пока скорость подвижного основания опять не станет равной нулю. Далее циклический процесс повторяется. Заметим, что в области высоких (зарезонансных) частот «перепад» скорости объекта в момент срабатывания импульсной ловушки уменьшается с увеличением относительной частоты.

В процессе наложения удерживающих связей параметр Δ , как элемент непрямого управления, позволяет исключить проявление резонансных явлений и достичь предельных показателей виброзащиты в рабочем диапазоне частот кинематического воздействия. При этом регламентированное увеличение продолжительности наложения удерживающей связи в области низких частот и, соответственно, уменьшение этой продолжительности в области высоких частот обеспечивает монотонно-убывающую зависимость для коэффициентов динамичности на всем диапазоне частот — и это вне зависимости от интенсивности демпфирования. Заметим, что приведенные в таблице 2 и на рисунке 3 значения параметра Δ являются оптимальными, то есть их изменение приведет к увеличению амплитуд колебаний объекта.

В результате моделирования установлено, что переходные процессы, вызываемые начальными условиями или случайными флуктуациями внешних возмущений, затухают в пределах одного периода кинематического воздействия, то есть реализуется процесс, который характеризуется как «один толчок — одно колебание».

4. Пример решения оптимизационной задачи управления процессом виброизоляции. Рассматривается базовая модель системы виброизоляции с управляемым демпфером [26]:

$$m\ddot{x} + b\dot{x} + b(t)\dot{x} + cx = P_0 \cos \omega t. \quad (35)$$

Ставится задача — обеспечить существенное снижение динамических реакций $R(t) = cx + b(t)\dot{x}$, воспринимаемых несущим элементом (основанием) виброизолятора при детерминированном силовом возмущении за счет оптимального процесса демпфирования.

Поставленную задачу будем решать, используя методы теории оптимального управления [11, 24, 27].

Исходное уравнение движения рассматриваемой системы преобразуем к форме Коши [24]:

$$\dot{x}_0 = x_1, \quad \dot{x}_1 = -nx_1 - ux_1 - k^2 x_0 + H_0 \cos \omega t. \quad (36)$$

Здесь приняты следующие обозначения: $H_0 = P_0/m$ — амплитуда силового возмущения, отнесенная к массе виброактивного объекта; $u = b(t)/m$ — функция управления (управление); x_0, x_1 — перемещение, скорость виброактивного объекта; $k = \sqrt{c/m}$ — частота собственных колебаний виброактивного объекта на несущем упругом элементе; ω — частота силового возмущения.

Очевидно, что для оценки уровня интенсивности воздействия динамической реакции $R(t) = cx + b(t)\dot{x}$ на несущий элемент и, соответственно, оптимальности системы виброизоляции, можно использовать функционал:

$$J = \int_0^T (ux_1 + k^2x_0)^2 dt \rightarrow \min. \quad (37)$$

Здесь T — некоторый (представительный) интервал времени.

Функционал (37) принимается за показатель качества исходной системы (36).

Для рассматриваемой оптимизационной задачи функция Гамильтона имеет вид:

$$H = -(ux_1 + k^2x_0)^2 + p_0x_1 + p_1(-nx_1 - ux_1 - k^2x_0 + H_0 \cos \omega t), \quad (38)$$

где p_0, p_1 — присоединенные переменные.

Поскольку вязкое трение $b(t) \geq 0$, то управление, отождествленное с демпфированием, не может быть отрицательным ($u \geq 0$).

Будем полагать, что $u = z^2$.

Тогда

$$H = -(z^2x_1 + k^2x_0)^2 + p_0x_1 + p_1(-nx_1 - z^2x_1 - k^2x_0 + H_0 \cos \omega t). \quad (39)$$

На переменную z ограничения не накладываются. Это позволяет установить зависимость переменной z от фазовых координат x_0, x_1 и присоединенных переменных p_0, p_1 из соотношения:

$$\frac{\partial H}{\partial z} = 0 \Rightarrow -4(z^2x_1 + k^2x_0)zx_1 - 2zp_1x_1 = 0. \quad (40)$$

Отсюда

$$z(x, p) = \begin{cases} -\frac{k^2 x_0 + 0,5 p_1}{x_1}, (k^2 x_0 + 0,5 p_1) x_1 \leq 0; \\ 0, (k^2 x_0 + 0,5 p_1) x_1 > 0, \end{cases} \quad (41)$$

и, соответственно, получаем структуру оптимального управления:

$$\tilde{u}(x, p) = \begin{cases} -\frac{k^2 x_0 + 0,5 p_1}{x_1}, (k^2 x_0 + 0,5 p_1) x_1 \leq 0; \\ 0, (k^2 x_0 + 0,5 p_1) x_1 > 0. \end{cases} \quad (42)$$

Определим присоединенные переменные. Для этого раскроем канонические уравнения Гамильтона:

$$\dot{p} = -\frac{\partial H}{\partial x} \Rightarrow \dot{p}_0 = 0, \dot{p}_1 = -p_0. \quad (43)$$

Имеем замкнутую систему дифференциальных уравнений. Общее решение: $p_0(t) = C_1$, $p_1(t) = C_1 t + C_2$.

Для оптимальности присоединенных переменных, обращающих в тождества дифференциальные уравнения (43), необходимо чтобы выполнялись следующие краевые условия:

$$p_0(0) = 0, p_1(0) = 0, p_0(T) = 0, p_1(T) = 0. \quad (44)$$

Это общий признак оптимальности для случая, когда краевые значения фазовых координат не определены и произвольны.

Выполнение конечных условий (44) возможно только тогда, когда $p_0 = 0$, $p_1 = 0$.

В результате подстановки $p_1 = 0$ в соотношение (42) найдем оптимальную синтезирующую функцию управления:

$$\tilde{u}(x) = \begin{cases} -\frac{k^2 x_0}{x_1}, x_0 x_1 \leq 0; \\ 0, x_0 x_1 > 0. \end{cases} \quad (45)$$

Как видно, оптимальное управление определяет прерывистый процесс демпфирования. Демпфер включается в работу при смене

знака скорости объекта, когда $x_1 = 0$, и выключается из работы, когда смещение объекта $x_0 = 0$.

Таким образом, установлено, что прерывистое демпфирование является необходимым признаком оптимальности системы виброизоляции.

5. Заключение. Виброзащитные системы с непрямым управлением обеспечивают определенный минимум энергетических затрат, связанных с управлением, и устранение резонансных режимов в рабочих диапазонах частот. Получены и апробированы цепочки новых вспомогательных математических конструкций для нахождения оптимальных синтезирующих функций управления в системах с непрямым управлением. Установлено, что основным признаком оптимальности изменяемых параметров системы, которые отождествляются с непрямым управлением, является их прерывистость. В рамках общей классификации виброзащитных систем с непрямым управлением предложены новые базовые модели, которые реализуют оптимальные и субоптимальные релейно-прерывистые последовательности переключений параметров упругодемпфирующих звеньев, что позволяет существенно улучшить их динамические свойства по сравнению с соответствующими пассивными системами по критерию вибрационной безопасности.

Литература

1. *Genfeng L., Jing J., Yuhe L., Ming Z.* Impact of system anisotropy on vibration reduction of rotating machinery and its evaluation method // *Mechanical Systems and Signal Processing*. 2017. vol. 93. pp. 299–311.
2. *Аврамов К.В., Михлин Ю.В.* Нелинейная динамика упругих систем. Приложения // М.-Ижевск: Институт компьютерных исследований. 2015. Т. 2. 700 с.
3. *Chernyshev V.I., Savin L.A., Fominova O.V.* Dynamics of the rotor on elastic-damping supports under action of kinematic effects // *IOP Conference Series: Materials Science and Engineering*. 2017. vol. 233. no. 1. pp. 012055.
4. *Linfeng D., Zhao R.* A vibration analysis method based on hybrid techniques and its application to rotating machinery // *Measurement*. 2013. vol. 46. no. 9. pp. 3671–3682.
5. *Дорф Р., Бишон Р.* Современные системы управления // М.: Лаборатория Базовых Знаний. 2013. 832 с.
6. *Bai X.X., Wereley N.M., Choi Y.T.* Magnetorheological energy absorber with dual concentric annular valves // *Journal of Intelligent Material Systems and Structures*. 2016. vol. 27. no.7. pp. 944–958.
7. *Дыхта В.А., Самсонок О.Н.* Оптимальное импульсное управление с приложениями // М.: Физматлит. 2003. 256 с.
8. *Дыхта В.А.* Позиционный принцип минимума для квазиоптимальных процессов в задачах управления с терминальными ограничениями // *Известия Иркутского государственного университета. Серия: Математика*. 2017. Т. 19. С. 113–128.
9. *Balthazar J.M., Gonçalves, P.B., Fenili A.* Nonlinear vibrations in elastic structures: Dynamics and control // *Shock and Vibration*. 2013. vol. 20. no. 6. pp. 1031–1032.

10. *Ibrahim R.A.* Recent advances in nonlinear passive vibration isolators // *Journal of Sound and Vibration*. 2008. vol. 314. no. 3-5. pp. 371–452.
11. *Фоминова О.В., Степанов Ю.С., Чернышев В.И.* Экстремальные задачи и оптимизация: введение в теорию непрямого импульсного управления процессами колебаний // М.: Издательский дом «Спектр». 2011. 218 с.
12. *Balandin D.V., Bolotnik N.N., Pilkey W.D.* Pre-acting control for shock and pact isolation systems // *Shock and Vibration*. 2005. vol. 12. no. 1. pp. 49–65.
13. *Ni Y.Q., Chen Z.H., Or S.W.* Experimental identification of a self-sensing magnetorheological damper using soft computing // *Journal of Engineering Mechanics*. 2015. vol. 141. no. 7. pp. 1–13.
14. *Елисеев С.В., Орленко А.И., Нгуен Д.Х.* Устройства для преобразования движения в структуре диады механической колебательной системы // *Вестник Донского государственного технического университета*. 2017. № 17(3). С. 46–59.
15. *Елисеев А.В., Сельвинский В.В., Елисеев С.В.* Динамика вибрационных взаимодействий элементов технологических систем с учетом неудерживающих связей // Новосибирск: Наука. 2015. 332 с.
16. *Дружинин В.В., Конторов Д.С.* Системотехника // М.: Радио и связь. 1985. 200 с.
17. *Бенсуан А., Лиож Ж.* Импульсное управление и квазивариационные неравенства // М.: Наука. 1987. 596 с.
18. *Ledezma D.F., Ferguson N.S, Zamarripa A.S.* Mathematical modeling of a transient vibration control strategy using a switchable mass stiffness compound system // *Shock and Vibration*. 2014. URL: <http://dx.doi.org/10.1155/2014/565181> (дата обращения: 18.06.2017).
19. *Ledezma D.F., Ferguson N.S., Brennan M.J., Tang B.* An experimental nonlinear low dynamic stiffness device for shock isolation // *Journal of Sound and Vibration*. 2015. vol. 347. pp. 1–13.
20. *Tang B., Brennan M.J.* On the shock performance of a nonlinear vibration isolator with high-static-low-dynamic-stiffness // *International Journal of Mechanical Sciences*. 2014. vol. 81. pp. 207–214.
21. *Пегат А.* Нечеткое моделирование и управление // М.: Бином Лаборатория знаний. 2018. 798 с.
22. *Фоминова О.В., Савин Л.А., Чернышев В.И.* Теоретические аспекты формирования оптимальных управляемых процессов виброзащиты // *Известия Юго-Западного государственного университета. Серия: Техника и технологии*. 2013. № 3. С. 044–050.
23. *Фоминова О.В.* Прерывистое демпфирование в системах виброзащиты: основы теории, приложения // М.: Машиностроение-1. 2005. 256 с.
24. *Пантелеев А.В., Бортановский А.С.* Теория управления в примерах и задачах // М.: Высшая школа. 2003. 583 с.
25. *Бесекерский В.А., Попов Е.П.* Теория систем автоматического управления // СПб: Профессия. 2003. 752 с.
26. *Фоминова О.В., Белозёрова Е.Б., Чернышев В.И.* Система виброизоляции с управляемым демпфером // *Справочник. Инженерный журнал с приложением*. 2012. № 6. С. 16–22.
27. *Черноузько Ф.Л., Ананьевский И.М., Решмин С.А.* Методы управления нелинейными механическими системами // М.: Физматлит. 2006. 328 с.

Чернышев Владимир Иванович — д-р техн. наук, профессор кафедры мехатроники, механики и робототехники, Орловский государственный университет им. И.С. Тургенева. Область научных интересов: динамика управляемых систем, оптимальное управление, моделирование, природоподобные роботы, механика. Число научных

публикаций — 214. chernyshev_@mail.ru; ул. Комсомольская, 95, Орел, 302026; р.т.: +7(920)287-2495.

Савин Леонид Алексеевич — д-р техн. наук, профессор, заведующий кафедрой мехатроники, механики и робототехники, Орловский государственный университет им. И.С. Тургенева. Область научных интересов: адаптивные опоры роторов, моделирование электрогидродинамических систем, динамика и вибрационная диагностика роторных систем, разработка и исследование мехатронных систем и устройств. Число научных публикаций — 514. savin@ostu.ru; ул. Комсомольская, 95, Орел, 302026; р.т.: +7(910)748-3766.

Фоминова Ольга Владимировна — к-т техн. наук, доцент кафедры мехатроники, механики и робототехники, Орловский государственный университет им. И.С. Тургенева. Область научных интересов: динамика управляемых виброзащитных систем, оптимальное управление, механика, моделирование. Число научных публикаций — 79. mechatronics.orel@yandex.ru; ул. Комсомольская, 95, Орел, 302026; р.т.: +7(919)209-0733.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проект № 16-19-00186).

V.I. CHERNYSHEV, L.A. SAVIN, O.V. FOMINOVA
**INDIRECT CONTROL OF OSCILLATIONS: ELEMENTS OF
THEORY**

Chernyshev V.I., Savin L.A., Fominova O.V. Indirect Control of Oscillations: Elements of Theory.

Abstract. A brief review of the main research areas in the field of controlled vibration protection systems is given. It is shown that Vibration systems with indirect control processes of oscillations allow with a minimum expenditure of energy to ensure programmable switching parameters and structures, in which the dissipative restoring and inertial forces generated on the basis of active impact. Within synthesis of indirect control the chains of new auxiliary mathematical constructs for finding optimal synthesizing functions of the elastic-damping units parameters control are obtained. It enabled to separate a base model with intermittent damping and base model with impulse trap. As a result of the study, based on the harmonic balance method, the dynamic properties of the basic model with intermittent damping, calculation formulas are obtained for determining the parameters of the compensation effect and calculating the dynamic coefficient. It is established that, with an optimal sequence of damping switching, the resonant phenomena are eliminated, and the transient processes decay within one period of the kinematic perturbation. The basic model with a pulse trap imitates the limiting variant of intermittent damping and realizes the process of superimposing constraining bonds, the sequence and duration of which are new variables essentially increasing controllability. And for indirect pulse control, there exists a certain minimum of power consumption independent of the achieved effect of vibration protection. A regulated increase in the duration of the application of the restraining coupling in the low-frequency region and a decrease in this duration in the high-frequency region provides a monotonically decreasing dependence on the dynamic coefficients over the entire frequency range. An example of a solution to the optimization problem of controlling the damping process for a basic model of a vibration isolation system is considered. It is established that intermittent damping is an indispensable feature of the optimality of the vibration isolation system: the damper switches on when the sign of the object's speed has changed and turns off when the object's displacement sign has changed.

Keywords: Oscillations, Vibration Protection Systems, Indirect Control, Optimal and Suboptimal Control, Basic Model With Intermittent Damping, Basic Model with Pulse Trap.

Chernyshev Vladimir Ivanovich — Ph.D., Dr. Sci., Professor of Mechatronics, Mechanics and Robotics Department, Oryol State University. Research interests: Dynamics of Controlled Systems, Optimal Control, Modeling of Dynamic Systems, Nature-Like Robots, Mechanics. The number of publications — 214. chernyshev_@mail.ru; 95, Komsomolskaya str., Orel, 302026, Russia; office phone: +7(920)287-2495.

Savin Leonid Alekseevich — Ph.D., Dr. Sci., Professor, Head of Mechatronics, Mechanics and Robotics Department, Oryol State University. Research interests: Adaptive Support of Rotors, Modeling of Electrohydrodynamic Systems, Dynamics And Vibration Diagnostics of Rotor Systems, Development And Research of Mechatronic Systems And Devices. The number of publications — 514. savin@ostu.ru; 95, Komsomolskaya str., Orel, 302026, Russia; office phone: +7(910)748-3766.

Fominova Olga Vladimirovna — Ph.D., Associate Professor of Mechatronics, Mechanics and Robotics Department, Oryol State University. Research interests: Dynamics of Controlled Vibration Protection Systems, Optimal Control, Mechanics. The number of publications — 79.

chernyshev @mail.ru; 95, Komsomolskaya str., Orel, 302026, Russia; office phone: +7(919)209-0733.

Acknowledgements. The work was supported by the RFBR (project No. 16-19-00186).

Reference

1. Genfeng L., Jing J., Yuhe L., Ming Z. Impact of system anisotropy on vibration reduction of rotating machinery and its evaluation method. *Mechanical Systems and Signal Processing*. 2017. vol. 93. pp. 299–311.
2. Avramov K.V., Mihlin Yu.V. *Nelinejnaya dinamika uprugih sistem. Prilozheniya* [Nonlinear Dynamics of Elastic Systems. Apps]. M.-Izhevsk: Institut komp'yuternyh issledovanij. 2015. Issue 2. 700 p. (In Russ.).
3. Chernyshev V.I., Savin L.A., Fominova O.V. Dynamics of the rotor on elastic-damping supports under action of kinematic effects. IOP Conference Series: Materials Science and Engineering. vol. 233. no.1. pp. 012055.
4. Linfeng D., Zhao R.A. Vibration analysis method based on hybrid techniques and its application to rotating machinery. *Measurement*. 2013. vol. 46. no. 9. pp. 3671–3682.
5. Dorf R., Bishop R. *Sovremennye sistemy upravleniya* [Modern management systems]. M.: Laboratoriya Bazovyh Znanij. 2013. 832 p. (In Russ.).
6. Bai. X.X., Wereley N.M., Choi Y.T. Magnetorheological energy absorber with dual concentric annular valves. *Journal of Intelligent Material Systems and Structures*. 2016. vol. 27. no. 7. pp. 944–958.
7. Dyhta V.A., Samsonyuk O.N. *Optimal'noe impul'snoe upravlenie s prilozheniyami* [Optimal impulse control with applications]. M.: Fizmatlit. 2003. 256 p. (In Russ.).
8. Dyhta V.A. [The positional minimum principle for quasioptimal processes in control problems with terminal constraints]. *Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika*. 2017. Issue 19. pp. 113–128. (In Russ.).
9. Balthazar J.M., Gonçalves, P.B., Fenili A. Nonlinear vibrations in elastic structures: Dynamics and control. *Shock and Vibration*. 2013. vol. 20. no. 6. pp. 1031–1032.
10. Ibrahim R.A. Recent advances in nonlinear passive vibration isolators. *Journal of Sound and Vibration*. 2008. vol. 314. no. 3-5. pp. 371–452.
11. Fominova O.V., Stepanov Yu.S., Chernyshev V.I. *Ehkstremal'nye zadachi i optimizaciya: vvedenie v teoriyu nepryamogo impul'snogo upravleniya processami kolebanij* [Extreme problems and optimization: introduction to the theory of indirect pulse control of oscillation processes]. M.: Izdatel'skij dom «Spektr». 2011. 218 p. (In Russ.).
12. Balandin D.V., Bolotnik N.N., Pilkey W.D. Pre-acting control for shock and pact isolation systems. *Shock and Vibration*. 2005. vol. 12. no. 1. pp. 49–65.
13. Ni Y.Q., Chen Z.H., Or S.W. Experimental identification of a self-sensing magnetorheological damper using soft computing. *Journal of Engineering Mechanics*. 2015. vol. 141. no. 7. pp. 1–13.
14. Eliseev S.V., Orlenko A.I., Nguen D.H. [Devices for the transformation of motion in the structure of a dyad of a mechanical oscillatory system]. *Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta – Vestnik of Don State Technical University*. 2017. vol. 17(3). pp. 46–59. (In Russ.).
15. Eliseev A.V., Sel'vinskij V.V., Eliseev S.V. *Dinamika vibracionnyh vzaimodejstvij ehlementov tekhnologicheskikh sistem s uchetom neuderzhivayushchih svyazej* [Dynamics of vibrational interactions of elements of technological systems with allowance for non-retentive links]. Novosibirsk: Nauka. 2015. 332 p. (In Russ.).
16. Druzhinin V.V., Kontorov D.S. *Sistemotekhnika* [System engineering]. M.: Radio i svyaz'. 1985. 200 p. (In Russ.).

17. Bensuan A., Liozh Zh. *Impul'snoe upravlenie i kvazivariacionnye neravenstva* [Pulse control and quasi-variational inequalities]. M. Nauka. 1987. 596 p. (In Russ.).
18. Ledezma D.F., Ferguson N.S., Zamarripa A.S. Mathematical modeling of a transient vibration control strategy using a switchable mass stiffness compound system. *Shock and Vibration*. 2014. Available at: <http://dx.doi.org/10.1155/2014/565181> (accessed: 18.06.2017)
19. Ledezma D.F., Ferguson N.S., Brennan M.J., Tang B. An experimental nonlinear low dynamic stiffness device for shock isolation. *Journal of Sound and Vibration*. 2015. vol. 347. pp. 1–13.
20. Tang B., Brennan M.J. On the shock performance of a nonlinear vibration isolator with high-static-low-dynamic-stiffness. *International Journal of Mechanical Sciences*. 2014. vol. 81. pp. 207–214.
21. Pegat A. *Nechetkoe modelirovanie i upravlenie* [Unclear modeling and control]. M.: Laboratoriya Bazovyh Znanij. 2009. 798 p. (In Russ.).
22. Fominova O.V., Savin L.A., Chernyshev V.I. [Theoretical aspects of the formation of optimal controlled vibration protection processes]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: tekhnika i tehnologii – Proceedings of the South-West State University Series: Engineering and Technology*. 2019. vol. 3. pp. 044–050. (In Russ.).
23. Fominova O.V. *Preryvistoe dempfirovanie v sistemah vibrozashchity: osnovy teorii, prilozheniya* [Intermittent damping in vibration protection systems: theory bases, applications]. M. Mashinostroenie-1. 2005. 256 p. (In Russ.).
24. Panteleev A.V., Bortanovskij A.S. *Teoriya upravleniya v primerah i zadachah* [Theory of control in examples and problems]. M. Vysshaya shkola 2003. 583 p. (In Russ.).
25. Besekerskiy V.A., Popov Ye.P. *Teoriya sistem avtomaticheskogo upravleniya* [Theory of automatic control systems]. SPb: Professiya. 2003. 752 p. (In Russ.).
26. Fominova O.V., Belozyorova E.B., Chernyshev V.I. [Vibration damping system with controlled damper]. *Spravochnik. Inzhenernyj Zhurnal – Handbook. An Engineering Journal*. 2012. vol. 6. pp. 3–10. (In Russ.).
27. Chernous'ko F.L., Anan'evskij I.M., Reshmin S.A. *Metody upravleniya nelinejnymi mekhanicheskimi sistemami* [Methods of control of nonlinear mechanical systems]. M.: Fizmatlit. 2006. 328 p. (In Russ.).

К. Л. ОВЧАРЕНКО, И. Ю. ЕРЕМЕЕВ, К. В. САЗОНОВ,
С. С. СЕМЕНЮК, А. Н. АБАКУМОВ

РАЗНОСТНО-ДАЛЬНОМЕРНЫЙ МЕТОД ОПРЕДЕЛЕНИЯ МЕСТОПОЛОЖЕНИЯ ЗЕМНЫХ СТАНЦИЙ СПУТНИКОВЫХ СИСТЕМ СВЯЗИ С ПРИМЕНЕНИЕМ РЕТРАНСЛЯТОРА НА БЕСПИЛОТНОМ ЛЕТАТЕЛЬНОМ АППАРАТЕ

Овчаренко К. Л., Еремеев И. Ю., Сазонов К. В., Семенюк С. С., Абакумов А. Н. Разностно-дальномерный метод определения местоположения земных станций спутниковых систем связи с применением ретранслятора на беспилотном летательном аппарате.

Аннотация. Представлен разностно-дальномерный метод определения местоположения современных земных станций с узкими диаграммами направленности. Координаты земной станции предложено вычислять с применением метода максимального правдоподобия путем решения системы из трех дифференциальных уравнений одним из численных методов. При этом дополнительные оценки параметра положения, получаемые в результате измерения взаимной задержки сигналов земной станции, ретранслированных через космический аппарат на геостационарной орбите и подвижный ретранслятор на беспилотном летательном аппарате, позволяют повысить точность оценивания координат земной станции.

Для разработанного метода получены аналитические выражения потенциальной точности вычисления координат земной станции на основе нижней границы Рао-Крамера. Получены аналитические выражения для элементов матрицы Фишера.

Чтобы оценить точность определения местоположения земных станций предложено использовать эллипсоид ошибок, соответствующий положению источника радиоизлучения в пространстве с заданной вероятностью.

Проведен анализ типовых маршрутов движения ретранслятора на беспилотном летательном аппарате и сделан вывод о том, что наилучшая точность при наименьшей протяженности маршрута достигается при движении беспилотного летательного аппарата по окружности, описывающей район контроля.

Выполнен расчет потенциальной точности определения местоположения земной станции для района размером 50 на 50 км. Показано, что погрешность оценок, полученных в результате статистических испытаний, с заданной вероятностью не превосходит размера большой полуоси эллипсоида ошибок, найденного с применением аналитических выражений.

Применение разработанного метода возможно при реализации программной части комплексов радиоэлектронного контроля для противодействия нелегитимному использованию частотного ресурса космических аппаратов-ретрансляторов спутниковых систем связи.

Ключевые слова: определение местоположения, спутниковые системы связи, земная станция, беспилотный летательный аппарат, космический аппарат-ретранслятор, разностно-дальномерный метод, метод максимального правдоподобия.

1. Введение. В настоящее время операторами коммерческих спутниковых систем связи (ССС) отмечается неуклонное увеличение случаев нелегитимного использования частотно-временного ресурса космических аппаратов-ретрансляторов (КА-ретрансляторов), расположенных на геостационарной орбите (ГСО) [1, 2]. С целью противодействия функцио-

нированию нелегитимных земных станций (ЗС) требуется своевременно получать данные об их координатах [3]. Это позволяет вести борьбу с нарушителями на законной правовой основе.

Требуемая точность оценивания координат ЗС, должна быть достаточной для возможности своевременного пресечения несанкционированного использования частотного ресурса КА-ретранслятора. Так, например, при ведении радиоэлектронного контроля (РЭК) в районе с городской застройкой для уверенной локализации нарушителя в пределах одного квартала допустимая погрешность оценивания координат ЗС не должна превышать сотни метров.

На практике наиболее широкое распространение получили методы определения местоположения (ОМП) ЗС с применением нескольких КА-ретрансляторов, расположенных на ГСО, схема реализации которых изображена на рисунке 1. Так, например, в работах [4-7] предлагается использовать метод ОМП ЗС, основанный на измерении взаимных задержек и разностей несущих частот ретранслированных сигналов. При этом в качестве параметра положения (ПП) выступают разность расстояний и разность скоростей, а типовая погрешность оценивания координат ЗС, которая обеспечивается с применением указанных подходов, может достигать нескольких километров.

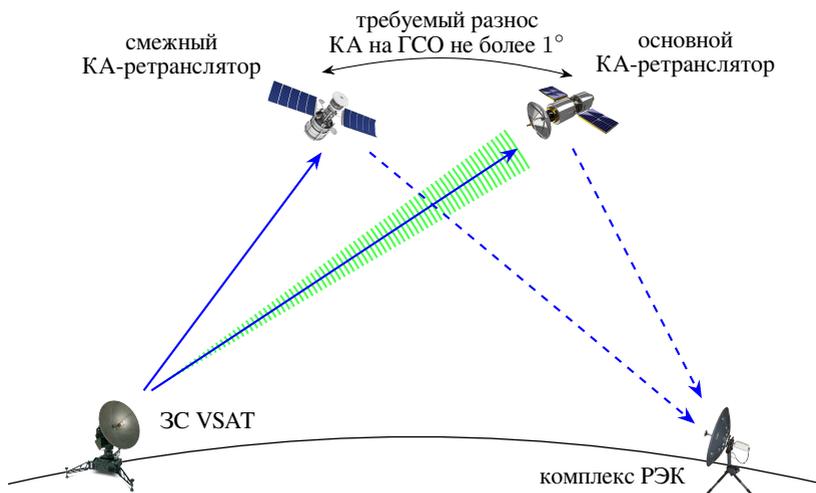


Рис. 1. Схема ОМП ЗС с применением нескольких КА-ретрансляторов

Следует отметить, что у коммерческих потребителей услуг связи все более широкое применение находят современные ССС, построенные на базе малогабаритных ЗС VSAT (Very Small Aperture Terminal) [8], динамика роста числа абонентов которых иллюстрируется на рисунке 2.

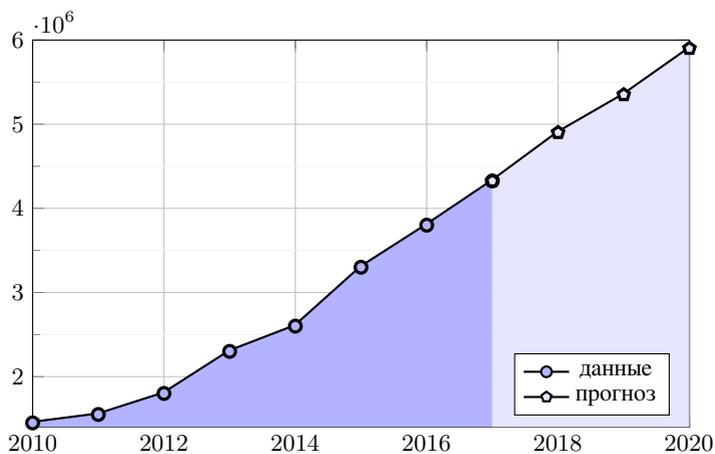


Рис. 2. Динамика роста числа абонентов VSAT в мире

Для ЗС ССС VSAT характерны сравнительно небольшие габариты антенных систем (до 1,8 м) и узкие диаграммы направленности (ДН), ширина основного лепестка которых не превышает нескольких градусов, а предельный уровень боковых лепестков ограничивается с целью недопущения создания помех смежным КА-ретрансляторам, расположенным на ГСО, и определяется следующим выражением [9]:

$$G(\theta) = \begin{cases} 29 - 25 \lg(\theta) & \text{при } 1^\circ < \theta \leq 20^\circ; \\ -3,5 & \text{при } 20^\circ < \theta \leq 26,3^\circ; \\ 32 - 25 \lg(\theta) & \text{при } 26,3^\circ < \theta \leq 48^\circ; \\ -10 & \text{при } 48^\circ < \theta \leq 180^\circ. \end{cases} \quad (1)$$

Вариант ДН в горизонтальной (вертикальной) плоскости для антенны ЗС VSAT изображен на рисунке 3.

Указанные особенности ДН антенных систем ЗС VSAT существенно затрудняют практическую реализацию методов ОМП с применением нескольких КА-ретрансляторов, вследствие сложности отыскания смежных КА-ретрансляторов для ЗС с узкими ДН.

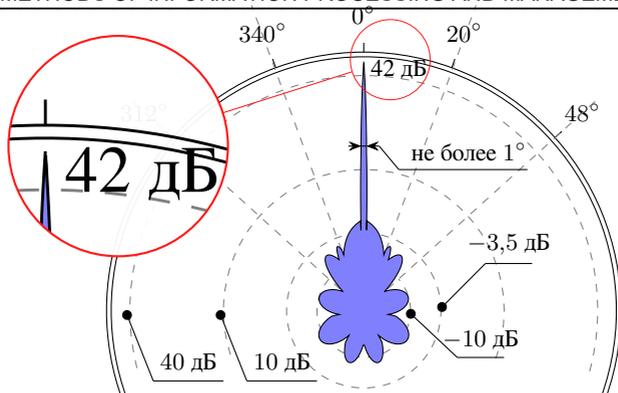


Рис. 3. Вариант диаграммы направленности антенны ЗС VSAT

В настоящее время широкое распространение получают комплексы ОМП на беспилотных летательных аппаратах (БЛА). Так в работах [10, 11] предлагается оценивать координаты на основе измерения энергетических параметров сигналов ЗС. При этом основным недостатком указанных подходов является низкая точность ОМП ЗС. Так, например, погрешность оценивания координат ЗС с применением подхода, описанного в работе [10], составляет несколько сотен метров.

Реализация методов ОМП источников радиоизлучения (ИРИ), где в качестве платформы для пеленгования выступает БЛА [12-15], приводит к возникновению ряда проблем [16], основными из которых являются:

- нестабильность ориентации БЛА в пространстве, которая приводит к резкому увеличению ошибок пеленгования и снижению точности оценивания координат ИРИ [17];
- ограничение массогабаритных показателей полезной нагрузки на БЛА, которые не позволяют разместить на нем громоздкие антенно-фидерные системы (АФС) и многоканальные радиоприемные устройства (РПРУ).

Следует отметить, что применение таких перспективных методов как поляризационное пеленгование [15] в условиях низких отношений сигнал/шум не позволяет обеспечить ошибку оценивания направления на ИРИ меньшую чем несколько градусов, что на расстоянии в десятки километров приводит к погрешности ОМП ИРИ более пяти сотен метров.

2. Постановка задачи. Таким образом, учитывая значимость решения задачи ОМП ЗС с узкими ДН, несанкционированно использующих частотно-временной ресурс КА-ретрансляторов коммерческих ССС, и несовершенство существующих подходов к ОМП современных ЗС VSAT

целью статьи является разработка нового метода ОМП ЗС, адаптированного к условиям применения узконаправленных ДН антенных систем ЗС.

Перспективным представляется разработка комбинированного метода ОМП ЗС с применением КА-ретранслятора и ретранслятора на БЛА. При этом низкое отношение сигнал/шум (ОСШ) на входе РПрУ комплекса РЭК обуславливает необходимость применения в качестве координатно-информативного параметра (КИП) взаимную задержку, многократно вычисляемую (N раз) при корреляционной обработке сигналов, ретранслированных в каналах ЗС-КА-РЭК и ЗС-БЛА-РЭК. Схема реализации предлагаемого метода изображена на рисунке 4.

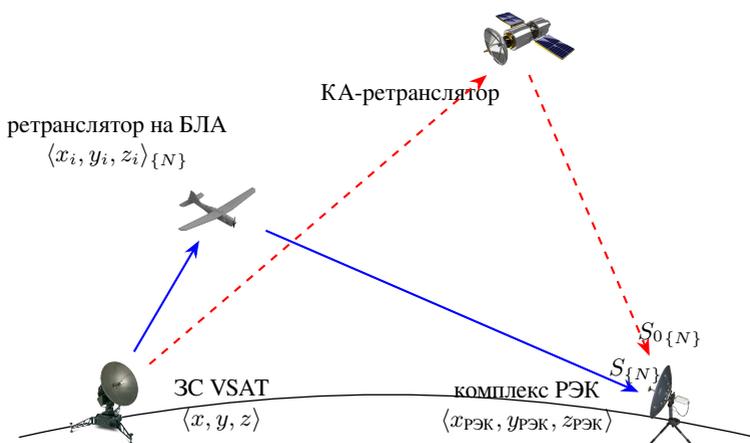


Рис. 4. Схема определения местоположения ЗС CCC

Исходными данными для разработанного метода ОМП ЗС CCC являются:

- множество реализаций сигналов $S_{0\{N\}}$, ретранслированных по линии ЗС-КА-РЭК;
- множество реализаций сигналов $S_{\{N\}}$, ретранслированных по линии ЗС-БЛА-РЭК;
- множество векторов координат $\langle x_{\text{БЛА}_i}, y_{\text{БЛА}_i}, z_{\text{БЛА}_i} \rangle_{\{N\}}$, соответствующих местоположению БЛА в i -й момент измерения КИП;
- вектор координат комплекса РЭК $\langle x_{\text{РЭК}}, y_{\text{РЭК}}, z_{\text{РЭК}} \rangle$,

где $\langle \circ \rangle$ — вектор-строка.

Как правило, при ведении РЭК ОМП ЗС, несанкционированно использующих ресурс коммерческих КА-ретрансляторов, выполняется в несколько этапов, а именно: обнаружение сигналов несанкционированно

функционирующей ЗС и измерение КИП, вычисление ПП и оценивание координат ЗС.

Принимая во внимание тот факт, что оценивание взаимной задержки $\Delta\tilde{\tau}$ сигналов ЗС, ретранслированных через КА $S_{0\{N\}}$ и БЛА $S_{\{N\}}$ в условиях частотного рассогласования, достаточно полно описано в работах [20-22]. Задача измерения КИП в рамках данной статьи рассматриваться не будет. Следовательно, требуется разработать метод ОМП ЗС с узконаправленными ДН, осуществляющий преобразование $F_{\text{ОМП}}$ множества КИП ретранслированных сигналов ЗС, множества координат БЛА и координат комплекса РЭК в координаты ЗС:

$$\langle \Delta\tilde{\tau}_{\{N\}}, \langle x_{\text{БЛА}_i}, y_{\text{БЛА}_i}, z_{\text{БЛА}_i} \rangle_{\{N\}}, \langle x_{\text{РЭК}}, y_{\text{РЭК}}, z_{\text{РЭК}} \rangle \rangle \xrightarrow{F_{\text{ОМП}}} \langle \tilde{x}, \tilde{y}, \tilde{z} \rangle. \quad (2)$$

3. Модель вычисления параметра положения. Наличие не менее четырех оценок КИП (взаимных задержек ретранслированных сигналов) делает возможным ОМП ИРИ в пространстве на основе разностно-дальномерного метода. При этом измерения КИП должны быть независимыми, а координаты измерителей в момент оценивания задержки не должны совпадать.

Вместе с тем наличие дополнительных измерений (избыточной информации о КИП) может быть использовано для повышения точности ОМП ИРИ. Так, например, накопление некоторого множества независимых измерений и последующая их обработка обеспечивает более высокую точность оценивания координат, чем при одиночном измерении.

В силу того, что искомая ЗС стационарна, а управление движением КА-ретранслятора на ГСО не представляется возможным, формирование базы измерений КИП (избыточности) целесообразно осуществлять путем изменения маршрута движения ретранслятора на БЛА.

Как следует из выражения (2), исходными данными для решения задачи ОМП ЗС являются: множество оценок КИП $\Delta\tilde{\tau}_{\{N\}}$; множество векторов координат, соответствующих местоположению БЛА в момент измерения КИП $\langle x_{\text{БЛА}_i}, y_{\text{БЛА}_i}, z_{\text{БЛА}_i} \rangle_{\{N\}}$; и вектор координат комплекса РЭК $\langle x_{\text{РЭК}}, y_{\text{РЭК}}, z_{\text{РЭК}} \rangle$.

Пусть ЗС излучает сигнал в момент времени t_0 , тогда на РПРУ комплекса РЭК он поступает в момент времени $t_{\text{КА}}$ (при ретрансляции через КА) и в момент времени $t_{\text{БЛА}}$ (при ретрансляции через БЛА)

$$\begin{aligned} t_{КА} &= t_{ЗС_КА} + t_{КА_РЭК}; \\ t_{БЛА} &= t_{ЗС_БЛА} + t_{БЛА_РЭК}, \end{aligned} \quad (3)$$

где $t_{ЗС_КА}$ — время распространения сигнала на трассе ЗС-КА; $t_{КА_РЭК}$ — время распространения сигнала на трассе КА-РЭК; $t_{ЗС_БЛА}$ — время распространения сигнала на трассе ЗС-БЛА; $t_{БЛА_РЭК}$ — время распространения сигнала на трассе БЛА-РЭК.

С учетом выражения (3) величина взаимной задержки $\Delta\tau$ может быть найдена по формуле:

$$\Delta\tau = t_{ЗС_КА} + t_{КА_РЭК} - t_{ЗС_БЛА} - t_{БЛА_РЭК}. \quad (4)$$

Вместе с тем очевидно, что ни одно измерение, как бы тщательно оно ни проводилось, не может быть абсолютно точным, поэтому наряду с истинной задержкой $\Delta\tau$ присутствует случайная составляющая $\hat{\xi}_{\tau}$, с учетом которой выражение (4) примет вид:

$$\Delta\tilde{\tau} = \Delta\tau + \hat{\xi}_{\tau} = t_{ЗС_КА} + t_{КА_РЭК} - t_{ЗС_БЛА} - t_{БЛА_РЭК} + \hat{\xi}_{\tau}. \quad (5)$$

От разности моментов времени приема ретранслированных сигналов (5) можно перейти к разности расстояний $\Delta\tilde{R}$ умножив оценку взаимной задержки $\Delta\tilde{\tau}$ на скорость распространения радиоволн C (рисунок 5), а именно:

$$\Delta\tilde{R} = \Delta\tilde{\tau} \cdot C = R_{ЗС_КА} + R_{КА_РЭК} - R_{ЗС_БЛА} - R_{БЛА_РЭК} + \hat{\xi}_R, \quad (6)$$

где $R_{ЗС_КА}$ — расстояние от ЗС до КА-ретранслятора; $R_{КА_РЭК}$ — расстояние от КА-ретранслятора до комплекса РЭК; $R_{ЗС_БЛА}$ — расстояние от ЗС до ретранслятора на БЛА; $R_{БЛА_РЭК}$ — расстояние от ретранслятора на БЛА до комплекса РЭК; $\hat{\xi}_R$ — случайная величина, равная $\hat{\xi}_{\tau} \cdot C$.

По причине отклонения параметров орбит от номинальных КА, расположенный на квазигеостационарной орбите, дрейфует относительно своей подспутниковой точки, описывая в пространстве некоторую кривую. На рисунке 6 изображена траектория суточного движения КА «Экспресс-АМУ1», который активно используется в качестве ретранслятора сигналов ЗС VSAT.

Если баллистические данные КА-ретранслятора известны, например в виде информации, предоставляемой службой NORAD в формате

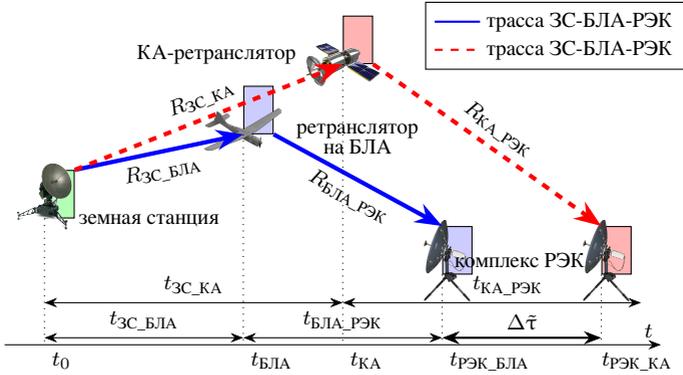


Рис. 5. Схема вычисления параметра положения

TLE (Two-line element), то, применяя модель движения КА [23, 24], можно вычислить вектор координат КА-ретранслятора в каждый i -й момент оценивания КИП.

С учетом этого в качестве ПП можно использовать разность расстояний, схема вычисления которой примет вид, указанный на рисунке 7.

Пусть положению ЗС в пространстве соответствует вектор координат в геоцентрической системе $\langle x, y, z \rangle$, тогда расстояние от ЗС до ретрансляторов на КА и БЛА можно описать следующими выражениями:

$$R_{ЗС_КА_i}(x, y, z) = \sqrt{(x - x_{КА_i})^2 + (y - y_{КА_i})^2 + (z - z_{КА_i})^2}; \quad (7)$$

$$R_{ЗС_БЛА_i}(x, y, z) = \sqrt{(x - x_{БЛА_i})^2 + (y - y_{БЛА_i})^2 + (z - z_{БЛА_i})^2}. \quad (8)$$

Расстояния $R_{КА_РЭК_i}$ и $R_{БЛА_РЭК_i}$ могут быть найдены по известным координатам ретранслятора на БЛА, КА и комплекса РЭК с некоторой погрешностью $\hat{\xi}_{РД_i}$, которая представляет собой сумму нескольких случайных величин, а именно:

$$\hat{\xi}_{РД_i} = \hat{\xi}_{R_i} + \hat{\xi}_{КА_РЭК_i} + \hat{\xi}_{БЛА_РЭК_i}, \quad (9)$$

где $\hat{\xi}_{R_i}$ — величина, пропорциональная погрешности i -го измерения взаимной задержки; $\hat{\xi}_{КА_РЭК_i}$ — погрешность i -го измерения расстояния КА-РЭК; $\hat{\xi}_{БЛА_РЭК_i}$ — погрешность i -го измерения расстояния БЛА-РЭК.

Основное влияние на погрешность оценки ПП оказывает случайная величина $\hat{\xi}_R = C \cdot \hat{\xi}_\tau$, которая определяется погрешностью измерения

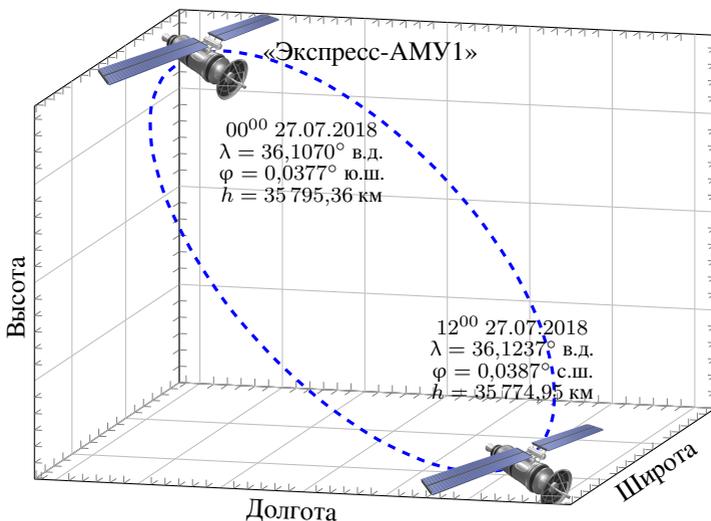


Рис. 6. Движение КА-ретранслятора на квазигеостационарной орбите

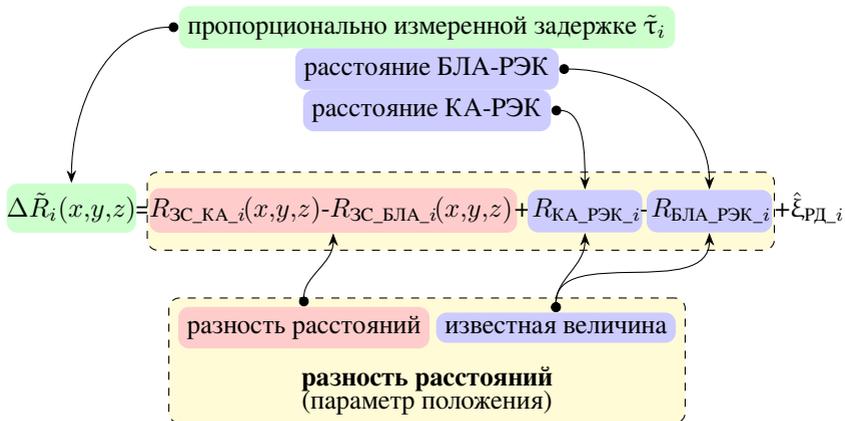


Рис. 7. Схема вычисления параметра положения при i -м измерении

взаимной задержки ретранслированных сигналов ЗС, зависящей от базы накопления сигналов и ОСШ [22].

Величины $\hat{\xi}_{КА_РЭК}$ и $\hat{\xi}_{БЛА_РЭК}$ представляет собой погрешности вычисления расстояния между объектами, которые зависят от точности используемой навигационной системы. Так, например, погрешность оцен-

ки координат, полученной с применением радионавигационных системы ГЛОНАСС и GPS, не превышает нескольких десятков метров [18].

Для оценивания закона распределения случайной величины $\tilde{\xi}_{рД_i}$ была проведена серия статистических испытаний [19] при следующих начальных условиях:

– база ретранслированных сигналов составляет $5 \cdot 10^4$, ОСШ равно минус 10 дБ, вычисление взаимной задержки производится корреляционным методом [21];

– погрешность местоопределения КА-ретранслятора и БЛА подчиняются нормальному закону с нулевым математическим ожиданием (МО) и среднеквадратическим отклонением (СКО) равным 15 м.

Применение метода К. Пирсона для проверки гипотезы о законе распределения случайных величин показало, что при проведении серии из 10 000 испытаний значение показателя согласованности не превышает критическую границу, соответствующую уровню значимости 0,01, а погрешность оценки ПП подчиняется нормальному закону распределения с нулевым МО.

Тот факт, что в рамках рассматриваемой модели оценки ПП независимы, а погрешность их измерения имеет нулевое МО и подчиняется нормальному закону распределения, делает возможным применение метода максимального правдоподобия для оценивания координат ЗС.

4. Метод определения местоположения ЗС с узконаправленными ДН. Метод максимального правдоподобия, как общий для нахождения оценок, впервые был предложен Р. Фишером [25]. Его основу составляет функция правдоподобия, выражающая плотность вероятности совместного появления результатов измерений в виде выборки $\langle \xi_1, \xi_2, \dots, \xi_N \rangle$ при некотором параметре Θ . Поскольку в рамках рассматриваемой модели оценки ПП независимы, функция правдоподобия представляет собой произведение условных гауссовских функций плотности вероятности случайной величины $\varphi_{\tilde{\xi}}(\tilde{\xi}_i/\Theta)$:

$$L_{\tilde{\xi}}(\tilde{\xi}_1, \tilde{\xi}_2, \dots, \tilde{\xi}_N/\Theta) = \prod_{i=1}^N \varphi_{\tilde{\xi}}(\tilde{\xi}_i/\Theta). \quad (10)$$

Для случая, когда координаты КА-ретранслятора в момент измерения i -го ПП $\langle x_{КА_i}, y_{КА_i}, z_{КА_i} \rangle$ известны, функция правдоподобия (10) представляет собой произведение условных гауссовских функций плотности вероятности погрешности оценок разностей расстояний:

$$\begin{aligned}
 & L_{\hat{\xi}_{\text{РД}}}(\Delta\tilde{R}_1, \Delta\tilde{R}_2, \dots, \Delta\tilde{R}_N/x, y, z) = \\
 & = \prod_{i=1}^N \varphi_{\hat{\xi}_{\text{РД}}}(\Delta\tilde{R}_i/x, y, z) = \left(\frac{1}{\sqrt{2\pi}}\right)^N \prod_{i=1}^N \left(\frac{1}{\sigma_{\text{РД}_i}}\right) \times \\
 & \times e^{-\frac{1}{2} \sum_{i=1}^N \left(\frac{\Delta\tilde{R}_i - R_{\text{ЗС_КА}_i}(x, y, z) + R_{\text{ЗС_БЛА}_i}(x, y, z) - R_{\text{КА_РЭК}_i} + R_{\text{БЛА_РЭК}_i}}{\sigma_{\text{РД}_i}}\right)^2},
 \end{aligned} \tag{11}$$

где $\sigma_{\text{РД}_i}$ — СКО случайной величины $\hat{\xi}_{\text{РД}}$ в условиях i -го измерения разности дальностей.

Нетрудно заметить, что функция правдоподобия (11) достигает наибольшего значения при максимальной величине аргумента экспоненты. Следовательно, оценкой координат ЗС по результатам измерений разностей дальности является аргумент минимизации целевой функции $F_{\text{РД}}(x, y, z) =$

$$= \sum_{i=1}^N \left(\frac{\Delta\tilde{R}_i - R_{\text{ЗС_КА}_i}(x, y, z) + R_{\text{ЗС_БЛА}_i}(x, y, z) - R_{\text{КА_РЭК}_i} + R_{\text{БЛА_РЭК}_i}}{\sigma_{\text{РД}_i}}\right)^2$$

$$\begin{aligned}
 \langle \tilde{x}, \tilde{y}, \tilde{z} \rangle & = \operatorname{argmax}_{\{x, y, z\}} \left(L_{\hat{\xi}_{\text{РД}}}(\Delta\tilde{R}_1, \Delta\tilde{R}_2, \dots, \Delta\tilde{R}_N/x, y, z) \right) = \\
 & = \operatorname{argmax}_{\{x, y, z\}} \left(\ln \left(L_{\hat{\xi}_{\text{РД}}}(\Delta\tilde{R}_1, \Delta\tilde{R}_2, \dots, \Delta\tilde{R}_N/x, y, z) \right) \right) = \\
 & = \operatorname{argmin}_{\{x, y, z\}} (F_{\text{РД}}(x, y, z)).
 \end{aligned} \tag{12}$$

Равенству (12) удовлетворяют такие значения $\langle \tilde{x}, \tilde{y}, \tilde{z} \rangle$, которые соответствуют минимуму целевой функции $F_{\text{РД}}(x, y, z)$, и могут быть найдены путем решения системы дифференциальных уравнений следующего вида:

$$\begin{cases} \frac{\partial F_{\text{РД}}(x, y, z)}{\partial x} = 0; \\ \frac{\partial F_{\text{РД}}(x, y, z)}{\partial y} = 0; \\ \frac{\partial F_{\text{РД}}(x, y, z)}{\partial z} = 0, \end{cases} \tag{13}$$

где $\frac{\partial F_{\text{рД}}(x, y, z)}{\partial x}$, $\frac{\partial F_{\text{рД}}(x, y, z)}{\partial y}$, $\frac{\partial F_{\text{рД}}(x, y, z)}{\partial z}$ — частные производные функции $F_{\text{рД}}(x, y, z)$ по x, y, z .

Из теории вероятности известно, что дисперсия случайной величины $\hat{\theta}$ не может быть меньше нижней границы, определяемой неравенством Крамера–Рао [26]

$$D(\hat{\theta}) \geq \frac{1}{I_{\hat{\theta}}}, \quad (14)$$

где $D(\circ)$ — знак дисперсии, I — информация Фишера [27].

В свою очередь, информацию Фишера можно связать с функцией правдоподобия следующим образом [27, 28]:

$$I_{\hat{\theta}} = -M \left(\frac{\partial^2 \ln L_{\xi}(\tilde{\xi}_1, \tilde{\xi}_2, \dots, \tilde{\xi}_N / \theta)}{\partial \theta^2} \right), \quad (15)$$

где $M(\circ)$ — знак математического ожидания.

Для многомерной случайной величины $\hat{\Theta} = \langle \hat{\theta}_1, \hat{\theta}_2, \dots, \hat{\theta}_i \rangle$ ковариационная матрица $K_{\hat{\Theta}}$ является аналогом дисперсии и характеризует степень случайного разброса отдельно по каждой одномерной составляющей $\langle \hat{\theta}_1, \hat{\theta}_2, \dots, \hat{\theta}_i \rangle$ и в целом по многомерной случайной величине $\hat{\Theta}$.

При подстановке функции правдоподобия (10) в выражение (15) информационная матрица Фишера принимает следующий вид:

$$I_{\xi} = -M \left\| \begin{array}{ccc} \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial x^2} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial x \partial y} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial x \partial z} \\ \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial x \partial y} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial y^2} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial y \partial z} \\ \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial x \partial z} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial y \partial z} & \frac{\partial^2 \ln L_{\xi}(\tilde{\xi}/x, y, z)}{\partial z^2} \end{array} \right\|, \quad (16)$$

где $\tilde{\xi} = \langle \tilde{\xi}_1, \tilde{\xi}_2, \dots, \tilde{\xi}_N \rangle$.

Далее, с целью оценивания точности ОМП ЗС представляется возможным подставить выражение для функции правдоподобия (11) в выражение (16).

Для случая, когда параметры движения КА-ретранслятора известны, функцию правдоподобия (11) можно представить следующим образом:

$$L_{\tilde{\xi}_{\text{РД}}}(\Delta\tilde{R}_1, \Delta\tilde{R}_2, \dots, \Delta\tilde{R}_N/x, y, z) = \prod_{i=1}^N \varphi_{\tilde{\xi}_{\text{РД}}}(\Delta\tilde{R}_i/x, y, z) = \left(\frac{1}{\sqrt{2\pi}}\right)^N \cdot \prod_{i=1}^N \left(\frac{1}{\sigma_{\text{РД}_i}}\right) \cdot e^{-\frac{1}{2} \sum_{i=1}^N \left(\frac{R_{\text{РД}_i}(x, y, z) + \tilde{R}_{\Sigma_i}}{\sigma_{\text{РД}_i}}\right)^2}, \quad (17)$$

где $R_{\text{РД}_i}(x, y, z) = R_{\text{ЗС_БЛА}_i}(x, y, z) - R_{\text{ЗС_КА}_i}(x, y, z);$
 $\tilde{R}_{\Sigma_i} = \Delta\tilde{R}_i - R_{\text{КА_РЭК}_i} + R_{\text{БЛА_РЭК}_i}.$

С учетом замены, используемой в выражении (17), логарифм функции правдоподобия преобразуется к виду:

$$\ln L_{\tilde{\xi}_{\text{РД}}}(\Delta\tilde{R}_1, \Delta\tilde{R}_2, \dots, \Delta\tilde{R}_N/x, y, z) = N \cdot \ln \left(\frac{1}{\sqrt{2\pi}}\right) + \sum_{i=1}^N \ln \left(\frac{1}{\sigma_{\text{РД}_i}}\right) - \frac{1}{2} \sum_{i=1}^N \left(\frac{R_{\text{РД}_i}(x, y, z) + \tilde{R}_{\Sigma_i}}{\sigma_{\text{РД}_i}}\right)^2, \quad (18)$$

тогда производные, входящие в состав информационной матрицы Фишера (16), можно представить следующим образом:

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial x^2} = -\sum_{i=1}^N \left(\left(R_{\text{РД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \frac{\partial^2 R_{\text{РД}_i}(x, y, z)}{\partial x^2} + \left(\frac{\partial R_{\text{РД}_i}(x, y, z)}{\partial x} \right)^2 \right) \sigma_{\text{РД}_i}^{-2}; \quad (19)$$

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial y^2} = -\sum_{i=1}^N \left(\left(R_{\text{РД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \frac{\partial^2 R_{\text{РД}_i}(x, y, z)}{\partial y^2} + \left(\frac{\partial R_{\text{РД}_i}(x, y, z)}{\partial y} \right)^2 \right) \sigma_{\text{РД}_i}^{-2}; \quad (20)$$

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial z^2} = -\sum_{i=1}^N \left(\left(R_{\text{PД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \right. \\ \left. \times \frac{\partial^2 R_{\text{PД}_i}(x, y, z)}{\partial z^2} + \left(\frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial z} \right)^2 \right) \sigma_{\text{PД}_i}^{-2}; \quad (21)$$

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial x \partial y} = -\sum_{i=1}^N \left(\left(R_{\text{PД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \right. \\ \left. \times \frac{\partial^2 R_{\text{PД}_i}(x, y, z)}{\partial x \partial y} + \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial x} \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial y} \right) \sigma_{\text{PД}_i}^{-2}; \quad (22)$$

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial x \partial z} = -\sum_{i=1}^N \left(\left(R_{\text{PД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \right. \\ \left. \times \frac{\partial^2 R_{\text{PД}_i}(x, y, z)}{\partial x \partial z} + \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial x} \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial z} \right) \sigma_{\text{PД}_i}^{-2}; \quad (23)$$

$$\frac{\partial^2 \ln L_{\tilde{\xi}}(\tilde{\xi}/x, y, z)}{\partial y \partial z} = -\sum_{i=1}^N \left(\left(R_{\text{PД}_i}(x, y, z) + \tilde{R}_{\Sigma_i} \right) \times \right. \\ \left. \times \frac{\partial^2 R_{\text{PД}_i}(x, y, z)}{\partial y \partial z} + \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial y} \frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial z} \right) \sigma_{\text{PД}_i}^{-2}. \quad (24)$$

Принимая во внимание тот факт, что МО составляющей \tilde{R}_{Σ_i} описывается следующим выражением:

$$M(\tilde{R}_{\Sigma_i}) = R_{\text{ЗС}_\text{КА}_i}(x, y, z) - R_{\text{ЗС}_\text{БЛА}_i}(x, y, z), \quad (25)$$

МО суммы, входящей в состав производных (19)-(24), будет равно нулю $M(\tilde{R}_{\Sigma_i} + R_{\text{PД}_i}(x, y, z)) = 0$, а матрица (16) примет вид:

$$I_{\tilde{\xi}} = \|i_{mn}\|_3^3, \quad (26)$$

при этом ее элементы можно представить следующим образом:

$$i_{11} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial x} \right)^2; \quad (27)$$

$$i_{22} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial y} \right)^2; \quad (28)$$

$$i_{33} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial z} \right)^2; \quad (29)$$

$$i_{12} = i_{21} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial x} \right) \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial y} \right); \quad (30)$$

$$i_{13} = i_{31} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial x} \right) \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial z} \right); \quad (31)$$

$$i_{23} = i_{32} = \sum_{l=1}^N \sigma_{\text{РД}_l}^{-2} \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial y} \right) \cdot \left(\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial z} \right). \quad (32)$$

Частные производные, входящие в состав выражений (27)–(32), примут вид:

$$\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial x} = \frac{x - x_{\text{БЛА}_l}}{\sqrt{(x-x_{\text{БЛА}_l})^2+(y-y_{\text{БЛА}_l})^2+(z-z_{\text{БЛА}_l})^2}} - \frac{x - x_{\text{КА}_l}}{\sqrt{(x-x_{\text{КА}_l})^2+(y-y_{\text{КА}_l})^2+(z-z_{\text{КА}_l})^2}}; \quad (33)$$

$$\frac{\partial R_{\text{РД}_l}(x, y, z)}{\partial y} = \frac{y - y_{\text{БЛА}_l}}{\sqrt{(x-x_{\text{БЛА}_l})^2+(y-y_{\text{БЛА}_l})^2+(z-z_{\text{БЛА}_l})^2}} - \frac{y - y_{\text{КА}_l}}{\sqrt{(x-x_{\text{КА}_l})^2+(y-y_{\text{КА}_l})^2+(z-z_{\text{КА}_l})^2}}; \quad (34)$$

$$\frac{\partial R_{\text{PД}_i}(x, y, z)}{\partial z} = \frac{z - z_{\text{БЛА}_i}}{\sqrt{(x-x_{\text{БЛА}_i})^2 + (y-y_{\text{БЛА}_i})^2 + (z-z_{\text{БЛА}_i})^2}} - \frac{z - z_{\text{КА}_i}}{\sqrt{(x-x_{\text{КА}_i})^2 + (y-y_{\text{КА}_i})^2 + (z-z_{\text{КА}_i})^2}}. \quad (35)$$

На основании полученных выражений (26)-(35) можно сделать вывод, что точность оценивания координат ЗС не зависит от вектора измеренного ПП \tilde{R}_i и определяется совокупностью координат БЛА $\langle x_{\text{БЛА}_i}, y_{\text{БЛА}_i}, z_{\text{БЛА}_i} \rangle$, КА-ретранслятора $\langle x_{\text{КА}_i}, y_{\text{КА}_i}, z_{\text{КА}_i} \rangle$ (в которых были сделаны N измерений разности дальностей), местоположением ЗС $\langle x, y, z \rangle$ и СКО оценки ПП $\sigma_{\text{PД}_i}$.

Важнейшей характеристикой качества функционирования системы ОМП является точность оценивания координат ИРИ. Ее можно оценить через статистические характеристики ошибки ОМП, а именно: среднеквадратическую ($\sigma_{\text{ОМП}}$), квазимаксимальную ($2\sigma_{\text{ОМП}}$) и максимальную ошибку ($3\sigma_{\text{ОМП}}$).

Вместе с тем наиболее полное представление о местоположении ИРИ дает эллипс ошибок на плоскости или эллипсоид в пространстве. Именно он соответствует области, внутри которой ИРИ находится с заданной вероятностью [29].

Оценки вектора координат ЗС $\tilde{S}_{\text{ЗС}} = \langle \tilde{x}, \tilde{y}, \tilde{z} \rangle$, полученные методом максимального правдоподобия, распределены по нормальному закону с математическим ожиданием $M(\tilde{S}_{\text{ЗС}})$, равным истинному положению ИРИ в пространстве. Поэтому трехмерная плотность распределения координат $\varphi_{\tilde{S}_{\text{ЗС}}}$ описывается многомерным распределением следующего вида:

$$\varphi_{\tilde{S}_{\text{ЗС}}} = \frac{1}{\sqrt{(2\pi)^3 |\mathbf{I}^{-1}|}} e^{-\frac{1}{2}(\mathbf{S}_{\text{ЗС}} - M(\tilde{S}_{\text{ЗС}})) \cdot \mathbf{I} \cdot (\mathbf{S}_{\text{ЗС}} - M(\tilde{S}_{\text{ЗС}}))^T}, \quad (36)$$

где \mathbf{I} — матрица Фишера, полученная на основе функции правдоподобия (10).

Поверхность равной плотности вероятности — эллипсоид ошибок может быть построен, если приравнять показатель степени экспоненты в выражении (36) к некоторой постоянной величине λ_P^2 :

$$(\mathbf{S}_{\text{ЗС}} - M(\tilde{S}_{\text{ЗС}})) \cdot \mathbf{I} \cdot (\mathbf{S}_{\text{ЗС}} - M(\tilde{S}_{\text{ЗС}}))^T = \lambda_P^2. \quad (37)$$

Следует отметить, что λ_P выбирается с учетом заданной вероятности нахождения ЗС внутри эллипсоида ошибок, которая вычисляется по формуле [29] и иллюстрируется графиком, представленным на рисунке 8.

$$P(\lambda_P) = \Phi(\sqrt{2}\lambda_P) - \frac{2}{\sqrt{\pi}} \cdot \lambda_P \cdot e^{-\lambda_P^2}, \quad (38)$$

где $\Phi(\circ)$ — функция распределения нормального закона (интеграл вероятности).

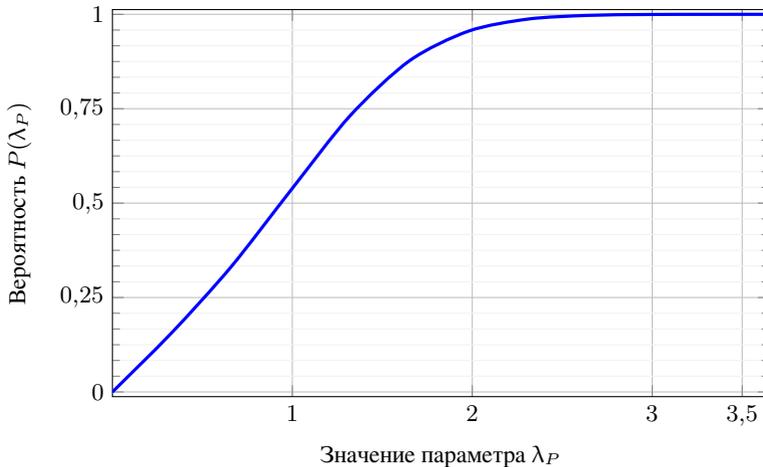


Рис. 8. Зависимость вероятности нахождения ЗС внутри эллипсоида ошибок от значения параметра λ_P

Методика вычисления параметров эллипсоида ошибок, к которым относится размер полуосей, а также его объем, подробно описана в работе [30] и в рамках данной статьи рассматриваться не будет.

5. Выбор маршрута движения ретранслятора на БЛА. Принимая во внимание тот факт, что для оценивания координат ИРИ в пространстве необходимо не менее четырех оценок ПП, а также то, что с увеличением числа независимых измерений снижается погрешность оценки координат ЗС, получаемой методом максимального правдоподобия, для проведения имитационного моделирования с целью выбора маршрута движения ретранслятора на БЛА представляется возможным ограничиться ста измерениями ПП.

Типовые маршруты полета ретранслятора БЛА и соответствующие им гистограммы объема эллипсоида ошибок, характеризующие величину погрешности ОМП ЗС [30], представлены на рисунках 9 и 10.

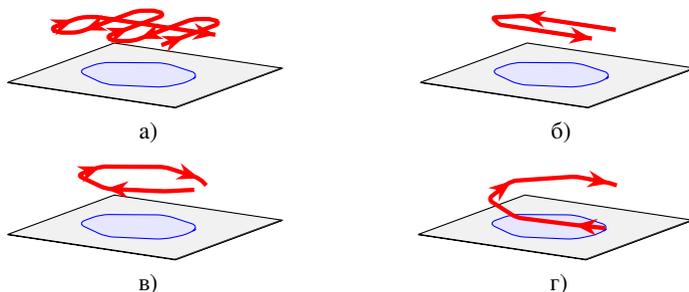


Рис. 9. Траектория движения ретранслятора на БЛА для маршрута:
а – № 1; б – № 2; в – № 3; г – № 4

Данные об объеме эллипсоида ошибок получены при условии $P(\lambda_P) = 0,95$ на основании оценок взаимной задержки, рассчитанных в момент нахождения ретранслятора в каждой из ста точек, равномерно распределенных по маршруту движения на БЛА, для фиксированного значения базы ретранслированного сигнала ЗС ($B = 10^5$).

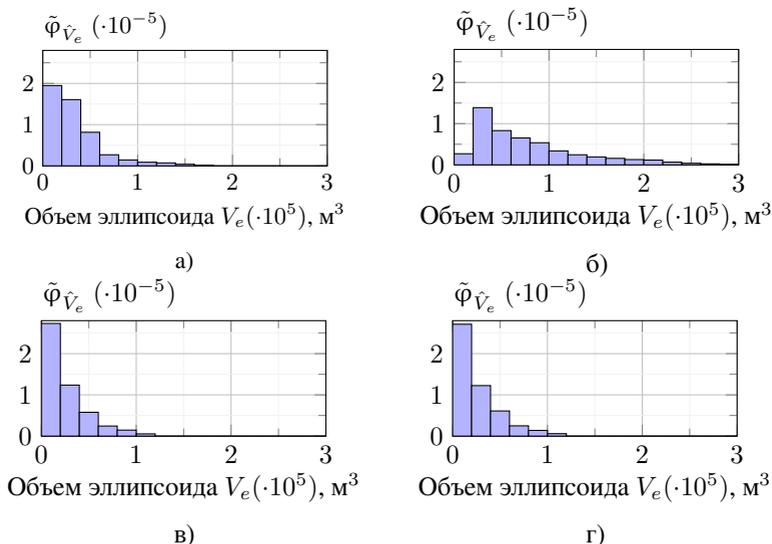


Рис. 10. Гистограмма объема эллипсоида ошибок для маршрута ретранслятора на БЛА: а – № 1; б – № 2; в – № 3; г – № 4

При построения гистограмм использована выборка значений объема эллипсоида ошибок, которые были получены для 400 точек,

соответствующих местоположению ЗС и равномерно распределенных в районе контроля.

Из гистограмм, изображенных на рисунке 10, следует, что наилучшую точность (минимальный объем эллипсоида ошибок) при наименьшей протяженности маршрута движения БЛА позволяет обеспечить круговая траектория (маршрут № 3) с радиусом, позволяющим облететь район контроля по периметру.

6. Потенциальная точность оценивания координат ЗС. Для иллюстрации потенциальной точности оценивания координат ЗС, достигаемой с применением разработанного метода, выполнен расчет параметров эллипсоида ошибок [30] при следующих условиях (рисунок 11):

- несанкционированно функционирующая ЗС VSAT находится в районе г. Санкт-Петербург ($59,84^\circ$ с.ш., $30,39^\circ$ в.д.);
- в качестве КА-ретранслятора выступает «Экспресс-АМУ1» (подспутниковая точка $36,0^\circ$ в.д.);
- комплекс РЭК расположен в точке с координатами $60,1^\circ$ с.ш., $30,64^\circ$ в.д.;
- ретранслятор на БЛА выполняет облет района вероятного нахождения ЗС по окружности с радиусом 25 км на высоте 2 000 м.

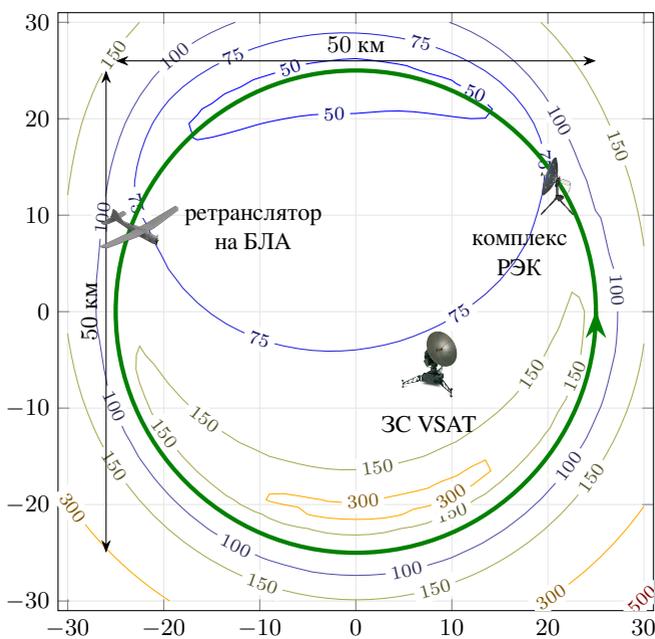


Рис. 11. Потенциальная точность ОМП ЗС VSAT

На рисунке 11 изображены изолинии потенциальной точности оценивания координат ЗС VSAT. В качестве показателя точности ОМП ЗС используется размер большой полуоси эллипсоида ошибок, полученный при вероятности попадания оценки координат ЗС VSAT внутрь эллипсоида ошибок, равной 0,95, на основании оценок взаимной задержки, рассчитанных в момент нахождения ретранслятора в каждой из ста точек, равномерно распределенных по маршруту движения БЛА.

С целью проверки соответствия результатов расчета потенциальной точности ОМП ЗС результатам вычисления координат ЗС предложенным методом проведено имитационное моделирование в среде Matlab.

Поиск минимума целевой функции $F_{рд}(x, y, z)$ выполнялся с применением встроенной процедуры *fminsearch*, основу которой составляет метод прямого поиска минимума функции нескольких переменных (метод Нелдера — Мида) [31]. Для минимизации целевой функции в качестве начальной была выбрана точка с координатами, соответствующими центру топоцентрической системы координат (рисунок 11).

По результатам проведения 10 000 испытаний в ходе которых выполнялось оценивание координат ЗС разработанным методом построена гистограмма погрешностей вычисления координат ЗС VSAT.

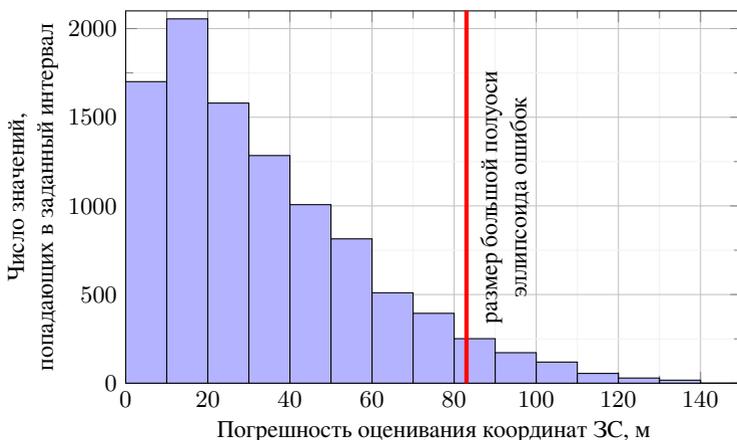


Рис. 12. Гистограмма погрешностей оценивания координат ЗС VSAT

Из гистограммы, изображенной на рисунке 12, следует, что погрешность оценивания координат ЗС VSAT с вероятностью 0,95 не превышает 83 м, что согласуется с результатами расчета потенциальной точности ОМП, полученными аналитическим путем.

7. Заключение. Применение разработанного метода определения местоположения земных станций ССС позволяет вычислять координаты земных станций с узкими диаграммами направленности. При этом в качестве параметра положения используется разность дальностей, полученная на основе оценок взаимной задержки сигналов земной станции, ретранслированных через космический аппарат и беспилотный летательный аппарат.

На основании полученных выражений потенциальной точности оценивания координат земных станций ССС можно сделать вывод о том, что погрешность определения местоположения не зависит от конкретных значений оценок параметра положения и определяется совокупностью координат беспилотного летательного аппарата, космического аппарата-ретранслятора (в которых были сделаны измерения разности дальностей), местоположением земной станции и среднеквадратическим отклонением оценок параметра положения.

При ведении радиоэлектронного контроля с применением разработанного метода в районе размером 50 на 50 км погрешность оценивания координат земных станций VSAT с вероятностью большей чем 0,95 не превышает сотни метров, что подтверждается аналитическими расчетами, а также результатами статистических испытаний при имитационном моделировании в среде Matlab.

Реализация на практике разработанного метода определения местоположения земных станций позволит существенно повысить точность оценивания их координат по сравнению с той, которая достигается в современных комплексах радиоэлектронного контроля, построенных на базе известных методов определения местоположения источников радиоизлучения [10, 15], что делает возможным уверенную локализацию нарушителя в пределах одного квартала района с городской застройкой.

Литература

1. *Верзунов Г. В., Корвяков П. В., Могучев В. И.* Спутниковая связь: радиопеленгация земных станций // Спутниковая связь и вещание. 2009. С. 98–102.
2. *Chan M. H.* Application of a dual satellite geolocation system on locating sweeping interference // World Academy of Science, Engineering and Technology. 2012. vol. 6. pp. 939–944.
3. *Haworth D. P., Smith N. G., Bardelli R., Clement T.* Interference localization for Eutelsat satellites – the first European transmitter location system // International Journal of satellite communications. 1997. vol. 15. pp. 155–183.
4. *Passion T., Chou S. I.* Sensitivity analysis of dual-satellite geolocation // IEEE Transactions on Aerospace and Electronic Systems. 2000. vol. 36. no. 1. pp. 56–71.
5. *Hima S. K., Murali P. P.* Geolocation using TDOA and FDOA Measurements in sensor networks Using Non-Linear Elements // International Journal of Engineering Trends and Technology. 2014. vol. 14. no. 1. pp. 35–39.

6. *Cao Y., Li P., Yang L., Guo F.* A new iterative algorithm for geolocating a known altitude target using TDOA and FDOA measurements in the presence of satellite location uncertainty // Chinese Journal of Aeronautics. 2015. vol. 28. no. 5. pp. 1510-1518.
7. *Волков Р. В., Севидов В. В., Богдановский С. В., Теслевич С. Ф.* Модель поверхности Земли при определении местоположения земной станции по сигналам спутников-ретрансляторов // Наукоемкие технологии. 2016. Т. 17. № 12. С. 44–50.
8. Northern Sky Research's Broadband Satellite Markets Report. URL: <http://www.nsr.com/research-reports/satellite-communications-1/> (дата обращения: 19.04.2018).
9. *Maral G.* VSAT Networks, Second Edition // John Wiley & Sons. 2004. 294 p.
10. *Маренков И. А., Бережных Д. Л., Голиков И. Ю., Печурин В. В.* Способ определения местоположения наземного источника радиоизлучения системы спутниковой связи. Патент № 2583450. 2016. 7 с.
11. *Engebråten A. E.* RF Emitter geolocation using PDOA algorithms and UAVs // Norwegian University of Science and Technology Department of Computer and Information Science. 2015. 138 p.
12. *Robert J. B., Jay G. M., Ravi P. G., David H. S.* Autonomous Geolocation of RF Emitters Using Small, Unmanned Platforms // Johns Hopkins Apl Technical Digest. 2013. vol. 32. no. 3. pp. 636–646.
13. *Богдановский С. В., Овчаренко К. Л., Симонов А. Н.* Метод определения координат источников радиоизлучения на основе поляризационных измерений // Труды ВКА имени А.Ф.Можайского. 2017. № 657. С. 38–43.
14. *Richard G. P.* Electronic Warfare Target Location Methods, Second Edition // Artech House. 2012. 442 p.
15. *Богдановский С. В., Симонов А. Н., Теслевич С. Ф.* Поляризационный метод пеленгования источников радиоизлучения в пространстве // Наукоемкие технологии. 2016. Т. 17. № 12. С. 40–43.
16. *Овчаренко К. Л.* Определение координат источников радиоизлучения дальномерным методом на базе однопозиционного подвижного измерителя // Телекоммуникации. 2013. № 10. С. 27–34.
17. *Богдановский С. В., Симонов А. Н., Севидов В. В.* Поляризационный способ определения ориентации БЛА // Успехи современной радиоэлектроники. 2017. № 10. С. 15–19.
18. *Sarkar S., Bose A.* Contribution of GLONASS in Multi-GNSS Solution Accuracy // Coordinates. 2015. vol. 11. pp. 13-16.
19. *Юсупов Р. М. и др.* Статистические методы обработки результатов измерений // Министерство обороны СССР. 1984. 563 с.
20. *Замарин А. И., Еремеев И. Ю., Овчаренко К. Л.* Сравнительный анализ подходов к оцениванию задержки сигналов в условиях априорной неопределенности взаимного частотного сдвига // Естественные и технические науки. 2017. № 2. С. 126–130.
21. *Еремеев И. Ю., Овчаренко К. Л.* Метод вычислительно-эффективного оценивания взаимных временных задержек в условиях априорной неопределенности частотных сдвигов сигналов спутниковых терминалов // Труды ВКА имени А.Ф.Можайского. 2016. № 651. С. 98–105.
22. *Овчаренко К. Л.* Потенциальная точность оценивания задержки сигналов при наличии частотного рассогласования на основе вычисления взаимной корреляционной функции модифицированных комплексных огибающих // Успехи современной радиоэлектроники. 2017. № 7. С. 39–44.
23. *Ma L., Xu X., Pang F.* Accuracy Assessment of Geostationary-Earth-Orbit with Simplified Perturbations Models // Artificial satellites. 2016. vol. 51. no. 2. pp. 55–59.

24. *San-Juan J. F., Perez I., San-Martin M., Vergara E. P.* Hybrid SGP4 orbit propagator // *Acta Astronautica*. 2017. vol. 137. pp. 254–260.
25. *Aldrich J.* RA Fisher and the Making of Maximum Likelihood 1912 – 1922 // *Statistical Science*. 1997. vol. 12. no. 3. pp. 162–176.
26. *Kay S. M.* Fundamentals of Statistical Signal Processing: Estimation Theory // Prentice Hall. 1993. 595 p.
27. *Lehmann E. L., Casella G.* Theory of Point Estimation, Second Edition // Springer. 1998. 590 p.
28. *Steven M. K., Casella G.* Fundamentals of Statistical Signal Processing: Estimation Theory // Prentice Hall PTR. 1993. 608 p.
29. *Сайбель А. Г.* Основы теории точности радиотехнических методов местоопределения: учеб. пособие // М.: Оборонгиз. 1958. 56 с.
30. *Овчаренко К. Л., Еремеев И. Ю., Гайчук Ю. Н., Петухов П. Е.* Методика построения эллипсоида ошибок для оценивания точности определения местоположения земных станций систем спутниковой связи с применением беспилотного летательного аппарата // *Наукоёмкие технологии*. 2017. Т. 18. № 11. С. 22–26.
31. *Lagarias J. C., Reeds J. A., Wright M. H., Wright P. E.* Convergence Properties of the Nelder-Mead Simplex Method in Low Dimensions // *SIAM Journal of Optimization*. 1998. vol. 9. no. 1. pp.112–147.

Овчаренко Константин Леонидович — адъюнкт кафедры технических средств комплексного контроля ракетно-космических объектов, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: определение местоположения источников радиоизлучения. Число научных публикаций — 20. kostao@ya.ru; ул. Ждановская, 13, г. Санкт-Петербург, 197198; р.т.: +7 (812) 347-95-57.

Еремеев Игорь Юрьевич — д-р техн. наук, профессор, начальник кафедры технических средств комплексного контроля ракетно-космических объектов, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: обработка сигналов со сложной частотно-временной структурой в условиях априорной неопределенности относительно параметров сигналаобразования. Число научных публикаций — 100. eremeevii@yandex.ru; ул. Ждановская, 13, г. Санкт-Петербург, 197198; р.т.: +7 (812) 347-95-57.

Сазонов Константин Викторович — д-р техн. наук, доцент, начальник кафедры инженерного анализа, Военно-космическая академия имени А. Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: системы сбора и обработки информации, обратное проектирование современных телекоммуникационных систем. Число научных публикаций — 70. Staffa78@mail.ru; ул. Ждановская, 13, г. Санкт-Петербург, 197198; р.т.: +7 (812) 230-28-15.

Семенов Сергей Сергеевич — канд. техн. наук, преподаватель кафедры технических средств комплексного контроля ракетно-космических объектов, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: определение местоположения источников радиоизлучения. Число научных публикаций — 20. sergio_ss@bk.ru; ул. Ждановская, 13, г. Санкт-Петербург, 197198; р.т.: +7 (812) 347-95-57.

Абакумов Артем Николаевич — канд. техн. наук, преподаватель кафедры технических средств комплексного контроля ракетно-космических объектов, Военно-космическая академия имени А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: определение местоположения источников радиоизлучения. Число научных публикаций — 20. koristinij_517@mail.ru; ул. Ждановская, 13, г. Санкт-Петербург, 197198; р.т.: +7 (812) 347-95-57.

K. L. OVCHARENKO, I. Yu. EREMEEV, K. V. SAZONOV,
S. S. SEMENJUK, A. N. ABAKUMOV

**DIFFERENTIAL RANGING METHOD OF LOCATING SATELLITE
COMMUNICATION SYSTEM EARTH STATIONS USING
REPEATER ON AN UNMANNED AERIAL VEHICLE**

Ovcharenko K. L., Ereemeev I. Yu., Sazonov K. V., Semenjuk S. S., Abakumov A. N. **Differential ranging method of locating satellite communication system earth stations using repeater on an unmanned aerial vehicle.**

Abstract. The article presents the differential ranging method of locating modern earth stations with narrow radiation patterns. Earth station position data is proposed to be calculated using maximum-likelihood procedure system solution from three differential equations using one of numerical methods. In this case supplementary assessment parameter of location, calculated by measuring a mutual signal delay of an earth station, relayed through a spacecraft on geostationary orbit and a mobile repeater on the unmanned aerial vehicle, can improve the accuracy of coordinate estimation earth station.

For the developed method the analytical expressions of potential accuracy of calculation of coordinates of the earth station on the basis of the Cramer–Rao lower bound are developed.

To measure the positioning accuracy of located emitters it is suggested to use the errors ellipsoid corresponding to the provision of a source of a radio emission in space.

The analysis of standard routes of the movement of a repeater on the unmanned aerial vehicle is carried out and the conclusion is drawn that the best accuracy and the shortest route simultaneously are achieved, if the unmanned aerial vehicle follows a circular trajectory along the control area.

Calculation of potential accuracy of positioning of the terrestrial station for the area of 50 by 50 km is executed. It is shown that the error of the estimates, received as a result of statistical tests, doesn't surpass the size of a big half shaft of the error ellipsoid calculated with application of analytical expressions.

The application of the developed method is possible in the implementation of the software of electronic control systems to counteract illegitimate use of frequency resource of space vehicles-satellite repeaters communication system.

Keywords: Position Location, Satellite Communications Systems, Earth Station, Unmanned Aerial Vehicle, Repeater Spacecraft, Differential Ranging Method, Method of Maximum Likelihood.

Ovcharenko Konstantin Leonidovich — Ph.D. student of the space-rocket object integrated control facilities department, Mozhaisky Military Space Academy. Research interests: Definition of the Locations of Radiowaves Sources. The number of publications — 20. kostao@ya.ru; 13, Zhdanovskaya str., St. Petersburg, 197198, Russia; office phone: +7 (812) 347-95-57.

Ereemeev Igor' Yur'evich — Ph.D., Dr. Sci., professor, head of the space-rocket object integrated control facilities department, Mozhaisky Military Space Academy. Research interests: Difficult Time-and-Frequency Structure Signal Processing under the Conditions Generation Signal Parameters Prior Indetermination. The number of publications — 100. eremeeviu@yandex.ru; 13, Zhdanovskaya str., St. Petersburg, 197198, Russia; office phone: +7 (812) 347-95-57.

Sazonov Konstantin Viktorovich — Ph.D., Dr. Sci., associate professor, head of the reverse engineering department, Mozhaisky Military Space Academy. Research interests: Data Acquisition

and Processing System, Reverse Engineering Modern Telecommunication System. The number of publications — 70. Staffa78@mail.ru; 13, Zhdanovskaya str., St. Petersburg, 197198, Russia; office phone: +7 (812) 230-28-15.

Semenjuk Sergej Sergeevich — Ph.D., lecturer of the space-rocket object integrated control facilities department, Mozhaisky Military Space Academy. Research interests: Definition of the Locations of Radiowaves Sources. The number of publications — 20. sergio_ss@bk.ru; 13, Zhdanovskaya str., St. Petersburg, 197198, Russia; office phone: +7 (812) 347-95-57.

Abakumov Artjom Nikolaevich — Ph.D., lecturer of the space-rocket object integrated control facilities department, Mozhaisky Military Space Academy. Research interests: Definition of the Locations of Radiowaves Sources. The number of publications — 20. koristnij_517@mail.ru; 13, Zhdanovskaya str., St. Petersburg, 197198, Russia; office phone: +7 (812) 347-95-57.

References

1. Verzunov G. V., Korvyakov P. V., Moguchev V. I. [Satellite communication: ground station radio direction]. *Sputnikovaja svjaz' i veshhanie – Satellite communication and broadcasting*. 2009. pp. 98-102. (In Russ.).
2. Chan M. H. Application of a dual satellite geolocation system on locating sweeping interference. *World Academy of Science, Engineering and Technology*. 2012. vol. 6. pp. 939–944.
3. Haworth D. P., Smith N. G., Bardelli R., Clement T. Interference localization for Eutelsat satellites – the first European transmitter location system. *International Journal of satellite communications*. 1997. vol. 15. no. 4. pp. 155–183.
4. Passion T., Chou S. I. Sensitivity analysis of dual-satellite geolocation. *IEEE Transactions on Aerospace and Electronic Systems*. 2000. vol. 36. no. 1. pp. 56–71.
5. Hima S. K., Murali P. P. Geolocation using TDOA and FDOA Measurements in sensor networks Using Non-Linear Elements. *International Journal of Engineering Trends and Technology*. 2014. vol. 14. no. 1. pp. 35–39.
6. Cao Y., Li P., Yang L., Guo F. A new iterative algorithm for geolocating a known altitude target using TDOA and FDOA measurements in the presence of satellite location uncertainty // *Chinese Journal of Aeronautics*. 2015. vol. 28. no. 5. pp. 1510-1518.
7. Volkov R. V., Sevidov V. V., Bogdanovskij S. V., Teslevich S. F. [Earth surface model at ground station determining location by a satellite repeater signal]. *Naukoemkie tekhnologii – Intensive Technologies*. 2016. Issue 17. vol. 12. pp. 44-50. (In Russ.).
8. Northern Sky Research's Broadband Satellite Markets Report. Available at: <http://www.nsr.com/research-reports/satellite-communications-1/> (accessed: 19.04.2018).
9. Maral G. VSAT Networks, Second Edition. John Wiley & Sons. 2004. 294 p.
10. Marenkov I. A., Bereznyh D. L., Golikov I. Ju., Pechurin V. V. Sposob opredeleniya mestopolozheniya nazemnogo istochnika radioizlucheniya sistemy sputnikovoj svjazi [Method of satellite communication system radio source determining location]. Patent RF. no. 2583450. 2016. 7 c.
11. Engebråten A. E. RF Emitter geolocation using PDOA algorithms and UAVs. Norwegian University of Science and Technology Department of Computer and Information Science. 2015. 138 p.
12. Robert J. B., Jay G. M., Ravi P. G., David H. S. Autonomous Geolocation of RF Emitters Using Small, Unmanned Platform. *Johns Hopkins Apl Technical Digest*. 2013. vol. 32. no. 3. pp. 636–646.
13. Bogdanovskij S. V., Ovcharenko K. L., Simonov A. N. [Radio source determining location method based on the of polarization measurements]. *Trudy VKA imeni A.F. Mozhajskogo – Proceeding MSA n.a. A.F.Mozhajskogo*. 2017. vol. 657. pp. 38-43. (In Russ.).

14. Richard G. P. *Electronic Warfare Target Location Methods: Second Edition*. Artech House. 2012. 442 p.
15. Bogdanovskij S. V., Simonov A. N., Teslevich S. F. [A polarization method of spatial radio source direction finding]. *Naukoemkie tekhnologii – Intensive Technologies*. 2016. Issue. 17. vol. 12. pp. 40-43. (In Russ.).
16. Ovcharenko K. L. [Determination of coordinates of sources of a radio emission by a ranging method on the basis of the one-position mobile measuring instrument]. *Telekommunikacii – Telecommunications*. 2013. vol. 10. pp. 27–34. (In Russ.).
17. Bogdanovskij S. V., Simonov A. N., Sevidov V. V. [Polarization method of determining the orientation of the unmanned aerial vehicle]. *Uspekhi sovremennoj radioelektroniki – Achievements of Modern Radioelectronics*. 2017. vol. 10. pp. 15-19. (In Russ.).
18. Sarkar S., Bose A. Contribution of GLONASS in Multi-GNSS Solution Accuracy. *Coordinates*. 2015. vol. 11. pp. 13-16.
19. Jusupov R. M. et al. *Statisticheskie metody obrabotki rezul'tatov izmerenij* [Statistical methods for processing measurement result]. Ministerstvo oborony SSSR. 1984. 563 s. (In Russ.).
20. Zamarin A. I., Ereemeev I. Ju., Ovcharenko K. L. [Treatment comparative analysis of signal delay appraisalment in prior uncertainty mutual frequency offset conditions]. *Estestvennyye i tekhnicheskie nauki – Natural and technical science*. 2017. vol. 2. pp. 126-130. (In Russ.).
21. Ereemeev I. Ju., Ovcharenko K. L. [The method of computationally effective estimation of mutual time delays under conditions of a priori uncertainty in the frequency shifts of the signals of satellite terminals.] *Trudy VKA imeni A.F. Mozhajskogo – Proceeding MSA n.a. A.F. Mozhajskogo*. 2016. vol. 651. pp. 98-105. (In Russ.).
22. Ovcharenko K. L. [Signal delay appraisalment potential accuracy involving frequency derivation based on calculation modify complex envelope cross-correlation function]. *Uspekhi sovremennoj radioelektroniki – Achievements of Modern Radioelectronics*. 2017. vol. 7. pp. 39-44. (In Russ.).
23. Ma L., Xu X., Pang F. Accuracy Assessment of Geostationary-Earth-Orbit with Simplified Perturbations Models. *Artificial satellites*. 2016. vol. 51. no. 2. pp. 55–59.
24. San-Juan J. F., Perez I., San-Martin M., Vergara E. P. Hybrid SGP4 orbit propagator. *Acta Astronautica*. 2017. vol. 137. pp. 254–260.
25. Aldrich J. RA Fisher and the Making of Maximum Likelihood 1912 – 1922. *Statistical Science*. 1997. vol. 12. no. 3. pp. 162–176.
26. Kay S. M. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice Hall. 1993. 595 p.
27. Lehmann E. L., Casella G. *Theory of Point Estimation*, Second Edition. Springer. 1998. 590 p.
28. Steven M. K., Casella G. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice Hall PTR. 1993. 608 p.
29. Saybel' A. G. *Osnovy teorii tochnosti radiotekhnicheskikh metodov mestoopredeleniya* [Bases of the theory of accuracy of radio engineering methods of a location determining]. M.: Oborongiz. 1958. 56 p. (In Russ.).
30. Ovcharenko K. L., Ereemeev I. Ju., Gajchuk Ju. N., Petuhov P. E. [A method of constructing the error ellipsoid for satellite communication system earth station position location determining accuracy appraisalment using UAV]. *Naukoemkie tekhnologii – Intensive Technologies*. 2017. Issue. 18. vol. 11. pp. 22-26. (In Russ.).
31. Lagarias J. C., Reeds J. A., Wright M. H., Wright P. E. Convergence Properties of the Nelder-Mead Simplex Method in Low Dimensions. *SIAM Journal of Optimization*. 1998. vol. 9. no. 1. pp.112–147.

В.И. Миронов, Ю.В. Миронов, И.В. Фоминов
**ЭНЕРГЕТИЧЕСКИ ОПТИМАЛЬНОЕ УПРАВЛЕНИЕ
СБЛИЖЕНИЕМ КОСМИЧЕСКИХ АППАРАТОВ В
НЕЦЕНТРАЛЬНОМ ГРАВИТАЦИОННОМ ПОЛЕ ЗЕМЛИ
НА ЭТАПЕ ДАЛЬНОГО НАВЕДЕНИЯ**

Миронов В.И., Миронов Ю.В., Фоминов И.В. Энергетически оптимальное управление сближением космических аппаратов в нецентральном гравитационном поле земли на этапе дальнего наведения.

Аннотация. Статья посвящена определению энергетически оптимальных программ управления сближением космического аппарата с орбитальным объектом на этапе дальнего наведения с использованием принципа максимума Л.С. Понтрягина. Предполагается, что космический аппарат оснащен продольной двигательной установкой, работающей на химическом топливе. Определению подлежат программы оптимального изменения секундного расхода топлива и вектора направляющих косинусов, определяющих ориентацию силы тяги двигательной установки. В качестве критерия оптимальности управления рассматривается функционал, определяющий минимальный расход рабочего тела. Задача оптимального управления решается в ограниченной области пространства состояний, определяемой диапазоном изменения угловой дальности полета космического аппарата в пределах одного витка. Приведены полные уравнения краевой задачи принципа максимума с использованием модели движения объекта в нормальном гравитационном поле Земли, краевые условия, а также аналитические зависимости, определяющие структуру управления в оптимальном режиме. Краевая задача оптимизации решается методом Ньютона. Для определения начального приближения сопряженных переменных дано аналитическое решение задачи энергетически оптимального управления сближением в однородном центральном поле. Приведены результаты численных исследований энергетически оптимальных программ управления перехватом в нормальном гравитационном поле Земли с конечной тягой на этапе дальнего наведения. В целом, применение алгоритмов оптимального управления сближением в бортовом и наземном комплексе позволяет уменьшить затраты топлива при выполнении маневра, сократить время, а также расширить область достижимости целевых объектов. Кроме того, оптимальное решение может рассматриваться в качестве эталона, с которым необходимо сравнивать различные варианты приближенных алгоритмов управления, оценивать их качество и принимать обоснованные решения по их практическому использованию.

Ключевые слова: космический аппарат, встреча на орбите, оптимальное управление, дальнее наведение.

1. Введение. В существующих и перспективных программах развития космической техники большое внимание уделяется вопросам создания маневрирующих космических аппаратов (КА), применение которых предусматривает выполнение операций сближения с целевыми орбитальными объектами (ЦО). В этом комплексе работ важную роль играют вопросы разработки автономных систем управления движением КА и их алгоритмического обеспечения,

реализующих принцип терминального управления на этапе дальнего наведения и другие. Это позволяет обеспечить высокую точность перевода КА с дежурной орбиты в заданную окрестность ЦО при наличии повышенных возмущений. В перспективных системах терминального управления предусматривается решение на борту в ходе полета сложной и трудоемкой задачи расчета программ управления движением КА для его перевода в окрестность ЦО на этапе дальнего наведения по текущим навигационным данным.

При разработке соответствующих методов и алгоритмов необходимо получение энергетически оптимальных решений в широкой области маневрирования с учетом требования реализуемости на бортовой цифровой вычислительной машине (БЦВМ). Многие из ранее разработанных методов и алгоритмов управления встречей на орбите нашли свое отражение в известных монографиях и [1-5]. Сложность данного класса задач оптимального управления ограничивает возможность использования строгих методов их решения в бортовом контуре оперативного управления движением КА. Компромисс может быть достигнут путем разработки алгоритмов квазиоптимального управления.

Для достижения этой цели в работах [6,7] были предложены модели и алгоритмы системы терминального управления движением КА, реализующие маневры типа перехвата и мягкого сближения ОЦ на этапе дальнего наведения как при импульсной, так и при конечной тяге двигательной установки (ДУ). Отличительная особенность этих алгоритмов состоит в том, что управляемое движение рассматривается в нормальном гравитационном поле Земли, а в алгоритме определения квазиоптимального управления учитывается изменение массы КА при постоянной ориентации вектора силы тяги.

В связи с этим, возникает вопрос: в какой мере получаемые квазиоптимальные решения соответствуют строго оптимальным по энергетическим затратам. Для ответа на этот вопрос, необходимо поставить и решить соответствующую задачу оптимального управления с использованием принципа максимума Л. С. Понтрягина.

Строго оптимальное решение в рассматриваемой задаче управления, с одной стороны, позволяет уменьшить затраты топлива при выполнении маневра, сократить время, а также расширить область достижимости ЦО. С другой стороны, оптимальное решение выступает в качестве эталона, с которым можно сравнивать различные варианты приближенных алгоритмов управления, оценивать их качество и принимать обоснованные решения по их практическому использованию.

Вопросам определения оптимальной программы управления сближением посвящено большое количество работ, как в отечественной, так и зарубежной литературе [1-5, 8-21 и др.], что объясняется большой значимостью данной проблематики в практике освоения и использования космического пространства в военных, научных и народно-хозяйственных целях. Работы [8-21] выполнены в последние годы. В [8, 13] рассмотрена задача определения оптимальной по затратам характеристической скорости двухимпульсной программы управления сближением КО, находящихся на некопланарных орбитах в центральном гравитационном поле Земли. Задача решается с использованием уравнения времени Кеплера и универсальных переменных. При этом оптимизации подлежит не только управляющие импульсы скорости, но и время ожидания активного КО на орбите до начала маневра встречи.

Работа [9] посвящена вопросам оптимизации программы встречи активного КО с группой элементов космического мусора, орбиты которых имеют достаточно близкие наклонения для их последующего удаления. Предложенная методика предусматривает приближенную оценку затрат характеристической скорости и времени перелета между любой парой целевых объектов, чтобы оценить затраты на любую возможную последовательность их обхода. Далее предполагается решать известную проблему коммивояжера с целью выбора лучшей последовательности обхода целевых объектов с точки зрения расхода массы активного КО и времени выполнения операции.

В [10] предложен приближенный алгоритм управления перехватом КО, когда активный объект имеет достаточно высокий уровень постоянной тяги, сравнимой с тягой импульсного типа. Основная особенность этой работы состоит в том, чтобы осуществить процесс перехвата итерационно путем периодического уточнения управления для отработки прогнозируемого промаха, который обусловлен как влиянием возмущений, так и методическими ошибками формирования управляющих воздействий.

В работе [11] исследуется задача управление КО при сближении с маневрирующей невзаимодействующей мишенью на участке ближнего наведения. Предложены алгоритмы управления перед маневром и управления режимом «скольжения» после маневра мишени с использованием принятой приближенной модели относительного движения.

В [12] в импульсной постановке рассматривается задача оптимального управления перехватом КО, в которой совместно определяется как начальный вектор скорости, так и время маневра.

Задача решается в центральном гравитационном поле Земли на основе численного решения известного уравнения Эйлера — Ламберта.

В [14, 18] рассматривается задача расчета параметров маневров встречи КО с крупногабаритными объектами космического мусора (КОКМ), расположенными на околокруговых орбитах с близкими наклонениями. Предполагается, что КО-сборщик подлетает к КОКМ и захватывает его или вставляет в его сопло малый КА, имеющий собственную ДУ. В [18] из каталога NORAD выделены пять компактных групп таких объектов в диапазоне высот от 500 до 1000 км, а также на солнечно-синхронных орбитах. Кроме того, предложены схемы импульсного управления перелетом от одного объекта к другому. Работа [14] дополняет эти исследования. В ней рассмотрен вопрос полета к КОКМ с заданной точностью с помощью двигателей малой тяги.

В [19] предложены схемы сближения с лунной орбитальной станцией космического корабля, стартующего с Земли. Внимание к задачам такого рода возрастает в связи с объявленным ведущими космическими агентствами возврата к программам освоения Луны. В работе рассмотрены несколько баллистических схем, позволяющих решить эту задачу с минимальными затратами топлива.

Работа [15] посвящена исследованию путей обеспечения ускоренного доступа к орбитальной станции для современных космических кораблей. В ней предложены новые схемы выведения с существенно меньшей продолжительностью автономного полета КА до стыковки с орбитальной станцией.

Ряд исследований, выполненных в последние годы, посвящены проблематике создания перспективной системы транспортно-технического обеспечения орбитальной группировки КА [16, 17, 20 и др.]. В этих работах для решения задач управления предполагается использование двигателей малой тяги. Так, в [20] рассматриваются перелеты между заданными орбитами при наличии возмущений разной природы. Предложен квазиоптимальный метод определения траектории перелета, основанный на линеаризации движения около опорных орбит. Однако возможности такого подхода ограничены, так как требуемая точность расчетов достигается путем увеличения числа опорных орбит. Работа [16] посвящена решению задачи минимизации тяги и ее приложении на базе принципа максимума Понтрягина. Задачей оптимизации являются вычисление минимальной величины тяги для перелета за заданное время между фиксированными точками при постоянной скорости истечения и постоянной мощности ДУ. Применение разработанного метода позволяет определять зависимость минимальной тяги от располагаемого удельного импульса,

минимального значения удельного импульса, а также нижние границы конечной массы КА и мощности электро-реактивной ДУ в зависимости от располагаемого удельного импульса. Кроме того, метод предполагает вычисление границы области существования траектории для КА с конечной тягой. В [17] предложен метод оптимизации проектных параметров энергодвигательного комплекса системы транспортно-технического обеспечения орбитальной группировки КА, базирующейся на использовании межорбитальных буксиров многократного применения. Их полезной нагрузкой являются топливо и резервные элементы КА орбитальной группировки, а также робототехнические комплексы для проведения ремонтных операций в космосе.

Анализ существующих методов и алгоритмов оптимального управления сближением КА показывает, что они в большинстве случаев ориентированы на решение задач в малой окрестности ЦО, характерной для этапа ближнего наведения, с использованием упрощенных линейных уравнений относительного движения. Несмотря на высокий уровень достигнутых результатов, соответствующие алгоритмы по области применения и своим характеристикам не в полной мере удовлетворяют предъявляемым требованиям, особенно на участке дальнего наведения. Вопросы оптимизации маневров сближения в широкой области пространства состояний, характерной для этапа дальнего наведения, рассматривались в небольшом числе работ. Нелинейность и сложность динамических моделей управления перехватом исключают возможность получения строгих аналитических решений и приводят к необходимости разработки и применения эффективных в вычислительном отношении итерационных методов. В имеющихся работах часто используется импульсный подход, в прямой постановке не делается акцента на обеспечение высоких точностных и вычислительных характеристик алгоритмов, обеспечения близости получаемых решений к оптимальным, их работоспособности в широком диапазоне возможных условий применения и подлета к целевым объектам, а также реализуемости в контурах оперативного управления. Таким образом, несмотря на имеющиеся результаты, вопросы разработки методов и алгоритмов оптимального управления сближением КА на этапе дальнего наведения нуждаются в дальнейшем исследовании.

Центральным моментом при численном решении краевой задачи принципа максимума является определение подходящего исходного приближения для неизвестных начальных значений вектора сопряженных переменных. От этого во многом зависит сходимость вычислительного процесса, а, следовательно, и сама

возможность получения оптимального решения. В настоящее время, как известно, универсальных методов решения этого вопроса не существует. Основная трудность состоит в том, что сопряженные переменные не имеют ясной физической интерпретации. Для получения надежного результата необходимо ставить и решать исходную задачу в приближенной постановке, связанной с введением возможных упрощений.

Данная статья посвящена разработке алгоритмов расчета энергетически оптимальных программ управления сближением на этапе дальнего наведения с использованием принципа максимума Л. С. Понтрягина. Предполагается, что КА оснащен продольной двигательной установкой (ДУ), работающей на химическом топливе. Определению подлежат программы оптимального изменения секундного расхода топлива и вектора направляющих косинусов, определяющих ориентацию силы тяги ДУ. В качестве критерия оптимальности управления рассматривается функционал, определяющий минимальный расход рабочего тела. Задача оптимального управления решается в ограниченной области пространства состояний в диапазоне изменения угловой дальности полета КА в пределах одного витка.

Приведены полные уравнения краевой задачи принципа максимума с использованием модели движения КА в гравитационном поле Земли (ГПЗ), краевые условия, а также аналитические зависимости, определяющие структуру управления в оптимальном режиме. Краевая задача оптимизации решается методом Ньютона. Для определения начального приближения сопряженных переменных дано аналитическое решение задачи энергетически оптимального управления сближением в однородном центральном поле (ОЦП). Приведены результаты численных исследований энергетически оптимальных программ управления сближением КА в нормальном ГПЗ с конечной тягой на этапе дальнего наведения.

2. Постановка задачи, модели динамики и алгоритм расчета оптимальной по расходу топлива программы управления движением космических аппаратов в поле сжатого сфероида. При постановке и решении конкретных прикладных задач оптимизации управления сближением КА необходимо, прежде всего, конкретизировать вид критерия оптимальности, тип ДУ, математические модели динамики полета, а также состав ограничений и краевых условий.

Рассмотрим задачу оптимального по расходу топлива управления движением КА при его переводе из начального состояния \bar{x}_0, \bar{V}_0 в требуемое конечное состояние $\bar{x}_{\text{тр}}$ за заданное время T .

Для описания движения КА в нецентральной ГПЗ общего вида будем использовать абсолютную геоцентрическую экваториальную систему координат (АГЭСК). При этом будем полагать, что КА оснащен продольной ДУ с постоянным секундным расходом топлива.

Тогда уравнения движения КА принимают следующий вид:

$$\begin{cases} \dot{x} = V_X, \dot{y} = V_Y, \dot{z} = V_Z; \\ \dot{V}_X = g_X(\bar{x}, t) + u(t)\alpha_X(t); \\ \dot{V}_Y = g_Y(\bar{x}, t) + u(t)\alpha_Y(t); \\ \dot{V}_Z = g_Z(\bar{x}, t) + u(t)\alpha_Z(t); \\ \dot{m}_1 = -\beta, \end{cases} \quad t \in [t_0, T]; \quad (1)$$

$$u(t) = \frac{c\beta(t)}{m_1(t)}, \quad \beta(t) = \frac{\dot{m}(t)}{m_0}, \quad m_1(t) = \frac{m(t)}{m_0},$$

где g_X, g_Y, g_Z — проекции вектора гравитационного ускорения на оси АГЭСК; $u(t)$ — модуль реактивного ускорения, создаваемого тягой ДУ КА; $\alpha_X, \alpha_Y, \alpha_Z$ — направляющие косинусы вектора тяги; $\bar{x} = (x, y, z)^T$ — вектор текущих координат КА; $\bar{V} = (V_X, V_Y, V_Z)^T$ — вектор текущей скорости КА; T — время перелета в окрестность КА-Ц; c — скорость истечения газов; $\dot{m}(t), m_0$ — секундный расход топлива и начальная масса КА; $m_1(t)$ — относительная текущая масса КА; $\beta(t)$ — относительный секундный расход топлива.

Введем следующие обозначения: $\bar{u}(t)$ — вектор управляющего ускорения; $\bar{\alpha}(t)$ — вектор направляющих косинусов тяги ДУ КА.

Тогда:

$$\bar{u}(t) = u(t)\bar{\alpha}(t). \quad (2)$$

Краевые условия задачи определяются следующим образом.

Для маневра типа перехвата:

а) при $t = t_0$: $\bar{x}(t) = x_0$; $\bar{V}(t_0) = \bar{V}_0$;

б) при $t = T$: $\bar{x}(T) = \bar{x}_T$.

Для маневра типа мягкого сближения:

$$а) \text{ при } t = t_0: \quad \bar{x}(t) = x_0; \quad \bar{V}(t_0) = \bar{V}_0;$$

$$б) \text{ при } t = T: \quad \bar{x}(T) = \bar{x}_T; \quad \bar{V}(T) = \bar{V}_T.$$

Требуется найти энергетически оптимальную программу изменения вектор-функции направляющих косинусов $\bar{\alpha}(t)$ и относительного секундного расхода топлива $\beta(t)$ по критерию минимума расхода массы топлива:

$$I = \int_0^T \beta(t) dt; \quad (3)$$

при наличии следующих ограничений:

$$0 \leq \beta(t) \leq \beta_{\max}; \quad \bar{\alpha}^T(t) \bar{\alpha}(t) = 1; \quad \bar{u} = [\bar{\alpha}(t), \beta(t)].$$

Найденные таким образом функции $\bar{\alpha}(t)$ и $\beta(t)$ позволяют определить энергетически оптимальную программу изменения вектора управляющих ускорений $\bar{u}(t)$.

Для решения рассматриваемой задачи необходимо конкретизировать модель действующего вектора ускорений $\bar{g} = [g_x, g_y, g_z]^T$. Согласно [1], при движении КА в околоземном космическом пространстве вектор \bar{g} может быть представлен следующим образом:

$$\bar{g}(\bar{x}) = \frac{\partial U}{\partial \bar{x}} + \Delta \bar{g},$$

где U — гравитационный потенциал Земли; $\Delta \bar{g}$ — вектор возмущений.

Общая формула для потенциала притяжения может быть описана в виде его классического разложения в ряд по сферическим функциям:

$$U = \frac{\mu}{r} \left\{ 1 + \left[\sum_{n=2}^{\infty} \left(\frac{R}{r} \right)^n \sum_{m=0}^n (c_{nm} \cos m\lambda + s_{nm} \sin m\lambda) P_{nm}(\sin \phi) \right] \right\},$$

где R — экваториальный радиус Земли; μ — гравитационная постоянная; c_{nm}, s_{nm} — постоянные коэффициенты; ϕ —

геоцентрическая широта данной точки пространства; r — расстояние от центра Земли до точки пространства; λ — долгота, измеренная вдоль экватора от Гринвичского меридиана до меридиана данной точки пространства.

$P_{nm}(\sin \phi)$ — присоединенные функции Лежандра степени n и порядка m , определяемые по формуле:

$$P_{nm}(Q) = \frac{(1-Q^2)^{m/2}}{2^n n!} \cdot \frac{d^{n+m}(Q^2-1)^n}{dQ^{n+m}};$$

$$Q = \sin \phi.$$

Вектор возмущений $\Delta \bar{g}$ в общем случае обусловлен влиянием Солнца, Луны, атмосферы и давления солнечного света на КА. Соответствующие расчетные формулы для определения всех составляющих $\Delta \bar{g}$ приведены в [1]. Однако при маневрировании в околоземном космическом пространстве они малы и не учитываются при рассмотрении управляемых движений на ограниченных временных интервалах.

Следуя принципу максимума, составим Гамильтониан задачи оптимизации:

$$H(\bar{x}, \bar{V}, \bar{u}, t) = \lambda_1 V_X + \lambda_2 V_Y + \lambda_3 V_Z + \lambda_4 [g_X(\bar{x}, t) + u(t) \alpha_X(t)] + \\ + \lambda_5 [g_Y(\bar{x}, t) + u(t) \alpha_Y(t)] + \lambda_6 [g_Z(\bar{x}, t) + u(t) \alpha_Z(t)] - \lambda_m \beta - \beta(t),$$

где $\lambda_i(t)$ — сопряженные переменные.

Тогда условие оптимальности управления примет следующий вид:

$$\bar{u}_{opt}(\bar{x}, \bar{V}, \bar{\lambda}_r, \bar{\lambda}_V, \lambda_m, t) = \max_{\bar{u} \in \Omega_u} H(\bar{x}, \bar{V}, \bar{u}, \bar{\lambda}_r, \bar{\lambda}_V, \lambda_m, t);$$

$$\bar{\lambda}_r = (\lambda_1, \lambda_2, \lambda_3)^T; \quad \bar{\lambda}_V = (\lambda_4, \lambda_5, \lambda_6)^T,$$

где Ω_u — ограниченная область управления;

Это условие и приведенные выше ограничения позволяют определить структуру оптимального управления в зависимости от параметров движения и сопряженных переменных.

$$\bar{\alpha}(t) = \frac{\bar{\lambda}_V}{|\bar{\lambda}_V|}; \quad \Delta_{\Pi} = \frac{c}{m_1(t)} |\bar{\lambda}_V| - \lambda_m; \quad \beta(t) = \begin{cases} \beta_{\max}, & \text{при } \Delta_{\Pi} \geq 1; \\ 0, & \text{при } \Delta_{\Pi} < 1, \end{cases}$$

где $\Delta_{\Pi}(t)$ — функция переключения тяги ДУ.

После дифференцирования гамильтониана H получаем полную систему дифференциальных уравнений движения и сопряженных уравнений принципа максимума (П-систему), которая имеет 14-й порядок:

$$\left\{ \begin{array}{l} \dot{x} = V_X, \quad \dot{y} = V_Y, \quad \dot{z} = V_Z; \\ \dot{V}_X = g_X(\bar{x}, t) + u(t) \alpha_X(t); \\ \dot{V}_Y = g_Y(\bar{x}, t) + u(t) \alpha_Y(t); \\ \dot{V}_Z = g_Z(\bar{x}, t) + u(t) \alpha_Z(t); \\ \dot{m}_1 = -\beta, \\ \dot{\lambda}_1 = -\lambda_4 \frac{\partial g_X}{\partial x} - \lambda_5 \frac{\partial g_Y}{\partial x} - \lambda_6 \frac{\partial g_Z}{\partial x}; \\ \dot{\lambda}_2 = -\lambda_4 \frac{\partial g_X}{\partial y} - \lambda_5 \frac{\partial g_Y}{\partial y} - \lambda_6 \frac{\partial g_Z}{\partial y}; \\ \dot{\lambda}_3 = -\lambda_4 \frac{\partial g_X}{\partial z} - \lambda_5 \frac{\partial g_Y}{\partial z} - \lambda_6 \frac{\partial g_Z}{\partial z}; \\ \dot{\lambda}_4 = -\lambda_1; \quad \dot{\lambda}_5 = -\lambda_2; \quad \dot{\lambda}_6 = -\lambda_3; \\ \dot{\lambda}_m = -\frac{c\beta}{m_1^2} |\bar{\lambda}_V|, \end{array} \right. \quad (4)$$

где

$$\bar{\alpha}(t) = \frac{\bar{\lambda}_V}{|\bar{\lambda}_V|}; \quad \Delta_{\Pi} = \frac{c}{m_1(t)} |\bar{\lambda}_V| - \lambda_m;$$

$$\beta(t) = \begin{cases} \beta_{\max}, & \text{при } \Delta_{\Pi} \geq 1; \\ 0, & \text{при } \Delta_{\Pi} < 1. \end{cases}$$

Таким образом, в результате применения принципа максимума исходная задача оптимального управления сводится к решению двухточечной краевой задачи для приведенной П-системы (4) при следующих краевых условиях.

Для маневра типа перехвата:

а) при $t = t_0$: $\bar{x} = \bar{x}_0$; $\bar{V} = \bar{V}_0$;

б) при $t = T$: $\bar{x} = \bar{x}_{\text{тр}}$; $\bar{\lambda}_V = 0$; $\lambda_m = 0$.

Для маневра типа мягкого сближения:

а) при $t = t_0$: $\bar{x} = \bar{x}_0$; $\bar{V} = \bar{V}_0$;

б) при $t = T$: $\bar{x}(T) = \bar{x}_T$; $\bar{V}(T) = \bar{V}_T$; $\lambda_m = 0$.

Здесь учтено, что из условий трансверсальности конечные значения сопряженных переменных, соответствующие свободным параметрам траектории движения, по которым не заданы терминальные условия, принимают нулевые значения.

Решение данных краевых задач сводится к решению соответствующего обобщенного краевого уравнения относительно начального значения вектора сопряженных переменных $\bar{\lambda}_0 = (\bar{\lambda}_{r0}, \bar{\lambda}_{V0}, \lambda_{m0})$.

При решении задачи перехвата это уравнение имеет вид:

$$\bar{S}(T, \bar{\lambda}_0) = [\bar{x}(T, \bar{\lambda}_0) - \bar{x}_{тр}, \bar{\lambda}_V(T, \bar{\lambda}_0), \lambda_m(T, \bar{\lambda}_0)]^T = 0,$$

а для маневра мягкого сближения:

$$\bar{S}(T, \bar{\lambda}_0) = [\bar{x}(T, \bar{\lambda}_0) - \bar{x}_{тр}, \bar{V}(T, \bar{\lambda}_0) - \bar{V}_{тр}, \lambda_m(T, \bar{\lambda}_0)]^T = 0.$$

Для решения задач применяется метод «пристрелки» с подбором недостающих начальных значений сопряженных переменных модифицированным методом Ньютона:

$$\bar{\lambda}_{0,k+1} = \bar{\lambda}_{0,k} - \gamma_k \cdot \left[\frac{\partial \bar{S}}{\partial \bar{\lambda}_0} \right]_k^{-1} \cdot \bar{S}(T, \bar{\lambda}_{0,k}), \quad k = 0, 1, 2, \dots,$$

где k — номер итерации; γ_k — параметр шага.

В процессе итераций определяется программа оптимального управления движением КА, в которую входят моменты времени включения и выключения ДУ на каждом активном участке траектории, а также программы изменения ориентации вектора тяги.

Матрицы $\left[\frac{\partial \bar{S}}{\partial \bar{\lambda}_0} \right]$ определяются методом конечных разностей.

Основная трудность при решении краевой задачи оптимального управления заключается в определении подходящего начального значения для вектора $\bar{\lambda}_0 = (\bar{\lambda}_{r0}, \bar{\lambda}_{V0}, \lambda_{m0})$. Этот вопрос рассматривается в п.4.

3. Уравнения краевой задачи принципа максимума в нормальном гравитационном поле Земли. Приведенная выше в п. 2 П-система дифференциальных уравнений представлена в обобщенном виде. Она справедлива при маневрировании КА для модели ГПЗ общего вида и нуждается в конкретизации.

Отметим основные факторы, поясняющие возможность и целесообразность упрощения уравнений движения и сопряженных уравнений (4) при решении задачи оптимального управления.

Во-первых, упрощение уравнений П-системы может приводить как к отклонениям оптимальной траектории от заданных граничных условий на правом конце траектории, так и к отклонению минимизируемого функционала от его строго оптимального значения.

В известной работе В. С. Новоселова [21] было показано, что при решении задач оптимального управления на базе принципа максимума для уравнений движения объекта с малым параметром допустимо упрощать сопряженную систему уравнений без существенной потери точности с точки зрения достижения экстремального значения минимизируемого функционала. Поэтому выполнение требований по точности выполнения краевых условий полностью определяется принятой моделью движения. Однако, близость минимизируемого функционала к его строго оптимальному значению определяется моделью сопряженных уравнений.

Во-вторых, при решении задач оптимизации программ управления движением КА, особенно на ограниченных временных интервалах, обычно нет необходимости учитывать малые возмущения в модели движения. Это обусловлено тем, что процесс реализации указанных программ всегда сопровождается влиянием большого числа других дополнительных возмущений, которые в совокупности приводят к значительно большим отклонениям траектории от расчетной по сравнению с малыми возмущениями в модели движения. К ним относятся ошибки навигации, ориентации, разброс характеристик ДУ и объекта управления и другие. В силу указанных обстоятельств в большинстве опубликованных работ, посвященных оптимизации управления движением КА, рассматриваются модели движения в центральном ГПЗ и в более простых полях [3, 4 и др.].

В-третьих, сложность применяемых моделей при оптимизации процессов управления движением КА в рассматриваемом классе задач не является принципиальным моментом с точки зрения обеспечения сходимости вычислительного процесса. Она определяет лишь вычислительную трудоемкость. Главной же проблемой при оптимизации управления движением КА с использованием принципа максимума является определение начальных значений сопряженных

переменных, которые гарантируют сходимость вычислительного процесса, то есть саму возможность получения оптимального решения. Об этом сказано выше в п.1. Общего решения для их определения не существует. В п.4 данной статьи дано аналитическое решение этой задачи с использованием модели ОЦП. Для задачи с более сложной моделью движения эти результаты используются как начальные приближения начальных значений сопряженных переменных. Кроме того, эти результаты могут использоваться для оптимизации управления в любом ГПЗ, то есть в ГПЗ произвольной сложности, в том числе с учетом малых возмущений.

В данной работе при численных исследованиях используется модель нормального ГПЗ, в котором учитывается вторая зональная гармоника в разложении геопотенциала в ряд по сферическим функциям. Особенность работы состоит в том, что эта модель ГПЗ используется не только в уравнениях движения КА, но и в системе уравнений для сопряженных переменных.

Приведем в развернутом виде полную систему основных и сопряженных дифференциальных уравнений для определения энергетически оптимальной программы управления сближением в нормальном ГПЗ, учитывающем сжатие Земли.

Как известно, возможны различные формы представления дифференциальных уравнений движения КА в нормальном ГПЗ, отличающиеся компактностью записи и вычислительной трудоемкостью. С этой точки зрения предпочтительна форма, принятая в [1].

Для такой модели ГПЗ дифференциальные уравнения управляемого движения КА можно представить в следующем компактном, удобном для программирования, виде:

$$\begin{aligned} \dot{x} &= V_x; & \dot{y} &= V_y; & \dot{z} &= V_z; \\ \dot{V}_x &= -A x + \frac{c \beta}{m_1} \alpha_x; \\ \dot{V}_y &= -A y + \frac{c \beta}{m_1} \alpha_y; \\ \dot{V}_z &= (2BC - A) z + \frac{c \beta}{m_1} \alpha_z; \\ \dot{m}_1 &= -\beta, \end{aligned} \tag{5}$$

где

$$A = B[\alpha_{00} + C(D-1)]; \quad B = \frac{1}{r^2} \frac{R_3}{r};$$

$$C = \frac{3}{2} \alpha_{20} \left(\frac{R_3}{r} \right)^2; \quad D = 5 \left(\frac{z}{r} \right)^2;$$

$$r = \sqrt{x^2 + y^2 + z^2}; \quad r_1 = \sqrt{x^2 + y^2};$$

$$V = \sqrt{V_x^2 + V_y^2 + V_z^2}; \quad \alpha_{00} = \frac{\mu}{R_3}; \quad \alpha_{20} = -\frac{c_{20}}{R_3^3};$$

$\alpha_x, \alpha_y, \alpha_z$ — компоненты вектора $\bar{\alpha}$ направляющих косинусов реактивного ускорения; μ, c_{20} — параметры модели ГПЗ; R_3 — экваториальный радиус Земли.

При конкретизации системы дифференциальных уравнений, описывающих изменение сопряженных переменных, будем также использовать модель динамики КА с учетом второй зональной гармоники в разложении геопотенциала в ряд по сферическим функциям геоцентрической широты, как и в уравнениях движения.

После проведения необходимых преобразований и введения дополнительных обозначений, приходим к следующей записи сопряженной системы дифференциальных уравнений:

$$\dot{\lambda}_1 = A\lambda_4 - PE_\lambda x + 10BC \frac{xz}{r^2} \lambda_6;$$

$$\dot{\lambda}_2 = A\lambda_5 - PE_\lambda y + 10BC \frac{yz}{r^2} \lambda_6$$

(6)

$$\dot{\lambda}_3 = -(2BC - A)\lambda_6 - PE_\lambda z + 10BC \frac{z^2}{r^2} \lambda_6 + F_\lambda;$$

$$\dot{\lambda}_4 = -\lambda_1; \quad \dot{\lambda}_5 = -\lambda_2; \quad \dot{\lambda}_6 = -\lambda_3,$$

где

$$P = 3A + 2BC(2D - 1).$$

Входящие в эти уравнения функции A , B , C , D имеют тот же смысл, что и ранее.

Эта система сопряженных уравнений дополняется ранее полученным в п. 3 уравнением, определяющим поведение сопряженной переменной λ_m , которое остается неизменным:

$$\dot{\lambda}_m = \frac{c\beta}{m_1^2} \bar{\lambda}_V^T \bar{\alpha}(t).$$

Краевые условия, а также аналитические зависимости управляющих функций от переменных состояния и сопряженных переменных, определяющие структуру управления в оптимальном режиме, приведены выше в п. 2.

При использовании принципа максимума поиск оптимальной программы управления сводится к решению двухточечной краевой задачи для приведенных выше основной и сопряженной систем дифференциальных уравнений и заключается в определении неизвестных начальных значений сопряженных переменных $\bar{\lambda}_{10}$, $\bar{\lambda}_{20}$, $\bar{\lambda}_{m0}$.

Для организации вычислительного процесса, например, в рамках итерационного метода Ньютона, необходимо предварительно определить приближенные начальные значения неизвестных параметров. Общей методики поиска $\bar{\lambda}_{10}$, $\bar{\lambda}_{20}$, $\bar{\lambda}_{70}$ не существует. Грубость начальных значений сопряженных переменных может нарушить сходимость вычислительного процесса. В интересах решения этого вопроса рассмотрим приближенное аналитическое решение задачи энергетически оптимального управления сближением, соответствующее модели движения КА в ОЦП с постоянным реактивным ускорением.

4. Приближенное аналитическое решение задачи энергетически оптимального управления сближением. Рассмотрим приближенное аналитическое решение задачи энергетически оптимального управления сближением применительно к модели движения КА в ОЦП, описывающей движение в узком шаровом слое [4], с учетом изменения массы КА при постоянном секундном расходе топлива.

В дальнейшем для удобства записи введем следующие обозначения: $x_7 = m_1$, $\lambda_7 = \lambda_m$, $\lambda_{70} = \lambda_{m0}$.

При использовании модели ОЦП уравнения движения КА имеют вид:

$$\begin{cases} \dot{\bar{x}} = \bar{V}; \\ \dot{\bar{V}} = -\omega^2 \cdot \bar{x} + \frac{c\beta}{x_7} \cdot \bar{\alpha}; \\ \dot{x}_7 = -\beta; \end{cases} \quad (7)$$

$$\omega = \frac{1}{2} \left(\sqrt{\frac{\mu}{r_1^3}} + \sqrt{\frac{\mu}{r_2^3}} \right),$$

где ω — средняя угловая скорость движения КА в рассматриваемом шаровом слое маневрирования.

Требуется найти оптимальное управление $\beta(t)$ и $\bar{\alpha}(t)$, обеспечивающие перелет КА из начального состояния $\bar{x}(0) = \bar{x}_0$, $\bar{V}(0) = \bar{V}_0$ в конечную целевую точку $\bar{x}(T) = \bar{x}_T$ при минимальном значении энергетических затрат, характеризующихся функционалом $I = \int_0^T \beta(t) dt$ при наличии тех же ограничений по секундному расходу топлива и вектору направляющих косинусов силы тяги ДУ, что и ранее:

$$0 \leq \beta(t) \leq \beta_{\max}, \quad \bar{\alpha}^T(t) \bar{\alpha}(t) = 1.$$

Составим гамильтониан системы:

$$H = \bar{\lambda}_1^T \cdot \bar{V} + \bar{\lambda}_2^T \left(-\omega^2 \bar{x} + \frac{c\beta}{x_7} \bar{\alpha} \right) - \beta \cdot \lambda_7 - \beta, \quad (8)$$

и сформируем сопряженную систему уравнений:

$$\begin{cases} \dot{\bar{\lambda}}_1 = \omega^2 \bar{\lambda}_2; \\ \dot{\bar{\lambda}}_2 = -\bar{\lambda}_1; \\ \dot{\lambda}_7 = \frac{c\beta}{x_7^2} \bar{\lambda}_2^T \cdot \bar{\alpha}. \end{cases} \quad (9)$$

Поскольку значения $\bar{V}(T)$ и $x_7(T)$ являются свободными, то для системы (9) имеем граничные условия $\bar{\lambda}_2(T) = 0$, $\lambda_7(T) = 0$.

Из условия максимума гамильтониана определим структуру оптимального управления с учетом имеющихся ограничений:

$$\bar{\alpha}(t) = \frac{\bar{\lambda}_2(t)}{\lambda(t)}; \quad \beta(t) = \begin{cases} \beta_{\max}, & \text{при } \Delta_{\Pi}(t) \geq 1; \\ 0, & \text{при } \Delta_{\Pi}(t) < 1; \end{cases} \quad (10)$$

$$\Delta_{\Pi}(t) = \frac{c|\lambda(t)|}{x_7(t)} - \lambda_7(t),$$

где $\Delta_{\Pi}(t)$ — функция переключения тяги; $\lambda(t) = (\bar{\lambda}_2^T(t) \bar{\lambda}_2(t))^{1/2}$ — модуль вектора $\bar{\lambda}_2(t)$.

Проинтегрируем первые два уравнения системы сопряженных уравнений (9) на интервале от 0 до t . В результате получим:

$$\begin{cases} \bar{\lambda}_1(t) = \cos \omega t \cdot \bar{\lambda}_{10} + \omega \cdot \sin \omega t \cdot \bar{\lambda}_{20}; \\ \bar{\lambda}_2(t) = -\frac{1}{\omega} \sin \omega t \cdot \bar{\lambda}_{10} + \cos \omega t \cdot \bar{\lambda}_{20}. \end{cases} \quad (11)$$

Воспользуемся граничными условиями на конечный момент времени сближения $\bar{\lambda}_2(T) = 0$. Тогда из второго уравнения (11) получим связь начальных значений $\bar{\lambda}_{10}$ и $\bar{\lambda}_{20}$:

$$\bar{\lambda}_{10} = \omega \cdot \operatorname{ctg} \omega T \cdot \bar{\lambda}_{20}. \quad (12)$$

Подставляя это выражение в первое уравнение (11), получим:

$$\bar{\lambda}_2(t) = \varphi(t, T) \cdot \bar{\lambda}_{20}, \quad (13)$$

где $\varphi(t, T) = -\sin \omega t \cdot \operatorname{ctg} \omega T + \cos \omega t$.

Тогда:

$$\lambda(t) = (\bar{\lambda}_2^T(t) \bar{\lambda}_2(t))^{1/2} = |\varphi(t, T)| \cdot (\bar{\lambda}_{20}^T \bar{\lambda}_{20})^{1/2}. \quad (14)$$

Функцию $\varphi(t, T)$ можно представить в виде:

$$\varphi(t, T) = \frac{-\sin \omega T \cdot \cos \omega t + \sin \omega t \cdot \cos \omega T}{\sin \omega T} = \frac{\sin \omega(T-t)}{\sin \omega T}. \quad (15)$$

Тогда при $\omega T < \pi$ функция $\varphi(t, T) > 0$.

Таким образом, при перехвате на первом полувитке, то есть при $T < \frac{\pi}{\omega}$, эта функция положительна и, следовательно, в выражении (14)

модуль можно исключить:

$$\lambda(t) = \varphi(t, T) \sqrt{\bar{\lambda}_{20}^T \cdot \bar{\lambda}_{20}}. \quad (16)$$

Теперь с учетом (10 и 13) получим:

$$\bar{\alpha}_{opt} = \frac{\bar{\lambda}_{20}}{\lambda_0}, \quad (17)$$

где $\lambda_0 = \sqrt{\bar{\lambda}_{20}^T \cdot \bar{\lambda}_{20}}$.

Из (17) следует, что оптимальное значение вектора направляющих косинусов тяги ДУ постоянно на всем активном участке траектории (АУТ) КА при заданной модели движения в ОЦП и зависит только от начальных значений вектора сопряженных переменных $\bar{\lambda}_{20}$.

Заметим далее, что согласно (10), в оптимальном режиме в момент окончания АУТ T_1 функция переключения принимает единичное значение, то есть должно выполняться равенство:

$$\Delta(T_1) = 1.$$

Тогда из (10) следует:

$$\frac{c}{x_7(T_1)} \lambda(T_1) - \lambda_7(T_1) = 1.$$

По условию задачи $\lambda_7(T) = 0$. Однако $\lambda_7(t)$ не изменяется с момента T_1 , поскольку управление на участке $[T_1, T]$ отсутствует, следовательно $\lambda_7(T_1) = 0$. С учетом этого имеем:

$$\lambda(T_1) = \frac{x_7(T_1)}{c} = \frac{1 - \beta T_1}{c}. \quad (18)$$

Согласно (16) на момент T_1 , получим:

$$\lambda(T_1) = \varphi(T_1, T)\lambda_0, \quad (19)$$

где

$$\varphi(T_1, T) = \frac{\sin \omega(T - T_1)}{\sin \omega T}.$$

Тогда из (18) и (19) определим λ_0 :

$$\lambda_0 = \frac{(1 - \beta T_1)}{c} \cdot \frac{\sin \omega T}{\sin \omega(T - T_1)}. \quad (20)$$

Далее определим связь между начальными значениями сопряженных переменных с краевыми условиями уравнений относительного движения. Для этого проинтегрируем систему (7) на интервале времени от 0 до T в предположении, что модуль реактивного ускорения $u(t)$ равен его постоянному среднему значению u_{cp} на АУТ. Тогда получим следующее приближенное решение:

$$\begin{cases} \bar{x}(T) = \cos \omega T \cdot \bar{x}_0 + \frac{1}{\omega} \sin \omega T \cdot \bar{V}_0 + \frac{u_{cp}}{\omega^2} [\cos \omega(T - T_1) - \cos \omega T] \frac{\bar{\lambda}_{20}}{\lambda_0}; \\ \bar{V}(T) = -\omega \cdot \sin \omega T \cdot \bar{x}_0 + \cos \omega T \cdot \bar{V}_0 + \frac{u_{cp}}{\omega} [\sin \omega T - \sin \omega(T - T_1)] \frac{\bar{\lambda}_{20}}{\lambda_0}. \end{cases}$$

Из первого уравнения имеем:

$$\bar{\alpha}_{opt} = \frac{\bar{\lambda}_{20}}{\lambda_0} = S_u(T_1, T),$$

где

$$\bar{S}_u(T_1, T) = \frac{\omega^2}{u_{cp}} \left[\frac{\bar{x}_T - \cos \omega T \cdot \bar{x}_0 - \frac{1}{\omega} \sin \omega T \cdot \bar{V}_0}{\cos \omega(T - T_1) - \cos \omega T} \right]; \quad (21)$$

Отсюда можно найти соотношение для определения $\bar{\lambda}_{20}$:

$$\bar{\lambda}_{20} = \bar{S}_u(T_1, T)\lambda_0. \quad (22)$$

Тогда с учетом (20) окончательно получаем:

$$\bar{\lambda}_{20} = \frac{(1-\beta T_1)}{c} \cdot \frac{\sin \omega T}{\sin \omega(T-T_1)} \cdot \bar{S}_u(T_1, T). \quad (23)$$

Принимая во внимание (13), находим расчетное соотношение для определения $\bar{\lambda}_{10}$:

$$\bar{\lambda}_{10} = \omega \cdot \frac{(1-\beta T_1)}{c} \cdot \frac{\cos \omega T}{\sin \omega(T-T_1)} \cdot \bar{S}_u(T_1, T). \quad (24)$$

Таким образом, начальные значения сопряженных переменных $\bar{\lambda}_{10}$, $\bar{\lambda}_{20}$ определены аналитически и вычисляются, соответственно, по формулам (23) и (24). Однако, эти соотношения зависят от момента переключения T_1 и среднего реактивного ускорения u_{cp} , которые пока неизвестны. Для их определения можно предварительно решить задачу расчета программы управления перехватом КА в импульсной постановке или с учетом конечной тяги при постоянной ориентации вектора тяги. При этом могут быть использованы более точные модели динамики КА по сравнению с ОЦП, такие как модели движения в центральном или нецентральном ГПЗ [6, 7 и др.].

Если определены затраты характеристической скорости $V_{хар}$ на АУТ, то указанные параметры можно рассчитать по следующим формулам:

$$T_1 = \frac{1}{\beta} \left(1 - e^{-\frac{V_{хар}}{c}} \right); \quad u_{cp} = \frac{V_{хар}}{T_1} = -\frac{c}{T_1} \ln(1-\beta T_1). \quad (25)$$

В рамках приближенного подхода можно воспользоваться результатами решения соответствующей модельной задачи сближения в ОЦП. В этом случае затраты характеристической скорости, необходимые для осуществления перехвата за заданное время, вычисляются по формуле:

$$\bar{V}_{хар} = \frac{\omega}{\sin \omega T} \bar{\rho}_T,$$

где

$$\bar{\rho}_T = \bar{x}_T - \cos \omega T \cdot \bar{x}_0 - \frac{1}{\omega} \sin \omega T \cdot \bar{V}_0,$$

$\bar{\rho}_T$ — отклонение прогнозируемых координат КА от координат КА-Ц на конечный момент времени полета при его свободном движении.

После определения $V_{\text{хар}}$ по приведенным выше формулам находятся значения T_1 и $u_{\text{ср}}$. Тогда продолжительность активного участка можно итерационно уточнить по формуле:

$$T_1 = T - \frac{1}{\omega} \arccos \left(\frac{\omega^2}{u_{\text{ср}}} |\bar{\rho}_T| + \cos \omega T \right), \quad (26)$$

а, следовательно, скорректировать и значение параметра $u_{\text{ср}}$.

Далее перейдем к определению значения параметра λ_{70} . С этой целью рассмотрим последнее дифференциальное уравнение сопряженной системы (9), которое для оптимальной программы изменения вектора направляющих косинусов (10) примет следующий вид:

$$\dot{\lambda}_7 = \frac{c\beta(t)}{x_7^2(t)} \lambda(t).$$

Принимая во внимание (15) и (16) запишем это уравнение как:

$$\dot{\lambda}_7 = \frac{c\beta(t)}{x_7^2(t)} \cdot \frac{\sin \omega(T-t)}{\sin \omega T} \cdot \lambda_0.$$

Проинтегрируем данное уравнение на интервале времени от 0 до T в предположении, что модуль реактивного ускорения $u(t)$ равен его постоянному среднему значению $u_{\text{ср}}$ на АУТ. Тогда, принимая во внимание граничные условия $\lambda_7(T) = \lambda_7(T_1) = 0$ получим следующее приближенное решение:

$$\lambda_{70} = \frac{u_{\text{ср}}^2}{c\beta} \cdot \frac{\lambda_0}{\omega \sin \omega T} [\cos \omega T - \cos \omega(T - T_1)].$$

Подставляя в это выражение значение параметра λ_0 согласно (20) окончательно получим:

$$\lambda_{70} = \frac{u_{\text{ср}}^2}{c^2\beta} \cdot \frac{(1 - \beta T_1)}{\omega \sin \omega(T - T_1)} [\cos \omega T - \cos \omega(T - T_1)].$$

Полученные результаты определяют исходное приближение для начальных значений сопряженных переменных, необходимых при итерационном решении полной краевой задачи оптимального управления в нормальном ГПЗ с постоянным секундным расходом топлива, рассмотренной в п.п. 2 и 3. Приведем их в окончательном виде, удобном для проведения расчетов.

$$\begin{aligned}\bar{\lambda}_{10} &= \omega \cdot \frac{(1-\beta T_1)}{c} \cdot \frac{\cos \omega T}{\sin \omega(T-T_1)} \cdot \bar{S}_u(T_1, T); \\ \bar{\lambda}_{20} &= \frac{(1-\beta T_1)}{c} \cdot \frac{\sin \omega T}{\sin \omega(T-T_1)} \cdot \bar{S}_u(T_1, T); \\ \lambda_{70} &= \frac{u_{cp}^2}{c^2 \beta} \cdot \frac{(1-\beta T_1)}{\omega \sin \omega(T-T_1)} [\cos \omega T - \cos \omega(T-T_1)]; \\ \bar{S}_u(T_1, T) &= \frac{\omega^2}{u_{cp}} \left[\frac{\bar{x}_T - \cos \omega T \cdot \bar{x}_0 - \frac{1}{\omega} \sin \omega T \cdot \bar{V}_0}{\cos \omega(T-T_1) - \cos \omega T} \right].\end{aligned}\tag{27}$$

5. Результаты тестовых расчетов. Для оценки сходимости предложенного способа расчета оптимального управления сближением, базирующихся на методологии принципа максимума, были проведены численные исследования.

Для анализа вычислительного процесса оптимизации программы управления КА принимались следующие исходные данные: $H_{КА} = 1000$ км, $H_{КА-Ц} = 1500$ км, $\Delta \varphi_0 = -5^\circ$, $T_{зад} = 700$ с, $\beta = 0.01$ с, которые соответствуют условиям быстрого сближения. Этот выбор продиктован тем, что основное влияние конечной тяги на значения энергетических затрат сказывается в области ограниченных угловых дальностей полета, что соответствует области повышенных энергетических затрат.

При проведении расчетов использовалась система дифференциальных уравнений (5), описывающая движение КА в нецентральной ГПЗ, и соответствующая ей система сопряженных уравнений (6). Для определения начальных значений сопряженных переменных применялись формулы (27), в которых параметры T_1 и u_{cp} вычислялись путем решения двухточечной краевой задачи

перехвата в центральном ГПЗ с учетом конечной тяги по методике, приведенной в [7]. Итерационный вычислительный процесс выполняется по алгоритму метода Ньютона (п.2).

В таблице 1 представлены результаты анализа сходимости вычислительного процесса расчетов программы энергетически оптимального управления сближением в нормальном ГПЗ с конечной тягой. Здесь приведены для каждой итерации значения модуля конечного промаха $\Delta\rho(T)$, продолжительности АУТ T_1 , начальные значения всех компонент вектора сопряженных переменных λ_{x_0} , λ_{y_0} , λ_{z_0} , $\lambda_{V_{x_0}}$, $\lambda_{V_{y_0}}$, $\lambda_{V_{z_0}}$, λ_{γ_0} и затрат характеристической скорости $V_{хар}$.

Таблица 1. Сходимость процесса оптимизации управления

Величина		№ итерации		
		0	1	2
$\Delta\rho(T)$	км	8.32	0.761	0.02
T_1	с	23.76	24.37	24.23
λ_{x_0}	10^{-4}	-3.69	-3.75	-3.76
λ_{y_0}	10^{-4}	6.06	6.04	5.99
λ_{z_0}	10^{-4}	10.48	10.43	10.41
$\lambda_{V_{x_0}}$	10^{-1}	-3.03	-3.09	-3.11
$\lambda_{V_{y_0}}$	10^{-1}	4.94	4.92	4.89
$\lambda_{V_{z_0}}$	10^{-1}	8.49	8.47	8.47
λ_{γ_0}	10^{-1}	-2.51	-2.46	-2.43
$V_{хар}$	км/с	0.809	0.817	0.824

Полученные результаты расчетов показывают, что в рассмотренных расчетных условиях вычислительный процесс определения оптимальной программы управления перелета КА сходится за 3 итерации. При этом модуль промаха по относительным координатам попадания в целевую точку составляет 20 м. Это обстоятельство свидетельствует о достаточно высокой вычислительной экономичности исследуемых алгоритмов, а также о возможности их практического применения для решения задачи оптимального управления сближением КА с ЦО на этапе дальнего наведения.

6. Заключение. Предложенные алгоритмические средства расчета оптимальной по энергетическим затратам программы

управления движения КА при его сближении с ЦО на этапе дальнего наведения обеспечивает решение задачи в широкой области маневрирования применительно к КА, оснащеному продольной ДУ. Это в значительной мере достигается за счет рационального определения нулевого приближения для вектора начальных значений сопряженных переменных по разработанной методике. При этом полностью учитываются нецентральность ГПЗ как в модели движения КА, так и в модели сопряженных дифференциальных уравнений, а также неимпульсный характер действия силы тяги ДУ при постоянном секундном расходе топлива. Проведенные тестовые расчеты подтверждают работоспособность представленных алгоритмов.

В целом, применение алгоритмов оптимального управления сближением в бортовом и наземном комплексе позволяет уменьшить затраты топлива при выполнении маневра, сократить время, а также расширить область достижимости ЦО. Кроме того, оптимальное решение может рассматриваться в качестве эталона, с которым необходимо сравнивать различные варианты приближенных алгоритмов управления, оценивать их качество и принимать обоснованные решения по их практическому использованию.

Литература

1. *Авдуевский В.С., Антонов Б.М.* Основы теории полета космических аппаратов // М.: Машиностроение. 1972. 608 с.
2. *Лысенко Л.Н., Бетанов В.В., Звягин Ф.В.* Теоретические основы баллистико-навигационного обеспечения космических полетов // М.: Изд-во МГТУ им. Н.Э. Баумана. 2014. 520 с.
3. *Лебедев А.А., Соколов В.Б.* Встреча на орбите // М.: Машиностроение. 1969. 366 с.
4. *Ильин В.А., Кузмак Г.Е.* Оптимальные перелеты космических аппаратов // М.: Наука. 1976. 744 с.
5. *Ермилов Ю.А., Иванова Е.Е., Пантюшин С.В.* Управление сближением космических аппаратов // М.: Наука. 1977. 448 с.
6. *Миронов В.И., Миронов Ю.В., Макаров М.М.* Алгоритм расчета программы управления перехватом в нецентральной гравитационном поле Земли с учетом конечной тяги на основе уравнений Эйлера–Ламберта // Сборник трудов ВКА им. А.Ф. Можайского. 2014. №4(645). С. 64–72.
7. *Миронов В.И., Миронов Ю.В., Бурмистров В.В., Макаров М.М.* Алгоритм расчета программы управления сближением в нецентральной гравитационном поле Земли с учетом конечной тяги // Сборник трудов ВКА им. А.Ф. Можайского. 2014. №1(646). С. 85–94.
8. *Oghim S., Mok S.H., Leeghim H.* Optimal Spacecraft Rendezvous by Minimum Velocity Change and Wait Time // Advances in Space Research. 2017. vol. 60. no. 6. pp. 1188–1200.
9. *Shen H., Zhang T., Casalino L., Pastrone D.* Optimization of Active Debris Removal Missions with Multiple Targets // Journal of Spacecrafts and Rockets. 2018. vol. 55. no. 1. pp. 181–189.
10. *Oghim S., Leeghim H., Kim D.* Real-time Spacecraft Intercept Strategy on J2-perturbed Orbits // Advances in Space Research. 2019. vol. 63. no. 2. pp. 1007–1016.

11. *Xu L., Zhang T., Zhou H., Li M.* Relative Orbit Control Method for Non-Cooperative Maneuvering Target Rendezvous // 2015 Chinese Automation Congress (CAC). 2015. pp. 1690–1695.
12. *Leeghim H., Kim D., Turner J.* Solution for Nonlinear Three-Dimensional Intercept Problem with Minimum Energy // *Mathematical Problems in Engineering*. 2013. vol. 2013. 8 p.
13. *Leeghim H.* Spacecraft intercept using minimum control energy and wait time // *Celestial Mechanics and Dynamical Astronomy*. 2013. vol. 115. no. 1. pp. 1–19.
14. *Баранов А.А., Будянский А.А., Разумный Ю.Н.* Управление движением космического аппарата при подлете к крупногабаритному объекту космического мусора // *Космические исследования*. 2017. Т. 55. № 4. С. 285–289.
15. *Муртазин Р.Ф.* Схемы ускоренного доступа к орбитальной станции для современных космических кораблей // *Космические исследования*. 2014. Т. 52. № 2. С. 162–175.
16. *Иванюхин А.В., Петухов В.Г.* Задачи минимизации тяги и ее приложения // *Космические исследования*. 2015. Т. 53. № 4. С. 320–331.
17. *Евдокимов Р.А., Чилин Ю.Н.* Параметрический синтез электродвигательного комплекса системы транспортно-технического обеспечения орбитальной группировки КА // *Космические исследования*. 2013. Т. 51. № 3. С. 250–264.
18. *Баранов А.А., Гришко Д.А., Медведевских В.В., Лапшин В.В.* Решение задачи облетов крупногабаритного космического мусора на солнечно-синхронных орбитах // *Космические исследования*. 2016. Т. 54. № 3. С. 242–250.
19. *Муртазин Р.Ф.* Схема сближения с лунной орбитальной станцией космического корабля, стартующего с Земли // *Космические исследования*. 2016. Т. 54. № 3. С. 268–274.
20. *Суханов А.А., Прадо А.Ф.Б.* Межорбитальные перелеты с малой тягой в произвольном поле сил // *Космические исследования*. 2013. Т. 51. № 2. С. 159–175.
21. *Новоселов В.С.* Аналитическая теория оптимизации в гравитационных полях // ЛГУ. 1972. 317 с.

Миронов Вячеслав Иванович — д-р техн. наук, профессор, ведущий научный сотрудник лаборатории информационных технологий в системном анализе и моделировании, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: фундаментальные и прикладные исследования проблем комплексного моделирования, теория оптимального наблюдения и управления динамическими процессами, вычислительная математика, баллистика космических полетов, методы навигации и управления движением ракет-носителей и космических аппаратов, статистический анализ характеристик сложных технических систем. Число научных публикаций — 350. vi-mironov@yandex.ru; 14-я линия В.О., 39, Санкт-Петербург; 199178; р.т.: +7(812)328-3337; факс: +7(812)328-4450.

Миронов Юрий Вячеславович — д-р техн. наук, доцент, ведущий специалист АО «НИЦ СПб ЭТУ». Область научных интересов: баллистика космических полетов, методы навигации и управления движением ракет-носителей и космических аппаратов, теория статистического оценивания, вычислительная математика. Число научных публикаций — 150. mironuv@yandex.ru; ул. Политехническая, 22, лит."Н", Санкт-Петербург, 194021; р.т.: +7(812)703-7583; факс: +7(812)703-7584.

Фоминов Иван Вячеславович — д-р техн. наук, начальник кафедры автономных систем управления, Военно-космическая академия им. А.Ф. Можайского (ВКА им. А.Ф. Можайского). Область научных интересов: системы навигации и управления движением космических аппаратов. Число научных публикаций — 30. i.v.fominov@gmail.com; ул. Ждановская, 13, Санкт-Петербург, 197198; р.т.: +7(812)347-9521.

V.I. MIRONOV, Y.V. MIRONOV, I.V. FOMINOV
**ENERGETICALLY OPTIMAL CONTROL OF THE
CONVERGENCE OF THE SPACECRAFT IN NON-CENTRAL
GRAVITATIONAL FIELD OF THE EARTH
ON THE FAR GUIDANCE STAGE**

Mironov V.I., Mironov Y.V., Fominov I.V. Energetically Optimal Control of the Convergence of the Spacecraft in Non-Central Gravitational Field of the Earth on the Far Guidance Stage.

Abstract. The article is devoted to the development of algorithms for calculating energy-optimal programs for controlling the approach of a spacecraft to an orbital object at the long-range guidance stage using the maximum principle L.S. Pontryagin. It is assumed that the spacecraft is equipped with a longitudinal propulsion system running on chemical fuel. The programs of optimal change in the second fuel consumption and the vector of cosine guides, which determine the orientation of the thrust force of the propulsion system, should be determined. As a criterion for optimal control, we consider a functional that determines the minimum consumption of the working fluid. The optimal control problem is solved in a limited region of the state space, which is determined by the range of variation of the angular range of the spacecraft within one revolution. The full equations of the boundary value problem of the maximum principle are given using the model of the object's motion in the normal gravitational field of the Earth, the boundary conditions, and also the analytical dependencies that determine the control structure in the optimal mode. The boundary optimization problem is solved with the Newton method. To determine the initial approximation of conjugate variables, an analytical solution is given to the problem of energy-optimal approach control in a uniform central field. The results of numerical studies of energy-optimal programs to control the interception in the normal gravitational field of the Earth with the final pitch at the stage of long-range guidance are presented. In general, the use of optimal approach control algorithms in the airborne and ground complex allows to reduce fuel costs when performing the maneuver, reduce time, and expand the reachability area of the target objects. In addition, the optimal solution can be considered as a reference, with which it is necessary to compare various variants of approximate control algorithms, evaluate their quality and make informed decisions on their practical use.

Keywords: Spacecraft, Meeting in Orbit, Optimal Control, Long-Range Guidance.

Mironov Vyacheslav Ivanovich — Ph.D., Dr. Sci., Professor, Chief Researcher of Information Technologies in System Analysis and Modeling Laboratory, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: Fundamental And Applied Researches in Complex Modeling; Theory of Optimal Observation and Control of Dynamic Processes; Computing Mathematics; Ballistics of Space Flight; Statistical Analysis of Complex Technical Systems. The number of publications — 350. vi-mironov@yandex.ru; 14 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-3337, fax: +7(812)328-4450.

Mironov Yuri Vyacheslavovich — Ph.D., Dr. Sci., Associate Professor, Leading Specialist of System Design Department, JSC "R&EC ETU". Research interests: Ballistics of Space Flights, Methods of Navigation and Control of The Motion of Carrier Rockets and Space Vehicles, Theory of Statistical Estimation, Computational Mathematics. The number of publications — 150. vi-mironov@yandex.ru; 22, Politechnicheskaya str., building N, St. Petersburg, 194021, Russia; office phone: +7(812) 703-7583, fax: +7(812) 703-7584.

Fominov Ivan Vyacheslavovich — Ph.D., Dr. Sci., Head of Autonomous Control Systems Department, Mozhaisky Military Space Academy. Research interests: Navigation and Control Systems of Spacecrafts. The number of publications — 30. i.v.fominov@gmail.com; 13, Zhdanovskaya str., St.-Petersburg, 197198, Russia; office phone: +7(812)347-9521.

References

1. Avduevskij V.S., Antonov B.M. *Osnovy teorii poleta kosmicheskikh apparatov* [Fundamentals of the theory of spacecraft flight]. M.: Mashinostroenie. 1972. 608 p. (In Russ.).
2. Lysenko L.N., Betanov V.V., Zvjagin F.V. *Teoreticheskie osnovy ballistiko-navigacionnogo obespechenija kosmicheskikh poletov* [Theoretical foundations of ballistic-navigational support of space flights of spacecraft flight theory]. M.: Bauman Moscow State Technical University. 2014. 520 p. (In Russ.).
3. Lebedev A.A., Sokolov V.B. *Vstrecha na orbite* [Meeting in orbit]. M.: Mashinostroenie. 1969. 366 p. (In Russ.).
4. Il'in V.A., Kuzmak G.E. *Optimal'nye perelety kosmicheskikh apparatov* [Optimal spacecraft flights]. M.: Nauka. 1976. 744 p. (In Russ.).
5. Ermilov Yu.A., Ivanova E.E., Pantyushin S.V. *Upravlenie sblizheniem kosmicheskikh apparatov* [Control of the approach of space vehicles]. M.: Nauka. 1977. 448 p. (In Russ.).
6. Mironov V.I., Mironov Yu.V., Makarov M.M. [Algorithm for calculating the interception control program in the noncentral gravitational field of the Earth with allowance for the final thrust based on the Euler-Lambert equations]. *Sbornik trudov VKA im. A.F.Mozhayskogo – Proceedings of Mozhaysky Academy*. 2014. vol. 4(645). pp. 64–72. (In Russ.).
7. Mironov V.I., Mironov Yu.V., Burmistrov V.V., Makarov M.M. [Algorithm for calculating the approach control program in the noncentral gravitational field of the Earth with allowance for the final thrust]. *Sbornik trudov VKA im. A.F.Mozhayskogo – Proceedings of Mozhaysky Academy*. 2014. vol. 1(646). pp. 85–94. (In Russ.).
8. Oghim S., Mok S.H., Leeghim H. Optimal Spacecraft Rendezvous by Minimum Velocity Change and Wait Time. *Advances in Space Research*. 2017. vol. 60. no. 6. pp. 1188–1200.
9. Shen H., Zhang T., Casalino L., Pastrone D. Optimization of Active Debris Removal Missions with Multiple Targets. *Journal of Spacecrafts and Rockets*. 2018. vol. 55. no. 1. pp. 181–189.
10. Oghim S., Leeghim H., Kim D. Real-time Spacecraft Intercept Strategy on J2-perturbed Orbits. *Advances in Space Research*. 2019. vol. 63. no. 2. pp. 1007–1016.
11. Xu L., Zhang T., Zhou H., Li M. Relative Orbit Control Method for Non-Cooperative Maneuvering Target Rendezvous. 2015 Chinese Automation Congress (CAC). 2015. pp. 1690–1695.
12. Leeghim H., Kim D., Turner J. Solution for Nonlinear Three-Dimensional Intercept Problem with Minimum Energy. *Mathematical Problems in Engineering*. 2013. vol. 2013. 8 p.
13. Leeghim H. Spacecraft intercept using minimum control energy and wait time. *Celestial Mechanics and Dynamical Astronomy*. 2013. vol. 115. no. 1. pp. 1–19.
14. Baranov A.A., Budjanskij A.A., Razumnyj Yu.N. [Spacecraft motion control when approaching a large space debris object]. *Kosmicheskije issledovaniya – Outer Space Research*. 2017. vol. 55. no 4. pp. 285–289. (In Russ.).
15. Murtazin R.F. [Schemes of accelerated access to the orbital station for modern spacecraft]. *Kosmicheskije issledovaniya – Outer Space Research*. 2014. vol. 52. no. 2. pp. 162–175. (In Russ.).

16. Ivanjuhin A.V., Petuhov V.G. [Tasks to minimize thrust and its applications]. *Kosmicheskie issledovaniya – Outer Space Research*. 2015. vol. 53. no. 4. pp. 320–331. (In Russ.).
17. Evdokimov R.A., Chilin Yu.N. [Parametric synthesis of the electric motor complex of the transport-technical support system of the orbital group of spacecraft]. *Kosmicheskie issledovaniya – Outer Space Research*. 2013. vol. 51. no. 3. pp. 250–264. (In Russ.).
18. Baranov A.A., Grishko D.A., Medvedevskih V.V., Lapshin V.V. [The solution of the problem of overflights of large-sized kosmoschek garbage in sun-synchronous orbits]. *Kosmicheskie issledovaniya – Outer Space Research*. 2016. vol. 54. no. 3. pp. 242–250. (In Russ.).
19. Murtazin R.F. [The approach to the lunar orbital station of a spacecraft starting from Earth]. *Kosmicheskie issledovaniya – Outer Space Research*. 2016. vol. 54. no. 3. pp. 268–274. (In Russ.).
20. Suhanov A.A., Prado A.F.B. [Small-scale interorbital flights in an arbitrary force field]. *Kosmicheskie issledovaniya – Outer Space Research*. 2013. vol. 51. no. 2. pp. 159–175. (In Russ.).
21. Novoselov V.S. *Analiticheskaya teoriya optimizacii v gravitacionnyh polyah* [Analytical theory of optimization in gravitational fields]. Publishing House of Leningrad University. 1972. 317 p. (In Russ.).

Л. К. БАБЕНКО, А. В. ТРЕПАЧЕВА
**О НЕСТОЙКОСТИ ДВУХ СИММЕТРИЧНЫХ ГОМОМОРФНЫХ
КРИПТОСИСТЕМ, ОСНОВАННЫХ НА СИСТЕМЕ
ОСТАТОЧНЫХ КЛАССОВ**

Бабенко Л.К., Трепачева А.В. О нестойкости двух симметричных гомоморфных криптосистем, основанных на системе остаточных классов.

Аннотация. Одной из наиболее актуальных задач, связанных с защитой облачных вычислений, является анализ криптостойкости гомоморфных шифров. Данная статья посвящена изучению вопроса о защищенности двух недавно предложенных гомоморфных криптосистем, которые, в связи с их высокой вычислительной эффективностью, могут быть использованы для шифрования данных на облачных серверах. Обе криптосистемы основаны на системах остаточных классов, что позволяет рассмотреть их с единых позиций. Именно использование систем остаточных классов делает применение этих криптосистем в реальных приложениях заманчивым с точки зрения эффективности по сравнению с другими гомоморфными шифрами, так как появляется возможность легко распараллелить вычисления. Однако их криптостойкость не была в достаточной мере изучена в литературе и нуждается в анализе.

Отметим, что ранее предшественниками была рассмотрена криптосистема похожая на один из шифров, криптостойкость которого исследуется. Была предложена идея адаптивной атаки по выбранным открытым текстам на эту конструкцию и дана оценка необходимого для раскрытия ключа количества пар «открытый текст, шифртекст». Здесь проводится анализ этой атаки и показываем, что иногда она может работать некорректно. Также описывается более общий алгоритм атаки с известными открытыми текстами. Приводятся теоретические оценки вероятности успешного раскрытия секретного ключа с его помощью и практические оценки этой вероятности, полученные в ходе вычислительного эксперимента.

Защищенность второй криптосистемы не была исследована ранее в литературе. Изучена её стойкость к атаке с известными открытыми текстами. Проанализирована зависимость необходимого для взлома количества пар «открытый текст, шифртекст» от параметров криптосистемы и даны рекомендации, которые могут помочь улучшить криптостойкость.

Итог проведенного анализа заключается в том, что обе криптосистемы являются уязвимыми к атаке с известными открытыми текстами. Поэтому использовать их для шифрования конфиденциальных данных может быть небезопасно.

Основным алгоритмом, используемым в предложенных атаках на криптосистемы, является алгоритм поиска наибольшего общего делителя. Как следствие, время, необходимое для реализации атак, является полиномиальным от размера входных данных.

Ключевые слова: гомоморфное шифрование, облачные вычисления, криптоанализ, атака с известными открытыми текстами, система остаточных классов.

1. Введение. Гомоморфное шифрование (ГШ) позволяет вычислять функции над зашифрованными данными без знания ключа расшифрования. Владелец ключа может извлечь результат вычислений над исходными данными из результата вычислений над соответствующими зашифрованными данными. Это делает ГШ перспективным решением для защищенного делегирования облачному серверу вычислений над

конфиденциальными данными клиента. Перед загрузкой данных на сервер клиент должен зашифровать их с помощью ГШ. Затем сервер проведет вычисление над зашифрованными данными и вернет зашифрованный результат клиенту.

Понятие ГШ было введено в 1978 году [1]. После этого криптографы предложили и проанализировали множество различных гомоморфных криптосистем [2-5], позволяющих выполнять одну арифметическую операцию (сложение или умножение). Криптосистема RSA [5] — наиболее известный пример: она позволяет вычислять умножение гомоморфно.

В 2009 году исследователь из IBM Крейг Джентри разработал первую схему *полностью гомоморфного шифрования* (ПГШ) на основе идеальных решеток [6]. Криптосистема Джентри позволяет выполнять *произвольные* вычисления над зашифрованными данными. Отправной точкой при построении криптосистемы Джентри является ГШ, разрешающее лишь ограниченное число гомоморфных умножений и сложений. Ограничение вызвано «шумом» в шифртекстах — некоторой величиной, встраиваемой в шифртекст в процессе шифрования. «Шум» необходим для обеспечения криптостойкости. Но после каждой гомоморфной операции его значение возрастает. В какой-то момент это приводит к невозможности корректно расшифровать. Поэтому второй шаг в конструкции Джентри — обновить шифртексты так, чтобы уменьшить «шум». Процедура обновления шифртекстов основана на вычислении функции расшифрования, но не непосредственно над битами шифртекста и секретного ключа, а над шифртекстами этих битов гомоморфно. Это так называемый метод «самокоррекции» (англ. «bootstrapping»).

В последующих работах был представлен широкий спектр схем ПГШ. Все эти криптосистемы можно разделить на две категории.

Первая категория содержит схемы ПГШ с открытым ключом, основанные на внесении «шума» [7-13]. Эти криптосистемы базируются на методике Джентри. Авторы пытаются улучшить производительность оригинальной криптосистемы [6]. Исходная криптосистема Джентри доказуемо криптостойка к атаке по выбранным открытым текстам, но практически нереализуема. Однако, несмотря на все усилия, криптосистемы ПГШ, разработанные на основе идей Джентри, по-прежнему криптостойки, но непрактичны [14].

Ко *второй категории* можно отнести симметричные криптосистемы ПГШ, не использующие «шум» и метод «самокоррекции». Здесь можно найти ПГШ, основанное на разных математических объектах. Кипнис (Kipnis), Сяо (Xiao) и другие [15-17] предложили ПГШ на основе матриц. Работы Ягисавы (Yagisawa) [18, 19] представляют ПГШ, использующее

октонионную алгебру. Очень популярны гомоморфные криптосистемы на основе полиномов [20–25]. И, наконец, существуют криптосистемы на системах остаточных классов (СОК) [26–28].

Большинство криптосистем второй категории устроено более просто и имеет большую вычислительную эффективность, чем криптосистемы, использующие метод Дженри. Для многих из них стойкость обосновывается с помощью того факта, что задача факторизации чисел сложна. Но эти обоснования не являются строгими доказательствами, и зачастую криптосистемы оказываются уязвимыми. В частности, работы [29–32] описывают эффективные атаки по известным открытым текстам (АИО) на матричные схемы ПГШ. В [33–38] можно найти АИО на ПГШ на основе полиномов. Криптосистемы, базирующиеся на октонионах, также уязвимы к АИО [39–41]. И, наконец, есть попытки провести атаки с использованием только шифртекстов (АТШ) [42–44]. Итак, вопрос о существовании *эффективного и криптостойкого* ПГШ на данный момент по-прежнему является открытым.

2. Постановка задачи и основные результаты. Основная цель настоящей работы – изучить криптостойкость против АИО двух недавно предложенных симметричных схем ПГШ на основе систем остаточных классов (СОК) — криптосистемы Вишневого и Князева [27] и криптосистемы Бабенко, Кучерова и Червякова [28]. Напомним, что АИО предполагает, что криптоаналитик перехватил s пар «открытый текст», шифртекст», созданных на одном ключе, и его задача — восстановить секретный ключ.

Криптосистема Вишневого и Князева была построена для решения систем линейных уравнений в недоверенной вычислительной среде. А криптосистема Бабенко, Кучерова и Червякова предназначена для защиты данных в облаках. Эти две криптосистемы очень похожи, поэтому схема атаки для них является общей. Отличие заключается в том, что в [27] базовый объект — целые числа, а в [28] — полиномы. Это влияет на метод оценки вероятности успеха атаки.

Обе криптосистемы не были проанализированы ранее в литературе на предмет стойкости к АИО, поэтому в данной работе мы восполняем этот пробел. Очень важно понять уровень стойкости криптосистемы перед тем, как начать использовать ее в реальных приложениях.

Описанная здесь атака на криптосистемы [27, 28] основана на том же подходе, что и АИО из работ [33–38]. Суть его заключается в том, что криптоаналитик проводит преобразования над перехваченными данными и получает некоторые величины (числа или полиномы), которые в качестве одного из сомножителей содержат секретный ключ или некоторую его

часть. Тогда основным инструментом поиска ключа становится алгоритм вычисления наибольшего общего делителя (НОД).

Отметим, что в работе [45] был рассмотрен вопрос о стойкости к адаптивной атаке по выбранным открытым текстам (ААВО) криптосистемы похожей на конструкцию [27]. Данная атака также подразумевает, что криптоаналитик имеет s пар «открытый текст, шифртекст». Эти пары он получает за счет того, что у него есть доступ к шифрующему устройству, как к черному ящику. Поэтому он может получить пары для открытых текстов, выбранных по своему усмотрению. Адаптивность атаки означает, что криптоаналитик имеет возможность получать новые пары непосредственно в ходе атаки.

В [45] была представлена идея того, как можно осуществить ААВО. Доказана теорема о том, что если $s = O(\tau)$, где τ — количество модулей в используемой для шифрования СОК, то секретный ключ может быть восстановлен однозначно. Однако представленный авторами результат не исключает того, что ключ можно раскрыть и при меньшем s .

В данной работе мы проанализировали ААВО, описанную в [45], и пришли к заключению, что в общем случае она не всегда будет гарантированно выдавать ключ при $s = O(\tau)$. Данное событие может произойти лишь с вероятностью < 1 . Мы приведем пример, демонстрирующий это. Для криптосистемы Вишневого и Князева [27], которую мы изучаем здесь, данный подход к проведению ААВО будет работать полностью корректно и при $s = O(\tau)$ ключ действительно будет всегда раскрыт однозначно.

В рамках ААВО криптоаналитик находится в более сильной позиции, чем в случае АИО. Поэтому факт уязвимости к ААВО не умаляет важности исследования стойкости к АИО. Здесь наш основной результат состоит в том, что при $s \approx O(\log(\tau))$ криптоаналитик может раскрыть секретный ключ в рамках АИО на криптосистему [27], однако не гарантированно, а с вероятностью ≈ 1 . Этот результат подтвержден большим количеством компьютерных экспериментов, хотя и нуждается в дополнительном более строгом теоретическом обосновании. Похожий результат получен и для криптосистемы [28].

3. Обозначения. Ниже мы используем следующие обозначения: \mathbb{Z}_n — кольцо вычетов по модулю n , $n \in \mathbb{Z}, n > 1$; $\mathbb{Z}_n[x]$ — кольцо полиномов с коэффициентами из \mathbb{Z}_n ; $\mathbb{Z}_{n,d}[x]$ — множество полиномов над \mathbb{Z}_n степени меньше d ; $M_N(\mathbb{Z}_n)$ — кольцо квадратных $N \times N$ -матриц над \mathbb{Z}_n . Для $a \in \mathbb{Z}$ его остаток от деления на n обозначается через $[a]_n \in \mathbb{Z}_n$, а остаток от деления полинома $f(x)$ на $g(x)$ соответственно — $[f(x)]_{g(x)}$. Строчными буквами полужирного шрифта (например, \mathbf{v}) будем обозначать

векторы $\mathbf{v} = (v_1, \dots, v_N)$, а прописными буквами жирным шрифтом (например, \mathbf{A}) — матрицы $\mathbf{A} = \{a_{i,j}\}_{i=\overline{1,N}, j=\overline{1,N}}$. Для $f(x) \in \mathbb{Z}_n[x]$ обозначим через f_i его i -й коэффициент. Для $\mathbf{A} \in M_N(\mathbb{Z})$ обозначим через $[\mathbf{A}]_n \in M_N(\mathbb{Z}_n)$ матрицу, имеющую элементы $[a_{i,j}]_n$. Аналогичные обозначения используются для векторов и полиномов.

Через $Pr\{A\}$ обозначается вероятность события A ; $x \stackrel{\$}{\leftarrow} R$ обозначает случайный элемент, полученный по равномерному распределению на множестве R ; $x \stackrel{\mathcal{D}}{\leftarrow} R$ — элемент, сгенерированный по распределению вероятностей \mathcal{D} на R ; $f(x) \stackrel{\$}{\leftarrow} \mathbb{Z}_n[x]$ означает, что $f_i \stackrel{\$}{\leftarrow} \mathbb{Z}_n, i = \overline{0, \deg(f) - 1}, f_{\deg(f)} \stackrel{\$}{\leftarrow} \mathbb{Z}_n \setminus \{0\}$.

Для $a, b \in \mathbb{Z}$ запись $a|b$ означает, что a делит b , GCD — наибольший общий делитель (от англ. greatest common divisor).

4. Сведения из теории чисел. В этом разделе собраны все необходимые известные утверждения и теоремы для представления криптосистем в рамках исследования и криптоанализа. В первую очередь напомним китайскую теорему об остатках (КТО).

Теорема 1. ([46]) Пусть $n = \prod_{i=1}^{\tau} n_i$, где $GCD(n_i, n_j) = 1$ при $i \neq j$. Существует изоморфизм:

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_{\tau}}.$$

Для вычисления $a \in \mathbb{Z}_n$, соответствующего вектору $([a]_{n_1}, \dots, [a]_{n_{\tau}}) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_{\tau}}$, используется формула:

$$a = CRT_{n_1, \dots, n_{\tau}}([a]_{n_1}, \dots, [a]_{n_{\tau}}) = \sum_{i=1}^{\tau} [a]_{n_i} \cdot S_i \cdot S_i^{-1}, \quad (1)$$

где $S_i = \frac{n}{n_i}, S_i^{-1} \equiv \frac{1}{S_i} \pmod{n_i}$.

Теорема 2. ([47]) Пусть $z_i \stackrel{\$}{\leftarrow} \{1, 2, \dots, n\}, i = \overline{1, s}, n \in \mathbb{N}, s > 1$ — случайные числа, полученные независимо по равномерному распределению. Для $s \geq 3$ справедливо равенство:

$$Pr\{GCD(z_1, \dots, z_s) = 1\} = \frac{1}{\zeta(s)} + O\left(\frac{1}{n}\right),$$

а для $s = 2$ справедливо:

$$Pr\{GCD(z_1, z_2) = 1\} = \frac{1}{\zeta(2)} + O\left(\frac{\log(n)}{n}\right),$$

где $\zeta(s)$ – дзета-функция Римана.

Значения функции $\frac{1}{\zeta(s)}$ проиллюстрированы в таблице 1 с точностью $\varepsilon = 10^{-4}$. Видно, что при $s \geq 5$ вероятность взаимной простоты s случайных чисел, выбранных из диапазона $\{1, 2, \dots, n\}$, равна ≈ 1 .

Таблица 1. Значения $\frac{1}{\zeta(s)}$

s	$1/\zeta(s)$
2	0.6079
3	0.8319
4	0.9259
5	0.9643
6	0.9829
7	0.9917
8	0.9959
9	0.9979

Теорема 3. [48] Пусть даны полиномы $f_i(x) \in \mathbb{Z}_{q,d}[x], i = \overline{1, s}$, где q – простое число. Тогда справедливо:

$$Pr\{GCD(f_1(x), \dots, f_s(x)) = 1\} = 1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{s \cdot d}}.$$

Ясно, что с ростом q, s и d вероятность, указанная в теореме 3, будет стремиться к 1.

5. Гомоморфное шифрование. Гомоморфное шифрование позволяет проводить вычисления над зашифрованными данными без знания секретного ключа. В ходе такого вычисления производится зашифрованный результат. Его расшифрование дает результат обработки соответствующих открытых текстов.

Часто симметричные полностью гомоморфные криптосистемы обладают следующим свойством: пространства открытых текстов и шифртекстов являются *кольцами*. Для произвольных открытых текстов m_1, m_2 выполняются равенства:

$$\begin{aligned} Dec_{sk}(Enc_{sk}(m_1) + Enc_{sk}(m_2)) &= m_1 \oplus m_2, \\ Dec_{sk}(Enc_{sk}(m_1) \cdot Enc_{sk}(m_2)) &= m_1 \odot m_2, \end{aligned} \quad (2)$$

где \oplus, \odot — операции в кольце открытых текстов, $+, \cdot$ — операции в кольце шифртекстов, Enc, Dec — функции зашифрования и расшифрования, параметризованные ключом sk .

6. Описание анализируемых гомоморфных криптосистем.

ГШ Вишневецкого и Князева ([27]). Криптосистема Вишневецкого и Князева построена с использованием числовой СОК. Она была предложена для решения специальной задачи. Авторы искали способ найти корни системы линейных уравнений $\mathbf{A} \cdot \vec{x} = \mathbf{b}$ в недоверенной вычислительной среде, где

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,N} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,N} \end{pmatrix} \in M_N(\mathbb{Z}), \mathbf{b} \in \mathbb{Z}^N = \begin{pmatrix} b_1 \\ \cdots \\ b_N \end{pmatrix}.$$

Входные данные \mathbf{A} , \mathbf{b} и полученные корни не должны раскрываться недоверенному серверу, выполняющему вычисления.

Алгоритмы шифрования и расшифрования основаны на теореме 1. Секретный ключ sk — вектор случайных и независимо выбранных простых чисел $(k_1, \dots, k_\tau) \in \mathbb{N}^\tau$, таких что $k_i > 1, i = \overline{1, \tau}, k_i \neq k_j$ при $i \neq j$. Пространство открытых текстов \mathcal{M} — множество $\mathcal{R}_t = \{0, \dots, t-1\} \subset \mathbb{Z}$, где $t = \prod_{i=1}^\tau k_i$, пространство шифртекстов \mathcal{C} — это подмножество \mathbb{Z}^τ .

Алгоритм зашифрования $Enc(m \in \mathcal{R}_t, sk)$:

– вычислить $\mathbf{c} = ([m]_{k_1}, \dots, [m]_{k_\tau}) \in \mathbb{Z}^\tau$.

Алгоритм расшифрования $Dec(\mathbf{c} = (c_1, \dots, c_\tau), sk)$:

– вычислить $m = CRT_{k_1, \dots, k_\tau}(c_1, \dots, c_\tau)$.

Умножение и сложение шифртекстов выполняется по коэффициентно. По теореме 1 такое шифрование обладает мультипликативным и аддитивным гомоморфизмами.

Рассмотрим, как это шифрование применяется для безопасного решения уравнения $\mathbf{A} \cdot \vec{x} = \mathbf{b}$ на облачном сервере. Числа k_i выбираются так, что:

$$k_i < k_{i-1},$$

$$\prod_{i=1}^{\tau-2} k_i \leq \max_{i,j} \{a_{i,j}\} < \prod_{i=1}^{\tau-1} k_i < \prod_{i=1}^{\tau} k_i.$$

Чтобы зашифровать \mathbf{A} и \mathbf{b} , клиент вычисляет набор матриц и векторов $\mathbf{A}_i = [\mathbf{A}]_{k_i}, \mathbf{b}_i = [\mathbf{b}]_{k_i}, i = \overline{1, \tau}$. Они отправляются на облачный сервер для вычисления зашифрованного решения. Из теоремы 1 следует,

что можно решать τ отдельных линейных систем:

$$\mathbf{A}_i \cdot x = \mathbf{b}_i, i = \overline{1, \tau}.$$

Пусть $\mathbf{x}_i = (x_{i,1}, \dots, x_{i,N}) \in \mathbb{Q}^N$ является решением $\mathbf{A}_i \cdot x = \mathbf{b}_i$. Сервер вычисляет $\mathbf{x}_i, i = \overline{1, \tau}$ и отправляет клиенту. Клиент может получить решение x исходной системы $\mathbf{A} \cdot x = \mathbf{b}$ следующим образом:

$$\mathbf{x} = \begin{pmatrix} CRT_{k_1, \dots, k_\tau}(x_{1,1}, \dots, x_{\tau,1}) \\ \dots \\ CRT_{k_1, \dots, k_\tau}(x_{1,N}, \dots, x_{\tau,N}) \end{pmatrix}.$$

ГШ Бабенко, Кучерова и Червякова ([28]). В криптосистеме [28] используется система полиномиальных остаточных классов и обобщенная версия КТО для полиномов. Пусть дано простое число $q, q \geq 2$ (это публичный параметр). Секретный ключ — это вектор полиномов $sk = (k_1(x), \dots, k_\tau(x)) \in (\mathbb{Z}_q[x])^\tau$, где $k_i(x) = x^d - \alpha_i \in \mathbb{Z}_q[x]$, $GCD(k_i(x), k_j(x)) = 1$ при $i \neq j$. Пространство открытых текстов \mathcal{M} — это $\mathbb{Z}_{q,t}[x]$, где $t < d \cdot \tau$, пространство шифртекстов \mathcal{C} — подмножество $(\mathbb{Z}_q[x])^\tau$.

Алгоритм зашифрования $Enc(m(x) \in \mathbb{Z}_q[x], sk)$:

– вычислить $\mathbf{c} = (c_1(x), \dots, c_\tau(x)) \in (\mathbb{Z}_q[x])^\tau, c_i(x) = [m(x)]_{k_i(x)}$.

Алгоритм расшифрования $Dec(\mathbf{c} = (c_1(x), \dots, c_\tau(x)), sk)$:

– вычислить $m(x) = CRT_{k_1(x), \dots, k_\tau(x)}(c_1(x), \dots, c_\tau(x))$.

В [28] описывается, как формула (1) может быть адаптирована для полиномов. Основная идея такова: по sk и $c_1(x), \dots, c_\tau(x)$ можно вычислить $m(x) = \sum_{i=1}^{\tau} c_i(x) \cdot B_i(x)$, где $B_i(x) \in \mathbb{Z}_q[x], i = \overline{1, \tau}$ — полиномы, составленные с использованием $k_i(x), i = \overline{1, \tau}$. Гомоморфные свойства также обеспечивает теорема 1.

Авторы [28] не отметили такой важный момент, что предложенный метод построения секретного ключа приводит к тому, что $\tau \leq q$.

7. Общие замечания о стойкости анализируемых криптосистем. Описанные криптосистемы являются детерминированными при условии, что используется некоторая фиксированная система вычетов. Это значит, что их алгоритмы шифрования отображают данный открытый текст всегда в один и тот же шифртекст на заданном ключе. Для такого типа шифрования характерна следующая уязвимость: злоумышленник всегда может по паре шифртекстов понять, шифруют ли они одно и то же сообщение или разные; эта уязвимость достаточно существенна [49].

Рассмотрим криптосистему Вишневого и Князева. Пусть $m \in \mathcal{R}_t$ — открытый текст. И пусть $\mathbf{c} = (c_1, \dots, c_\tau) \in \mathbb{Z}^\tau$ шифрует m на ключе (k_1, \dots, k_τ) . Предположим, что алгоритм шифрования использует стандартную полную систему вычетов $K_j = \{0, \dots, k_j - 1\}$ для каждого k_j и тогда $c_j = [m]_{k_j} \in K_j$. Если для некоторого j выполняется $m < k_j$, то $c_j = m$. А если $m < \min_{j=\overline{1, \tau}} \{k_j\}$, то получим $\mathbf{c} = (m, \dots, m) \in \mathbb{Z}^\tau$. Таким образом, открытый текст, по сути, остается незашифрованным.

Поэтому очевидной мерой безопасности здесь является требование $k_j \ll t, j = \overline{1, \tau}$. Это предотвратило бы высокую вероятность появления m в векторе \mathbf{c} в случае равномерного распределения на \mathcal{R}_t . Вспоминая, что $t = \prod_{j=1}^{\tau} k_j$, получаем, что для улучшения безопасности предпочтительнее выбирать большее τ и меньшие числа k_j . Для других распределений вероятностей выбор (k_1, \dots, k_τ) может быть более сложным.

Отметим, что авторы криптосистемы не указали четких требований к тому, как будут соотноситься между собой битовые длины чисел t и $k_j, j = \overline{1, \tau}$. Исходя из численных примеров, можно предположить, что отдается предпочтение такой конфигурации: большое число t ($\log_2(t) \geq 32$) и $k_j \ll t, j = \overline{1, \tau}$.

Также эту проблему можно решить с помощью небольшой модификации алгоритма шифрования. Если $m < k_j$, то необходимо сгенерировать $r_j \stackrel{\$}{\leftarrow} \mathcal{R}_t \setminus \{0\}$, и j -ю координату шифртекста положить равной $c_j = [m]_{k_j} + r_j \cdot k_j$. Более того, можно поступать так для всех координат шифртекста. И тогда шифрование станет вероятностным.

Для криптосистемы Бабенко, Кучерова и Червякова ситуация аналогична, если используется стандартная система полиномиальных остатков. Если $\deg(m(x)) < d$, то $\mathbf{c} = (m(x), \dots, m(x))$. Поэтому лучше выбирать $d \ll t$, где t — верхняя граница для степеней открытого текста, а d — степень полинома в секретном ключе. Также можно рандомизировать координаты шифртекста посредством прибавления к ним полиномов вида $k_j(x) \cdot r_j(x)$, где $r_j(x)$ — случайный полином.

8. Общая схема атаки по известным открытым текстам. Криптосистемы [27, 28] очень похожи по своему устройству. Для них можно составить следующее общее описание. Пространство открытых текстов \mathcal{M} — это подмножество некоторого Евклидова кольца \mathcal{E} , sk — случайный вектор $(k_1, \dots, k_\tau) \in \mathcal{E}^\tau$, такой что $GCD(k_i, k_j) = 1$ при $i \neq j$, пространство шифртекстов \mathcal{C} — подмножество \mathcal{E}^τ . Открытый текст $m \in \mathcal{M}$ шифруется по формуле $\mathbf{c} = ([m]_{k_1}, \dots, [m]_{k_\tau})$, где $[m]_{k_j}$ — остаток от деления m на k_j в \mathcal{E} . Для расшифрования применяется КТО, адаптированная для \mathcal{E} .

Входные данные: пары $(m_1, c_1), \dots, (m_s, c_s)$

Выходные данные: либо секретный ключ sk , либо сообщение «Атака не успешна»

```

1 for  $i = 1$  to  $\tau$  do
2 |    $d_j := GCD(m_1 - c_{1,j}, \dots, m_s - c_{s,j});$ 
3 end
4 if  $GCD(d_1, \dots, d_\tau) = 1$  then
5 |   Выдать  $d$  в качестве результата;
6 end
7 else
8 |   Выдать сообщение «Атака не успешна»;
9 end
    
```

Алгоритм 1: АИО($(m_1, c_1), \dots, (m_s, c_s)$)

Исходя из этого описания, можно составить следующую схему атаки с известными открытыми текстами на самом общем уровне. Предположим, у криптоаналитика есть пары $(m_i, c_i), i = \overline{1, s}$, где $m_i \in \mathcal{E}$, $c_i = (c_{i,1}, \dots, c_{i,\tau}), c_{i,j} = [m_i]_{k_j} \in \mathcal{E}$. Цель криптоаналитика — определить $sk = (k_1, \dots, k_\tau)$. Чтобы найти k_j , криптоаналитик может вычислить:

$$d_j = GCD(m_1 - c_{1,j}, \dots, m_s - c_{s,j}).$$

Действительно, существует следующее представление:

$$m_i = r_{i,j} \cdot k_j + c_{i,j}, \tag{3}$$

где $r_{i,j} \in \mathcal{E}$ — некоторый случайный элемент. Следовательно, мы имеем:

$$d_j = k_j \cdot GCD(r_{1,j}, \dots, r_{s,j}). \tag{4}$$

Вероятность найти k_j указанным способом равна $p_{j,s} = Pr\{k_j = d_j\}$. И, очевидно, выполняется

$$p_{j,s} = Pr\{GCD(r_{1,j}, \dots, r_{s,j}) = 1\}. \tag{5}$$

Величина $p_{j,s}$ зависит от закона, по которому распределены случайные элементы $r_{i,j}$ кольца \mathcal{E} . Вероятностное распределение чисел $r_{i,j}$, в свою очередь, зависит от распределения вероятностей \mathcal{D} на пространстве открытых текстов \mathcal{M} . Вышеизложенное может быть формализовано в виде алгоритма 1, являющегося общей схемой АИО на [27, 28].

В следующих разделах мы проанализируем величину $p_{j,s}$ и общую вероятность раскрыть sk для [27] и [28].

9. АИО на криптосистему Вишневого и Князева. Во-первых, отметим, что алгоритм 1 для криптосистемы Вишневого и Князева можно дополнить еще одним шагом, если проверка на шаге 2 успешно пройдена: провести тест на простоту для каждого d_j [50].

Оценка вероятности раскрыть один элемент ключа k_j . Теперь перейдем к оценке вероятности $p_{j,s}$. Предположим, что все $r_{i,j}$ из формулы (3) являются независимыми и равномерно случайными положительными целыми числами. Тогда по теореме 2 выполняется $p_{j,s} \approx \frac{1}{\zeta(s)}$. Учитывая данные таблицы 1, получаем, что при $s \geq 5$ противник получит k_j с вероятностью ≈ 1 .

Проанализируем, какое распределение имеют числа $r_{i,j}$ для криптосистемы Вишневого и Князева в случае равномерного распределения вероятностей на пространстве открытых текстов M . Пусть есть случайная величина $m \xleftarrow{\$} \mathcal{R}_t$, где $t = \prod_{i=1}^{\tau} k_i$. Выполняется $m = r \cdot k_j + c$, где k_j — фиксированное число, частное $r = \lfloor \frac{m}{k_j} \rfloor$ — случайная величина, имеющая диапазон значений $\mathcal{R}_q = \{0, 1, \dots, q - 1\}$, где $q = \frac{t}{k_j}$.

Лемма 1. Случайная величина r имеет равномерное распределение над \mathcal{R}_q , где $q = \frac{t}{k_j}$.

Доказательство. Множество \mathcal{R}_t можно представить как объединение $\mathcal{R}_t = \cup_{i=0}^q \overline{\mathcal{R}}_i$, где $\overline{\mathcal{R}}_i = \{i \cdot k_j, i \cdot k_j + 1, \dots, i \cdot k_j + k_j - 1\}$. Тогда $|\overline{\mathcal{R}}_i| = k_j$ и для $m \in \overline{\mathcal{R}}_i$ имеем $r = i$. Поэтому получаем $Pr\{r = i\} = \frac{k_j}{t} = \frac{1}{q}$. \square

Теорема 4. Для криптосистемы Вишневого и Князева выполняется $p_{j,s} = \sum_{l=0}^{s-2} C_s^l \cdot \left(\frac{q-1}{q}\right)^{s-l} \cdot \left(\frac{1}{q}\right)^l \cdot \left(\frac{1}{\zeta(s-l)} + O\left(\frac{1}{q-1}\right)\right) + s \cdot \left(\frac{1}{q}\right)^s$, $q = \frac{t}{k_j}$.

Доказательство. Вероятность $p_{j,s}$ можно представить в виде следующей суммы: $Pr\{r_{i,j} \neq 0, i = \overline{1, s} \ \& \ GCD(r_{1,j}, \dots, r_{s,j}) = 1\} + \sum_{z=2}^{s-1} Pr\{\exists r_{k_1,j}, \dots, r_{k_z,j} | r_{k_l,j} \neq 0 \ \& \ GCD(r_{k_1,j}, \dots, r_{k_z,j}) = 1\} + Pr\{\exists r_{i,j} = 1 \ \& \ r_{l,j} = 0, l \neq i\}$. Поясним, что событие, вероятность которого указана под знаком суммы, состоит в том, что z чисел из $r_{i,j}$ оказались не равными нулю и взаимно простыми, где $2 \leq z < s$, а остальные $r_{i,j}$ равны нулю.

Вероятность того, что l чисел из $r_{i,j}, i = \overline{1, s}$ равны нулю, а остальные нет, составляет $C_s^l \cdot \left(\frac{q-1}{q}\right)^{s-l} \cdot \left(\frac{1}{q}\right)^l$. А вероятность того, что ненулевые $s - l$ чисел взаимно просты, равна $\frac{1}{\zeta(s-l)} + O\left(\frac{1}{q-1}\right)$ по теореме 2. Эти два

события можно считать независимыми. Все вместе это дает формулу для $p_{j,s}$. \square

Следствием данной теоремы является следующая лемма.

Лемма 2. Для криптосистемы Вишневецкого и Князева выполняется $p_{j,s} > \eta_{j,s}$, где $\eta_{j,s} = \left(\frac{q-1}{q}\right)^s \cdot \left(\frac{1}{\zeta(s)} + O\left(\frac{1}{q-1}\right)\right)$, $q = \frac{t}{k_j}$.

Предположим, что $\log_2(t) \geq 32$ и $k_j \ll t, j = \overline{1, \tau}$ (см. раздел 7). Тогда $\left(\frac{q-1}{q}\right)^s \approx 1$ и можно положить $\eta_{j,s} \approx \frac{1}{\zeta(s)}$.

Таблица 2. Оценки вероятности $p_{j,s}$

s	$\widetilde{p}_{j,s}$	$1/\zeta(s)$
3	0.8323	0.8319
4	0.9269	0.9259
5	0.9664	0.9643
6	0.9812	0.9829
7	0.992	0.9917
8	0.9964	0.9959
9	0.9985	0.9979
10	0.999	0.999

Были проведены эксперименты для получения практической оценки $\widetilde{p}_{j,s}$ вероятности раскрыть один элемент ключа, который выбирался случайно по равномерному распределению из первой тысячи простых чисел. Здесь и далее для получения каждой оценки проводилось десять тысяч компьютерных экспериментов.

В таблице 2 представлены практические оценки $\widetilde{p}_{j,s}$ для $p_{j,s}$ и соответствующие значения $\frac{1}{\zeta(s)}$ для сравнения. Можно видеть, что выполняется $\widetilde{p}_{j,s} \approx \frac{1}{\zeta(s)}$ с вычислительной точностью $\varepsilon = 10^{-2}$.

Оценка вероятности раскрыть ключ sk полностью. Для вероятности $\overline{p}_{s,\tau}$ раскрыть ключ целиком справедлива следующая формула

$$\overline{p}_{s,\tau} = Pr\{GCD(r_{1,1}, \dots, r_{s,1}) = 1, \dots, GCD(r_{1,\tau}, \dots, r_{s,\tau}) = 1\}. \quad (6)$$

Если используется детерминированный алгоритм шифрования, описанный в разделе 6, то события $GCD(r_{1,j}, \dots, r_{s,j}) = 1, j = \overline{1, \tau}$ нельзя считать независимыми друг от друга, поскольку для каждого $i \in \overline{1, s}$ случайные величины $r_{i,1}, \dots, r_{i,\tau}$ зависимы между собой. Поэтому

формула

$$\overline{p}_{s,\tau} = \prod_{j=1}^{\tau} p_{j,s} \tag{7}$$

не справедлива в этом случае.

Однако, если для шифрования использовать вероятностный алгоритм, упомянутый в разделе 7, то зависимости будут устранены прибавкой ко всем $r_{i,j}$ случайных равномерно распределенных независимых величин. Тогда (7) окажется справедливой и выполнится:

$$\overline{p}_{s,\tau} > \prod_{j=1}^{\tau} \left(\frac{q_j - 1}{q_j} \right)^s \cdot \left(\frac{1}{\zeta(s)} + O\left(\frac{1}{q_j - 1} \right) \right), \tag{8}$$

где $q_j = t/k_j$.

Если снова предположить, что $\log_2(t) \geq 32$ и $k_j \ll t, j = \overline{1, \tau}$, то правая часть (8) будет равна $\approx \frac{1}{\zeta(s)^\tau}$.

Таблица 3. Практические оценки вероятности $\overline{p}_{s,\tau}$

s	$\widetilde{p}_{s,10}$	$\frac{1}{\zeta(s)^{10}}$	$\widetilde{p}_{s,50}$	$\frac{1}{\zeta(s)^{50}}$	$\widetilde{p}_{s,100}$	$\frac{1}{\zeta(s)^{100}}$
3	0.1546	0.1587	0.0001	0.0001	0	10^{-17}
4	0.4629	0.4533	0.018	0.0191	0.0003	0.0003
5	0.697	0.6952	0.1561	0.1631	0.0298	0.0266
6	0.8406	0.8415	0.4244	0.4232	0.1748	0.1791
7	0.921	0.9200	0.6631	0.6598	0.4342	0.4354
8	0.9609	0.9679	0.8164	0.8159	0.663	0.6657
9	0.9809	0.9801	0.901	0.9045	0.818	0.8182
10	0.9907	0.9901	0.9523	0.9515	0.9059	0.9053
11	0.9962	0.9945	0.9761	0.9755	0.9574	0.9517
12	0.9974	0.9975	0.9883	0.9877	0.9739	0.9756
13	0.9986	0.9987	0.9941	0.9938	0.9878	0.9878
14	0.9994	0.9993	0.9962	0.9969	0.993	0.9938
15	0.9999	0.9996	0.9983	0.9984	0.9961	0.9969

В таблице 3 показаны практические оценки $\widetilde{p}_{s,\tau}$ вероятности $\overline{p}_{s,\tau}$ полного раскрытия sk для $\tau = 10, 50$ и 100 , полученные в ходе вычислительного эксперимента для детерминированного варианта алгоритма шифрования. То есть формулы (7),(8) не выполняются в данном случае. Также приведены соответствующие значения функции $\frac{1}{\zeta(s)^\tau}$ для сравнения. Можно видеть, что её значения совпадают с $\widetilde{p}_{s,\tau}$ с точностью не

менее $\varepsilon = 10^{-2}$ в большинстве случаев. Поэтому, несмотря на отсутствие строгого теоретического обоснования, можно сделать вывод, что $\frac{1}{\zeta(s)^\tau}$ является хорошим приближением для $\overline{p_{s,\tau}}$.

Итак, мы получили следующую эмпирическую оценку:

$$\overline{p_{s,\tau}} \approx \frac{1}{\zeta(s)^\tau}. \quad (9)$$

Отметим, что при проведении эксперимента числа k_j выбирались случайно по равномерному распределению из первой тысячи простых чисел.

Из таблицы 3 видно, что с ростом τ криптоаналитику нужно все большее количество пар «открытый текст, шифртекст» для того, чтобы найти sk с вероятностью ≈ 1 . К примеру, для длины ключа $\tau = 100$ необходимо не менее 11 пар.

Интересно выяснить общее соотношение между τ и числом пар s , которого будет достаточно для восстановления sk с вероятностью θ . Согласно (9) для получения $\overline{p_{s,\tau}} \approx \theta$ при данном τ нужно, чтобы s удовлетворяло равенству:

$$\frac{1}{\zeta(s)} = \sqrt[\tau]{\theta}. \quad (10)$$

Дзета-функция Римана при $s > 1$ представима в виде ряда Дирихле $\zeta(s) = 1 + \sum_{i=n}^{\infty} \frac{1}{n^s}$. Из этого легко видеть, что $\psi(s) = \frac{1}{1+\frac{1}{2^s}}$ можно использовать как значение, приближенное к $\frac{1}{\zeta(s)}$. Действительно, уже при $s \geq 5$ выполняется $|\frac{1}{\zeta(s)} - \psi(s)| < 10^{-2}$.

Чтобы получить некоторое представление о характере зависимости s от τ , заменим в (10) $\frac{1}{\zeta(s)}$ на $\psi(s)$. Тогда мы получим следующую формулу:

$$s \approx \log_2 \left(\frac{\sqrt[\tau]{\theta}}{1 - \sqrt[\tau]{\theta}} \right), \quad (11)$$

где $0 < \theta < 1$. Последовательность, указанная в правой части равенства (11), является бесконечно большой при $\tau \rightarrow \infty$. По мере того как θ становится все ближе к 1, порядок ее роста увеличивается.

Зафиксируем, к примеру, значение $\theta = 0.999$. Тогда будет выполняться $\frac{\sqrt[\tau]{\theta}}{1 - \sqrt[\tau]{\theta}} < \tau^2$ и соответственно $s < 2 \cdot \log_2(\tau)$. Общий же характер

зависимости s от τ имеет вид:

$$s = O(\log(\tau)). \tag{12}$$

Эксперименты подтвердили, что (12) отражает реальную зависимость s от τ . На рисунке 1 представлены значения s для $\tau \in \overline{2, 10000}$, для которых согласно данным экспериментов выполняется $\theta = 0.999$. Из графика видно, что с ростом τ количество пар s , необходимых для раскрытия ключа, возрастает, но не очень быстро. Видно, что достаточно иметь $s \approx O(\log(\tau))$ пар, чтобы раскрыть секретный ключ.

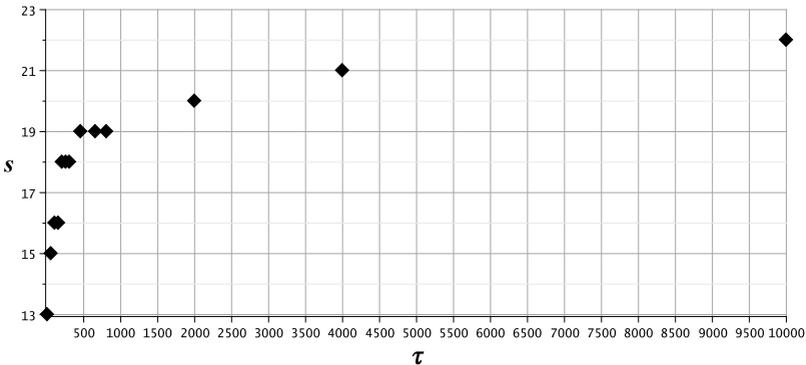


Рис. 1. Экспериментальные данные о числе пар «открытый текст, шифртекст» s , необходимом для раскрытия ключа размерности τ с вероятностью $\theta \geq 0.999$.

При построении данного графика для каждого τ элементы ключа k_j выбирались равномерно случайно из первых $5 \cdot \tau$ простых чисел.

Наконец, необходимо отметить, что алгоритм 1 применительно к криптосистеме Вишневого и Князева имеет полиномиальную временную сложность от параметров s , τ и $\log_2(t)$. В частности, временную сложность вычисления всех наибольших общих делителей можно оценить с помощью $s \cdot \tau \cdot O((\log(t))^2)$ [51]. А сложность тестов на простоту составляет $\tau \cdot O((\log_2(t))^3)$ [50].

Криптосистема Вишневого и Князева и АИО на нее были реализованы на языке C++ с использованием среды разработки Qt 1.3.1 и библиотеки NTL [53]. Для тестирования программы использовалась рабочая станция среднего класса: четырехъядерный процессор AMD Phenom (tm) II P960 1,80 ГГц, оперативная память 4 Гб. Таблица 4 демонстрирует время работы описанной АИО для $\tau = 100$ и разных s . Числа k_j

были выбраны случайным образом из первой тысячи простых чисел. Из таблицы 4 видно, что атака достаточно эффективна.

Таблица 4. Время работы АИО на криптосистему Вишневого и Князева при $\tau = 100$

s	Время(мсек)
5	751.21
6	2147.27
7	2573.16
8	2718.41
9	3020.51
10	3235.11
11	3521.14
12	4011.36
13	4918.38
14	5100.41

10. АИО на криптосистему Бабенко, Кучерова и Червякова [28]. Алгоритм 1 для криптосистемы Бабенко, Кучерова и Червякова можно также дополнить еще одним шагом, если шаг 2 успешно пройден: провести проверку, что все найденные полиномы $d_j(x)$ имеют одну и ту же степень и вид $x^d - \alpha_j$.

Оценка вероятности раскрыть один элемент ключа $k_j(x)$. Проанализируем значения вероятности $p_{j,s}$ для криптосистемы Бабенко, Кучерова и Червякова. Предположим, что все $r_{i,j}(x)$ являются независимыми и равномерно случайными полиномами. Тогда по теореме 3 справедливо:

$$p_{j,s} > 1 - \frac{1}{q^{s-1}}. \quad (13)$$

Ясно, что с ростом s величина, указанная в (13), будет стремиться к 1. К примеру, при уже $q = 2$ и $s = 5$ выполнится $p_{j,s} \approx 1$.

Докажем, что $r_{i,j}(x), i = \overline{1, s}$ действительно являются случайными величинами с равномерным распределением, если распределение вероятностей на \mathcal{M} равномерно.

Теорема 5. Для случайной величины $m(x) \stackrel{\S}{\leftarrow} \mathbb{Z}_{q,t}[x]$ и фиксированного полинома $k(x) \in \mathbb{Z}_q[x]$, где $d = \deg(k(x)) \leq t$, существует представление $m(x) = r(x) \cdot k(x) + c(x)$, где $r(x)$ — частное и $c(x)$ — остаток. При этом $r(x)$ — случайная величина, имеющая распределение $r(x) \stackrel{\S}{\leftarrow} \mathbb{Z}_{q,t-d}[x]$.

Таблица 5. $\widetilde{p}_{j,s}$ и $p_{j,s}$ для $q = 2, d = 3$

s	$\widetilde{p}_{j,s}$	$p_{j,s}$
4	0.86	0.875
5	0.957	0.9525
6	0.967	0.96875
7	0.991	0.984375
8	0.99	0.992188
9	0.997	0.996094
10	0.999	0.998047

Доказательство. Для фиксированного $k(x)$ существует взаимно-однозначное соответствие между полиномами $m(x) \in \mathbb{Z}_{q,t}[x]$ и парами $\{r(x) \in \mathbb{Z}_{q,t-d}[x], c(x) \in \mathbb{Z}_{q,d}[x]\}$. При этом каждому $r(x) \in \mathbb{Z}_{q,t-d}[x] \setminus \{0\}$ соответствует множество, состоящее из q^d различных полиномов $m(x) \in \mathbb{Z}_{q,t}[x]$ степени $d + \deg(r(x))$, имеющих частное $r(x)$ при делении на $k(x)$. А частному $r(x) = 0$ соответствуют все $m(x)$ такие, что $\deg(m(x)) < d$, и таких полиномов тоже будет q^d штук. Из этого следует, что $r(x)$ имеет равномерное распределение вероятностей. \square

Тогда по теореме 3 мы получаем следующее утверждение

Теорема 6. Для криптосистемы Бабенко, Кучерова и Червякова выполняется $p_{j,s} = 1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}}$.

Были проведены компьютерные эксперименты для того, чтобы определить практическую оценку $\widetilde{p}_{j,s}$ вероятности раскрыть один элемент ключа для различных значений параметров q, d, t . К примеру, таблица 5 иллюстрирует значения $p_{j,s}$ в соответствии с теоремой 6 и $\widetilde{p}_{j,s}$ для $q = 2, d = 3, t = 51$. Для указанных значений параметров для раскрытия одного элемента ключа $k_j(x)$ с вероятностью ≈ 1 нужно, чтобы выполнялось $s \geq 5$. Для больших q нужно еще меньшее количество пар.

Оценка вероятности раскрыть ключ sk полностью. Проанализируем вероятность $\overline{p}_{s,\tau}$ определить $sk = (k_1(x), \dots, k_\tau(x)) \in (\mathbb{Z}_q[x])^\tau$. Для неё справедлива формула (6), адаптированная для случая полиномов. Так же, как и для криптосистемы Вишневого и Князева, равенство $\overline{p}_{s,\tau} = \prod_{j=1}^{\tau} p_{j,s}$ не выполняется, если используется детерминированный алгоритм шифрования, описанный в разделе 6. Однако, если использовать вероятностный алгоритм (см. раздел 7), то равенство будет справедливо и для криптосистемы Бабенко, Кучерова и Червякова получим следующее:

$$\overline{p}_{s,\tau} = \left(1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}} \right)^\tau. \tag{14}$$

Таблица 6. Количество пар s , необходимых для взлома криптосистемы Бабенко Кучерова и Червякова при $2 \leq d \leq 60$, $2 \leq \tau \leq q$, $\theta = 0.95$

q	s
2	5..7
3	4..6
5	3..5
7	3..4
11	3..4
13	2..4

Эксперименты показали, что формула (14), несмотря на отсутствие строгого обоснования, хорошо работает и для случая детерминированного шифрования. Значения вероятностей, полученные по ней, хорошо коррелируют с практическими оценками $\widetilde{p}_{s,\tau}$.

На основании (14) можно получить представление о характере зависимости числа пар s , необходимого для раскрытия ключа с вероятностью θ , от τ и q . Для упрощения выкладок положим $\widetilde{p}_{s,\tau} \approx \left(1 - \frac{1}{q^{s-1}}\right)^\tau$. Тогда получим:

$$s \approx 1 + \log_q \left(\frac{1}{1 - \sqrt[\tau]{\theta}} \right). \quad (15)$$

При заданных q, θ зависимость s от τ имеет вид $\approx O(\log(\tau))$.

В таблице 6 приведены данные, полученные на основе экспериментов, о минимальном числе пар «открытый текст, шифртекст», необходимом для раскрытия секретного ключа с вероятностью $\theta = 0.95$, для различных значений q . Для каждого q степень полиномов ключа d перебиралась в диапазоне $2 \leq d \leq 60$, а для τ был сделан исчерпывающий перебор в диапазоне $2 \leq \tau \leq q$ (напоминаем, что τ не может превышать q). В правой колонке таблицы 6 указан диапазон для количества пар s , который был получен при указанном переборе для d и τ . Можно видеть, что с ростом q уменьшается количество пар s «открытый текст, шифртекст», необходимых для гарантированного взлома криптосистемы.

В ходе построения таблицы 6 было выявлено, что для фиксированного q с ростом τ увеличивается s . При $\tau = q$ достигается максимум. Но влияние τ на s не столь значительно, как влияние q .

Отметим, что значения s , которые можно получить по формуле (15), имеют хорошую корреляцию с данными таблицы 6.

В таблице 7 собрана подробная статистика о минимальном числе s пар, необходимом для раскрытия секретного ключа, для различных

Таблица 7. Зависимость количества пар s , необходимых для взлома криптосистемы Бабенко Кучерова и Червякова с вероятностью более 0.95 при $\tau = q$, от d

d	q									
	2	3	5	7	11	13	17	19	23	29
2	6	5	4	4	4	4	3	3	3	3
5	6	5	5	4	4	4	3	4	3	3
10	6	5	4	4	4	4	4	4	3	3
15	5	5	4	4	4	4	3	3	3	3
20	7	5	5	4	4	4	4	4	3	3
25	6	5	4	4	4	4	4	4	3	3
29	6	5	4	4	4	4	4	3	3	3

Таблица 8. Среднее время, необходимое для осуществления атаки на криптосистему Бабенко, Кучерова и Червякова с использованием **трех** пар (мсек)

d	q					
	5	7	11	13	17	19
2	1.5	2.156	3.48	4.26	6.84	9.08
5	2.132	3.688	8.52	12.81	27.19	32.78
10	4.062	7.9	24.51	38.95	79.44	132.81
15	6.428	14.86	51.14	96.208	171.19	246.54
20	9.908	23.728	104.30	151.41	275.36	407.02
25	14.124	34.914	138.47	195.50	422.23	533.58
29	18.094	54.684	167.59	299.92	560.84	704.88

значений q, d и максимального значения $\tau = q$. Таблица демонстрирует, что степень d довольно слабо влияет на s . Этот факт объясняется видом формулы для $p_{j,s}$ из теоремы 6.

В заключение этого раздела отметим, что алгоритм 1 применительно к криптосистеме Бабенко, Кучерова и Червякова имеет полиномиальную временную сложность от параметров s, τ и t . В частности, сложность вычисления всех наибольших общих делителей равна $s \cdot \tau \cdot O(t \cdot (\log(t))^2)$ элементарных операций в \mathbb{Z}_q [52].

Криптосистема Бабенко, Кучерова и Червякова и атака на нее также были реализованы на языке программирования C++ с помощью среды разработки Qt 1.3.1 и библиотеки NTL [54]. Таблица 8 демонстрирует время работы описанной АИО для разных q, d и $\tau = q, s = 3$.

11. Адаптивная атака по выбранным открытым текстам. В работе [45] была описана идея адаптивной атаки по выбранным открытым

текстам для криптосистемы, похожей на криптосистему Вишневого и Князева. Основное отличие состоит в том, что в [45] ключ $sk = (k_1, \dots, k_\tau) \in \mathbb{N}^\tau$ не обязательно состоит лишь из простых чисел, но $GCD(k_i, k_j) = 1$ при $i \neq j$.

Ниже представлен алгоритм 2 поиска одного модуля k_j ключа, идея которого предложена в [45]. Он принимает на вход пару «открытый текст, шифртекст» и имеет доступ к оракулу $\mathcal{O}_{Enc_{sk}}$, умеющему шифровать любые открытые тексты на ключе sk . С точки зрения криптоаналитика, $\mathcal{O}_{Enc_{sk}}$ представляет собой черный ящик. Изучая выходы, которые $\mathcal{O}_{Enc_{sk}}$ производит на различных входах, он пытается определить sk .

Далее будем использовать обозначение $(m, \mathbf{c}) \leftarrow \mathcal{O}_{Enc_{sk}}(m)$, смысл которого в том, что $\mathcal{O}_{Enc_{sk}}$, получив на вход открытый текст m , на выходе выдает пару $(m, \mathbf{c} = (c_1, \dots, c_\tau))$, где $\mathbf{c} = Enc_{sk}(m)$.

Входные данные: $(m_1, \mathbf{c}_1), j$

Выходные данные: Модуль k_j

- 1 Вычислить факторизацию (если она не известна) на простые множители $m_1 - c_{1,j} = \prod_{i=1}^{L_j} p_{j,i}$;
- 2 $m_2 := \prod_{i=1}^{\lfloor \frac{L_j}{2} \rfloor} p_{j,i}$, $m_3 := \prod_{i=\lfloor \frac{L_j}{2} \rfloor + 1}^{L_j} p_{j,i}$;
- 3 $(m_2, \mathbf{c}_2) \leftarrow \mathcal{O}_{Enc_{sk}}(m_2)$, $(m_3, \mathbf{c}_3) \leftarrow \mathcal{O}_{Enc_{sk}}(m_3)$;
- 4 **if** $(c_{2,j} \neq 0) \ \& \ (m_2 \neq c_{2,j}) \ \& \ (c_{3,j} \neq 0) \ \& \ (m_3 \neq c_{3,j})$ **then**
- 5 | **Выдать** $GCD(m_2, c_{2,j}) \cdot GCD(m_3, c_{3,j})$;
- 6 **end**
- 7 **else if** $(c_{2,j} = 0) \ \& \ (c_{3,j} \neq 0)$ **then**
- 8 | **Выдать** $CalcOneModulus((m_2, \mathbf{c}_2), j)$;
- 9 **end**
- 10 **else if** $(c_{2,j} \neq 0) \ \& \ (c_{3,j} = 0)$ **then**
- 11 | **Выдать** $CalcOneModulus((m_3, \mathbf{c}_3), j)$;
- 12 **end**
- 13 **else**
- 14 | **Выдать** сообщение «Атака не успешна»;
- 15 **end**

Алгоритм 2: $CalcOneModulus((m_1, \mathbf{c}_1), j)$

Пара (m_1, \mathbf{c}_1) , которая изначально подается на вход $CalcOneModulus$, вычисляется оракулом $\mathcal{O}_{Enc_{sk}}$ для некоторого случайно выбранного открытого текста m_1 .

Авторы [45] утверждают, что если выполняется условие, указанное в строке 4 алгоритма 2, то справедливо $k_j = \alpha_j$, где $\alpha_j = GCD(m_2, c_{2,j})$.

$GCD(m_3, c_{3,j})$. Однако это не так: может оказаться, что $\alpha_j = v_j \cdot k_j$, где v_j — некоторый случайный множитель.

Действительно, имеем $m_2 = k_j \cdot r_{2,j} + c_{2,j}$, $m_3 = k_j \cdot r_{3,j} + c_{3,j}$ и разложение на простые множители $k_j = \prod_{t=1}^{l_j} p_{j,k_{z_t}}$. Числа m_2, m_3 построены таким образом, что одна часть сомножителей $p_{j,k_{z_t}}$ числа k_j делит m_2 и $c_{2,j}$, а другая часть делит m_3 и $c_{3,j}$. Исходя из этого, имеем $k_j | \alpha_j$. Однако не обязательно выполняется $k_j = \alpha_j$, так как, к примеру, в $GCD(m_2, c_{2,j})$ (или $GCD(m_3, c_{3,j})$) могут попасть простые сомножители числа $r_{2,j}$ (или $r_{3,j}$ соответственно).

Входные данные: $(m_1, c_1), j$

Выходные данные: Модуль k_j

- 1 Вычислить факторизацию (если она не известна) на простые множители $m_1 - c_{1,j} = \prod_{i=1}^{L_j} p_{j,i}$;
- 2 $m_2 := \prod_{i=1}^{\lfloor \frac{L_j}{2} \rfloor} p_{j,i}$, $m_3 := \prod_{i=\lfloor \frac{L_j}{2} \rfloor + 1}^{L_j} p_{j,i}$;
- 3 $(m_2, c_2) \leftarrow \mathcal{O}_{Enc_{sk}}(m_2)$, $(m_3, c_3) \leftarrow \mathcal{O}_{Enc_{sk}}(m_3)$;
- 4 **if** $(c_{2,j} = 0) \ \& \ (c_{3,j} \neq 0) \ \& \ (m_2 - \text{простое число})$ **then**
- 5 | **Выдать** m_2 ;
- 6 **end**
- 7 **else if** $(c_{2,j} \neq 0) \ \& \ (c_{3,j} = 0) \ \& \ (m_3 - \text{простое число})$ **then**
- 8 | **Выдать** m_3 ;
- 9 **end**
- 10 **else if** $(c_{2,j} = 0) \ \& \ (c_{3,j} \neq 0)$ **then**
- 11 | **Выдать** $\text{CalcOnePrimeModulus}((m_2, c_2), j)$;
- 12 **end**
- 13 **else if** $(c_{2,j} \neq 0) \ \& \ (c_{3,j} = 0)$ **then**
- 14 | **Выдать** $\text{CalcOnePrimeModulus}((m_3, c_3), j)$;
- 15 **end**
- 16 **else**
- 17 | **Выдать** сообщение «Атака не успешна»;
- 18 **end**

Алгоритм 3: $\text{CalcOnePrimeModulus}((m_1, c_1), j)$

Нетрудно привести соответствующий численный пример. Пусть $k_j = 15$, $m_1 - c_{1,j} = 2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2$, $m_2 = 2^2 \cdot 3^2$, $m_3 = 5^2 \cdot 7^2$. Выполняется $c_{2,j} = [m_2]_{k_j} = 6$, $c_{3,j} = [m_3]_{k_j} = 10$ и тогда $GCD(m_2, c_{2,j}) = 6$, $GCD(m_3, c_{3,j}) = 5$, $GCD(m_2, c_{2,j}) \cdot GCD(m_3, c_{3,j}) = 30 \neq k_j$.

Итого, событие $k_j = \alpha_j$ на шаге 5 алгоритма 2 происходит не гарантированно, как утверждает в [45], а лишь с некоторой вероят-

ностью. Поэтому в общем случае данный алгоритм, возможно, требует существенной доработки. Мы оставим этот вопрос для дальнейшего исследования.

Однако для случая, когда все k_j простые (как в схеме ПГШ [27]), алгоритм 2 с небольшим изменением будет работать и гарантированно выдавать k_j не более, чем за $\lceil \log_2(L_j) \rceil$ рекурсивных вызовов. При этом максимальное количество пар, которое придется запросить у оракула, составляет $2 \cdot \lceil \log_2(L_j) \rceil + 1$.

Здесь представлен алгоритм 3, позволяющий раскрыть один элемент ключа k_j , для криптосистемы Вишневого и Князева в рамках адаптивной атаки по выбранным открытым текстам. Полный алгоритм атаки будет состоять в том, что `CalcOnePrimeModulus` нужно вызвать τ раз для каждого k_j . Количество пар «открытый текст, шифртекст», которое необходимо запросить у оракула для того, чтобы гарантированно определить sk , составляет $O(\tau)$.

Похожий алгоритм можно предложить и для криптосистемы [28]. Однако, так же как и в случае конструкции, которая изначально анализировалась в [45], он не будет гарантированно выдавать k_j . В [28] элемент ключа $k_j(x) = x^d - \alpha_j$ не является неприводимым полиномом. Поэтому алгоритм раскрытия $k_j(x)$ — это, по сути, алгоритм 2, адаптированный для полиномов. На шаге 5 он будет вычислять корректный $k_j(x)$ лишь с некоторой вероятностью.

12. Заключение. Были изучены две симметричные полностью гомоморфные криптосистемы, основанные на применении систем остаточных классов и китайской теоремы об остатках — криптосистема Вишневого и Князева и криптосистема Бабенко, Кучерова и Червякова. Эти криптосистемы являются детерминированными, а потому для них априори характерна следующая уязвимость: злоумышленник всегда способен отличить пару шифртекстов, шифрующих одно и то же сообщение, от пары шифртекстов, шифрующих разные сообщения. Использование вероятностного шифрования всегда является более предпочтительным с точки зрения защищенности. Уже, исходя из этого, анализируемые криптосистемы не желательно применять в реальных приложениях. Здесь мы описали один из вариантов, как можно сделать их вероятностными. Примером может послужить еще одна схема ПГШ «HORNS» [26], основанная на системах остаточных классов, однако являющаяся вероятностной.

Проведенный в данной работе анализ показал, что анализируемые криптосистемы уязвимы к атаке по известным открытым текстам. Их секретный ключ представляет собой вектор $sk = (k_1, \dots, k_\tau)$. Были получены точные формулы вероятности раскрытия одного элемента k_j

этого вектора. Согласно этим формулам необходимо перехватить хотя бы 5 пар «открытый текст, шифртекст» для обеих криптосистем в случае равномерного распределения на пространстве открытых текстов, чтобы найти k_j с вероятностью ≈ 1 . Для криптосистемы Бабенко, Кучерова и Червякова с ростом размера используемого базового конечного поля q может хватить и двух пар. Эта информация подтверждена вычислительным экспериментом.

Также была проанализирована вероятность $\overline{p_{s,\tau}}$ полностью раскрыть ключ в зависимости от количества перехваченных пар s . Для криптосистемы Вишневого и Князева было установлено, что имеет место формула $\overline{p_{s,\tau}} \approx \frac{1}{\zeta(s)^\tau}$, где ζ — дзета-функция Римана. Она нуждается в дополнительном теоретическом обосновании, но при этом хорошо коррелирует с экспериментальными оценками вероятностей. Исходя из данной формулы и результатов экспериментов, было установлено, что для того, чтобы определить sk с вероятностью ≈ 1 при заданном τ , нужно перехватить $s = O(\log(\tau))$ пар. К примеру, при размерности секретного ключа $\tau = 10$ криптоаналитику необходимо иметь ≈ 13 пар, а при $\tau = 10000$ — соответственно 22 пары.

Для криптосистемы Бабенко, Кучерова и Червякова была получена формула $\overline{p_{s,\tau}} = \left(1 - \frac{1}{q^{s-1}} + \frac{q-1}{q^{(t-d)\cdot s}}\right)^\tau$. Она также нуждается в дополнительном более строгом обосновании. Однако значения вероятностей, посчитанные по ней, близки к оценкам вероятностей, полученным в ходе экспериментов. При фиксированном параметре q здесь также нужно иметь $\approx O(\log(\tau))$ пар, чтобы определить ключ с вероятностью ≈ 1 .

Было выявлено, что для криптосистемы Бабенко, Кучерова и Червякова максимальным образом на рост числа пар s , необходимого для взлома, влияет параметр q . От степени полиномов секретного ключа d величина s зависит очень слабо. И, наконец, увеличение τ влечет за собой увеличение s . Однако способ генерации секретного ключа, выбранный авторами криптосистемы, приводит к естественному ограничению $\tau \leq q$. Поэтому при оценке вероятности раскрыть ключ можно сразу зафиксировать максимальную его размерность $\tau = q$. Исходя из полученных результатов экспериментов, было выявлено, что уже при $q = 29$ и $\tau = q$ количество пар s , необходимых для взлома с вероятностью ≈ 1 , равно трем. С ростом q число s может только убывать.

В целом, можно отметить, что криптосистема Бабенко, Кучерова и Червякова находится в «тисках» жестких ограничений:

- нельзя существенно увеличивать q , так как тогда упадет сложность взлома;

- нельзя сделать размерность ключа τ больше, чем q ;
- нельзя увеличить степень полиномов секретного ключа d , т.к. тогда открытые тексты небольшой степени фактически останутся незашифрованными.

В качестве рекомендации по увеличению сложности взлома крипто-системы Бабенко, Кучерова и Червякова можно предложить генерировать полиномы секретного ключа более произвольным образом. Это, по крайней мере, отменит ограничение $\tau \leq q$.

Отметим также, что в ходе анализа вероятности раскрытия ключа для анализируемых криптосистем использовалось предположение, что пространство открытых текстов имеет равномерное распределение вероятностей. Ситуация может отличаться, если пространство открытых текстов имеет другое распределение вероятностей, что может быть предметом отдельных исследований. Но необходимо напомнить, что наиболее трудный для криптоаналитика случай — это когда распределение на множестве открытых текстов равномерно.

Основным инструментом проведения атаки с известными открытыми текстами на анализируемые криптосистемы является алгоритм поиска наибольшего общего делителя. Поэтому, время, необходимое для реализации атак, является полиномиальным от размера входных данных.

Также в данной работе была проанализирована адаптивная атака по выбранным открытым текстам из работы [45] на шифр, похожий на криптосистему Вишневого и Князева. Было установлено, что алгоритм определения элемента ключа k_j , представленный в [45], не будет всегда гарантированно выдавать k_j . Это событие происходит с некоторой вероятностью < 1 . Поэтому алгоритм нуждается в дополнительном исследовании и доработке. Но мы установили, что небольшая модификация делает его пригодным для криптоанализа криптосистемы Вишневого и Князева. Он будет гарантированно раскрывать ключ sk . Для работы ему нужно $O(\tau)$ пар «открытый текст, шифртекст». Аналогичный алгоритм можно предложить и для ПГШ [28]. Однако он, как и исходный алгоритм из [45], требует доработки.

Итог проведенного анализа заключается в том, что криптосистема Вишневого и Князева и криптосистема Бабенко, Кучерова и Червякова являются уязвимыми к атаке по выбранным открытым текстам и атаке с известными открытыми текстами. Поэтому использовать их для шифрования конфиденциальных данных может быть небезопасно.

В дальнейшем планируется провести анализ стойкости данных криптосистем к атаке только по шифртекстам.

Литература

1. Rivest R. L., Adleman L., Dertouzos M. L. On data banks and privacy homomorphisms // Foundations of secure computation. 1978. vol. 32. no. 4. pp. 169-178.
2. Brickell E. F., Yacobi Y. On privacy homomorphisms // Proceedings of Advances in Cryptology—EUROCRYPT'87. 1988. pp. 117-125.
3. Goldwasser G., Micali S. Probabilistic encryption & how to play mental poker keeping secret all partial information // Proceedings of the fourteenth annual ACM symposium on Theory of computing. 1982. pp. 365-377.
4. Paillier P. Public-key cryptosystems based on composite degree residuosity classes // Proceedings of Advances in cryptology—EUROCRYPT'99. 1999. pp. 223-238.
5. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. 1978. vol. 21. no. 2. pp. 120-126.
6. Gentry C. A fully homomorphic encryption scheme // PhD thesis. Stanford University, 2009. 209 p.
7. Cheon J. H., Coron J. S., Kim J., Lee M. S., Lepoint T., Tibouchi M., Yun A. Batch fully homomorphic encryption over the integers // Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013. pp. 315-335.
8. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping // Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ACM). 2012. pp. 309-325.
9. Brakerski Z. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP // Proceedings of Advances in cryptology—CRYPTO 2012. 2012. pp. 868-886.
10. Chillotti I., Gama N., Georgieva M., Izabachene M. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds // Proceedings of Advances in Cryptology—ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security. 2016. pp. 3-33.
11. Cheon J. H., Han K., Kim D. Faster Bootstrapping of FHE over the Integers // IACR Cryptology ePrint Archive. 2017. no. 79.
12. Micciancio D., Sorrell J. Ring packing and amortized FHEW bootstrapping // IACR Cryptology ePrint Archive. 2018. no. 532.
13. Brakerski Z. Quantum FHE (Almost) As Secure As Classical // Proceedings of Annual International Cryptology Conference. 2018. pp. 67-95.
14. Бабенко Л.К., Буртыка Ф.Б., Макаревич О.Б., Трепачева А.В. Полностью гомоморфное шифрование (Обзор) // Вопросы защиты информации. 2015, № 3. С. 3–25.
15. Kipnis A., Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encryption, randomization and verification // IACR Cryptology ePrint Archive. 2012. no. 637.
16. Xiao L., Bastani O, Yen I.-L. An efficient homomorphic encryption protocol for multi-user systems // IACR Cryptology ePrint Archive. 2012. no. 193.
17. Sharma I. Fully homomorphic encryption scheme with symmetric keys // Master's of technology diss. in Department of Computer Science & Engineering (with specialization in Computer Engineering). 2013. 64 p.
18. Yagisawa M. Fully Homomorphic Encryption without bootstrapping // IACR Cryptology ePrint Archive. 2015. no. 474.
19. Yagisawa M. Improved Fully Homomorphic Encryption with Composite Number Modulus // IACR Cryptology ePrint Archive. 2016. no. 50.

20. *Ростовцев А.Г., Богданов А.Г., Михайлов М.Ю.* Метод безопасного вычисления полинома в недоверенной среде с помощью гомоморфизмов колец // Проблемы информационной безопасности. Компьютерные системы. 2011. № 2. С. 76-85.
21. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings // Proceedings of 2013 World Congress on Internet Security (WorldCIS). 2013. pp. 70-75.
22. *Жиров А. О., Жирова О. В., Кренделев С. Ф.* Безопасные облачные вычисления с помощью гомоморфной криптографии // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 6-12.
23. *Dasgupta S., Pal S. K.* Design of a polynomial ring based symmetric homomorphic encryption scheme // Perspectives in Science. 2016. vol. 8. pp. 692-695.
24. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism // Information Security. 2002. pp. 471-483.
25. *Domingo-Ferrer J.* A new privacy homomorphism and applications // Information Processing Letters. 1996. vol. 60. no 5. pp. 277-282.
26. *Gomathisankaran M., Tyagi A., Namuduri K.* HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System // Proceedings of 2011 45th Annual Conference Information Sciences and Systems (CISS). 2011. pp. 1-5.
27. *Вишневский А. К., Князев В. В.* Комплексное применение гомоморфных криптографических преобразований для решения систем линейных алгебраических уравнений // Научное издание. 2015. Т. 16. № 11. С. 28-35.
28. *Бабенко М. Г., Кучеров Н. Н., Червяков Н. И.* Разработка системы гомоморфного шифрования информации на основе полиномиальной системы остаточных классов // Сибирские электронные математические известия. Труды VI международной молодежной школы-конференции «Теория и численные методы решения обратных и некорректных задач». 2015. Т. 12. С. 33-41. URL: <http://semr.math.nsc.ru/v12/c1-283.pdf> (дата обращения: 02.12.2018).
29. *Vizár D., Vaudenay S.* Cryptanalysis of chosen symmetric homomorphic schemes // Studia Scientiarum Mathematicarum Hungarica. 2015. vol. 52. no. 2. pp. 288-306.
30. *Tsaban B., Lifshitz N.* Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme // Journal of Mathematical Cryptology. 2015. vol. 9. no. 2. pp. 75-78.
31. *Трепачева А. В.* Криптоанализ симметричных полностью гомоморфных линейных криптосистем на основе задачи факторизации чисел // Известия Южного федерального университета. Технические науки. 2015. Т. 166, № 5. С. 89-100.
32. *El-Yahyaoui, A., Elkettani, M. D.* Cryptanalysis of fully homomorphic encryption schemes // International Journal of Computer Science and Information Security, LJS Publishing, 2016. vol. 14. no. 5. pp. 677-685.
33. *Cheon J. H., Kim W. H., Nam H. S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme // Information Processing Letters. 2006. vol. 97 no. 3. pp. 118-123.
34. *Wagner D.* Cryptanalysis of an algebraic privacy homomorphism // Proceedings of International Conference on Information Security. 2003. pp. 234-239.
35. *Трепачева А. В.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem // Труды Института системного программирования РАН. 2014. Т. 26. № 5. С. 83-98.
36. *Трепачева А. В.* О криптоанализе одной полностью гомоморфной криптосистемы на основе задачи факторизации // Безопасность информационных технологий. 2015. Т. 22, № 2. С. 19-25.

37. *Trepacheva A.V.* Known plaintext attack on a fully homomorphic cryptosystem based on factorization // Proceedings of 4th Workshop on Current Trends in Cryptology (СТСCrypt'2015). 2015. pp. 205-215.
38. *Babenko L., Trepacheva A.* Known plaintexts attack on polynomial based homomorphic encryption // Proceedings of the 7th International Conference on Security of Information and Networks (ACM). 2014. pp.157-165.
39. *Трепачева А.В.* Криптоанализ полностью гомоморфных криптосистем, основанных на алгебре октонионов // Обозрение прикладной и промышленной математики. 2016. Т. 23. вып. 4. 2 с.
40. *Wang Y.* Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping // IACR Cryptology ePrint Archive. 2015. no. 519.
41. *Wang Y.* Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes // IACR Cryptology ePrint Archive. 2016. no. 68.
42. *Babenko L.K., Trepacheva A.V.* Cryptanalysis of factoring-based fully homomorphic encryption // Proceedings of the 8th International Conference on Security of Information and Networks. 2015. pp. 80-83.
43. *Трепачева А.В.* Атака по шифртекстам на одну линейную полностью гомоморфную криптосистему // Прикладная дискретная математика. Приложение. 2015. № 8. С. 75-78.
44. *Трепачева А.В.* О соотношениях между атаками на симметричные шифры, гомоморфные над кольцом вычетов // Безопасность информационных технологий. 2017. Т. 24. № 2. С. 82–91.
45. *Babenko, M., Chervyakov, N., Tchernykh, A., Kucherov, N., Deryabin, M., Radchenko, G., Navaux Ph., Syvatkin, V.* Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack // Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). 2018. pp. 270-274.
46. *Бухштаб А. А.* Теория чисел // М.: Просвещение. 1966. 384 С.
47. *Nymann J. E.* On the probability that k positive integers are relatively prime // Journal of Number Theory. 1972. vol. 4. no. 5. pp. 469-473.
48. *Benjamin A. T., Bennett C. D.* The probability of relatively prime polynomials // Mathematics Magazine. 2007. vol. 80. no. 3. pp. 196-202.
49. *Goldreich O.* Foundations of cryptography. // Cambridge university press. 2009. 800 p.
50. *Weenink T.* Deterministic primality testing // Bachelor's thesis. Technische Universiteit Eindhoven. 2015. 24 p.
51. *Knuth D. E.* The Art of Computer Programming – Volume 3 (Sorting and Searching) // Addison-Wesley professional. 1997. 800 p.
52. *Ахо А., Ульман Дж., Хопкрофт Дж.* Построение и анализ вычислительных алгоритмов // М.: Мир. 1979. 536 с.
53. Реализация криптосистемы Вишневецкого и Князева и атаки на нее. URL: <https://github.com/alina1989malina/CryptanalysisVishnevskyKnyazev> (дата обращения: 02.12.2018).
54. Реализация криптосистемы Бабенко, Кучерова и Червякова и атаки на нее. URL: <https://github.com/alina1989malina/CryptanalysisBabenkoKucherovChervjakov> (дата обращения: 02.12.2018).

Бабенко Людмила Климентьевна — д-р техн. наук, профессор, главный научный сотрудник, Южно-Российского регионального учебно-научного центра по проблемам информационной безопасности в системе высшей школы, профессор кафедры безопасности информационных технологий, Инженерно-технологическая академия Южного федерального университета

(ИТА ЮФУ). Область научных интересов: криптография, анализ стойкости криптографических алгоритмов, программно-аппаратная защита информации, анализ безопасности криптографических протоколов, вредоносное программное обеспечение, поведенческий анализ, параллельный алгоритм, распределенные многопроцессорные вычисления, нейро-процессорные вычисления. Число научных публикаций — более 200. lkbabenko@sfedu.ru, <https://sfedu.ru/person/lkbabenko>; ул. Чехова, 2, Таганрог, 347922; р.т.: +7(8634)312-018, факс: +7(8634)312-018.

Трепачева Алина Викторовна — младший научный сотрудник кафедры безопасности информационных технологий, Инженерно-технологическая академия Южного федерального университета (ИТА ЮФУ). Область научных интересов: криптоанализ гомоморфных шифров, анализ защищенности облачных систем, вычисления в недоверенной среде, математическая статистика, теория вероятности, дискретные функции, алгебраическая геометрия. Число научных публикаций — 22. alina1989malina@yandex.ru; ул. Чехова, 2, Таганрог, 347922; р.т.: +7(850)865-5415.

Поддержка исследований. Работа выполнена при финансовой поддержке Минобрнауки РФ (проект № 2.6264.2017/8.9).

L. K. BABENKO, A. V. TREPACHEVA
**TOWARDS UNSECURITY OF TWO HOMOMORPHIC
ENCRYPTIONS BASED ON RESIDUE SYSTEM**

Babenko L.K., Trepacheva A.V. Towards Unsecurity of Two Homomorphic Encryptions Based on Residue System.

Abstract. The security of two recently proposed symmetric homomorphic encryption schemes based on residue system is analyzed. Both schemes have a high computational efficiency since using residue system naturally allows parallelizing computations. So they could be good candidates to protect the data in clouds. But to the best of our knowledge there is a lack of security analysis for these encryption schemes.

It should be noted that the first cryptosystem under our consideration was already considered in literature. The sketch of adaptive chosen-plaintext attack was proposed and estimation of its success was given. In this paper the attack is analyzed and it is shown that in some cases it may work incorrectly. Also more general algorithm of known-plaintext attack is presented. Theoretical estimations of probability to recover the key using it and practical estimations of this probability obtained during the experiments are provided.

The security of the second cryptosystem has not been analyzed yet and we fill this gap for known-plaintext attack. The dependency between the number of «plaintext, ciphertext» pairs required to recover the key and parameters of the cryptosystem is analyzed. Also some recommendations for increasing the security level are provided.

The final conclusion of our analysis is that both cryptosystems are vulnerable to known-plaintext attack. And it may be dangerous to encrypt private data using them.

Finally it should be noted that the key element of the proposed attacks is the algorithm of computing the greatest common divisor. So their computational complexity depends polynomially on the size of input data.

Keywords: Homomorphic Encryption, Cloud Computing, Cryptanalysis, Known-Plaintext Attack, Residue Number System.

Babenko Ludmila Kliment'evna — Ph.D., Dr. Sci., Professor, leading researcher of South-Russian regional scientific-educational centre, Professor of Information Technologies Security Department, Academy for Engineering and Technologies of Southern Federal University. Research interests: Cryptography, Security Analysis of Cryptographic Algorithms, Software and Hardware Information Protection, Security Analysis of Cryptographic Protocols, Malicious Software, Behavioral Analysis, Parallel Algorithm, Distributed Multiprocessor Computing, Neuroprocessor Computing. The number of publications — >200. lkbabenko@sfnu.ru, <https://sfnu.ru/person/lkbabenko/>; 2, Chekhova str., Taganrog, 347922, Russia; office phone: +7(8634)312-018, fax: +7(8634)312-018.

Trepacheva Alina Viktorovna — Junior Researcher of Information Technologies Security Department, Academy for Engineering and Technologies of Southern Federal University. Research interests: Cryptanalysis of Homomorphic Encryption, Mathematical Statistics, Probability Theory, Algebraic Geometry. The number of publications — 18. alina1989malina@yandex.ru; 2, Chekhova str., Taganrog, 347922, Russia; office phone: +7(812)328-3337.

Acknowledgements. This research is supported by Russian Ministry of Education and Science (grant no. 2.6264.2017/8.9).

References

1. Rivest R. L., Adleman L., Dertouzos M. L. On data banks and privacy homomorphisms. *Foundations of secure computation*. 1978. vol. 32. no. 4. pp. 169-178.
2. Brickell E. F., Yacobi Y. On privacy homomorphisms. *Proceedings of Advances in Cryptology—EUROCRYPT’87*. 1988. pp. 117–125.
3. Goldwasser G., Micali S. Probabilistic encryption & how to play mental poker keeping secret all partial information. *Proceedings of the fourteenth annual ACM symposium on Theory of computing*. 1982. pp. 365-377.
4. Paillier P. Public-key cryptosystems based on composite degree residuosity classes. *Proceedings of Advances in cryptology—EUROCRYPT’99*. 1999. pp. 223-238.
5. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978. vol. 21. no. 2. pp. 120-126.
6. Gentry C. A fully homomorphic encryption scheme. PhD thesis. Stanford University. 2009. 209 p.
7. Cheon J. H., Coron J. S., Kim J., Lee M. S., Lepoint T., Tibouchi M., Yun A. Batch fully homomorphic encryption over the integers. *Proceedings of In Annual International Conference on the Theory and Applications of Cryptographic Techniques*. 2013. pp. 315-335.
8. Brakerski Z., Gentry C., Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ACM)*. 2012. pp. 309-325.
9. Brakerski Z. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. *Proceedings of Advances in cryptology—CRYPTO’2012*. 2012. pp. 868-886.
10. Chillotti L., Gama N., Georgieva M., Izabachene M. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. *Proceedings of 22nd International Conference on the Theory and Application of Cryptology and Information Security*. 2016. pp. 3-33.
11. Cheon J. H., Han K., Kim D. Faster Bootstrapping of FHE over the Integers. *IACR Cryptology ePrint Archive*. 2017. no. 79.
12. Micciancio D., Sorrell J. Ring packing and amortized FHEW bootstrapping. *IACR Cryptology ePrint Archive*, 2018. no. 532.
13. Brakerski Z. Quantum FHE (Almost) As Secure As Classical. *Proceedings of Annual International Cryptology Conference*. 2018. pp. 67-95.
14. Babenko L. K., Burtyka F. B., Makarevich O. B. Trepacheva A.V. Polnost’ju gomomorfnoe shifrovaniye (obzor) [Fully Homomorphic Encryption (A Survey)]. *Voprosy zashhity informacii [The information security issues]*. 2015. no. 3. pp. 3–25. (in Russ.).
15. Kipnis A., Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encryption, randomization and verification. *IACR Cryptology ePrint Archive*. 2012. no. 637.
16. Xiao L., Bastani O, Yen I.-L. An efficient homomorphic encryption protocol for multi-user systems. *IACR Cryptology ePrint Archive*. 2012. no. 193.
17. Sharma I. Fully homomorphic encryption scheme with symmetric keys. Master of Technology thesis in Department of Computer Science & Engineering (with specialization in Computer Engineering). 2013. 64 p.
18. Yagisawa M. Fully Homomorphic Encryption without bootstrapping. *IACR Cryptology ePrint Archive*. 2015. no. 474.
19. Yagisawa M. Improved Fully Homomorphic Encryption with Composite Number Modulus. *IACR Cryptology ePrint Archive*. 2016. no. 50.
20. Rostovtsev A. G., Bogdanov A. G., Mikhaylov M. Yu. Secure evaluation of polynomial using privacy ring homomorphisms. *IACR Cryptology ePrint Archive*. 2011. no. 24.

21. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Practical fully homomorphic encryption over polynomial quotient rings. Proceedings of 2013 World Congress on Internet Security (WorldCIS). 2013. pp. 70-75.
22. *Zhirov A. O., Zhirova O. V., Krendelev S. F.* Bezopasnye oblachnye vychisleniya s pomoshhyu homomorfnoj kriptografii [Secure Computing in the Cloud Storage Using Homomorphic Encryption]. Bezopasnost' informacionnyh tehnologij [Information Technologies Security]. 2013. no. 1. pp. 6-12. (In Russian)
23. *Dasgupta S., Pal S. K.* Design of a polynomial ring based symmetric homomorphic encryption scheme. Perspectives in Science. 2016. vol. 8. pp. 692-695.
24. *Domingo-Ferrer J.* A provably secure additive and multiplicative privacy homomorphism. Proceedings of International Conference on Information Security. 2002. pp. 471-483.
25. *Domingo-Ferrer J.* A new privacy homomorphism and applications. Information Processing Letters. 1996. vol. 60. no. 5. pp. 277-282.
26. *Gomathisankaran M., Tyagi A., Namuduri K.* HORNS: A homomorphic encryption scheme for Cloud Computing using Residue Number System. Proceedings of 2011 45th Annual Conference Information Sciences and Systems (CISS). 2011. pp. 1-5.
27. *Vishnevskij A. K., Knjazev V. V.* Kompleksnoe primenenie gomomorfnyh kriptograficheskikh preobrazovanij dlja reshenija sistem linejnyh algebraicheskikh uravnenij [Complex application of homomorphic cryptographic transformations for solving systems of linear algebraic equations]. Naukoemkie tehnologii [High technology]. 2015. vol. 16, no. 11, pp. 28-35. (In Russ.).
28. *Chervjakov N. I., Babenko M. G., Kucherov N. N.* Razrabotka sistemy gomomorfnoho shifrovaniya informacii na osnove polinomial'noj sistemy ostatochnyh klassov [Development of a homomorphic information encryption system based on a polynomial residual classes system]. Sibirskie Elektronnye Matematicheskie Izvestiya. Trudy VI mezhdunarodnoj molodezhnoj shkoly-konferencii «Teorija i chislennye metody reshenija obratnyh i nekorrektnykh zadach» [Siberian Electronic Mathematical Reports. Proceedings of the VI International Youth School-Conference «Theory and numerical methods for solving inverse and ill-posed problems»]. 2015. vol. 12. pp. 33-41. Available at <http://semr.math.nsc.ru/v12/c1-283.pdf> (accessed: 02.12.2018). (In Russ.).
29. *Vizár D., Vaudenay S.* Cryptanalysis of chosen symmetric homomorphic schemes. Studia Scientiarum Mathematicarum Hungarica. 2015. vol. 52. no. 2. pp. 288-306.
30. *Tsaban B., Lifshitz N.* Cryptanalysis of the MORE symmetric key fully homomorphic encryption scheme. Journal of Mathematical Cryptology. 2015. vol. 9, no. 2. pp. 75-78.
31. *Trepacheva A.V.* Cryptanalysis of symmetric fully homomorphic linear cryptosystems based on numbers factorization problem. Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki [The SFEDU proceedings. Engineering Science]. 2015. vol. 166, no. 5. pp. 89-100. (In Russ.).
32. *El-Yahyaoui A., Elkettani M. D.* Cryptanalysis of fully homomorphic encryption schemes. International Journal of Computer Science and Information Security. 2016. vol. 14. no. 5. pp. 677-685.
33. *Cheon J. H., Kim W. H., Nam H. S.* Known-plaintext cryptanalysis of the Domingo-Ferrer algebraic privacy homomorphism scheme. Information Processing Letters. 2006. vol. 97, no. 3. pp. 118-123.
34. *Wagner D.* Cryptanalysis of an algebraic privacy homomorphism. Proceedings of International Conference on Information Security. 2003. pp. 234-239.
35. *Trepacheva A.V.* Improved known plaintexts attack on Domingo-Ferrer homomorphic cryptosystem. Trudy Instituta sistemnogo programmirovaniya RAN [Proceedings of the Institute for System Programming]. 2014. vol. 26. Issue 5. pp. 83-98.

36. *Trepacheva A.V.* O kriptozanalize odnoj polnost'ju gomomorfnoj kriptosistemy na osnove zadachi faktorizacii [About Cryptanalysis of One Fully Homomorphic Cryptosystem Based on Factorization Problem]. *Bezopasnost' informacionnyh tehnologij* [Information Technologies Security]. 2015. vol. 22. no. 2. pp. 19-25. (In Russ.).
37. *Trepacheva A.V.* Known plaintext attack on a fully homomorphic cryptosystem based on factorization. *Proceedings of 4th Workshop on Current Trends in Cryptology CTCrypt'2015*. 2015. pp. 205-215.
38. *Babenko L., Trepacheva A.* Known plaintexts attack on polynomial based homomorphic encryption. *Proceedings of the 7th International Conference on Security of Information and Networks (ACM)*. 2014. pp.157-166.
39. *Trepacheva A.V.* Kriptoanaliz polnost'ju gomomorfnyh kriptosistem, osnovannyh na algebre oktonionov [Cryptanalysis of fully homomorphic cryptosystem, based on octonion algebra]. *Obozrenie prikladnoj i promyshlennoj matematiki* [A survey of applied and industrial mathematics]. 2016. 2 p. (In Russ.).
40. *Wang Y.* Notes on Two Fully Homomorphic Encryption Schemes Without Bootstrapping. *IACR Cryptology ePrint Archive*. 2015. no. 519.
41. *Wang Y.* Octonion Algebra and Noise-Free Fully Homomorphic Encryption (FHE) Schemes. *IACR Cryptology ePrint Archive*. 2016. no. 68.
42. *Babenko L.K., Trepacheva A.V.* Cryptanalysis of factoring-based fully homomorphic encryption. *Proceedings of the 8th International Conference on Security of Information and Networks (ACM)*. 2015. pp. 80-83.
43. *Trepacheva A.V.* Ataka po shifrttekstam na odnu linejniju polnost'ju gomomorfnuju kriptosistemu [Ciphertexts-only attack on one linear fully homomorphic cryptosystem]. *Prikladnaja diskretnaja matematika. Prilozhenie* [Applied discrete mathematics. Annex.]. 2015. no. 8. pp. 75-78. (In Russ.).
44. *Trepacheva A.V.* On the relations between the attacks on symmetric homomorphic encryption over the residue ring. *Bezopasnost' informacionnyh tehnologij* [Information Technologies Security]. 2017. no. 2. pp. 82-91. (In Russ.).
45. *Babenko M., Chervyakov N., Tchernykh A., Kucherov N., Deryabin M., Radchenko G., Navaux Ph., Syvatkin V.* Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack. *Proceedings of 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. 2018. pp. 270-274.
46. *Buhsttab A. A.* *Teoriya chisel* [The Number Theory]. M.: Prosveshcheniye. 1966. 384 p. (In Russ.).
47. *Nymann J. E.* On the probability that k positive integers are relatively prime. *Journal of Number Theory*. 1972. vol. 4, no. 5, pp. 469-473.
48. *Benjamin A. T., Bennett C. D.* The probability of relatively prime polynomials. *Mathematics Magazine*. 2007. vol. 80. no. 3. pp. 196–202.
49. *Goldreich O.* *Foundations of Cryptography*. Cambridge University press. 2009. 800 p.
50. *Weenink T.* Deterministic primality testing. Bachelor thesis. Technische Universiteit Eindhoven. 2015. 24 p.
51. *Knuth D. E.* *The Art of Computer Programming – Volume 3 (Sorting and Searching)*. Addison-Wesley. 1998. 800 p.
52. *Aho A., Ulman J., Hopcroft J.* *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company. 1974. 536 p.
53. Implementation of Vishnevsky-Knyazev's cryptosystem and attack on it. Available at: <https://github.com/alina1989malina/CryptanalysisVishnevskyKnyazev> (accessed: 02.12.2018).

54. Implementation of Babenko-Kucherov-Chervjakov's cryptosystem and attack on it. Available at: <https://github.com/alina1989malina/CryptanalysisBabenkoKucherovChervjakov> (accessed: 02.12.2018).

Signed to print 12.02.2019

Printed in Publishing center GUAP, 67, B. Morskaya, St. Petersburg, 190000, Russia

The journal is registered in Russian Federal Agency for Communications
and Mass-Media Supervision, certificate ПИ № ФС77-41695 dated August 19, 2010 г.
Subscription Index П5513, Russian Post Catalog

Подписано к печати 12.02.2019. Формат 60×90 1/16. Усл. печ. л. 16,63 Заказ № 69.

Тираж 150 экз., цена свободная.

Отпечатано в Редакционно-издательском центре ГУАП, 190000, Санкт-Петербург, Б. Морская, д. 67

Журнал зарегистрирован Федеральной службой по надзору в сфере связи
и массовых коммуникаций,
свидетельство ПИ № ФС77-41695 от 19 августа 2010 г.

Подписной индекс П5513 по каталогу «Почта России»

РУКОВОДСТВО ДЛЯ АВТОРОВ

Взаимодействие автора с редакцией осуществляется через личный кабинет на сайте журнала «Труды СПИИРАН» <http://www.proceedings.spiiras.nw.ru>. При регистрации авторам рекомендуется заполнить все предложенные поля данных.

Подготовка статьи ведется с помощью текстовых редакторов MS Word 2007 и выше. Объем основного текста – от 20 до 30 страниц включительно. Формат страницы документа – А5 (148 мм ширина, 210 мм высота); ориентация – портретная; все поля – 20 мм. Верхний и нижний колонтитулы страницы – пустые. Основной шрифт документа – Times New Roman, основной кегль (размер) шрифта – 10 pt. Переносы разрешены. Абзацный отступ устанавливается размером в 10 мм. Межстрочный интервал – одинарный. Номера страниц не проставляются.

В основную часть допускается помещать рисунки, таблицы, листинги и формулы. Правила их оформления подробно рассмотрены на нашем сайте в разделе «Руководство для авторов».

AUTHOR GUIDELINES

Interaction between each potential author and the Editorial board is realized through the personal account on the website of the journal "Proceedings of SPIIRAS" <http://www.proceedings.spiiras.nw.ru>. At the registration the authors are requested to fill out all data fields in the proposed form.

The submissions should be prepared using MS Word 2007 text editor or higher versions, at that, only manuscripts in *.docx format will be considered. The text of the paper in the main part of it should be from 20 – 30 pages of A5 size that is 210 X 148 mm; orientation – portrait; all margins – 20 mm. The font of the main paper text is Times New Roman of 10 pt font size. The pages' headers and footers should be empty; indentation – 10 mm; line spacing – single; pages are not numbered; hyphenations are allowed.

Certain figures, tables, listings and formulas are allowed in the main section, and their typography is considered by the paper template in more detail in journal web.

