

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Сигов А.С. Главный редактор журнала, академик РАН, профессор, д.ф.-м.н., президент РТУ МИРЭА

Кудж С.А. Профессор, д.т.н., ректор РТУ МИРЭА

Банис Ю.Й. Профессор, хабилированный доктор наук, проректор Вильнюсского университета, Литва

Боков А.А. Старший научный сотрудник, химический факультет и 4D LABS, Университет Саймона Фрейзера, Ванкувер, Британская Колумбия, Канада

Буслаева Т.М. Профессор, д.х.н., РТУ МИРЭА

Буш А.А. Профессор, д.т.н., директор Института материалов твердотельной электроники РТУ МИРЭА

Вахрушев С.Б. Профессор, д.ф.-м.н., зав. лабораторией нейтронных исследований Физико-технического института им. А.Ф. Иоффе РАН, профессор кафедры Физической электроники СПбГПУ

Голованова Н.Б. Профессор, д.э.н., заместитель первого проректора РТУ МИРЭА

Гуляев Ю.В. Академик РАН, член Президиума РАН, профессор, д.ф.-м.н., научный руководитель Института радиотехники и электроники им. В.А. Котельникова РАН

Жуков Д.О. Профессор, д.т.н., зав. кафедрой интеллектуальных технологий и систем РТУ МИРЭА

Кимель А.В. Доцент, к.ф. - м.н., Университет Радбауд, г. Наймеген, Нидерланды

Козлов Г.В. Профессор, д.ф.-м.н., заместитель руководителя аппарата генерального директора АО «Концерн ВКО „Алмаз-Антей“»

Кондратенко В.С. Профессор, д.т.н., зав. кафедрой оптических и биотехнических систем и технологий РТУ МИРЭА

Крамаров С.О. Профессор, д.ф.-м.н., главный научный сотрудник Сургутского государственного университета

Мишина Е.Д. Профессор, д.ф.-м.н., зав. специализированной учебно-научной лабораторией фемтосекундной оптики для нанотехнологий РТУ МИРЭА

Пасечник С.В. Профессор, д.ф.-м.н., профессор кафедры оптических и биотехнических систем и технологий РТУ МИРЭА

Перно Ф. Профессор, проректор по научной работе, Центральная Школа г. Лилль, Франция

Романов М.П. Профессор, д.т.н., директор Института кибернетики РТУ МИРЭА

Савиных В.П. Член-корреспондент РАН, д.т.н., профессор, президент Московского государственного университета геодезии и картографии (МИИГАиК)

Скотт Дж. Профессор, член Лондонского Королевского общества, Университет Кембриджа, Великобритания

Соколов В.В. Профессор, д.ф.-м.н., советник по научной работе РТУ МИРЭА

Тимошенко А.В. Профессор, д.т.н., проректор по учебной работе РТУ МИРЭА

Фетисов Ю.К. Профессор, д.ф.-м.н., профессор кафедры нанoeлектроники РТУ МИРЭА

Харин Ю.С. Член-корреспондент НАН Беларуси, профессор, д.ф.-м.н., директор Научно-исследовательского института прикладных проблем математики и информатики Белорусского государственного университета, Беларусь

Цветков В.Я. Профессор, д.т.н., советник ректората РТУ МИРЭА

РЕДАКЦИЯ:

Буслаева Т.М. Профессор, д.х.н.; e-mail: buslaeva@mirea.ru

Есипова О.В. Ответственный секретарь, к.х.н., доцент; e-mail: esipova@mirea.ru

Семерня Л.Г. Технический редактор; e-mail: semernya@mirea.ru

Середина Г.Д. Зав. редакцией, к.т.н.; e-mail: seredina@mirea.ru

Адрес редакции:

Россия, 119571, Москва, пр. Вернадского, д. 86, оф. Л-119

Тел.: +7 (495) 246-05-55 (#2-88); e-mail: seredina@mirea.ru; <http://rtj.mirea.ru>

EDITORIAL BOARD

Alexander S. Sigov – Editor-in-Chief of the Journal, Academician of the Russian Academy of Sciences, D.Sc. (Phys.-Math.), Professor, President of RTU MIREA

Stanislav A. Kudzh – Professor, D.Sc. (Eng.), Rector of RTU MIREA

Yuras Banis – Professor, Habilitated Doctor of Sciences, Vice-Rector of Vilnius University, Lithuania

Tatyana M. Buslaeva – Professor, D.Sc. (Chem.), RTU MIREA

Alexander A. Bush – Professor, D.Sc. (Eng.), Director of the Institute of Materials of Solid State Electronics, RTU MIREA

Sergey B. Vakhrushev – Professor, D.Sc. (Phys.-Math.), Head of the Laboratory of Neutron Research, A.F. Ioffe Physico-Technical Institute RAS, Professor of the Department of Physical Electronics of SPbSPU

Nataliya B. Golovanova – Professor, D.Sc. (Economics), Deputy First Vice-Rector of RTU MIREA

Yury V. Gulyaev – Academician of the Russian Academy of Sciences, Member of the Presidium of the Russian Academy of Sciences, Professor, D.Sc. (Phys.-Math.), Supervisor of V.A. Kotelnikov Institute of Radio Engineering and Electronics RAS

Dmitry O. Zhukov – Professor, D.Sc. (Eng.), Head of the Department of Intelligent Technologies and Systems, RTU MIREA

Alexey V. Kimel – Associate Professor, Ph.D. (Phys.-Math.), Radboud University, Nijmegen, Netherlands

Gennady V. Kozlov – Professor, D.Sc. (Phys.-Math.), Deputy Head of the Office of the General Director of JSC Concern “VKO Almaz-Antey”

Vladimir S. Kondratenko – Professor, D.Sc. (Eng.), Head of the Department of Optical and Biotechnical Systems and Technologies, RTU MIREA

Sergey O. Kramarov – Professor, D.Sc. (Phys.-Math.), Senior Researcher, Surgut State University

Elena D. Mishina – Professor, D.Sc. (Phys.-Math.), Head of the Specialized Educational and Research Laboratory of Femtosecond Optics for Nanotechnologies, RTU MIREA

Sergey V. Pasechnik – Professor, D.Sc. (Phys.-Math.), Professor of the Department of Optical and Biotechnical Systems and Technologies, RTU MIREA

Philippe Pernod – Professor, Dean of Research, Ecole Centrale de Lille, France

Mikhail P. Romanov – Professor, D.Sc. (Eng.), Director of the Institute of Cybernetics, RTU MIREA

Viktor P. Savinykh – Member-Correspondent of the Russian Academy of Sciences, Professor, D.Sc. (Eng.), President of Moscow State University of Geodesy and Cartography (MIIGAiK), Twice Hero of the Soviet Union

James F. Scott – Professor, Fellow of the Royal Society of London, Cambridge University, UK

Viktor V. Sokolov – Professor, D.Sc. (Phys.-Math.), Adviser on Scientific Work of RTU MIREA

Andrey V. Timoshenko – Professor, D.Sc. (Eng.), Vice Rector for Academic Affairs of RTU MIREA

Yury K. Fetisov – Professor, D.Sc. (Phys.-Math.), Professor of the Department of Nanoelectronics, RTU MIREA

Yury S. Kharin – Corresponding Member of the National Academy of Sciences of Belarus, Professor, D.Sc. (Phys.-Math.), Director of the Research Institute of Applied Problems of Mathematics and Informatics of the Belarusian State University, Belarus

Viktor Y. Tsvetkov – Professor, D.Sc. (Eng.), Councilor of the Administration of RTU MIREA

EDITORIAL:

Tatyana M. Buslaeva – Professor, D.Sc. (Chem.). E-mail: buslaeva@mirea.ru

Olga V. Esipova – Executive Editor, Ph.D. (Chem.), Associate Professor. E-mail: esipova@mirea.ru

Larisa G. Semernya – Technical Editor. E-mail: semernya@mirea.ru

Galina D. Seredina – Managing Editor, Ph.D. (Engineering). E-mail: seredina@mirea.ru

Address:

86, Vernadskogo Pr., Moscow 119571, Russia (office L-119)

Phone: +7(495)246-05-55 (#288); e-mail: seredina@mirea.ru; <http://rtj.mirea.ru>

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ. ИНФОРМАТИКА. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Сигов А.С., Андрианова Е.Г., Жуков Д.О., Зыков С.В.,
Тарасов И.Е.*** **5**
Квантовая информатика: обзор основных достижений
- Григорьев В.К., Илющечкин А.С., Овчинников М.А.*** **38**
Оценка качества пользовательского интерфейса на основе
ментального времени выполнения пользовательских задач
предметной области
- Nazarenko M.A., Gorobets A.I., Miskov D.V., Muravyev V.V.,
Novikov A.S.*** **48**
Antivirus software and industrial cyber security system certification
in Russia

СОВРЕМЕННЫЕ РАДИОТЕХНИЧЕСКИЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

- Костин М.С., Воруничев Д.С., Корж Д.А.*** **57**
Контрреинжиниринг радиоэлектронных средств
- Харалгин С.В., Куликов Г.В., Котельников А.Б., Снастин М.В.,
Добычина Е.М.*** **80**
Прототипирование СВЧ-устройств с заданными электродинамическими
характеристиками по технологии аддитивной 3D-печати

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ

- Чехова Р.В., Пышный В.М., Пьянкова Л.А., Елохин В.А.*** **102**
Разделение дифракционных спектров методом главных компонент
на примере лекарственного средства Ариффон

CONTENTS

INFORMATION SYSTEMS. INFORMATICS. PROBLEMS OF INFORMATION SECURITY

- Sigov A.S., Andrianova E.G., Zhukov D.O., Zykov S.V., Tarasov I.E.*** **5**
Quantum informatics: overview of the main achievements
- Grigoriev V.K., Ilyushechkin A.S., Ovchinnikov M.A.*** **38**
Quality assessment of a user interface based on the mental time of performing the user tasks of the subject area
- Nazarenko M.A., Gorobets A.I., Miskov D.V., Muravyev V.V., Novikov A.S.*** **48**
Antivirus software and industrial cyber security system certification in Russia

MODERN RADIO ENGINEERING AND TELECOMMUNICATION SYSTEMS

- Kostin M.S., Vorunichev D.S., Korzh D.A.*** **57**
Counterreengineering of electronic devices
- Kharalgin S.V., Kulikov G.V., Kotelnikov A.B., Snastin M.V., Dobychina E.M.*** **80**
Prototyping of microwave devices with specified electrodynamic characteristics using additive 3D printing technology

MATHEMATIC MODELING

- Chekhova R.V., Pyshniy V.M., Pyankova L.A., Elokhin V.A.*** **102**
Separation of diffraction spectra by principal component method by the example of Arifon drug

КВАНТОВАЯ ИНФОРМАТИКА: ОБЗОР ОСНОВНЫХ ДОСТИЖЕНИЙ

**А.С. Сигов¹,
Е.Г. Андрианова¹,
Д.О. Жуков¹,
С.В. Зыков²,
И.Е. Тарасов¹**

¹МИРЭА – Российский технологический университет, Москва 119454, Россия

²НИУ «Высшая школа экономики», Москва 101000, Россия

@Автор для переписки, e-mail: andrianova@mirea.ru

Обоснована актуальность проведения и выделены перспективные направления научных исследований в области квантовой информатики. По иностранным и российским публикациям и материалам сделан обзор основных научных результатов, характеризующих современное состояние исследований в квантовой информатике. Отмечено, что наиболее интенсивно знания и средства инвестируются в разработку архитектуры квантового компьютера и его элементов. Несмотря на то, что сегодня нет информации о создании физической реализации квантового компьютера, сравнимого по функциональным возможностям с классическим цифровым вычислителем, разработка квантовых алгоритмов является одним из актуальных направлений исследований. Преимущество квантовых алгоритмов заключается в снижении времени решения задачи за счет распараллеливания операций путем генерирования запутанных квантовых состояний и их последующего использования. Указанное преимущество (квантовое ускорение) является наиболее выигрышным при решении задачи моделирования динамики сложных систем и переборных математических задач (общий случай перебора – схема Гровера и ее варианты; задачи поиска скрытых периодов – схема Шора использования быстрого квантового преобразования Фурье и ее аналоги). Отмечена востребованность разработок в области кибербезопасности (поиск уязвимостей в умных пространствах, безопасное хранение и использование больших данных, квантовая криптография). Представлено более десятка статей, посвященных квантовым алгоритмам поиска ключей, распределению ключей на оптическом волокне различной длины, анализу квантовых ресурсов, необходимых для проведения кибератаки. В области искусственного квантового интеллекта внимание уделяется, в первую очередь, «поискам» модели квантовой нейронной сети, оптимальной с точки зрения использования всех преимуществ, представляемых квантовыми вычислениями и нейронными сетями, а также алгоритмам машинного обучения. Приведены примеры использования квантовых вычислений в когнитивных и социальных науках для исследования механизма принятия решений при неполных данных. Сделан вывод о перспективности применения квантовой информатики при моделировании сложных естественных и искусственных явлений и процессов.

Ключевые слова: квантовая информатика, квантовый компьютер, квантовые алгоритмы, моделирование сложных явлений и процессов, нейронные сети, машинное обучение, криптография, когнитивные технологии.

QUANTUM INFORMATICS: OVERVIEW OF THE MAIN ACHIEVEMENTS

A.S. Sigov¹,
E.G. Andrianova¹,
D.O. Zhukov¹,
S.V. Zykov²,
I.E. Tarasov¹

¹MIREA – Russian University of Technology, Moscow 119454, Russia

²National Research University "Higher School of Economics", Moscow 101000, Russia

@Corresponding author e-mail: andrianova@mirea.ru

The urgency of conducting research in the field of quantum informatics is grounded. Promising areas of research are highlighted. For foreign and Russian publications and materials, a review of the main scientific results that characterize the current state of research in quantum computer science is made. It is noted that knowledge and funds are invested most intensively in the development of the architecture of a quantum computer and its elements. Despite the fact that today there is no information on the creation of a physical implementation of a quantum computer comparable in functionality to a classical digital computer, the development of quantum algorithms is one of the popular areas of research. An advantage of quantum algorithms is the fact that they reduce the time required to solve the problem due to the parallelization of operations by generating entangled quantum states and their subsequent use. This advantage (quantum acceleration) is most important when solving the problem of modeling the dynamics of complex systems and enumerated mathematical problems. (The general case of enumeration is the Grover scheme and its variants; the tasks of searching for hidden periods: Shor's scheme of using the fast quantum Fourier transform and its analogues.) The demand for cybersecurity developments (search for vulnerabilities in smart spaces, secure storage and use of big data, quantum cryptography) is noted. More than a dozen articles are devoted to quantum algorithms of key search, key distribution on optical fibers of various lengths, and the analysis of quantum resources necessary for conducting a cyber attack. In the field of artificial quantum intelligence, attention is paid, first of all, to the "search" for a model of a quantum neural network that is optimal from the point of view of using all the advantages presented by quantum computing and neural networks, as well as machine learning algorithms. Examples of the use of quantum computing in cognitive and social sciences for studying the decision-making mechanism with incomplete data are given. It is concluded that quantum informatics is promising for the simulation of complex natural and artificial phenomena and processes.

Keywords: quantum computer science, quantum computer, quantum algorithms, modeling of complex phenomena and processes, neural networks, machine learning, cryptography, cognitive technologies.

Введение

В докладе «Цифровая Россия: новая реальность», подготовленным экспертной группой Digital McKinsey, названы наиболее востребованные бизнес-сообществом направления деятельности в области IT-технологий в 2017–2018 гг.: это – облачные техно-

логии, Интернет вещей, технологии больших данных, кибербезопасность [1]. По мнению экспертов, «в соответствии с теорией циклов Кондратьева современный IT-рынок находится в самом начале очередного технологического цикла, который эксперты называют NBIC-конвергенция (конвергенция нано-, био-, информационных и когнитивных технологий). Она должна стать таким же прорывом, как в свое время прядильные, а потом паровые машины. И основной будущий тренд в сфере услуг, не только в IT, но и в конвергенции самых различных сервисов и услуг» [1].

В Программе «Цифровая экономика Российской Федерации», утвержденной летом 2017 года [2], определены направления государственной политики по созданию необходимых правовых, технических, организационных и финансовых условий для развития цифровой экономики в России, и перспективе ее интеграции в пространство цифровой экономики государств – членов Евразийского экономического союза. Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, обслуживания, хранения, продажи, доставки товаров и услуг [3].

Для формирования исследовательских компетенций и технологических заделов, как одного из базовых направлений развития цифровой экономики в Российской Федерации [2], необходимо создание исследовательской инфраструктуры цифровых платформ. Исследовательские цифровые платформы должны стать инструментальным средством поддержки поисковых прикладных исследований в области цифровой экономики, обеспечивая технологическую независимость страны по таким сквозным цифровым технологиям, как большие данные, Интернет вещей и квантовые вычисления.

Эффективная обработка больших объемов данных требует высокопроизводительных вычислений в области искусственного интеллекта, наукоемких производственных направлений, моделирования химических и физических явлений и процессов, то есть там, где перестает хватать возможностей современных суперкомпьютеров. Существует мнение, что развитие транзисторных вычислителей почти достигло своего предела и что закон Мура, суть которого состоит в удваивании компьютерной мощности каждые полтора-два года, скоро перестанет действовать, так как размер транзисторов перестанет уменьшаться каждые 18 месяцев [4–7].

Квантовая обработка информации имеет существенный потенциал для повышения производительности вычислений. Она основана не на использовании традиционной булевой алгебры, а на логических представлениях квантовой механики, что обещает вычислительную мощность, выходящую за пределы возможностей любого классического компьютера, гарантируя при этом безопасную связь.

В связи с вышеизложенным обзор основных направлений развития и достижений квантовой информатики является актуальной задачей.

Квантовая информатика включает в себя вопросы квантовых вычислений и квантовых алгоритмов, физику квантовых компьютеров, квантовую криптографию и квантовую теорию информации, в частности, касается проблемы измерений и описания декогерентности. Базовое физическое явление, которое изучается в квантовой информатике – это запутанные квантовые состояния и порождаемые ими нелокальные свойства кван-

товой физики многих тел. К такому же мнению пришли и зарубежные исследователи. Например, в работе [8] отмечено, что вызовы со стороны секторов торговли, финансов, безопасности и логистики способствуют постоянному росту вычислительной техники. Квантовые вычисления представляют собой перспективную стратегию, которая предлагает новые возможности в безопасном вычислении, надежном хранении данных и эффективных приложениях. В бизнес-сообществе также растет осознание влияния квантовых вычислений на широкий спектр проблем и приложений потребителей.

Современными сферами приложения квантовой информатики являются квантовые вычисления (алгоритмы), квантовый компьютер, квантовая криптография, компьютерное моделирование систем многих частиц, применение в когнитивных технологиях, системах искусственного интеллекта. Рассмотрим важнейшие направления исследований в указанных областях.

Квантовый компьютер

Квантовый компьютер – средство вычислительной техники, в котором в основу работы центрального процессора заложена логика квантовой механики. Такой компьютер принципиально отличается от традиционного компьютера, имеющего архитектуру фон Неймана. Квантовый компьютер применяет для вычисления не классические алгоритмы, а процессы квантовой природы – квантовые алгоритмы, использующие явления квантовой механики, такие, как квантовый параллелизм и квантовая запутанность [9].

Базой квантовых вычислений является кубит (*Qubit*). Чтобы объяснить понятие «кубит», необходимо воспользоваться представлениями квантовой механики. Квантовые частицы имеют определенные характеристики, с помощью которых можно описывать их поведение и которые можно определять на практике (и, соответственно, реализовывать в квантовых компьютерах). В частности, фотоны обладают поляризацией, которую определяют через поведение вектора их электрического поля; некоторые микрочастицы обладают собственным магнитным моментом (спином), проекции которого на направление внешнего магнитного слоя находят экспериментально. В ходе традиционных вычислений используется понятие бита. Оно основано на том, что технически может быть реализовано только два состояния: 0 и 1 – например, ток протекает или нет проводимости (есть заряд или нет заряда) (рис. 1).

У кубита возможно существование не только двух состояний (например, спин квантовой частицы расположен по направлению внешнего поля – 0 или против – 1), но и их суперпозиции, что обусловлено квантовой природой явлений микромира. Суперпозицию состояний кубита представляют графически в виде координатной сетки на сфере, где каждый узел соответствует некоторому состоянию (центральная часть рис. 1).

Если каждое из состояний кубита обозначить $\alpha|0\rangle$ (функция, описывающая состояние, когда спин квантовой частицы направлен против внешнего поля) и $\beta|1\rangle$ (спин квантовой частицы направлен по направлению внешнего поля), то любое из множества возможных состояний будет определяться соотношением (суперпозицией):

$$\alpha|0\rangle + \beta|1\rangle$$

где α и β – комплексные функции, удовлетворяющие соотношению $|\alpha|^2 + |\beta|^2 = 1$ ($|\alpha|^2$ и $|\beta|^2$ являются амплитудами вероятностей переходов в состояния $\alpha|0\rangle$ и $\beta|1\rangle$). На рис. 1 справа

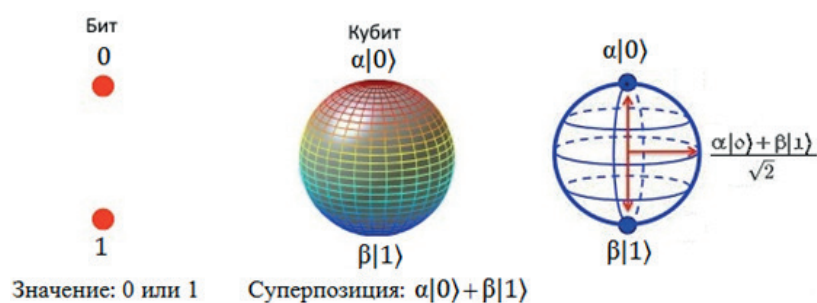


Рис. 1. Представление кубита [10].

показана возможность реализации состояния, когда спин квантовой частицы имеет направление, перпендикулярное внешнему магнитному полю.

Кубиты могут быть связаны (или запутаны) между собой. Это означает, что на них может быть наложена связь, вследствие чего при всяком изменении состояния одного из нескольких кубитов остальные меняются согласованно с ним, а совокупность запутанных между собой кубитов интерпретируется как заполненный квантовый регистр. Подобно отдельному кубиту, квантовый регистр гораздо сложнее классического регистра битов. Он способен не только находиться во всевозможных комбинациях составляющих его битов, но и реализовывать тонкие зависимости между ними, что существенно повышает вычислительные возможности систем, основанных на кубитах.

В состоянии связанности и суперпозиции кубиты представляют собой квантовый регистр. В ходе вычислений в квантовом регистре происходит выстраивание амплитуд кубитов ($|\alpha|^2$ и $|\beta|^2$) таким образом, что положительные значения амплитуды одних кубитов нейтрализуют отрицательные амплитуды других кубитов, и происходит отмена неверных вычислений (положительные амплитуды кубитов, напротив, усиливают друг друга). Так формируются сценарии получения верного ответа.

В [10] работа обычного и квантового компьютеров иллюстрируется поиском выхода из лабиринта: обычный компьютер последовательно перебирает все возможные варианты, упираясь в тупики и возвращаясь, а квантовый компьютер может проверить все возможные ходы за один раз.

Основная инженерная сложность состоит в поддержке состояния суперпозиции и спутанности кубитов в течение времени вычисления – времени когерентности.

Работы по созданию квантового компьютера активно ведутся Microsoft, IBM и Google. В марте 2018 г. из голландского центра Microsoft, расположенного в Техническом университете в Делфте (Delft University of Technology), сообщили об исследованиях по созданию квантового компьютера на базе майорановских фермионов, физические свойства которых позволят создать вычислитель с гораздо более низкой частотой ошибок, чем в проектах IBM и Google [11]. В России также ведутся подобные разработки: 15 февраля 2018 г. Внешэкономбанк, Фонд перспективных исследований, МГУ имени М.В. Ломоносова, «ВЭБ-Инновации» и АНО «Цифровая экономика» подписали соглашение о реализации комплексного научно-технического проекта по созданию в России многокубитного (не менее пятидесяти кубитов) оптического квантового симулятора на основе фотонных чипов и нейтральных атомов [12].

Между тем в статье [13], написанной два года назад, представлен квантовый компьютер на пяти кубитах, который был запрограммирован для реализации произвольных

квантовых алгоритмов на основе последовательности универсальных квантовых логических вентилей и обеспечил среднюю точность вычислений 98%. Переконфигурирование последовательности вентилей дает возможность гибкой реализации алгоритмов без изменения аппаратного обеспечения. В качестве примеров были реализованы алгоритмы Deutsch-Jozsa и Bernstein-Vazirani со средними коэффициентами успеха, соответственно, 95 и 90%. Реализовано также когерентное квантовое преобразование Фурье на пяти кубитах для оценки фазы и нахождения периода преобразования со средней точностью, соответственно, 62 и 84%. Представленный квантовый компьютер можно масштабировать до большего числа кубитов в одном регистре и дополнительно расширить посредством соединения нескольких модулей через челночный или квантовый канал.

Методика и результаты экспериментального сравнения двух архитектур пятикубитовых квантовых компьютеров (рис. 2), основанных на разных технологических платформах, даны в [14]. Здесь использован публичный доступ, предоставленный IBM, через облачную службу IBM «Quantum Experience» (www.research.ibm.com/ibm-q). Это дало возможность авторам работы реализовать в своем эксперименте 5-ти-кубитный квантовый компьютер на основе сверхпроводящих кубитов, связанных микроволновыми резонаторами (рис. 2А). Авторы статьи [14] запустили два одинаковых набора алгоритмов на компьютере IBM и на собственном квантовом компьютере идентичного размера и сопоставимых возможностей, но с физической реализацией на базе массива ионных ловушек, т.е. линейной цепи захваченных ионов, связанных лазерно-опосредованными взаимодействиями (рис. 2В).

Искусственные сверхпроводящие схемы в квантовом компьютере IBM можно рассматривать как «искусственные атомы». Это трансмонитные кубиты или сверхпроводящие островки, соединенные джозефсоновскими контактами и шунтирующими конденсаторами, которые обеспечивают суперпозиции зарядовых состояний, не чувствительных к флуктуациям заряда. Используемое здесь устройство имеет диапазон частот кубита от 5

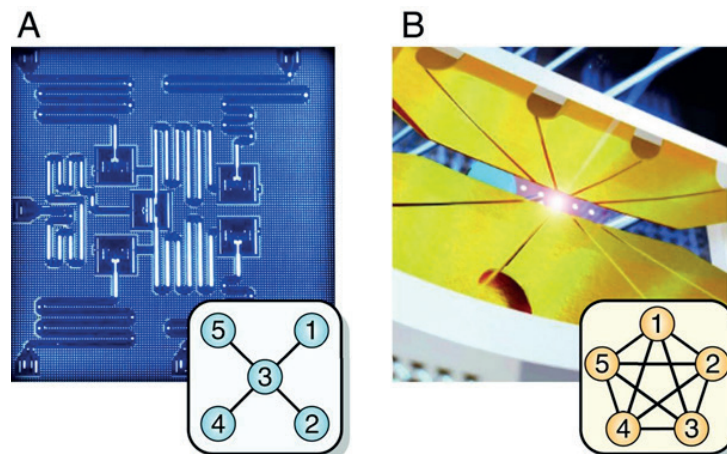


Рис. 2. Графическое представление архитектуры квантовых компьютеров, задействованных в эксперименте [14]: А – архитектура компьютера IBM на основе сверхпроводящих кубитов, связанных микроволновыми резонаторами (на вставке под изображением – график связности Qubit в форме звезды); В – архитектура компьютера авторов статьи, основанная на линейной цепи захваченных ионов, связанных лазерно-опосредованными взаимодействиями (на вставке под изображением – полносвязанный график связности Qubit).

до 5.4 ГГц (www.research.ibm.com/ibm-q). Кубиты связаны между собой и классической системой управления микроволновыми резонаторами. Состояния подготовки и считывания, а также одно- и двухкубитных ворот достигаются путем применения адаптированных микроволновых сигналов к этой сети и измерения отклика. Кубиты разрешаются в частотной области во время адресации и считывания. В аппаратуре Quantum Experience кубиты соединены в форме звезды, обеспечивающей четыре взаимодействия по второму кубиту (см. рис. 2А), которые представляют собой управляемые вентили NOT (CNOT), нацеленные на центральный кубит. Точность считывания с одного кубита обычно составляет 96%, а средняя точность считывания для произвольного состояния с 5 кубитами – 80%. Общедоступная система работает автономно, не требуя вмешательства человека, в течение многих недель (www.research.ibm.com/ibm-q).

Принцип работы второго компьютера (рис. 2В) является одним из подходов к построению крупномасштабного квантового компьютера. Ионы или заряженные атомные частицы могут быть ограничены и приостановлены в свободном пространстве с использованием электромагнитных полей. Кубиты хранятся в стабильных электронных состояниях каждого иона, а квантовая информация может передаваться через коллективное квантованное движение ионов в общей ловушке (взаимодействующей через кулоновскую силу). Лазеры применяются для индуцирования связи между кубитными состояниями (для операций с одним кубитом) или связью между внутренними состояниями кубитов и состояниями внешнего движения (для перепутывания между кубитами). Оба компьютера были запрограммированы независимо от базового оборудования, что позволило сравнить характеристики выполнения идентичных квантовых алгоритмов, работавших на различных физических основах (системах). Исследование показало, что квантовые алгоритмы, использующие больше возможностей подключения, выигрывают за счет более качественной связи системы кубитов. Хотя данное исследование проводилось на маленьких (по сравнению с классическими компьютерами) квантовых компьютерах, представлялось возможным оценить такие критические факторы масштабирования квантовых компьютеров, как связность кубитов и изменчивость сценария выполнения алгоритма. Кроме того, результаты показывают, что координирование конкретных квантовых приложений с самим компьютером будет иметь в дальнейшем решающее значение для успешного использования квантовых компьютеров.

К такому же выводу пришли в исследовании [15], где оценивались перспективы интеграции новых функциональных компонентов (блоков) квантовой обработки (QPU) квантовых процессоров в современные высокопроизводительные вычислительные системы (HPC – *high performance computing*) с учетом требований к функциональности и физическому дизайну. Намечены два подхода к интеграции, дифференцированные по инфраструктурным ограничениям в QPU и вариантам использования, традиционным для современных высокопроизводительных вычислительных систем. То есть возможен подход, когда QPU встраивается полностью, как один из компонентов системы, и параллельная работа, когда инфраструктурные ограничения трудно преодолимы. Получено, что производительность обоих подходов с большой вероятностью будет зависеть от квантового межсоединения, которое служит для запутывания множества кубитов QPU. Выявлены также несколько проблем в оценке производительности QPU для HPC и введены новые

показатели, фиксирующие взаимодействие между системной архитектурой и квантовым параллелизмом, лежащим в основе вычислительной производительности.

Квантовые алгоритмы

Несмотря на отсутствие физической реализации квантового компьютера, сравнимого по функциональным возможностям с классическим цифровым вычислителем, разработка квантовых алгоритмов является одним из востребованных направлений исследований.

Квантовый алгоритм является классическим алгоритмом, задающим последовательность унитарных операций (гейтов или вентилях) с указанием кубитов, над которыми их надо совершить. Квантовый алгоритм задается либо в виде словесного описания таких команд, либо с помощью их графической записи в виде системы вентилях (*quantum gate array*). Наиболее близким классическим аналогом квантового вычисления является вероятностное вычисление, т. е. правильность результата работы квантового алгоритма определена с некоторой вероятностью. Для повышения вероятности правильного результата в квантовых алгоритмах специально увеличивается кратность операций, которые подбираются таким образом, чтобы неправильные результаты с большой вероятностью взаимно уничтожались, и вероятность правильного результата увеличивалась. Множества задач, допускающих решение на квантовом компьютере и на классическом, совпадают.

Преимущество квантовых алгоритмов заключается в снижении времени решения задачи за счет распараллеливания операций путем генерирования запутанных квантовых состояний и их последующего использования. Такие случаи называются квантовым ускорением. Применение квантового ускорения является наиболее выигрышным при решении задачи моделирования динамики сложных систем и переборных математических задач (общий случай перебора – схема Гровера и ее варианты; задачи поиска скрытых периодов – схема Шора использования быстрого квантового преобразования Фурье и ее аналоги). Более подробно с различиями квантовых и классических алгоритмов можно ознакомиться в статьях [16, 17]. Существует и полный список разработанных на настоящий момент квантовых алгоритмов [18].

Одним из самых востребованных для множества задач является алгоритм поиска. Отмечается [19], что переборные задачи, в том числе алгоритм поиска Гровера (Grover), используемый для поиска определенного элемента в неструктурированной базе данных, квантовый компьютер решает быстрее, чем классический. Здесь же [19] приводится пример квантового варианта алгоритма поиска Гровера, исследуется функциональность квантового варианта алгоритма, обсуждаются преимущества квантовой реализации.

Рассмотрен в литературе и улучшенный квантовый алгоритм для подгонки модели линейной регрессии к заданному набору данных с использованием метода наименьших квадратов [20]. В отличие от предыдущих алгоритмов, которые дают квантовое состояние, кодирующее оптимальные параметры, улучшенный алгоритм выводит эти числа в классической форме. Таким образом, запустив его один раз, удастся полностью определить установленную модель, а затем использовать ее для прогнозирования новых данных. Улучшенный алгоритм работает в стандартной модели «Оракула» и может обрабатывать наборы данных с несравненными матрицами проектирования. Временная характеристика алгоритма:

$$\text{poly}(\log_2(N), d, k, 1/\epsilon),$$

где N – размер набора данных;

d – количество регулируемых параметров;

k – номер условия проектной матрицы;

ϵ – заданная точность результата.

Авторы доказали, что полиномиальная зависимость от d и k является объективной и, следовательно, данный алгоритм не может быть значительно улучшен. Кроме того, они показали, что разработанный квантовый алгоритм оценивает качество соответствия наименьших квадратов без явного вычисления его параметров, работая быстрее, чем алгоритмы, находящие это соответствие, и, следовательно, его целесообразно рекомендовать для проверки соответствия входного набора данных для линейной регрессии.

Со временем квантовые вычисления могут стать аппаратной платформой, способной существенно ускорить выполнение отдельных семейств классических алгоритмов. Уже сейчас экспериментально получены хорошие результаты в области масштабирования и отказоустойчивости для небольших квантовых вычислений, подтверждающие возможность полномасштабного квантового вычисления. Как и любой классический алгоритм, квантовый алгоритм должен быть эффективно реализован для получения максимально возможного преимущества от его выполнения. Как правило, квантовый алгоритм описывается в терминах процедур высокого уровня, таких, как арифметические операции (сложение, умножение, возведение в степень), или специальные преобразования, такие, как квантовое преобразование Фурье (QFT). Эти преобразования затем комбинируют в логические операции более высокого уровня, например, используя логические вентили Тоффли, Фредкина. В публикации [21] описан созданный и реализованный авторами квантовый алгоритм аппроксимации одноцикловых вращений $R_z(\phi)$ с использованием схемы Clifford+T. Алгоритм способен обрабатывать ошибки в приближении вплоть до размера 10^{-15} , что позволяет применять оптимальные схемы с одним кубитом, удобным для реализации масштабируемых квантовых алгоритмов.

Эффективный рандомизированный алгоритм аппроксимации произвольного элемента системы S произведением операторов Clifford+T с точностью до любого заданного порога ошибки $\epsilon > 0$ представлен в [22]. При слабой гипотезе о распределении простых чисел ожидаемое время выполнения алгоритма является полиномиальным $1/\epsilon$. Если оператор, который должен быть аппроксимирован, является z -вращением, то результирующая последовательность ворот равна $T\text{-count}(K) + 4\log_2(1/\epsilon)$, где K приблизительно равно 10. Наихудшая нижняя граница равна $K + 4\log_2(1/\epsilon)$ и достигается при $K = -9$. Следовательно, алгоритм находится в аддитивной постоянной оптимального для некоторых z -поворотов. Для произвольного члена S мы достигаем приближений с T -счетом $K + 12\log_2(1/\epsilon)$. Напротив, алгоритм Соловея–Китаева достигает $T\text{-count}(K) + 12\log_2(1/\epsilon)$, что составляет приблизительно 3.97. Приведенные показатели разработанного авторами алгоритма существенно лучше, чем показатели алгоритма Соловея–Китаева (Solovay–Kitaev).

В [23] описан эффективный синтез вероятностных квантовых цепей с запаздыванием. Цепи с повторением-до-успеха (RUS) могут аппроксимировать заданный единичный кубит с ожидаемым числом T -ворот около $1/3$ от того, что требуется оптимальными, детерминированными, безразмерными разложениями по набору ворот Clifford+T. Пред-

лагается более общий и концептуально более простой метод декомпозиции схем [23], позволяющий синтезировать протоколы, которые вероятностно реализуют квантовые схемы над несколькими универсальными наборами ворот, включая, но не ограничиваясь, набором ворот Clifford+T. Протокол, названный авторами вероятностными квантовыми цепями с запаздыванием (PQF), реализует проход по дискретной цепи Маркова. В ней целевое унитарное состояние является поглощающим состоянием, и переходы индуцируются многократными унитарными единицами, за которыми следуют измерения. В отличие от протоколов RUS, представленные протоколы PQF гарантированно завершаются после конечного числа шагов [23]. Здесь же описано применение разработанного метода к наборам Clifford+T, Clifford+V и Clifford+ $\pi/12$ для достижения разложений с ожидаемыми подсчетами ворот $\log b(1/\varepsilon) + O\{\ln[\ln(1/\varepsilon)]\}$, где b – величина, связанная со свойством расширения базового набора универсальных ворот.

Основные применения квантовых вычислений

Существует два типа задач, которые квантовые компьютеры способны решать намного эффективнее классических компьютеров. Первый тип – это задачи криптографии. На сегодняшний день многие системы шифрования основываются на перемножении больших чисел и их поиске с целью получения взломостойкого шифра. Самый большой интерес состоит в возможности дешифрования данных. В настоящее время безопасность шифрования заключается в том, что на расшифровку данных требуются несоизмеримо большие вычислительные мощности и огромное время, измеряемое в тысячелетиях. Квантовые компьютеры способны раскрыть такой шифр намного быстрее, примерно за то же время, что затрачено на само шифрование. Именно поэтому банковские и технологические компании заинтересованы в развитии квантовых вычислений.

Второй тип задач заключается в способности квантовых компьютеров эмулировать различные квантовые системы. И именно эта возможность, вероятно, перевернет человеческие представления о биологических системах, сверхпроводимых материалах или выведет на новый уровень понимания квантовой химии, не говоря уже о квантовой физике. Моделирование наблюдаемых явлений является незаменимым инструментом для разработки новых технологий, понимания естественного мира и изучения человеческого общества, однако наиболее интересные системы зачастую настолько сложны, что имитация их будущего поведения требует хранения огромных объемов информации о том, как они себя вели в прошлом. В случае более сложных систем симуляция становится все сложнее и, в конечном итоге, ограничивается такими ресурсами, как компьютерная память. Показано [24], что применение квантовых алгоритмов позволит уменьшить указанную потребность в памяти, измеряемую статистической сложностью процесса. Описано экспериментальное исследование приведенного квантового преимущества для моделирования стохастических процессов. Авторская квантовая реализация учитывает потребность в памяти $C_q = 0.05 \pm 0.01$, что намного ниже предельного классического предела $C = 1$. Масштабирование этого метода существенно уменьшит объем памяти, необходимый для моделирования более сложных систем.

Рассмотрим направления исследований в различных сферах.

Кибербезопасность. Умные пространства и безопасное хранение и использование больших данных. Рассмотрена возможность применения квантовых вычислений для поиска уязвимостей в умных пространствах [25]. Отмечено, что оба направления сегодня развиваются достаточно бурно и обе технологии вошли в десятку самых значительных трендов 2019 г. по версии исследовательского агентства Gartner, одного из лидеров в области систем хранения данных. Умное пространство должно объединить людей, процессы, сервисы и вещи, что позволит перевести на новый уровень выполнение многих привычных функций, позволит создать «умный дом», «цифровые места» и даже «умные города», подключив всю инфраструктуру к одной сети. Широкое распространение умных пространств потребует изменения подхода к системам хранения данных. В умной среде устройства периодически обмениваются данными по сети – либо напрямую от устройства к устройству, либо через облачные серверы. Появятся новые возможности для кибератак. Эксперты Gartner прогнозируют, что к 2023–2025 гг. бизнес-структуры начнут активно внедрять квантовые технологии, что заставит ввести новые стандарты кибербезопасности для систем хранения данных. Выход видится в разработке новых квантовых алгоритмов поиска уязвимостей и киберзащиты.

В развитие вышеуказанной темы в работе [26] обсуждаются «слепые» квантовые вычисления (*blind quantum computing*, BQC). Понятие «слепое» означает, что квантовый компьютер не имеет полной информации о задачах, которые он решает. Это гарантирует безопасность клиентских вычислительных задач. «Слепые» квантовые вычисления пока не получили распространения, поскольку требуют наличия у клиентов квантовых устройств, с которых задачи передаются на квантовые серверы. Конфиденциальность выполнения квантовых вычислений особенно важна, поскольку многие потенциальные задачи (как, например, умные пространства) требуют высокой степени безопасности. Желательным свойством для любого протокола BQC является проверка, в соответствии с которой клиент может с большой вероятностью проверить, выполнял ли сервер инструкции или произошло некоторое отклонение, приводящее к поврежденному состоянию вывода. Протокол BQC можно рассматривать как интерактивную систему доказательств. Авторами [26] предложена универсальная безопасная схема BQC, в которой клиенту нужно только подготовить отдельные кубиты в разделяемых состояниях, случайным образом выбранных из конечного набора, и отправить их на сервер, имеющий все необходимые квантовые вычислительные ресурсы. Добавив в описанный протокол дополнительные функции, авторы приводят строгое доказательство, что вероятность невозможности обнаружения неправильного вывода экспоненциально мала по параметру безопасности, тогда как затраты ресурсов остаются полиномиальными по этому параметру. Введенные дополнительные функции дают состояние ресурса, позволяющее выполнять запутывание шлюзов между произвольными парами логических кубитов только с постоянными служебными данными. Предложенное улучшение имеет важные последствия для порогов эффективности и отказоустойчивости.

В [27] рассмотрены последние разработки в квантовых алгоритмах, с акцентом на оценках ресурсов для взлома криптографических протоколов на квантовом компьютере. Полученные оценки, в свою очередь, могут быть использованы для получения квантовых параметров безопасности для различных схем. Авторы сравнивают эти криптографические приложения с приложениями, основанными на способности квантового компьютера эффективно имитировать другие системы квантовой механики.

Квантовая криптография. Квантовая криптография направлена на решение практической проблемы построения масштабируемых и защищенных квантовых сетей.

Одной из задач квантовой криптографии является удаленное распространение секретных ключей. Значительным шагом в этом направлении стало введение независимости измерительного устройства, когда секретный ключ между двумя сторонами устанавливается путем измерения ненадежного реле [28]. Ключевые показатели протоколов, реализованных в кубите, как правило, очень низкие, непригодные для требований городской сети. Показано [28], что решением может стать использование квантовых систем связи за счет сетевого протокола с когерентным состоянием. Разработанный протокол по своим количественным показателям превышает существующие на три порядка, и его можно использовать для создания высокоскоростных квантовых сетей, где устройства надежно подключаются к ближайшим точкам доступа или прокси-серверам.

Ключи. В данном обзоре представлено более десятка статей [29–40], посвященных квантовым алгоритмам поиска ключей, распределению ключей на оптическом волокне различной длины, анализу квантовых ресурсов, необходимых для проведения кибератаки.

В [29] представлен квантовый алгоритм Гровера для реализации исчерпывающего поиска ключа применительно к Advanced Encryption Standard (AES, расширенный стандарт шифрования) и анализу квантовых ресурсов, необходимых для проведения атаки. Авторами [29] рассмотрены количество операций алгоритма, количество кубитов и глубина алгоритма как исходная информация оценки трудоемкости квантового алгоритма Гровера. В качестве базового набора выбран Clifford+T gates как основной отказоустойчивый логический набор квантовых вентилях (ворот). Для всех трех вариантов AES (размеры ключа 128, 192 и 256 бит), которые стандартизованы в FIPS-PUB 197, установлены точные оценки числа кубитов и числа элементарных логических квантовых ворот, которые необходимы, чтобы реализовать представленный квантовый алгоритм Гровера для извлечения ключа из небольшого числа пар AES plain text–cipher text.

При базовой атаке ключа, связанного с блочным шифрованием, противник имеет доступ к шифрам под ключами, которые отличаются от целевого ключа бит-флипами. Показано [30], что для квантового противника такие атаки достаточно сильны при условии, что: 1) секретный ключ однозначно определяется небольшим числом пар символов открытого текста; 2) блочный шифр может быть эффективно оценен и 3) может быть запрошена суперпозиция связанных ключей. Тогда ключ может быть эффективно извлечен.

Быстрая и универсальная система распределения квантовых ключей (QKD, *quantum key distribution*) с аппаратным переключением ключей и мультиплексированием по длине волны рассматривается в [31]. Авторы описали компактно интегрированную когерентную одностороннюю систему распределения квантовых ключей с тактовой частотой 625 МГц, которая непрерывно распределяет секретные ключи по волоконно-оптической линии связи. Для поддержки высоких скоростей секретных ключей внедрен быстрый механизм перегонки аппаратного ключа, позволяющий в режиме реального времени увеличить скорость передачи до 4 Мбит/с. Данная система использует мультиплексирование по длине волны, чтобы работать только с одним оптическим волокном. На основе использования быстродействующих одиночных фотонных детекторов InGaAs реализовано надежное распределение секретных ключей со скоростью выше 21 кбит/с на 25 км опти-

ческого волокна. Авторы выполнили оптимизацию системы с учетом результатов анализа безопасности, включающих эффекты конечного размера, затраты на аутентификацию и системные ошибки для параметра безопасности $\varepsilon_{\text{QKD}} = 4 \times 10^{-9}$.

Авторы [32] позиционируют свое исследование как первый эксперимент по распределению квантовых ключей (QKD) с потерей в канале 72 дБ с использованием сверхнизких сверхпроводящих нанопроволочных однофотонных детекторов (SSPD, SNSPD) со скоростью теневого счета (DCR) 0.01 сП. Они используют схему дифференциального фазового сдвига QKD (DPS-QKD) с тактовой частотой 1 ГГц. Достигается значение коэффициента квантовой битовой ошибки (QBER) ниже 3%, когда длина волокна с дисперсией сдвига (DSF) составляет 336 км (потеря 72 дБ), что является достаточно низким для создания защищенных ключей.

Как мера противодействия квантовым кибератакам предложено независимое от измеряющего устройства квантовое распределение ключей (*measurement-device-independent quantum key distribution*, MDI-QKD).

Выбор протокола и оптимизация параметров в MDI-QKD обсуждается в [33]. MDI-QKD продемонстрировано в лабораторных условиях и в полевых испытаниях с использованием ослабленных лазеров в сочетании с техникой приманки. Отмечено [33], что на сегодняшний день отсутствуют результаты строгого сравнения различных протоколов MDI-QKD на основе приманки с двумя или тремя ее состояниями, следовательно, не определено количество типов состояний приманки, необходимое для реализации MDI-QKD. Системные параметры для реализации MDI-QKD с декомпозицией частично оптимизированы в известных авторам предыдущих работах, что ставит под сомнение фактическую производительность указанных демонстраций. Авторы приводят аналитические и численные методы декомпозиции с одним, двумя и тремя состояниями приманки, дают четкое сравнение этих методов и делают вывод, что два состояния приманки уже позволяют получить почти оптимальную оценку, а большее количество состояний приманки не могут значительно улучшить ключевую скорость в настройках асимптотики или конечных данных. Выполнена полная оптимизация параметров системы и показано, что полная оптимизация может значительно улучшить скорость ключа в настройке конечных данных. При проведении эксперимента установлено, что полная оптимизация может увеличить коэффициент ключа более, чем на один порядок по сравнению с неоптимизацией. Предложен локальный метод поиска для эффективной оптимизации параметров системы. Этот метод на четыре порядка быстрее, чем тривиальный исчерпывающий поиск для достижения аналогичной оптимальной скорости ключа.

Анализу конечных ключей для MDI-QKD посвящена работа [34]. Авторы предполагают, что хотя распределение квантовых ключей обещает безоговорочно безопасную связь, реальные устройства могут отклоняться от своих спецификаций, следовательно, безопасность практических систем не может быть гарантирована. В частности, противник может использовать несовершенные извещатели, чтобы изучить большую часть секретного ключа, даже несмотря на то, что обеспечение безопасности доказано иначе. Для решения этой проблемы и предложен практический подход – независимое от измерительного устройства распределение квантовых ключей. Однако до сих пор его безопасность полностью доказана только в предположении, что легальные пользователи си-

стемы имеют неограниченные ресурсы. Авторы восполнили этот пробел и обеспечили строгую защиту от общих атак в режиме с конечным ключом. Данный результат получен применением теории больших уклонений, в частности границ Чернова, для оценки параметров. Впервые продемонстрирована возможность реализации на дальних дистанциях MDI-QKD в приемлемые сроки передачи сигнала.

Продemonстрирована первая реализация поляризационного кодирования MDI-QKD [35], которое невосприимчиво ко всем атакам с боковым каналом извещателя. Активная фазовая рандомизация каждого индивидуального импульса применяется для защиты от атак на несовершенные источники. Путем оптимизации параметров в протоколе состояния decoy (состояние-ловушка) показано, что возможно реализовать поляризационное кодирование MDI-QKD с коммерческими готовыми устройствами. Для оценки безопасной скорости ключа применялся строгий анализ конечных ключей. Данное исследование открывает возможность для реализации сети MDI-QKD, при которой пользователям нужны только компактные и недорогие устройства для подготовки состояний кубитов.

Традиционно статистические флуктуации, принимаемые из различных источников, обрабатываются отдельно. Так, предложена методика улучшенного статистического флуктуационного анализа для MDI-QKD с использованием метода трехуровневых ложных состояний-ловушек [36]. Рассматривая статистические флуктуации, принимаемые из различных источников, как единый поток, авторы представили формулы для ключевых величин, используемых при вычислении безопасного финального ключа. Численное моделирование показало, что с учетом общего количества импульсов, равного 10^{12} , предложенный метод улучшает ключевую скорость примерно на 97% на расстояние 50 км по сравнению с предыдущими результатами и улучшает коэффициент ключа на 145% на расстояние 100 км по сравнению с результатом полной оптимизации всех параметров.

MDI-QKD является существенным шагом на пути к практической теоретико-информационной безопасности для обмена ключами между удаленными легальными пользователями [37]. Как и в случае с другими стандартными протоколами распределения квантовых ключей, зависящими от устройства, такими, как BB84, MDI-QKD предполагает, что эталонные фреймы были разделены между пользователями. На практике часто необходима нетривиальная процедура выравнивания, которая требует системных ресурсов и может значительно снизить скорость генерации безопасного ключа. Авторы [37] предлагают схему MDI-QKD с фазовым кодированием, не требующую фазового выравнивания между интерферометрами двух отдаленных легальных сторон. В качестве демонстрации представлен эксперимент с доказательством принципа с использованием интерферометров Фарадея–Майкельсона. Экспериментальная система работала на частоте 1 МГц, и средняя скорость ключа 8.309 б.п. была получена при длине волокна 20 км между пользователями. Система может поддерживать положительную скорость генерации ключа без компенсации фазы в нормальных условиях. Результаты показывают возможность данной системы для использования в готовых к практическому использованию устройствах MDI-QKD и ее значение для сетевых сценариев.

Распределение квантовых ключей без детекторных уязвимостей с использованием оптических затравочных лазеров показано в [38]. Из-за высокой чувствительности и сложного дизайна детекторы являются наиболее часто атакованными компонентами. Не-

давно было показано, что для устранения любой уязвимости от детекторов может быть использована двухфотонная интерференция из независимых источников света. Эта новая форма MDI-QKD была экспериментально продемонстрирована, но со скромными ключевыми скоростями и использованием новых импульсных методов для получения высокочувствительных помех от лазеров с коммутацией каналов и, таким образом, выполняет MDI-QKD с беспрецедентными скоростями ключа, превышающими 1 мегабит в секунду в режиме конечного размера. Это представляет собой улучшение на два-шесть порядков над существующими реализациями и поддерживает новую схему в качестве практического ресурса для обеспечения надежной квантовой связи.

MDI-QKD на оптическом волокне длиной 404 км обсуждается в [39]. Рассмотренное квантовое распределение ключей не зависит от измерения методом декомпозиции, отрицает угрозы безопасности от несовершенного однофотонного источника, а также от потерь обнаружения. Удлинение дистанции и улучшение ключевой скорости квантового распределения ключей являются жизненно важными проблемами в практических приложениях QKD. Приведены результаты MDI-QKD на более 404 км сверхнизкого оптического волокна и 311 км стандартного оптического волокна при использовании оптимизированного метода четырехуровневых ложных состояний-ловушек [39]. Эта рекордная реализация метода MDI-QKD не только обеспечивает новую дистанционную запись для MDI-QKD и всех типов QKD-систем, но и – что более важно – достигает расстояния, которое традиционный ВКК-Bassart 1984 ВКД не сможет достичь с помощью тех же устройств обнаружения даже с идеальными однофотонными источниками. Указанная публикация [39] представляет собой значительный шаг к доказательству и разработке возможного дальнего QKD.

Организация независимого квантового распределения ключей (QKD) на гибридной логической основе – множественном кубите, который первоначально введен в контексте отказоустойчивых квантовых вычислений в декогерентности свободного подпространства (DFS), имеет конкретные приложения для решения проблемы несоосности опорного кадра в квантовых информационных протоколах [40]. Предлагается безрисковая схема MDI-QKD [40] с вращательно-инвариантным состоянием, которая невосприимчива к коллективному шуму, вызванному несоосностью между двумя удаленными легитимными сторонами. В предложенном протоколе начальный логический кубит создается в гибридном пространстве с поляризованным орбитальным угловым моментом, в то время как передача полностью выполняется в инвариантной по повороту DFS при наличии коллективного шума, связанного с несоосностью. Частичное измерение состояния Белла выполняется на логических кубитах для его сортировки. По сравнению с оригинальными протоколами MDI-QKD численное моделирование показывает, что модифицированная схема существенно лучше и по расстоянию передачи, и по скорости генерации ключей. Кроме того, в предложенном протоколе требуются только обычные оптические элементы.

Квантовые нейронные сети и системы машинного обучения. Существует мнение [41], что интеллектуальная обработка и анализ больших данных – это работа именно для квантового интеллекта. Слияние квантовых вычислений, нейронных сетей и машинного обучения стало быстро развивающейся областью исследований. Однако «камень преткновения» здесь в том, что квантовый компьютер работает на квантовых состояниях, а не

на человекочитаемых данных, и быстрый интерфейс передачи большого объема данных квантовому компьютеру пока не реализован. В качестве примера приводится мощный сотовый телефон, подключенный к медленно работающей сотовой сети, сводящей «на нет» все его мощные характеристики [41].

«Нейронная сеть представляет собой программную или (опто-)электронную систему, обеспечивающую принятие решений путем эволюции сложной нелинейной системы, на вход которой подается вектор входных данных, а выходной сигнал (в общем случае многомерный) кодирует принимаемое решение. По сути, нейронная сеть представляет собой некий черный ящик, способный (в зависимости от своего внутреннего состояния) отображать N -мерный вектор входных данных в M -мерный вектор выходных данных. При этом внутреннее состояние нейронной сети адаптивно, т. е. изменяется в процессе обучения» [42]. Обучение нейронной сети может проходить двумя способами. Первый способ – это самообучение нейронной сети, при котором достаточно иметь только векторы входных данных; изменение состояния сети происходит за счет самоорганизации, т. е. зависит от корреляций между векторами. Второй способ – это обучение с учителем, когда на вход нейронной сети подаются данные, для которых результат работы нейронной сети является известным, и работа сети, соответственно, может быть оценена и скорректирована.

Нейронная сеть состоит из базовых вычислительных единиц-«нейронов», преобразователей входного сигнала в выходной с использованием нелинейной переходной функции. «Сеть представляет собой нелинейный параллельный процессор, основанный в общем случае на связи всех нейронов со всеми» [42]. В процессе обучения сети изменяются интенсивности связей, соединяющих нейроны, и в результате существенно отличными от нуля остаются лишь те связи, которые ведут к правильному решению.

Нейроны располагаются обычно по слоям, контролируя вывод нескольких других нейронов, и меняют свое состояние при определенных условиях. Например, при распознавании изображения начальный слой нейронов принимает входные данные – пиксели, промежуточные слои создают различные комбинации ввода, отображающие некие геометрические фигуры, а заключительный уровень создает описание изображения.

Известно и другое определение нейронной сети [43]: нейронная сеть представляет собой существенно параллельную распределенную систему обработки информации, состоящую из простых идентичных блоков – нейронов, обладающих способностью хранить информацию и предоставлять ее для использования. Квантовая нейронная сеть заменяет классические сигналы, поступающие на вход нейрона, на квантовые состояния, обладающие амплитудой и фазами. На выходе квантовой нейронной сети должно формироваться квантовое состояние, зависящее от линейной суперпозиции входящих состояний [42], т. е. квантовая нейронная сеть построена из набора модели кубитов нейрона, внутреннее состояние которого является когерентной суперпозицией кубитовых состояний.

В настоящее время происходит «поиск» модели квантовой нейронной сети, оптимальной с точки зрения использования всех преимуществ, которые представляют квантовые вычисления и нейронные сети. Например, в [44] дано систематическое перечисление и описание различных подходов и результатов таких исследований. Сделан акцент на сети типа Хопфилда и задачу ассоциативной памяти, и поставлена задача объединить нелинейную диссипативную динамику нейронных вычислений и линейную унитарную

динамику квантовых вычислений. Выработаны также критерии эффективности архитектуры квантовой нейронной сети. В результате из рассмотренных исследований по потенциальной модели квантовой нейронной сети ни один из вариантов не признан полностью удовлетворительным. В качестве перспективного направления исследований отмечена идея открытых квантовых нейронных сетей на основе диссипативных квантовых вычислений.

Имеется информация о новой квантовой сети нейронных деревьев Qubit с улучшенными нейронами Qubit, устанавливаемыми межслойными связями и различными фазовыми операционными функциями для каждого нейрона [45]. Сеть нейронного дерева Qubit может быть построена и оптимизирована с помощью древовидной кодировки на основе эволюционного алгоритма. В отличие от других подобных сетей Qubit разрешает выбор набора терминалов и установку межслойных соединений. Улучшенный нейрон Qubit применяется вместо сигмовидной функции для решения нелинейных задач моделирования. Для оценки эффективности и производительности предлагаемой сети были выбраны три нелинейные задачи моделирования. Результаты моделирования показали, что сеть нейронных деревьев Qubit имеет хорошие показатели по производительности и эффективности при нелинейном моделировании.

Предлагается [46] квантовая нейронная сеть, называемая квантовым персептроном над полем (QPF), которую невозможно смоделировать на классическом компьютере. QPF является прямым обобщением классического персептрона, избавленного от ряда ограничений. В статье приведен основанный на суперпозиции алгоритм обучения с алгоритмом SAL, который оптимизирует веса и архитектуры нейронной сети. SAL ищет лучшую архитектуру в конечном наборе нейронных сетевых архитектур с линейным временем по количеству шаблонов в обучающем наборе. SAL является первым алгоритмом обучения для определения нейронных сетевых архитектур в полиномиальное время, данный результат получен за счет использования квантового параллелизма и нелинейного квантового оператора.

Описан эффективный метод разработки нейронных сетей с несколькими соединениями и высокой степенью классификации: эволюционный алгоритм (QEA), основанный на принципах квантовых вычислений [47]. Получено, что при схождении квантовой эволюционной нейронной сети (QENN) на этапе обучения, последующее обучение бессмысленно. Поэтому важно контролировать количество поколений QENN. Анализ свойства сходимости квантовой эволюции битов дает возможность сформулировать всегда достижимый безопасный критерий завершения обучения, например, основанный на средней скорости конвергенции (ACR). Метод экспериментально опробован и подтвержден на задачах классификации. Результаты показали, что критерий завершения, основанный на ACR, может должным образом остановить процесс обучения QENN и преодолеть ограничения критерия завершения, основанные на вероятности генерации наилучшего решения (PBS).

С целью повышения аппроксимирующей способности традиционной искусственной нейронной сети (ANN) предложена основанная на квантовых началах нейронная сеть (SIQNN) [48]. В этой модели скрытые узлы состоят из нескольких многобайтовых управляемых-НЕ-логических ворот, входы описываются многомерными дискретными

последовательностями кубитов, выходными узлами являются традиционные нейроны. Параметры модели включают в себя углы квантовых вращений в скрытом слое и веса – в выходном слое. Алгоритмы обучения получены с использованием алгоритма Левенберга–Марквардта. Результаты моделирования прогнозирования стока Хунцзядуйского водохранилища в Китае показывают, что SIQNN, очевидно, превосходит ANN.

Эвристические и детерминированные методы оптимизации широко применяются для обучения искусственных нейронных сетей. Оба эти метода имеют свои преимущества и недостатки. Эвристические методы стохастической оптимизации, такие, как генетический алгоритм, выполняют глобальный поиск, но имеют медленную скорость конвергенции вблизи глобального оптимума. Детерминированные методы (например, градиентный спуск) демонстрируют быструю скорость сходимости вокруг глобального оптимума, но могут отставать в локальном оптимуме. Предложен алгоритм гибридного обучения, сочетающий генетический алгоритм (GA) с градиентным спуском (GD), названный HGAGD [49]. Новый алгоритм сочетает в себе глобальную способность исследования GA с точной локальной эксплуатационной способностью GD для достижения более быстрой конвергенции, а также лучшей точности конечного решения. Описано применение HGAGD в качестве нового метода обучения для оптимизации параметров нейронной сети с квантовым введением (QINN) для двух разных приложений [49]. Во-первых, при решении задач аппроксимации функций выбираются две контрольные функции для демонстрации потенциала предлагаемого QINN с алгоритмом HGAGD; во-вторых, изучается эффективность предлагаемого метода в прогнозировании временных рядов Маккея-Гласса и аттрактора Лоренца. Результаты этих исследований показывают преимущество предлагаемого подхода по сравнению с традиционными подходами. Те же авторы в работе [50] описывают возможность применения аналогичного метода для проектирования непрямого адаптивного контроллера для затухания низкочастотных колебаний в энергетических системах. Результаты этих исследований показывают, что предлагаемый контроллер, обученный HGAGD, способен достичь эффективных характеристик управления.

Оценена эффективность кубитной нейронной сети (QNN) посредством предсказания известного аттрактора Лоренца, который создает хаотичные временные ряды тремя динамическими системами [51]. Экспериментально установлено, что QNN способна более точно прогнозировать временные ряды по сравнению с обычными (реальными) нейронными сетями.

Классические автокодеры – нейронные сети, которые могут изучать эффективные низкоразмерные представления данных в пространстве с более высоким пространством и позволяют применять обучение без учителя при использовании метода обратного распространения ошибки. Задача автокодера – задавать вход X для отображения X в более низкую размерную точку Y , так что X , скорее всего, будет восстановлен из Y . Структуру базовой сети автокодера можно выбирать для представления данных меньшего размера, эффективно сжимающих входные данные. Представлена модель квантового автокодера для выполнения подобных задач по квантовым данным [52]. Квантовый автокодер обучен сжимать определенный набор данных квантовых состояний, где классический алгоритм сжатия не может быть использован. Параметры квантового автокодера обучаются с использованием классических алгоритмов оптимизации. Приведен пример простой про-

граммируемой схемы, которую обучают в контексте квантового моделирования как эффективный автокодер для сжатия основных состояний модели Хаббарда и молекулярных гамильтонианов.

Квантовое машинное обучение отвечает за исследование и разработку методов машинного обучения, способных эффективно задействовать параллелизм квантовых компьютеров. Наиболее важные задачи квантового машинного обучения, такие, как распознавание изображений, распознавание речи, оптимизация стратегий, обсуждаются в [53]. Идеи улучшения классических алгоритмов машинного обучения с учетом возможностей квантовой информатики варьируются от эффективных ресурснообъемных дорогостоящих алгоритмов до перевода стохастических методов на язык квантовой теории. Обсуждаются возможные подходы, технические детали данного процесса, оценивается потенциал будущей теории квантового обучения [53].

Несмотря на прилагаемые усилия, разрыв, существующий между большинством исследовательских предложений по квантовому машинному обучению и практическими потребностями, достаточно велик. Сложные задачи машинного обучения, которые могут быть решены с помощью гибридных квантовых устройств, рассмотрены в [54]. Здесь авторы выделили также классические наборы данных с потенциальными квантоподобными статистическими корреляциями для проблемно-ориентированных квантовых устройств. Ориентируясь на гибридные квантово-классические подходы, авторы выделяют ключевые проблемы, которые считают подходящими для реализации на гибридных квантовых устройствах. Представлена и квантово-вспомогательная машина Гельмгольца (QАНМ) [54], как попытка использования гибридных квантовых устройств при обработке больших данных. QАНМ использует глубокое обучение для извлечения низкоразмерного двоичного представления данных, подходящего для относительно небольших квантовых процессоров, которые могут помочь в обучении неконтролируемой генеративной модели. Хотя авторы [54] рассмотрели данный вариант на квантовом отжиге, другие квантовые платформы также могут использовать описанную гибридную квантово-классическую структуру.

Рассмотрен случай реализации контролируемого машинного обучения (классификация новых данных на основе уже классифицированных примеров обучения) на квантовой опорной векторной машине [55]. Показано, что опорная векторная машина, организующая работу оптимизированного бинарного классификатора, реализуется на квантовом компьютере со сложностью логарифмической величины векторов и количеством примеров обучения. В тех случаях, когда классические алгоритмы выборки требуют полиномиального времени, получается экспоненциальное ускорение. В основе этого алгоритма с квантовыми большими данными лежит методика экспоненциального несопоставимого матричного метода для эффективного выполнения матричной инверсии матрицы внутреннего продукта (ядра) обучающих данных. Те же авторы в [56] выполнили анализ квантовых базисных компонент. Обычный способ выявления свойств неизвестного квантового состояния, учитывая множество копий системы в этом состоянии, заключается в выполнении измерений дивергентных наблюдаемых и статистическом анализе результатов. Для нерезонансных, но низкоуровневых квантовых состояний выявление собственных векторов и соответствующих собственных значений в классической форме суперли-

нейно масштабируется с размерностью системы 3-6. Показано [56], что для построения унитарного преобразования $e^{-i\rho t}$ можно использовать несколько копий квантовой системы с матрицей плотности ρ . Это позволяет выполнить квантовый анализ главных компонент неизвестной матрицы плотности низкого ранга, выявляя в квантовой форме собственные векторы, соответствующие большим собственным значениям во времени, экспоненциально быстрее любого существующего алгоритма. Возможное применение: анализ данных, технологическая томография.

Алгоритм квантового машинного обучения для эффективного решения класса задач, закодированных в квантовоконтролируемых унитарных операциях, описан в [57]. Центральным физическим механизмом протокола является итерация квантового уравнения с запаздыванием, которое вводит обратную связь в динамике и исключает необходимость промежуточных измерений. Выполнение квантового алгоритма анализируется путем сравнения результатов, полученных при численном моделировании, с результатами классических методов машинного обучения для одной и той же задачи. Использование уравнений с задержкой по времени улучшает инструментарий поля квантового машинного обучения, что может обеспечить беспрецедентное применение в квантовых технологиях.

Рассмотрен алгоритм предсказания на квантовом компьютере, основанный на линейной регрессионной модели с оптимизацией наименьших квадратов [58]. В отличие от предшествующих решений, связанных с проблемой считывания оптимальных параметров соответствия, данный алгоритм фокусируется на задаче машинного обучения угадывания вывода, соответствующего новому вводу, приведенным примерам точек данных. Кроме того, алгоритм адаптирован для обработки несравнимых матриц данных, которые представлены приближениями низкого ранга, что значительно улучшит зависимость от его номера условия. Результат предсказания можно получить через единичное измерение и затем использовать для дальнейших процедур обработки квантовой информации. При линейном росте входных данных время выполнения алгоритма увеличивается по логарифмической зависимости.

Известна работа, посвященная квантовому обучению аппаратно-встроенным вероятностным графическим моделям [59]. Отмечено, что основные методы машинного обучения, такие, как глубокое обучение и вероятностное программирование, в значительной степени зависят от отбора проб из обычно трудноразрешимых распределений вероятностей. Возрастает интерес к потенциальным преимуществам использования технологий квантовых вычислений в качестве механизмов выборки для ускорения этих задач или повышения их эффективности. Однако на данный момент трудно оценить фактическую производительность данных алгоритмов. Редкая связь, возникающая из-за локального взаимодействия между квантовыми битами в физических аппаратных реализациях, считается самым серьезным ограничением качества построения мощных генеративных моделей без надзора в машинном обучении. Стоит отметить, что в [59] использованы методы внедрения для добавления избыточности к наборам данных, что позволило увеличить способность моделирования квантовых отжигов. Результаты проиллюстрированы графическими моделями, встроенными в аппаратные средства, в бинаризованный набор данных рукописных цифр и два набора синтетических данных в экспериментах до 940 квантовых битов. Такая модель может быть обучена без полного знания эффективных

параметров, определяющих соответствующее квантовое распределение Гиббса. Указанный подход позволяет уйти от необходимости определять эффективную температуру на каждой итерации алгоритма отжига, ускоряя обучение; также смягчается влияние шума в контрольных параметрах, делая его устойчивым к отклонениям от эталонного распределения Гиббса. Он обеспечивает возможность использования квантовых отжигов для реализации генерирующих моделей и создает подходящую основу для сопоставления этих квантовых технологий по задачам, связанным с машинным обучением.

В [60] рассмотрены марковские логические сети (MLNs), объединяющие две противоположные школы в машинном обучении и искусственном интеллекте: причинно-следственные сети, которые очень хорошо учитывают неопределенность, и логику первого порядка, которая допускает формальные выводы. MLN – это, по сути, логический шаблон первого порядка для создания сетей Маркова. Вывод в MLN является вероятностным, и его часто выполняют с помощью приближительных методов, таких, как выборка Гиббса по методу Маркова в цепи Монте-Карло (MCMC). MLN имеет множество регулярных симметричных структур, которые разумно использовать и на уровне первого порядка, и в генерируемой сети Маркова. Различными способами проанализированы созданные графовые структуры и определено, в какой степени квантовые протоколы могут использоваться для ускорения выборки Гиббса с помощью схем подготовки и измерения состояния [60]. На основе анализа различных подходов, оценки их преимуществ, теоретических ограничений, возможностей реализации сделан также вывод, что прямое применение полученного результата приводит к экспоненциальному ускорению по сравнению с классическими эвристиками, что подтверждает их потенциальную полезность для применения в машинном обучении.

В современных моделях глубокого обучения используются высоко оптимизированные сверточные нейронные сети (CNN), обучающиеся на компьютерах с большим графическим процессором (GPU) и довольно простой многоуровневой топологией сети, то есть с высокосвязанными уровнями без внутрислойных соединений. Построение топологий сети глубокого обучения требует ручной настройки, а внедрение сети в аппаратное обеспечение является дорогостоящим как по стоимости, так и по мощности. Выполнена оценка модели глубокого обучения с использованием трех различных вычислительных архитектур для решения этих проблем [61]: квантовых вычислений для обучения сложных топологий, высокопроизводительных вычислений (HPC) для автоматического определения топологии сети и нейроморфных вычислений для маломощной аппаратной реализации. Из-за ограничений на количество вводимых данных в существующих моделях квантовых компьютеров авторы использовали для оценки набор данных MNIST. Результаты оценки показали возможность использования трех архитектур в tandem для изучения сложных сетей глубокого обучения, которые не подлежат обработке с использованием архитектуры фон Неймана. Показано, что квантовый компьютер может находить высококачественные значения внутрислойных соединений и весов, получая при этом сдержанный результат времени по мере увеличения сложности сети; высокопроизводительный компьютер может найти оптимальные топологии на основе слоев; и нейроморфный компьютер может представлять сложную топологию и весовые коэффициенты, полученные из других архитектур в маломощном мемарном оборудовании. Полученный результат был невозможен при архитектуре фон Неймана.

Квантовые структуры в когнитивных и социальных науках. Одной из проблем социологии и психологии является определение принципов и условий, определяющих такие человеческие когнитивные акты, как принятие решений, категоризация и поведение в условиях неопределенности. Идентификация этих механизмов интересна для большинства сфер человеческой деятельности от психологии до экономики, финансов, политики, информатики и искусственного интеллекта. Преобладающая на сегодня теоретическая парадигма основывается на классической концепции логики и теории вероятностей. Согласно этой парадигме, люди принимают решения, следуя правилам булевой логики, а вероятностные аспекты принятия решений могут быть формализованы теорией вероятности Колмогорова. Подход Колмогорова обеспечивает достаточно полный и точный учет принятия решений людьми как на нормативном уровне (описывая, что люди должны делать), так и на описательном уровне (описывая, что на самом деле делают люди). Однако экспериментальные исследования концептуальной классификации, человеческого суждения и восприятия и поведенческой экономики показали, что эта классическая концепция принципиально проблематична в том смысле, что когнитивные модели, основанные на этих математических структурах, не способны охватить то, как люди принимают решения в условиях неопределенности. В последнее десятилетие возникла альтернативная научная парадигма, в которой используется более общая схема моделирования на основе математического формализма квантовой теории для моделирования ситуаций и процессов в когнитивной и социальной науке [62]. Конъюнктивные и дизъюнктивные заблуждения, эффекты дизъюнкции, нарушения принципа Sure-Thing, парадоксы Allais, Ellsberg и Machina являются лишь некоторыми из примеров, когда применение квантовомеханического формализма показывает значительно большую эффективность по сравнению с традиционными схемами моделирования классического типа.

Обзор текущих исследований, в которых применяется формализм квантовой теории в когнитивных и социально-экономических областях, выполнен в [62]. Цель данных исследований – не изучить микрофизические процессы, происходящие в человеческом мозге, и затем управлять суждениями человека, а рассмотреть квантовую теорию как общую, когерентную и унитарную парадигму человеческого познания. В этом отношении важен обзор [62] исследований аксиоматических и операционных основ квантовой физики, основанных на теории, а не на экспериментах; хотя иногда допускается использование эмпирических данных. Модели построены по общим эпистемологическим и техническим ограничениям квантовой теории; следовательно, успех этого моделирования на основе квантовой теории предполагает, что он может обеспечить общую теорию человеческого познания. Исследования идут по трем направлениям:

- определение причин, лежащих в основе успеха квантовой парадигмы в когнитивной и социально-экономической областях;
- идентификация эмпирических ситуаций, когда квантовый формализм дает преимущества по сравнению с традиционными схемами моделирования и появляются новые подлинные квантовые структуры;
- распространение квантовой парадигмы на новые сферы человеческой деятельности.

Анализ результатов когнитивного теста на конъюнкции и отрицание естественных

понятий [63] показал, что квантово-теоретическая вероятностная модель в гильбертовом пространстве достоверно представляет собранные данные, противоречащие теоретико-множественной колмогоровской модели. Этот результат объясняется предположением о существовании двух типов рассуждений в человеческом познании: доминирующих возникающих рассуждений и вторичных логических рассуждений. Некоторые математические аспекты этой квантово-теоретической модели концептуальных союзов и отрицаний развиваются в [64] путем введения унитарных операторов в гильбертовом пространстве. Исследования показали [63], что квантово-теоретический подход может служить обобщением теории прототипов Е. Rosch, в которой признается зависимость прототипа от контекста.

В работе [63], в которой моделируется принятие решений людьми, исследовано взаимное влияние концептуальной конъюнктуры и отрицания путем измерения весомости членов списка экземпляров в отношении двух понятий. Выявлены систематические отклонения от классической (нечеткой) логики и теории вероятностей. Полученные результаты дают еще более весомое доказательство обоснованности квантово-теоретической основы для сочетания двух понятий. Представление концептуального отрицания, естественно, вытекает из общих предположений нашей двухсекторной пространственной модели Фока, и это представление верно согласуется с экспериментальными данными. Обнаружено новое значительное и априорно неожиданное отклонение от классики, и его можно точно объяснить, полагая, что человеческое мышление является суперпозицией «возникающего рассуждения» и «логического рассуждения» и что эти два процесса представлены в пространственной алгебраической структуре Фока.

Человеческое восприятие является объектом исследования в [65], где развивается квантовая модель динамики восприятия, иллюстрируемая с помощью модели бистабильного восприятия конкретной двусмысленной фигуры, лестницы Шредера.

Выполнена проверка возможности применения статистической модели, полученной из физики конденсированных сред, для восстановления структуры социальной сети [66]. Обратная модель Поттса, традиционно применяемая для рекурсивных наблюдений квантовых состояний в ансамбле частиц, здесь обращена к наблюдениям состояний членов в организации и их (анти)корреляциям, тем самым выводя взаимодействия в качестве связей между членами. Решение обратной задачи на основе LBP применено в первый раз для восстановления общей структуры графа, т. е. впервые в области социальных наук применена модель Q-состояния (вместо модели Изинга) для вывода структуры реальной сети. Рассмотрена роль разнообразных вариантов моделирования и конкретных параметров с целью выяснения вопроса, как максимальное значение Q-разрешения моделью Поттса может привести к существенным различиям результатов, наряду с априорными знаниями о структуре сети.

На основе обобщения и анализа литературных данных можно сделать вывод, что квантовые структуры систематически присутствуют в объектах и предметах исследования когнитивной и социальной науки и что квантово-подобные модели более эффективны, чем традиционные теоретико-множественные модели вероятности.

Заключение

Квантовая информатика – новый раздел науки, посвященный использованию квантовых объектов для обработки и передачи информации. Сегодня в разработку квантового компьютера инвестируется много усилий и средств. По всему миру идет работа по созданию квантовых элементов, проектированию квантовых алгоритмов и разработке архитектуры квантового компьютера.

Определены перспективные направления применения квантовой информатики:

- моделирование сложных естественных и искусственных явлений и процессов, одним из которых является сам квантовый компьютер;
- квантовая криптография, методы передачи которой гарантируют невозможность расшифровки сообщения;
- квантовые нейронные сети и машинное обучение позиционируется как путь к созданию квантового интеллекта;
- применение квантовых вычислений в когнитивных и социальных науках дает возможность исследовать механизм принятия решений при неполных данных.

Литература:

1. Доклад экспертной группы Digital McKinsey «Цифровая Россия: новая реальность». 2017. 122 с. URL: <http://www.mckinsey.com/global-locations/europe-andmiddleeast/russia/ru/our-work/mckinsey-digital> (Дата обращения 15.01.2019).
2. Программа «Цифровая экономика Российской Федерации», утвержденная Распоряжением № 1632-р Правительства Российской Федерации от 28 июля 2017 г.
3. Программа «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», утвержденная Указом Президента Российской Федерации от 9 мая 2017 г. № 203.
4. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years // Nature. 2017. V. 543. Iss. 7644. P. 171–174. DOI: 10.1038/543171a
5. Гренштейн С. Новое исследование Ассоциации полупроводниковой промышленности: «Через 5 лет закон Мура перестанет действовать». URL: <https://habr.com/post/307158/>
6. Levchaev P.A. The digital economy as the future of our lives // Russian Journal of Management. 2017. V. 5. № 4. P. 515–523. URL: https://doi.org/10.29039/article_5a5df35550f2d6.65514969
7. Карасев С. Глава Intel: об отношениях с Apple, законе Мура, новых устройствах и материалах // Электронное СМИ «3ДНьюс». URL: <https://3dnews.ru/about> (Дата обращения 15.01.2019).
8. Humble T. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications // IEEE Consumer Electronics Magazine. 2018. V. 7. Iss. 6. P. 8–14. DOI:10.1109/MCE.2017.2755298
9. Кулик С.Д., Берков А.В., Яковлев В.П. Введение в теорию квантовых вычислений (методы квантовой механики в кибернетике): уч. пособие в 2-х кн. Книга 1. М.: МИФИ, 2008. 212 с.
10. Квантовые вычисления для любопытных. URL: <https://cloudcoin.ru/quantum->

computing (Дата обращения 15.01.2019).

11. Квантовый компьютер и квантовая связь. URL: <http://www.tadviser.ru/index.php> (Дата обращения 15.01.2019).

12. Фонд перспективных исследований. URL: https://fpi.gov.ru/press/media/jekspert_mnogokubitniy_kvantoviy_kompyuter_mozhno_sozdaty_v_rossii_za_god (Дата обращения 15.01.2019).

13. Debnath S., Linke N.M., Figgatt C., Landsman K.A., Wrigh, K., Monroe C. Demonstration of a small programmable quantum computer with atomic qubits // Nature. 2016. V. 536. Iss. 7614. P. 63–66. DOI: 10.1038/nature18648

14. Linke N.M., Maslov D., Roetteler M., Debnath S., Figgatt C., Landsma, K.A., Wright K., Monroe C. Experimental comparison of two quantum computing architectures // Proc. Natl. Acad. Sci. U.S.A. 2017. V. 114. Iss. 13. P. 3305–3310. DOI: 10.1073/pnas.1618020114

15. Britt K.A., Humble T.S. High-performance computing with quantum processing units // ACM Journal. Emerging Technologies in Computing Systems. 2017. V. 13. Iss. 3. Article No. 39. DOI: 10.1145/3007651

16. Сапаев Д., Булычков Д. Квантовые вычисления против классических: зачем нам столько цифр. URL: <https://habr.com/company/sberbank/blog/343308/> (Дата обращения 15.01.2019).

17. Сапаев Д., Булычков Д. Квантовые вычисления: отжиг с выключателями и прочее веселье. URL: <https://habr.com/company/sberbank/blog/344830/> (Дата обращения 15.01.2019).

18. Список квантовых алгоритмов. URL: <https://math.nist.gov/quantum/zoo/> (Дата обращения 15.01.2019).

19. Dumas J.P., Soni K., Rasool A. An introduction to quantum search algorithm and its implementation // In: Balas V., Sharma N., Chakrabarti A. (eds) Data Management, Analytics and Innovation // Advances in Intelligent Systems and Computing. 2019. V. 808. P. 19–31. Springer, Singapore. DOI: 10.1007/978-981-13-1402-5_2

20. Wang G. Quantum algorithm for linear regression // Phys. Rev. A. 2017. V. 96. Iss. 1. Article No. 012335. DOI: 10.1103/PhysRevA.96.012335

21. Kliuchnikov V., Maslov D., Mosca, M. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits // IEEE Trans. Comp. 2016. V. 65. Iss. 1. P. 161–172. Article No. 7056491. DOI: 10.1109/TC.2015.2409842

22. Selinger P. Efficient Clifford+T approximation of single-qubit operators // Quantum Information and Computation. 2014. V. 15. Iss. 1-2. P. 159–180.

23. Bocharov A., Roetteler M., Svore K.M. Efficient synthesis of probabilistic quantum circuits with fallback // Phys. Rev. A. Atomic, Molecular, and Optical Physics. 2015. V. 91. Iss. 5. Article No. 052317. DOI: 10.1103/PhysRevA.91.052317

24. Palsson M.S., Gu M., Ho J., Wiseman H.M., Pryde G.J. Experimentally modeling stochastic processes with less memory by the use of a quantum processor // Science Advances. 2017. V. 3. Iss. 2. Article No. e1601302. DOI: 10.1126/sciadv.1601302

25. Столяров А. Квантовые вычисления и умные пространства могут изменить рынок СХД. URL: http://safe.cnews.ru/news/top/2018-11-14_kvantovye_vychisleniya_i_umnye_prostranstva_mogut (Дата обращения 15.01.2019).

26. Fitzsimons J.F., Kashefi E. Unconditionally verifiable blind quantum computation // *Phys. Rev. A*. 2017. V. 96. Iss. 1. Article No. 012303. DOI: 10.1103/PhysRevA.96.012303
27. Roetteler M., Svore K.M. Quantum computing: Codebreaking and beyond // *IEEE Security and Privacy*. 2018. V. 16. Iss. 5. P. 22–36. Article No. 8490171. DOI: 10.1109/MSP.2018.3761710
28. Pirandola S., Ottaviano C., Spedalieri G., Weedbroo C., Braunstein S.L., Lloyd S., Gehring T., Jacobsen C.S., Andersen U.L. High-rate measurement-device-independent quantum cryptography // *Nature Photonics*. 2015. V. 9. Iss. 6. P. 397–402. DOI: 10.1038/nphoton.2015.83
29. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: Quantum resource estimates // *Lecture Notes in Computer Science*. 2016. V. 9606. P. 29–43. 7th Int. Workshop on Post-Quantum Cryptography, PQ Crypto 2016; Fukuoka; Japan; February 24–26, 2016; code 164489. DOI: 10.1007/978-3-319-29360-8_3
30. Roetteler M., Steinwandt R. A note on quantum related-key attacks // *Information Processing Lett.* 2015. V. 115. Iss. 1. P. 40–44. DOI: 10.1016/j.ipl.2014.08.009
31. Walenta N., Burg A., Caselunghe D., Constantin J., Gisin N., Guinnard O., Houlmann R., Junod P., Korzh B., Kulesza N., Legré M., Lim C.W., Lunghi T., Monat L., Portmann C., Soucarros M., Thew R.T., Trinkler P., Trollet G., Vannel F., Zbinden H. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing // *New Journal of Physics*. 2014. V. 16. Article No. 013047. DOI: 10.1088/1367-2630/16/1/013047
32. Shibata H., Honjo T., Shimizu K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors // *Optics Lett.* 2014. V. 39. Iss. 17. P. 5078–5081. DOI: 10.1364/OL.39.005078
33. Xu F., Xu H., Lo H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution // *Phys. Rev. A. Atomic, Molecular, and Optical Physics*. 2014. V. 89. Iss. 5. Article No. 052333. DOI: 10.1103/PhysRevA.89.052333
34. Curty M., Xu F., Cui W., Lim C.C.W., Tamaki K., Lo H.-K. Finite-key analysis for measurement-device-independent quantum key distribution // *Nature Commun.* 2014. V. 5. Article No. 3732. DOI: 10.1038/ncomms4732
35. Tang Z., Liao Z., Xu F., Qi B., Qian L., Lo H.-K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution // *Phys. Rev. Lett.* 2014. V. 112. Iss. 19. Article No. 190503. DOI: 10.1103/PhysRevLett.112.190503
36. Yu Z.-W., Zhou Y.-H., Wang X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method // *Phys. Rev. A. Atomic, Molecular, and Optical Physics*. 2015. V. 91. Iss. 3. Article No. 032318. DOI: 10.1103/PhysRevA.91.032318
37. Wang C., Song X.-T., Yin Z.-Q., Wang S., Chen W., Zhang C.-M., Guo G.-C., Han Z.-F. Phase-reference-free experiment of measurement-device-independent quantum key distribution // *Phys. Rev. Lett.* 2015. V. 115. Iss. 16. Article No. 160502. DOI: 10.1103/PhysRevLett.115.160502
38. Comandar L.C., Lucamarini M., Fröhlich B., Dynes J.F., Sharpe A.W., Tam S.W.-B., Yuan Z.L., Penty R.V., Shields A.J. Quantum key distribution without detector vulnerabilities using optically seeded lasers // *Nature Photonics*. 2016. V. 10. Iss. 5. P. 312–315. DOI: 10.1038/nphoton.2016.50
39. Yin H.-L., Chen T.-Y., Yu Z.-W., Liu H., You L.-X., Zhou Y.-H., Chen S.-J., Mao Y.,

Huang M.-Q., Zhang W.-J., Chen H., Li M.J., Nolan D., Zhou F., Jiang X., Wang Z., Zhang Q., Wang X.-B., Pan J.-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber // *Phys. Rev. Lett.* 2016. V. 117. Iss. 19. Article No. 190501. DOI: 10.1103/PhysRevLett.117.190501

40. Chen D., Wei L., YaLiang C., Qing P., Lei S. Reference-frame-independent measurement-device-independent quantum key distribution using hybrid logical basis // *Quantum Information Processing*. 2018. V. 17. Iss. 10. Article No. 256. DOI: 10.1007/s11128-018-2030-7

41. Musser G. Job one for quantum computers: Boost artificial intelligence. // *Quanta Magazine*. URL: <https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/> (Дата обращения 15.01.2019).

42. Алтайский М.В., Капустина Н.Е., Крылов В.А. Квантовые нейронные сети: современное состояние и перспективы развития // *Физика элементарных частиц и атомного ядра*. 2014. Т. 45. Вып. 5-6. С. 1825–1856.

43. Haykin S. *Neural Networks*. Pearson Education. NY: IEEE, 1999. 600 p.

44. Schuld M., Sinayskiy I., Petruccione F. The quest for a quantum neural network // *Quantum Information Processing*. 2014. V. 13. Iss. 11. P. 2567–2586. DOI: 10.1007/s11128-014-0809-8

45. Qi F., Chen C. Qubit neural tree network with applications in nonlinear system modeling // *IEEE Access*. 2018. V. 6. P. 51598–51606. Article No. 8463464. DOI: 10.1109/ACCESS.2018.2869894

46. da Silva A.J., Ludermir T.B., de Oliveira W.R. Quantum perceptron over a field and neural network architecture selection in a quantum computer // *Neural Networks*. 2016. V. 76. P. 55–64. DOI: 10.1016/j.neunet.2016.01.002

47. Lv F., Yang G., Yang W., Zhang X., Li K. The convergence and termination criterion of quantum-inspired evolutionary neural networks // *Neurocomputing*. 2017. V. 238. P. 157–167. DOI: 10.1016/j.neucom.2017.01.048

48. Panchi L.I., Zhao Y. Model and algorithm of sequence-based quantum-inspired neural networks // *Chinese Journal of Electronics*. 2018. V. 27. Iss. 1. P. 9–18. DOI: 10.1049/cje.2017.11.007

49. Ganjefar S., Tofighi M. Optimization of quantum-inspired neural network using memetic algorithm for function approximation and chaotic time series prediction // *Neurocomputing*. 2018. V. 291. P. 175–186. DOI: 10.1016/j.neucom.2018.02.074

50. Ganjefar S., Tofighi M. Training qubit neural network with hybrid genetic algorithm and gradient descent for indirect adaptive controller design // *Engineering Applications of Artificial Intelligence*. 2017. V. 65. P. 346–360. DOI: 10.1016/j.engappai.2017.08.007

51. Ueguchi T., Matsui N., Isokawa T. Chaotic time series prediction by qubit neural network with complex-valued representation // 2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE). Tsukuba; Japan; September 20-23, 2016. Article No. 7749232. P. 1353–1358. DOI: 10.1109/SICE.2016.7749232

52. Romero J., Olson, J.P., Aspuru-Guzik A. Quantum autoencoders for efficient compression of quantum data // *Quantum Science and Technology*. 2017. V. 2. Iss. 4. Article No. 045001. DOI: 10.1088/2058-9565/aa8072

53. Schuld M., Sinayskiy I., Petruccione F. An introduction to quantum machine learning //

- Contemporary Physics. 2015. V. 56. Iss. 2. P. 172–185. DOI: 10.1080/00107514.2014.964942
54. Perdomo-Ortiz A., Benedetti M., Realpe-Gómez J., Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers // Quantum Science and Technology. 2018. V. 3. Iss. 3. Article No. 030502. DOI: 10.1088/2058-9565/aab859
55. Rebentrost P., Mohseni M., Lloyd S. Quantum support vector machine for big data classification // Phys. Rev. Lett. 2014. V. 113. Iss. 3. Article No. 130503. DOI: 10.1103/PhysRevLett.113.130503
56. Lloyd S., Mohseni M., Rebentrost P. Quantum principal component analysis // Nature Physics. 2014. V. 10. Iss. 9. P. 631–633. DOI: 10.1038/NPHYS3029
57. Alvarez-Rodriguez U., Lamata L., Escandell-Montero P., Martín-Guerrero J.D., Solano E. Supervised quantum learning without measurements // Scientific Reports. 2017. V. 7. Iss. 1. Article No. 13645. DOI: 10.1038/s41598-017-13378-0
58. Schuld M., Sinayskiy I., Petruccione F. Prediction by linear regression on a quantum computer // Phys. Rev. A. 2016. V. 94. Iss. 2. Article No. 022342. DOI: 10.1103/PhysRevA.94.022342
59. Benedetti M., Realpe-Gómez J., Biswas R., Perdomo-Ortiz A. Quantum-assisted learning of hardware-embedded probabilistic graphical models // Phys. Rev. X. 2017. V. 7. Iss. 4. Article No. 041052. DOI: 10.1103/PhysRevX.7.041052
60. Wittek P., Gogolin C. Quantum enhanced inference in Markov logic networks // Scientific Reports. 2017. V. 7. Article No. 45672. DOI: 10.1038/srep45672
61. Potok T.E., Schuman C.D., Young S.R., Patton R.M., Spedalieri F., Liu J., Yao K.-T., Rose G., Chakma G. A study of complex deep learning networks on high performance, neuromorphic, and quantum computers // 2016 2nd Workshop on Machine Learning in HPC Environments (MLHPC). Salt Lake City, Utah, USA, 2016. P. 47–55. DOI: 10.1109/MLHPC.2016.009
62. Aerts D., Broekaert J., Gabora L., Sozzo S. Quantum structures in cognitive and social science (Editorial) // Front. Psychol. 2016. V. 7. Iss. APR. Article No. 577. DOI: 10.3389/fpsyg.2016.00577
63. Aerts D., Sozzo S., Veloz T. Quantum structure of negation and conjunction in human thought // Front. Psychol. 2015. V. 6. Article No. 1447. DOI: 10.3389/fpsyg.2015.01447
64. Aerts D., Sozzo S. Quantum entanglement in conceptual combinations // Int. J. Theor. Phys. 2014. V. 53. P. 3587–3603. DOI: 10.1007/s10773-013-1946-z
65. Khrennikov A. Quantum-like model of unconscious–conscious dynamics // Front. Psychol. 2015. V. 6. Article No. 997. DOI: 10.3389/fpsyg.2015.00997
66. Bisconti C., Corallo A., Fortunato L., Gentile A.A., Massafra A., Pellè P. Reconstruction of a real world social network using the Potts model and loopy belief propagation // Front. Psychol. 2015. V. 6. Article No. 1698. DOI: 10.3389/fpsyg.2015.01698

References:

1. The report of the Digital McKinsey expert group “Digital Russia: a new reality”. 2017. 122 p. URL: <http://www.mckinsey.com/global-locations/europe-andmiddleeast/russia/ru/our-work/mckinsey-digital> (Access date 01/15/2019). (in Russ.)
2. The program “Digital economy of the Russian Federation”, approved by Decree No. 1632-p of the Government of the Russian Federation of July 28, 2017. (in Russ.)

3. The program "On the strategy for the information society development in the Russian Federation for 2017-2030", approved by the Decree of the President of the Russian Federation dated May 9, 2017. No. 203. (in Russ.)
4. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years. *Nature*. 2017; 543(7644): 171-174. DOI: 10.1038/543171a
5. Grenshtein S. A new study by the Association of the semiconductor industry: "After 5 years, Moore's law will cease to operate". URL: <https://habr.com/post/307158/> (Access date 01/15/2019) (in Russ.)
6. Levchaev P.A. The digital economy as the future of our lives. *Russian Journal of Management*. 2017; 5(4): 515-523. URL: https://doi.org/10.29039/article_5a5df35550f2d6.65514969
7. Karasev S. Head of Intel: On relations with Apple, Moore's law, new devices and materials. *Electronic media "3DNews"*. URL: <https://3dnews.ru/about> (Access date 01/15/2019). (in Russ.)
8. Humble T. Consumer applications of quantum computing: A promising approach for secure computation, trusted data storage, and efficient applications. *IEEE Consumer Electronics Magazine*. 2018; 7(6): 8-14. DOI: 10.1109/MCE.2017.2755298
9. Kulik S.D., Berkov A.V., Yakovlev V.P. Introduction to the theory of quantum computation (methods of quantum mechanics in cybernetics): in 2 books. Book 1. Moscow: MEPhI Publ., 2008. 212 p. (in Russ.)
10. Quantum computing for the curious. URL: <https://cloudcoin.ru/quantum-computing> (Access date 01/15/2019). (in Russ.)
11. Quantum computer and quantum communication. URL: <http://www.tadviser.ru/index.php> (Access date 01/15/2019). (in Russ.)
12. Foundation for Advanced Studies. URL: https://fpi.gov.ru/press/media/jekspert_mnogokubitniy_kvantoviy_kompyuter_mozhno_sozdaty_v_rossii_za_god (Access date 01/15/2019). (in Russ.)
13. Debnath S., Linke N.M., Figgatt C., Landsman K.A., Wright K., Monroe C. Demonstration of a small programmable quantum computer with atomic qubits. *Nature*. 2016; 536(7614): 63-66. DOI: 10.1038/nature18648
14. Linke N.M., Maslov D., Roetteler M., Debnath S., Figgatt C., Landsman K.A., Wright K., Monroe C. Experimental comparison of two quantum computing architectures. *Proc. Natl. Acad. Sci. U.S.A.* 2017; 114(13): 3305-3310. DOI: 10.1073/pnas.1618020114
15. Britt K.A., Humble T.S. High-performance computing with quantum processing units. *ACM Journal on Emerging Technologies in Computing Systems*. 2017; 13(3): Article No. 39. DOI: 10.1145/3007651
16. Sapaev D., Bulychikov D. Quantum computing versus classical: Why do we need so many digits. URL: <https://habr.com/company/sberbank/blog/343308/> (Access date 01/15/2019). (in Russ.)
17. Sapaev D., Bulychikov D. Quantum calculations: Annealing with switches and other fun. URL: <https://habr.com/company/sberbank/blog/344830/> (Access date 01/15/2019) (in Russ.)
18. List of quantum algorithms. URL: <https://math.nist.gov/quantum/zoo/> (Access date 01/15/2019). (in Russ.)

19. Dumas J.P., Soni K., Rasool A. An introduction to quantum search algorithm and its implementation. In: Balas V., Sharma N., Chakrabarti A. (eds) *Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing*. 2019; 808: 19-31. Springer, Singapore. DOI: 10.1007/978-981-13-1402-5_2
20. Wang G. Quantum algorithm for linear regression. *Phys. Rev. A*. 2017; 96(1): Article No. 012335. DOI: 10.1103/PhysRevA.96.012335
21. Kliuchnikov V., Maslov D., Mosca M. Practical approximation of single-qubit unitaries by single-qubit quantum Clifford and T circuits. *IEEE Trans. Comp.* 2016; 65(1): 161-172. Article No. 7056491. DOI: 10.1109/TC.2015.2409842
22. Selinger P. Efficient Clifford+T approximation of single-qubit operators. *Quantum Information and Computation*. 2014; 15(1-2): 159-180.
23. Bocharov, A., Roetteler M., Svore K.M. Efficient synthesis of probabilistic quantum circuits with fallback. *Phys. Rev. A. Atomic, Molecular, and Optical Physics*. 2015; 91(5): Article No. 052317. DOI: 10.1103/PhysRevA.91.052317
24. Palsson M.S., Gu, M., Ho J., Wiseman H.M., Pryde G.J. Experimentally modeling stochastic processes with less memory by the use of a quantum processor. *Science Advances*. 2017; 3(2): Article No. e1601302. DOI: 10.1126/sciadv.1601302
25. Stolyarov A. Quantum computing and smart spaces can change the storage market. URL: http://safe.cnews.ru/news/top/2018-11-14_kvantovye_vychisleniya_i_umnye_prostranstva_mogut (Access date 01/15/2019). (in Russ.)
26. Fitzsimons J.F., Kashefi E. Unconditionally verifiable blind quantum computation. *Phys. Rev. A*. 2017; 96(1): Article No. 012303. DOI: 10.1103/PhysRevA.96.012303
27. Roetteler M., Svore K.M. Quantum computing: Codebreaking and beyond. *IEEE Security and Privacy*. 2018; 16(5): 22-36. Article No. 8490171. DOI: 10.1109/MSP.2018.3761710
28. Pirandola S., Ottaviani C., Spedalieri G., Weedbrook C., Braunstein S.L., Lloyd S., Gehring T., Jacobsen C.S., Andersen U.L. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*. 2015; 9(6): 397-402. DOI: 10.1038/nphoton.2015.83
29. Grassl M., Langenberg B., Roetteler M., Steinwandt R. Applying Grover's algorithm to AES: Quantum resource estimates. *Lecture Notes in Computer Science*. 2016; 9606: 29-43. 7th Int. Workshop on Post-Quantum Cryptography, PQ Crypto 2016; Fukuoka; Japan; February 24-26, 2016; code 164489. DOI: 10.1007/978-3-319-29360-8_3
30. Roetteler M., Steinwandt R. A note on quantum related-key attacks. *Information Processing Lett.* 2015; 115(1): 40-44. DOI: 10.1016/j.ipl.2014.08.009
31. Walenta N., Burg, A., Caselunghe D., Constantin J., Gisin N., Guinnard O., Houlmann R., Junod, P., Korzh B., Kulesz, N., Legré M., Lim C.W., Lunghi T., Monat L., Portmann C., Soucarros M., Thew R.T., Trinkler P., Trollet G., Vannel F., Zbinden H. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New Journal of Physics*. 2014; 16: Article No. 013047. DOI: 10.1088/1367-2630/16/1/013047
32. Shibata H., Honjo T., Shimizu K. Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors. *Optics Lett.* 2014; 39(17): 5078-5081. DOI: 10.1364/OL.39.005078
33. Xu F., Xu H., Lo H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A. Atomic, Molecular,*

and *Optical Physics*. 2014; 89(5): Article No. 052333. DOI: 10.1103/PhysRevA.89.052333

34. Curty M., Xu F., Cui W., Lim C.C.W., Tamaki K., Lo H.-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Commun.* 2014; 5: Article No. 3732. DOI: 10.1038/ncomms4732

35. Tang Z., Liao Z., Xu F., Qi B., Qian L., Lo H.-K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 2014; 112(19): Article No. 190503. DOI: 10.1103/PhysRevLett.112.190503

36. Yu Z.-W., Zhou Y.-H., Wang X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A. Atomic, Molecular, and Optical Physics*. 2015; 91(3): Article No. 032318. DOI: 10.1103/PhysRevA.91.032318

37. Wang C., Song X.-T., Yin Z.-Q., Wang S., Chen W., Zhang C.-M., Guo G.-C., Han Z.-F. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* 2015; 115(16): Article No. 160502. DOI: 10.1103/PhysRevLett.115.160502

38. Comandar L.C., Lucamarini M., Fröhlich B., Dynes J.F., Sharpe A.W., Tam S.W.-B., Yuan Z.L., Penty R.V., Shields A.J. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics*. 2016; 10(5): 312-315. DOI: 10.1038/nphoton.2016.50

39. Yin H.-L., Chen T.-Y., Yu Z.-W., Liu H., You L.-X., Zhou Y.-H., Chen S.-J., Mao Y., Huang M.-Q., Zhang W.-J., Chen H., Li M.J., Nolan D., Zhou, F., Jiang X., Wang Z., Zhang Q., Wan X.-B., Pan J.-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* 2016; 117(19): Article No. 190501. DOI: 10.1103/PhysRevLett.117.190501

40. Chen D., Wei L., YaLiang C., Qing P., Lei S. Reference-frame-independent measurement-device-independent quantum key distribution using hybrid logical basis. *Quantum Information Processing*. 2018; 17(10): Article No. 256. DOI: 10.1007/s11128-018-2030-7

41. Musser G. Job one for quantum computers: Boost artificial intelligence. *Quanta Magazine*. URL: <https://www.quantamagazine.org/job-one-for-quantum-computers-boost-artificial-intelligence-20180129/> (Access date 01/15/2019).

42. Altayskiy M.V., Kapustina N.E., Krylov V.A. Quantum neural networks: Current state and development prospects. *Fizika elementarnykh chastits i atomnogo yadra* (Physics of Elementary Particles and Atomic Nucleus). 2014; 45(5-6): 1825-1856. (in Russ.)

43. Haykin S. Neural Networks. Pearson Education. NY: IEEE, 1999. 600 p.

44. Schuld M., Sinayskiy I., Petruccione F. The quest for a quantum neural network. *Quantum Information Processing*. 2014; 13(11): 2567-2586. DOI: 10.1007/s11128-014-0809-8

45. Qi F., Chen C. Qubit neural tree network with applications in nonlinear system modeling. *IEEE Access*. 2018; 6: 51598-51606. Article No. 8463464. DOI: 10.1109/ACCESS.2018.2869894

46. da Silva A.J., Ludermir T.B., de Oliveira W.R. Quantum perceptron over a field and neural network architecture selection in a quantum computer. *Neural Networks*, 2016; 76: 55-64. DOI: 10.1016/j.neunet.2016.01.002

47. Lv F., Yang G., Yang W., Zhang X., Li K. The convergence and termination criterion of quantum-inspired evolutionary neural networks. *Neurocomputing*. 2017; 238: 157-167.

DOI: 10.1016/j.neucom.2017.01.048

48. Panchi L.I., Zhao Y. Model and algorithm of sequence-based quantum-inspired neural networks. *Chinese Journal of Electronics*. 2018; 27(1): 9-18. DOI: 10.1049/cje.2017.11.007

49. Ganjefar S., Tofighi M. Optimization of quantum-inspired neural network using memetic algorithm for function approximation and chaotic time series prediction. *Neurocomputing*. 2018; 291: 175-186. DOI: 10.1016/j.neucom.2018.02.074

50. Ganjefar S., Tofighi M. Training qubit neural network with hybrid genetic algorithm and gradient descent for indirect adaptive controller design. *Engineering Applications of Artificial Intelligence*. 2017; 65(10): 346-360. DOI: 10.1016/j.engappai.2017.08.007

51. Ueguchi T., Matsui N., Isokawa T. Chaotic time series prediction by qubit neural network with complex-valued representation. 2016 *55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*. Tsukuba; Japan; September 20-23, 2016. Article No. 7749232. P. 1353–1358. DOI: 10.1109/SICE.2016.7749232

52. Romero J., Olson J.P., Aspuru-Guzik A. Quantum autoencoders for efficient compression of quantum data. *Quantum Science and Technology*. 2017; 2(4): Article No. 045001. DOI: 10.1088/2058-9565/aa8072

53. Schuld M., Sinayskiy I., Petruccione F. An introduction to quantum machine learning. *Contemporary Physics*. 2015; 56(2): 172-185. DOI: 10.1080/00107514.2014.964942

54. Perdomo-Ortiz A., Benedetti M., Realpe-Gómez J., Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers. *Quantum Science and Technology*. 2018; 3(3): Article No. 030502. DOI: 10.1088/2058-9565/aab859

55. Rebentrost P., Mohseni M., Lloyd S. Quantum support vector machine for big data classification. *Phys. Rev. Lett.* 2014; 113(3): Article No. 130503. DOI: 10.1103/PhysRevLett.113.130503/

56. Lloyd S., Mohseni M., Rebentrost P. Quantum principal component analysis. *Nature Physics*. 2014; 10(9): 631-633. DOI: 10.1038/NPHYS3029

57. Alvarez-Rodriguez U., Lamata L., Escandell-Montero P., Martín-Guerrero J.D., Solano E. Supervised quantum learning without measurements. *Scientific Reports*. 2017; 7(1): Article No. 13645. DOI: 10.1038/s41598-017-13378-0

58. Schuld M., Sinayskiy I., Petruccione F. Prediction by linear regression on a quantum computer. *Phys. Rev. A*. 2016; 94(2): Article No. 022342. DOI: 10.1103/PhysRevA.94.022342

59. Benedetti M., Realpe-Gómez J., Biswas R., Perdomo-Ortiz A. Quantum-assisted learning of hardware-embedded probabilistic graphical models. *Phys. Rev. X*. 2017; 7(4): Article No. 041052. DOI: 10.1103/PhysRevX.7.041052

60. Wittek P., Gogolin C. Quantum enhanced inference in Markov logic networks. *Scientific Reports*. 2017; 7: Article No. 45672. DOI: 10.1038/srep45672

61. Potok T.E., Schuman C.D., Young S.R., Patton R.M., Spedalieri F., Liu J., Yao K.-T., Rose G., Chakma G. A study of complex deep learning networks on high performance, neuromorphic, and quantum computers. 2016 *2nd Workshop on Machine Learning in HPC Environments (MLHPC)*, Salt Lake City, Utah, USA, 2016: 47-55. doi:10.1109/MLHPC.2016.009

62. Aerts D., Broekaert J., Gabora L., Sozzo S. Quantum structures in cognitive and social science (Editorial). *Front. Psychol.* 2016; 7(APR): Article No. 577. DOI: 10.3389/fpsyg.2016.00577

63. Aerts D., Sozzo S., Veloz T. Quantum structure of negation and conjunction in human thought. *Front. Psychol.* 2015; 6: Article No. 1447. DOI: 10.3389/fpsyg.2015.01447
64. Aerts D., Sozzo S. Quantum entanglement in conceptual combinations. *Int. J. Theor. Phys.* 2014; 53: 3587-3603. DOI: 10.1007/s10773-013-1946-z
65. Khrennikov A. Quantum-like model of unconscious-conscious dynamics. *Front. Psychol.* 2015; 6: Article No. 997. DOI: 10.3389/fpsyg.2015.00997
66. Bisconti C., Corallo A., Fortunato L., Gentile A.A., Massafra A., Pellè P. Reconstruction of a real world social network using the Potts model and loopy belief propagation. *Front. Psychol.* 2015; 6: Article No. 1698. DOI: 10.3389/fpsyg.2015.01698

Об авторах:

Сигов Александр Сергеевич, доктор физико-математических наук, академик РАН, президент ФГБОУ ВО «МИРЭА – Российский технологический университет», заведующий кафедрой наноэлектроники Физико-технологического института ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Андрианова Елена Гельевна, кандидат технических наук, доцент, доцент кафедры корпоративных информационных систем Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Жуков Дмитрий Олегович, доктор технических наук, профессор, профессор кафедры информационного противоборства Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Зыков Сергей Викторович, доктор технических наук, доцент, профессор Департамента программной инженерии факультета компьютерных наук Национального исследовательского университета «Высшая школа экономики» (101000, Россия, г. Москва, ул. Мясницкая, д. 20).

Тарасов Илья Евгеньевич, доктор технических наук, профессор, профессор кафедры корпоративных информационных систем Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Alexander S. Sigov, D.Sc. (Physics and Mathematics), Academician of RAS, President of MIREA – Russian Technological University; Head of the Chair of Nanoelectronics, Physics and Technology Institute, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Elena G. Andrianova, Ph.D. (Engineering), Docent, Associate Professor of the Chair of Corporate Information Systems, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Dmitriy O. Zhukov, D.Sc. (Engineering), Professor, Professor of the Chair of Information Confrontation, Institute of Integrated Security and Special Instrument Engineering, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Sergey V. Zykov, D.Sc. (Engineering), Associate Professor, Professor of the Department of Software Engineering, Faculty of Computer Science, National Research University “Higher School of Economics” (20, Myasnitskaya st., Moscow, 101000, Russia).

Ilya E. Tarasov, D.Sc. (Engineering), Professor, Professor of the Chair of Corporate Information Systems, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454, Russia).

Для цитирования: Сигов А.С., Андрианова Е.Г., Жуков Д.О., Зыков С.В., Тарасов И.Е. Квантовая информатика: обзор основных достижений // Российский технологический журнал. 2019. Т. 7. № 1. С. 5–37. DOI: 10.32362/2500-316X-2019-7-1-5-37

For citation: Sigov A.S., Andrianova E.G., Zhukov D.O., Zykov S.V., Tarasov I.E. Quantum informatics: Overview of the main achievements. *Rossiyskiy tekhnologicheskiy zhurnal* (Russian Technological Journal). 2019; 7(1): 5-37. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-5-37

ОЦЕНКА КАЧЕСТВА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА НА ОСНОВЕ МЕНТАЛЬНОГО ВРЕМЕНИ ВЫПОЛНЕНИЯ ПОЛЬЗОВАТЕЛЬСКИХ ЗАДАЧ ПРЕДМЕТНОЙ ОБЛАСТИ

**В.К. Григорьев[@],
А.С. Илюшечкин,
М.А. Овчинников**

МИРЭА – Российский технологический университет, Москва 119454, Россия

[@]Автор для переписки, e-mail: grigoriev@mirea.ru

Общее развитие информационных систем и их постоянно возрастающее влияние на все сферы развития общества определяет большую значимость пользовательских интерфейсов. Качество и адекватность интерфейса задачам предметной области становится определяющим параметром выбора программного продукта для компьютерной поддержки работы конкретной организации. Исследованием пользовательских интерфейсов занимаются с 70-х годов прошлого века. Некоторые методы исследования качества интерфейса, в частности, метод GOMS используется до настоящего времени. Однако применение технологии опережающего обучения массовых профессиональных пользователей информационных систем позволяет эффективно оценить интерфейс в процессе обучения, не применяя метод GOMS.

В настоящей статье рассматривается методика количественной оценки качества пользовательского интерфейса в виде таких характеристик, как ошибки и ментальное время выполнения задач предметной области. Анализируется структура времени выполнения задач предметной области. Выделяется ментальное время как характеристика, наибольшим образом определяющая удобство работы с пользовательским интерфейсом. Ментальное время строится на основе полного времени шага, времени вычислений на этом шаге и механического времени, необходимого для совершения человеком действия, вызывающего выполнение этого шага. Показывается, что использование технологии опережающего обучения массового профессионального пользователя позволяет существенным образом упростить выделение ментального времени путем исключения времени выполнения задачи вычислительной машиной. В структуре времени существенное значение имеет механическое время, необходимое для совершения человеком действия, вызывающего выполнение шага. В методе GOMS для оценки механического времени используются некоторые стандартные численные характеристики, однако в работе выдвигается гипотеза и экспериментально показывается, что в качестве механического времени можно использовать статистически значимое минимальное время выполнения действий. Данная гипотеза подтверждена экспериментально. Разработанная методика оценки качества интерфейса может быть использована при переобучении пользователей в процессе перехода организаций на отечественное программное обеспечение.

Ключевые слова: опережающее обучение, пользовательский интерфейс, массовый профессиональный пользователь, качество интерфейса, качество обучения, метод GOMS.

QUALITY ASSESSMENT OF A USER INTERFACE BASED ON THE MENTAL TIME OF PERFORMING THE USER TASKS OF THE SUBJECT AREA

V.K. Grigoriev@,
A.S. Ilyushechkin,
M.A. Ovchinnikov

MIREA – Russian Technological University, Moscow 119454, Russia

@Corresponding author e-mail: grigoriev@mirea.ru

The overall development of information systems and their increasingly significant impact on all areas of the society expressed in such terms as "information society", etc., determines the increasing importance of user interfaces. Moreover, the quality and adequacy of the interface to the tasks of the subject area becomes the determining parameter when choosing a specific organization software product for computer support of the organization. The study of user interfaces involved with the 70s of the last century. Some methods of interface quality research, in particular, the GOMS method is used to date. However, the use of advanced training technology for mass professional users of information systems for the study of interfaces allows to effectively evaluate the interface in the learning process without using the GOMS method. This article is devoted to this issue.

The article deals with the method of quantitative evaluation of the quality of the user interface in the form of such characteristics as errors and mental time of the tasks of the subject area. The structure of time of performing tasks of the subject area is analyzed. Mental time is allocated as the characteristic that chiefly determines the usability of the user interface. Mental time is based on the total time of the step, the calculation time at this step, and the mechanical time required for a person to perform an action that causes the step to be performed. It is shown that the use of anticipated training technology of mass professional user can significantly simplify the allocation of mental time by eliminating the time of the task computer. In the structure of time, the mechanical time required for a person to perform an action that causes the step to be performed is essential. In the GOMS method some standard numerical characteristics are used to estimate mechanical time. However, a hypothesis is put forward, and it is experimentally shown that a statistically significant minimum time for performing actions can be used as mechanical time. This hypothesis was experimentally confirmed. The method and results of this experiment are presented in the article.

Developed on this basis, the methodology for assessing the quality of the interface can be used when retraining users in the process of transition of organizations to domestic software in order to evaluate the interfaces.

Keywords: anticipated training, user interface, mass professional user, interface quality, training quality, GOMS method.

Введение

Современное общество можно назвать информационным обществом [1]. И для этого есть все основания: действительно, всё большее количество людей в той или иной степени становятся пользователями программных продуктов [2]. Выделим из общего массива пользователей класс профессиональных пользователей – служащих государственных органов (федеральных, региональных, муниципальных), тем более, что в связи

с программой перехода на отечественное программное обеспечение (ПО) этот класс претерпевает существенные новации в своей текущей работе. Основной тип пользователей, затрагиваемый при переходе на российское ПО, можно отнести к массовому профессиональному пользователю (МПП) [3]. Переход на российское ПО большого количества организаций с огромным числом профессиональных пользователей за полтора-два года порождает целый комплекс организационно-технических и психолого-педагогических задач.

Остановимся на двух из них:

1. Переобучение большого количества пользователей;
2. Выбор конкретной организацией программного продукта из предлагаемых отечественных программных продуктов.

Решение первой задачи требует переучивания и сертификации большого количества пользователей для работы с новым интерфейсом [4], и оно возможно с высокой эффективностью на основе технологии электронного опережающего обучения [5].

Методика технологии электронного опережающего обучения заключается в следующих процессах. На основе описания функциональных обязанностей МПП и инструкций пользователя создается сценарий деятельного обучения в виде последовательности ситуаций и заданий по их разрешению с помощью программного продукта. Далее проводится выполнение заданий этого сценария на версии программного продукта. Каждое задание может состоять из одного или нескольких шагов. В процессе выполнения задания на каждом шаге с помощью специального авторского ПО «Захватчик» проводится запись образа экрана и триггера, вызвавшего переход к следующему шагу. Далее из последовательности экранов и триггеров создается эквивалентная (в смысле Крипке) модель программного продукта, на основе которой строится обучающая программа. После реализации сценария в виде обучающей программы по сети организации осуществляется тиражирование (для любого количества пользователей) и распространение (простое и быстрое) обучающей программы. Оно обеспечивает обучение и сертификацию практически неограниченного числа пользователей с помощью обучающей программы. В процессе обучения собираются данные о выполнении j -ым пользователем i -ого шага обучающей программы: время прохождения шага T_{ij} , количество ошибок во время прохождения шага Q_{ij} .

С целью решения второй задачи организациям с большим количеством пользователей необходимо выбрать программный продукт из единого реестра российских программ для электронных вычислительных машин и баз данных – для замены импортного программного продукта. Вероятнее всего, одним из наиболее важных параметров, которые влияют на процесс выбора программного обеспечения, будет качество пользовательского интерфейса. Таким образом, оценка качества пользовательского интерфейса является актуальной задачей.

Модификация способа оценки элементов интерфейса, базирующаяся на технологии опережающего деятельного ситуационного обучения пользователей

Проблемами оценки качества пользовательского интерфейса разработчики занимаются фактически с появления первых программ и до настоящего времени [6–8]. В большинстве случаев используются методы субъективной, качественной оценки, а именно, метод фокус-групп, прототипирование, анализ задач, экспертная оценка [9, 10]. Наиболее

распространенными эргономическими показателями качества пользовательского интерфейса являются показатели Шнейдермана [11]:

- 1) скорость работы пользователя;
- 2) количество человеческих ошибок;
- 3) субъективная удовлетворенность;
- 4) скорость обучения навыкам оперирования интерфейсом.

Третий из этих показателей относится к субъективным и качественным, а первый, второй и четвертый могут быть оценены количественно. Скорость работы пользователя представляет собой время, которое пользователь затрачивает на выполнение задания предметной области. Чтобы описать процесс выполнения задания, сформулируем следующий алгоритм работы пользователя [12]:

1. Среди действий, выполняющих это задание, необходимо выделить действия, которые проводятся через пользовательский интерфейс программного продукта.
2. Выделить в пользовательском интерфейсе данные, относящиеся к текущему заданию.
3. Сформулировать действия, проводимые через пользовательский интерфейс, в виде последовательности шагов.
4. Выполнить последовательность шагов задания в пользовательском интерфейсе.
5. Дождаться и получить результат выполнения последовательности шагов задания компьютером.
6. Переформулировать полученный результат в терминах предметной области.
7. Перейти к выполнению следующего задания.

Из алгоритма работы пользователя видно, что пункты 1, 6, 7 относятся к предметной области, пункты 2, 3 – описание всего задания, которое может состоять из нескольких шагов, пункты 4, 5 относятся к последовательному выполнению отдельных шагов задания в пользовательском интерфейсе.

В общем случае всё время T выполнения задания, состоящего из n шагов, можно разделить на следующие составляющие:

1. Время на обдумывание выполнения задания в терминах предметной области обозначим $T^{обдум.}$.
2. Время на восприятие текущего содержимого экрана (ментальное) на i -ом шаге выполнения задания обозначим $T_i^{воспр.}$.
3. Время на выделение действия, необходимого на i -ом шаге, обозначим $T_i^{выд.}$.
4. Механическое время – время, затрачиваемое на ввод i -го шага через пользовательский интерфейс, обозначим $T_i^{мех.}$.
5. Время выполнения i -го шага в программном продукте обозначим $T_i^{выполн.}$. Это время существенным образом зависит от мощности и нагрузки компьютера и может существенно превышать время работы в интерфейсе, то есть оно не стабильно.
6. Время, затрачиваемое на интерпретацию полученных результатов выполнения n шагов задания, обозначим $T^{интерпр.}$.

Представим T в виде формулы:

$$T = T^{обдум.} + \sum_{i=0}^n T_i^{воспр.} + \sum_{i=0}^n T_i^{выд.} + \sum_{i=0}^n T_i^{мех.} + \sum_{i=0}^n T_i^{выполн.} + T^{интерпр.} \quad (1)$$

Анализируя (1), приходим к выводу, что ко времени отдельного шага относится время восприятия, время выделения, время механическое и время выполнения. Таким образом, получаем T_i – время отдельного i -го шага, которое мы можем измерить. T_i представим в виде суммы соответствующих времен, относящихся к i -му шагу:

$$T_i = T_i^{\text{воспр.}} + T_i^{\text{выд.}} + T_i^{\text{выполн.}} + T_i^{\text{мех.}} \quad (2)$$

Выделим из (2) времена $T_i^{\text{воспр.}}$ и $T_i^{\text{выд.}}$, которые характеризуют понимание пользователем интерфейса программного продукта. В работе [10] $T_i^{\text{воспр.}} + T_i^{\text{выд.}}$ определяется как время, необходимое пользователю, чтобы умственно подготовиться к следующему шагу. Оно обозначается $T_i^{\text{мент.}}$ и называется ментальной подготовкой [13]:

$$T_i^{\text{мент.}} = T_i^{\text{воспр.}} + T_i^{\text{выд.}} \quad (3)$$

Для вычисления времени $T_i^{\text{мент.}}$ преобразуем (2) в (4):

$$T_i^{\text{мент.}} = T_i - T_i^{\text{выполн.}} - T_i^{\text{мех.}} \quad (4)$$

Время шага T_i может быть измерено в процессе обучения, а время выполнения $T_i^{\text{выполн.}}$ и механическое время $T_i^{\text{мех.}}$ необходимо оценить.

Сначала проанализируем время выполнения. Оно зависит от текущей нагрузки системы и сильно варьируется. Поэтому время выполнения рассматривают как шум, значение которого может быть больше полезного сигнала (времени работы в интерфейсе). Отсюда следует, что оценить время работы пользователя в интерфейсе очень сложно. Однако при использовании технологии опережающего обучения $T_i^{\text{выполн.}}$ пренебрежимо мало. Действительно, в обучающей программе переход к следующему шагу осуществляется путем раскрытия изображения после срабатывания триггера. Проведенный авторами анализ времени раскрытия изображения представления шага на экране показал, что на раскрытие изображения тратится меньше 0.01 с. Так как эта величина на порядок меньше чувствительности человеческого глаза, то она может не учитываться. Таким образом, использование для оценки качества интерфейса программного продукта технологии опережающего обучения существенно облегчает оценку времени работы пользователя в интерфейсе. Действительно, исходя из выражения (4), при отбрасывании времени выполнения остается необходимость определения только механического времени.

На протяжении длительного времени для решения рассматриваемой задачи применяется модель KLM-GOMS, предложенная в 1980 г. С.К. Кардом, Т.П. Мораном и А. Ньюэллом [6]. Идея метода заключается в представлении всех действий пользователя в виде некоторого набора типовых составляющих. В качестве типовых составляющих в методике KLM-GOMS получены статистические оценки времени выполнения элементарных действий:

- $K = 0.2$ с – время, необходимое для нажатия клавиши клавиатуры;
- $P = 1.1$ с – время, необходимое для перемещения указателя мыши к определенной позиции на мониторе;
- $H = 0.4$ с – время, необходимое для перемещения руки пользователя с клавиатуры на мышь.

Оценка механического времени заключается в разложении действий пользователя на элементарные составляющие и вычислении среднего времени, которое будет затрачиваться пользователем на выполнение задачи. Несмотря на то, что метод KLM-GOMS был создан давно, его модификациями пользуются до сих пор [14–16].

Нами выдвигается гипотеза, что при обучении большого количества пользователей для определения механического времени вместо метода KLM-GOMS для i -го шага целесообразно использовать $T_i^{мин.}$ – минимальное время выполнения конкретного шага множеством пользователей:

$$T_i^{мин.} = \min_j T_{ij}, \text{ где } j - \text{от } 1 \text{ до количества пользователей} \quad (5)$$

Таким образом, предлагается вместо значений параметров выполнения элементарных действий, предложенных в KLM-GOMS, использовать значения $T_i^{мин.}$, получаемые с помощью инструментального комплекса «Построитель тьюторов», поддерживающего технологию опережающего обучения. В соответствии с этой гипотезой

$$T_i^{мех.} \text{ по GOMS больше } T_i^{мин.} \text{ для всех } i. \quad (6)$$

Для подтверждения выдвинутой гипотезы проведено экспериментальное исследование: создана обучающая программа, включающая все типы элементарных действий и содержащая 38 шагов. Нами построена оценка механического времени каждого шага, выполненная в соответствии с GOMS. Группа обучающихся из 23 человек прошла обучение в соответствии с обучающей программой. В процессе обучения записывалось время выполнения каждого шага. В результате построили массив T_{ij} времен выполнения шагов. В соответствии с (5) на основе этого массива было построено $T_i^{мин.}$ – минимальное время выполнения каждого шага. Далее для каждого шага в соответствии с (6) выполнено сравнение $T_i^{мин.}$ со временем, полученным по GOMS, а именно построена разность между значением по GOMS и минимальным временем на i -ом шаге (рис. 1).

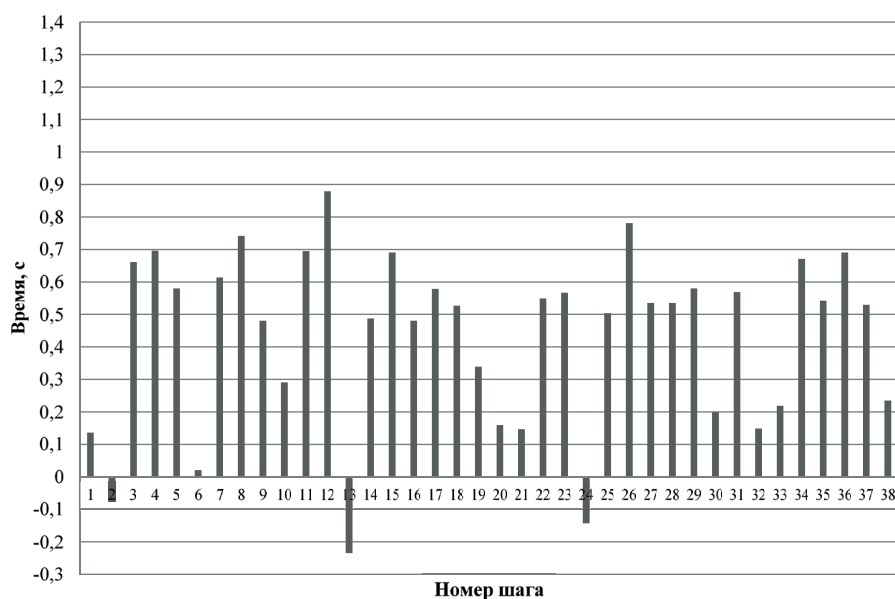


Рис. 1. Разница между временем по GOMS и минимальным временем $T_i^{мин.}$.

Из рис. 1 видно, что механическое время по KLM практически всегда больше, чем минимальное время выполнения шага. Отличия на трех шагах (2, 13, 24) объясняются тем, что на этих шагах происходит переход к следующему заданию. Для такого случая в модели GOMS выделяется 1.35 с. Отсюда получаем, что во всех случаях минимальное время меньше, чем $T_i^{мех.}$ по GOMS (рис. 2).

Следовательно, механическое время по GOMS может быть заменено самым быстрым реальным временем выполнения шага. Так подтверждается авторская гипотеза о возможности использования вместо механического времени по GOMS времени $T_i^{мин.}$, полученного при обучении.

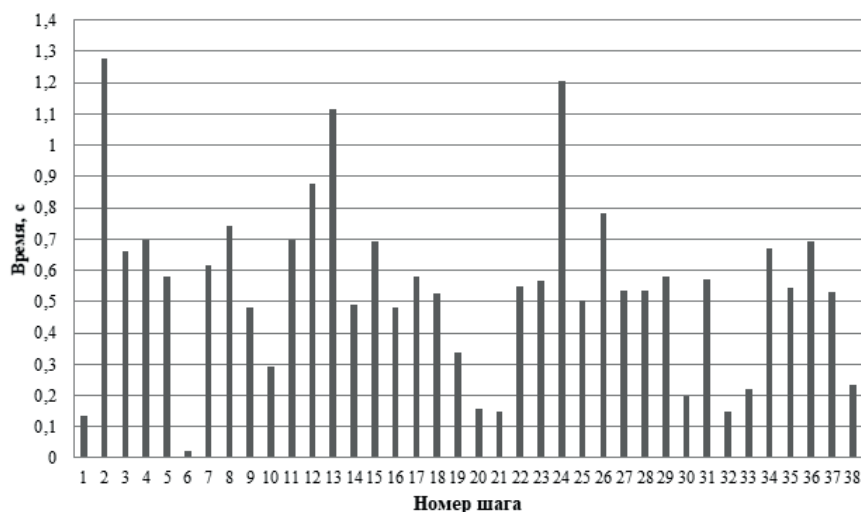


Рис. 2. Разница между GOMS с ментальным временем и минимальным временем.

Так как в выражении (4) вместо $T_i^{мех.}$ может быть использовано $T_i^{мин.}$, $T_i^{выполн.}$ игнорируется в силу своей малости в обучающей программе, а T_i замеряется в процессе обучения работе с программным продуктом. Согласно (4), мы можем строить $T_i^{мент.}$ для каждого шага, и формула (4) преобразуется в (7), которая приведена ниже:

$$T_i^{мент.} = T_i - T_i^{мин.} \quad (7)$$

Экспериментально ментальное время одного шага строят на основе статистической обработки данных обучения n пользователей. В качестве ментального времени на i -ом шаге брали T_i – среднее время при выполнении i -го шага n испытуемыми с вычетом $T_i^{мин.}$. Таким образом, в процессе ситуационного обучения n пользователей в качестве побочного результата могут быть получены ментальные времена $T_i^{мент.}$ для всех шагов в соответствии с (7) и среднее количество ошибок Q_i на каждом шаге. Для оценки и сертификации пользователя нам не столько важно время, потраченное им на конкретном шаге, сколько суммарное время выполнения задания по разрешению конкретной ситуации (состоящее из нескольких шагов) и общее время разрешения всех ситуаций сценария, а также количество ошибок, сделанных при выполнении каждого задания и при выполнении всего сценария.

Исходя из вышеизложенного можно заключить, что получена методика построения двух объективных характеристик результата обучения: скорость работы пользователя и количество человеческих ошибок.

Заключение

Показана высокая значимость интерфейса для программного продукта с большим количеством массовых профессиональных пользователей. Представлен авторский алгоритм работы МПП, как основы для анализа качества интерфейса целого класса программных продуктов (информационных систем с большим количеством МПП). Выделены количественные показатели качества интерфейса, такие, как ментальное время и количество ошибок. Показано, что использование технологии опережающего обучения дает в качестве побочного результата количественные оценки ментального времени. Важно заметить, что при использовании для обучения модели программного продукта (точной в смысле Крипке) отсутствует временная помеха в виде времени исполнения вычислительных команд. Выдвигается гипотеза о возможности замены расчета по GOMS механического времени работы с интерфейсом на минимальное время при обучении большого количества массовых профессиональных пользователей. Эта гипотеза подтверждена экспериментально. На основе гипотезы предложена методика оценки качества интерфейса программных продуктов с массовым профессиональным пользователем в процессе использования технологии опережающего обучения.

Литература:

1. Зацаринный А.А., Колин К.К. Методологические основы системного подхода к созданию информационных систем в условиях глобализации общества // Стратегические приоритеты. 2018. № 1. С. 38–61.
2. Сидоров К.В., Филатова Н.Н. Программный комплекс для мониторинга эмоционального состояния человека по электроэнцефалограммам и речевым сигналам // В сб. тр. VII Междунар. науч.-техн. конф. «Энергетика, информатика, инновации – 2017 (экономика и менеджмент, научные исследования в области физической культуры, спорта, общественных наук и лингвистики)». В 3-х т. Смоленск: Филиал ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2017. С. 252–256.
3. Григорьев В.К., Бирюкова А.А. Экспериментальное исследование комплекса для создания обучающих программ «Построитель тьюторов» // Информатизация и связь. 2016. № 4. С. 90–96
4. Филатова Н.Н., Вавилова Н.И. Вопросы проектирования мультимедиа-тренажеров // Программные продукты и системы. 2004. № 1. С. 41–49.
5. Григорьев В.К., Бирюкова А.А., Овчинников М.А. Инфраструктурная поддержка импортозамещения программного обеспечения // Открытое образование. 2018. № 3. С. 52–60.
6. Card S.K., Moran T.P., Newell A. The keystroke-level model for user performance time with interactive systems // Communications of the ACM. 1980. V. 23(7). P. 396–410.
7. Nielsen J., Molich R. Heuristic evaluation of user interfaces // Proceed. of the SIGCHI Conf. on Human Factors in Computing Systems. ACM. 1990. P. 249–256.
8. Басок Б.М., Захаров В.Н., Френкель С.Л. Об оценке чувствительности к сбоям тестов программ // Российский технологический журнал. 2016. Т. 4. № 2. С. 39–44.

9. Broy N., Lidner V., Alt F. The S3D-UI designer – Creating user interface prototypes for 3D displays // ACM Int. Conf. Proceed. Ser. 12. 15th Int. Conf. on Mobile and Ubiquitous Multimedia, MUM 2016; Rovaniemi, Finland; 12–15 December, 2016. P. 49–55. Код статьи 125832.
10. Раскин Д. Интерфейс: новые направления в проектировании компьютерных систем: Пер. с англ. СПб.: Символ-Плюс, 2007. 272 с.
11. Wilson M.L., Kules B., Schraefel M.C., Shneiderman B. From keyword search to exploration: Designing future search interfaces for the web // Foundations and Trends in Web Science. 2010. V. 2. P. 1–97.
12. Григорьев В.К., Регентов Г.А., Метод бета-тестирования, базирующийся на опережающем обучении массового профессионального пользователя // Дистанционное и виртуальное обучение. 2016. № 8 (110). С. 72–82.
13. Купер А., Рейман Р., Кронин Д., Носсел К. Интерфейс. Основы проектирования взаимодействия. СПб.: Питер, 2017. 720 с.
14. Rice A.D., Lartigue J.W. Touch-level model (TLM): Evolving KLM-GOMS for touchscreen and mobile devices // Proceed. of the 2014 ACM Southeast Regional Conference, ACM SE 2014. 28 March, 2014. Номер статьи 2638532.
15. Fernandez-Lanvin D., de Amdres-Suarez J., Gonzalez-Rodriguez M., Pariente-Martinez B. The dimension of age and gender as user model demographic factors for automatic personalization in e-commerce sites // Computer Standards and Interfaces. 2018. V. 59. P. 1–9.
16. Huang P.-H., Chiu M.-C. Integrating user centered design, universal design and goal, operation, method and selection rules to improve the usability of DAISY player for persons with visual impairments // App. Ergonomics. 2016. V. 52. P. 29–42.

References:

1. Zatsarinnyy A.A., Kolin K.K. Methodological foundations of a systems approach to creating information systems in the context of globalization societies and globalization of society. *Strategicheskiye priority* (Strategic Priorities). 2018; 1: 38-61. (in Russ.)
2. Sidorov K.V., Filatova N.N. Software package for monitoring the emotional state of a person by electroencephalogram and speech signals. In: Collection of works of the VII Int. Scientific and Technical Conf. "Energy, Informatics, Innovations – 2017 (Economics and Management, Research in the Field of Physical Culture, Sports, Social Sciences and Linguistics". In 3 volumes. Smolensk: Branch of NIU "MEI" in Smolensk, 2017: 252-256. (in Russ.)
3. Grigoriev V.K., Biryukova A.A. Experimental study of the complex to create training programs "Builder tutors". *Informatizatsiya i svyaz'* (Informatization and Communication). 2016; 4: 90-96. (in Russ.)
4. Filatova N.N., Vavilova N.I. The design of the multimedia simulators. *Programmnyye produkty i sistemy* (Software Products and Systems). 2004: 1: 41-49. (in Russ.)
5. Grigoriev V.K., Biryukova A.A., Ovchinnikov M.A. Infrastructure support for import substitution software. *Otkrytoye obrazovaniye* (Open Education). 2018; 22(3): 52-60. (in Russ.)
6. Card S.K., Moran T.P., Newell A. The keystroke-level model for user performance time with interactive systems. *Communications of the ACM*. 1980; 23(7): 396-410.
7. Nielsen J., Molich R. Heuristic evaluation of user interfaces. Proceed. of the SIGCHI Conf. on Human Factors in Computing Systems. ACM. 1990. P. 249-256.
8. Basok B.M., Zakharov V.N., Frenkel S.L. On the assessment of the sensitivity to failures

of test programs. *Rossiyskiy tekhnologicheskii zhurnal* (Russian Technological Journal). 2016; 4(2): 39-44. (in Russ.)

9. Broy N., Lidner V., Alt F. The S3D-UI designer – Creating user interface prototypes for 3D displays. ACM Int. Conf. Proceed. Ser. 12. 15th Int. Conf. on Mobile and Ubiquitous Multimedia, MUM 2016; Rovaniemi, Finland; 12–15 December, 2016. P. 49-55. Code 125832.

10. Raskin J. The Humane Interface: New Directions for Designing Interactive Systems: transl. from Engl. Saint-Petersburg: Simvol-Plyus Publ., 2007. 272 p. (in Russ.)

11. Wilson M.L., Kules B., Schraefel M.C., Shneiderman B. From keyword search to exploration: Designing future search interfaces for the web. *Foundations and Trends in Web Science*. 2010; 2: 1-97.

12. Grigoriev V.K., Regentov G.A. Beta testing method which based on mass professional user advanced training. *Distantionnoe i virtual'noe obuchenie* (Remote and Virtual Learning). 2016; 8(110): 72-82. (in Russ.)

13. Kuper A., Reyman R., Kronin D., Nossel K. Interface. The Essentials of Interaction Design. Saint-Petersburg: Piter Publ., 2017. 720 p. (in Russ.)

14. Rice A.D., Lartigue J.W. Touch-level model (TLM): Evolving KLM-GOMS for touchscreen and mobile devices. Proceed. of the 2014 ACM Southeast Regional Conference, ACM SE 2014. 28 March, 2014. Article No 2638532.

15. Fernandez-Lanvin D., de Amdres-Suarez J., Gonzalez-Rodriguez M., Pariente-Martinez B. The dimension of age and gender as user model demographic factors for automatic personalization in e-commerce sites. *Computer Standards and Interfaces*. 2018; 59: 1-9.

16. Huang P.-H., Chiu M.-C. Integrating user centered design, universal design and goal, operation, method and selection rules to improve the usability of DAISY player for persons with visual impairments. *App. Ergonomics*. 2016; 52: 29-42.

Об авторах:

Григорьев Виктор Карлович, кандидат технических наук, доцент кафедры математического обеспечения и стандартизации информационных технологий Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Илюшечкин Александр Сергеевич, магистрант кафедры математического обеспечения и стандартизации информационных технологий Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Овчинников Михаил Андреевич, магистрант кафедры математического обеспечения и стандартизации информационных технологий Института информационных технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Viktor K. Grigoriev, Ph.D. (Eng.), Associate Professor of the Chair of Mathematical Software and Standardization of Information Technology, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Alexander S. Ilyushechkin, Graduate Student of the Chair of Mathematical Software and Standardization of Information Technology, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Mikhail A. Ovchinnikov, Graduate Student of the Chair of Mathematical Software and Standardization of Information Technology, Institute of Information Technology, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Для цитирования: Григорьев В.К., Илюшечкин А.С., Овчинников М.А. Оценка качества пользовательского интерфейса на основе ментального времени выполнения пользовательских задач предметной области // Российский технологический журнал. 2019. Т. 7. № 1. С. 38–47. DOI: 10.32362/2500-316X-2019-7-1-38-47

For citation: Grigoriev V.K., Ilyushechkin A.S., Ovchinnikov M.A. Quality assessment of a user interface based on the mental time of performing the user tasks of the subject area. *Rossiyskiy tekhnologicheskii zhurnal* (Russian Technological Journal). 2019; 7(1): 38-47. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-38-47

**ANTIVIRUS SOFTWARE AND INDUSTRIAL CYBER SECURITY
SYSTEM CERTIFICATION IN RUSSIA**

**M.A. Nazarenko[@],
A.I. Gorobets,
D.V. Miskov,
V.V. Muravyev,
A.S. Novikov**

*MIREA – Russian Technological University, Moscow 119454, Russia
@Corresponding author e-mail: Nazarenko@mirea.ru*

The article is dedicated to issues in certification of antivirus software and industrial cyber security systems. It was shown that certification time in Russia is much longer than in the USA, European Union and Germany. The life time and the development time of products of this field were analyzed in the article. Each variable was specified for new products and for new versions of existing products. Some statistical methods were used in the article: Cronbach's alfa, t-statistics, and median value similarity that are typical for the articles in quality management. As a result, it was found that certification time in Russia for industrial cyber security systems is significantly longer than in other analyzed countries, up to three-fold. Product development and life time are also longer. However, the most important result is that certification in Russia adds from 32.1 to 40 percent of time to the development of a new version or a new product, correspondingly, whereas in other investigated countries these numbers are about 17 percent. Reduction of certification time will increase new product development efficiency in the field of cyber security, which will improve positions of Russian products at the international market.

Keywords: cyber security, industrial cyber security system, antivirus software, certification, Russia.

**СЕРТИФИКАЦИЯ АНТИВИРУСНОГО ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ И СИСТЕМ КИБЕРБЕЗОПАСНОСТИ
АСУ ТП В РОССИИ**

**М.А. Назаренко[@],
А.И. Горобец,
Д.В. Миськов,
В.В. Муравьев,
А.С. Новиков**

*МИРЭА – Российский технологический университет, Москва 119454, Россия
@Автор для переписки, e-mail: Nazarenko@mirea.ru*

Статья посвящена вопросам сертификации антивирусного программного обеспечения и систем промышленной кибербезопасности. Показано, что время сертификации в России промышленной системы кибербезопасности (кибербезопасности АСУ ТП) значительно больше (до трех раз), чем в США, Европейском Союзе и Германии. В статье проанализированы продукты этих отраслей по времени жизни и времени разработки. Время разработки и использования продуктов также больше. Каждая переменная представлена для новых продуктов и для новых версий существующих продуктов. В статье использованы статистические методы: Альфа Кронбаха, Т-статистика и сравнение медианных значений. Перечисленные методы нередко используются в статьях по управлению качеством. Однако самый важный результат состоит в том, что в России сертификация добавляет от 32.1 до 40% ко времени на разработку новой версии или нового продукта, соответственно, в то время как в других странах – около 17%. Сокращение сроков сертификации приведет к повышению эффективности разработки новых продуктов в области кибербезопасности, что позволит улучшить позиции российской продукции на международном рынке.

Ключевые слова: кибербезопасность, промышленная система кибербезопасности, антивирусное программное обеспечение, сертификация, Россия.

Introduction

One of the most important issues in the modern world is cybersecurity. Vast majority of population in developed countries are using different devices for work and in their everyday life. As a result, there are about 3 devices per person in the age of 12–65 years old in developed countries including Russia [1]. Each of these devices can be probably attacked. As a result, they have been secured by relevant cyber secure systems and software. In this study, antivirus software means software products for personal computers, laptops and mobile phones, including smartphones, and industrial cyber security system means cyber security software and products for industrial objects, including SCADA, DCS and PLC. Undoubtedly, both of these software products are included into one class, whereas, according to the Russian legislation, there are substantially different procedures of registration and certification for these software products.

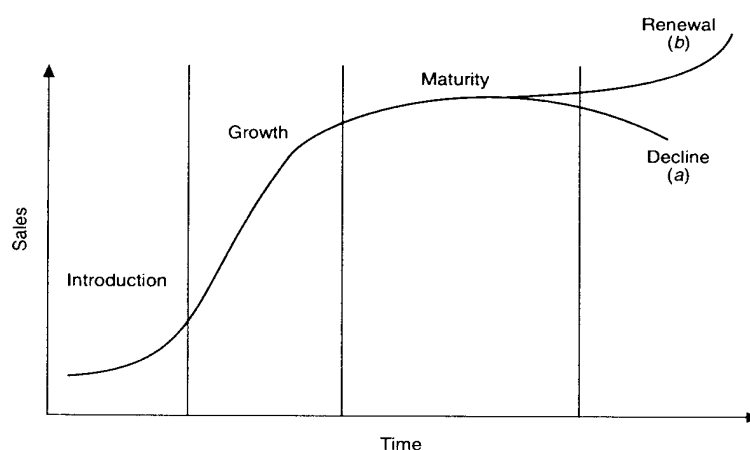
In the article, procedures of registration and certification of antivirus software and industrial cyber security systems in Russia will be analyzed. At present, a vast majority of the research in this field is dedicated to TQM accordance, including usability characteristics [2–6], specifics of this products' technical quality [7, 8], laws in this field and their meaningfulness [9–11]. Moreover, some studies in similar or close fields are dedicated to certification processes and such issues of standardization as reclamation activities [12]. In this article, studies dedicated to technical innovations, procedures and other development issues of antivirus software and industrial cyber security systems will be not covered due to the fact that they are far from standardization topicality.

In modern standardization theory, branch standards and certificates are instruments of government regulation. Usually, government certification and accreditation of IT products aims to archive several goals [13]:

- market regulation;
- consumers defense;

- risk minimization;
- social losses minimization;
- providing of key industries stable functioning.

Government certification is applied in key fields of public and scientific development. Cyber security is definitely one of them. Usually, certification and standardization are based on technical characteristics, applied methods, types of tasks and potential customers groups. Moreover, certification time is interdependent with the development cycle and life period of the product. In IT field it is usually dependent on several issues [13]. The first of them is information product update and new version presenting. Ordinary product life cycle includes introduction, growth, maturity and decline. However, an IT product with new versions and updates has the possibility of renewal (Fig.). Thus, certification should be significantly shorter in time than product life time. They should be more or less equal to the product introduction time. The second issue is time for new version development. Certification time should be significantly less than time required for developing a new version of the product [18].



IT product life cycle.

Antivirus software and industrial cyber security systems are similar in kind. Therefore, it is reasonable to assume that their certification and standardization should be similar too. However, certification of antivirus software and industrial cyber security systems have significant differences in Russia.

The aim of the article is to analyze the consistency of certification procedures for antivirus software and industrial cyber security systems with life time and development cycle of these products. It is assumed that current certification time in Russia is not efficient and leads to market failures. Therefore, optimization and reduction of certification time can increase the efficiency of antivirus software and industrial cyber security systems.

Methods

The article compares development time for antivirus software and industrial cyber security systems, including the development of new versions of the products, with time for their certification. For valuable comparison, data from certification organizations of several countries are provided. The data cover time for discussible products certification. Moreover, information about product life time and development time is presented. The data are analyzed with the help

of several statistical methods typical for this research field [14]:

- Cronbach's alfa – for data internal reliability analysis;
- t-statistics – for data stability estimation;
- median value similarity.

Data about certification time are based on open information of national certification agencies, including Federal Service for Technical and Export Control (Russia), National Institute of Standards and Technology (USA), Cyber and Information Security (EU), Federal Office for Information Security (Germany).

Results

First of all, it is important to underline that antivirus software and industrial cyber security system certification are regulated differently in Russia. Antivirus software has no government certification. However, the industrial cyber security system has extremely strong standards. Whereas, in other countries, especially, in the USA, the difference between these two IT products is significantly less. In foreign countries the basic of regulation in this field is licensing and patterns. In Russia the key difference is the object of the defense. In foreign countries responsibility for the choice of industrial cyber security system is on the customer [9]. However, the government can restrict or even forbid the usage of some foreign products [10]. In Russia, the question is presented in an opposite way. Each cyber security system for an industrial object should be firstly certificated (not to be confused with licensed) by a government organization, and only then it can be purchased at the market [9]. Therefore, for providing comparable data, this study analyzes industrial cyber security system certification.

In table 1 key figures about efficiency and certification time for 4 cyber security agencies are presented: Federal Service for Technical and Export Control, National Institute of Standards and Technology, Cyber and Information Security, Federal Office for Information Security. For each agency data about average and median certification time in months, Cronbach's alfa and t-statistics are presented.

Table 1. Efficiency and certification time

Agency	New version				New product			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Federal Service for Technical and Export Control	–	–	–	–	11	–	–	11
National Institute of Standards and Technology	1.8	0.89	3.87	1.9	4	0.91	3.2	4.1
Cyber and Information Security	2.1	0.74	4.94	2.0	3.5	0.84	2.81	3.4
Federal Office for Information Security	2.0	0.92	3.52	2.2	3.7	0.9	3.15	3.4

As shown in table 1, in the USA, European Union and Germany as a separated country certification and licensing procedures take rather similar time. In contrast, in Russia there are no cases of new product version certification and just one for new product. Therefore,

no statistical calculations are available for Federal Service for Technical and Export Control. For National Institute of Standards and Technology median values are usually a little bit higher than average. It means that distribution is shifted to the right. In other words, there are cases with significantly less than average certification time, whereas vast majority of the companies are forced to face a bit longer certification time. For Cyber and information security and Federal Office for Information Security the opposite statement is true. Moreover, it is important to add that in Cyber and Information Security certification time is slightly less than in Federal Office for Information Security, whereas is National Institute of Standards and Technology certification time for new products is more for new products and less for new versions.

According to the research question, data about product life cycle and product development time should be presented (Tables 2 and 3). The presented data are based on previous studies [12, 15].

Table 2. Product life time (consumption)

Country	<i>New version</i>				<i>New product</i>			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Russia	18.5	0.71	4.32	19.0	25.1	0.68	5.48	27.8
USA	14.5	0.85	2.98	13.9	17.2	0.84	4.89	17.0
EU	15.2	0.87	5.14	14.3	18.1	0.79	4.31	18.4
Germany	14.7	0.79	3.71	14.1	17.4	0.82	5.15	17.6

Thus, according to the data in tables 2 and 3, product life cycle is significantly longer in Russia than in the USA and the European countries. It is true both for new products and new versions of existing products. For new versions the difference in life time period is about 4.9 months, and for new products even more: 10.1 months. New products here are understood to be products that have no other versions. Simultaneously, there are quite similar values for the USA, European Union and Germany. Thus, it can be concluded that Russia is far from this group of the countries in product life time.

Table 3. Product development time

Country	<i>New version</i>				<i>New product</i>			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Russia	17.2	0.67	3.98	16.9	28.1	0.78	3.33	27.9
USA	11.2	0.71	4.65	11.4	24.4	0.89	5.15	23.8
EU	11.9	0.79	4.71	11.7	26.3	0.92	4.27	25.7
Germany	13.2	0.77	4.23	12.8	25.9	0.9	5.48	25.4

Characterizing product development time, it should be highlighted that time for new product development for Russia and other countries mentioned in the research is more or less equal. In Russia it is longer than in the USA by 4.1 months (14.7%), European Union by 2.2 (7.9%) and Germany by 2.5 (9%), whereas, for new version development the difference is significantly more. For comparison, it is 5.5 months (32.5%) longer than in the USA, 5.2 months (30.8%) longer than in European Union and 4.1 months (24.3%) longer than in Germany.

For tables 1–3 all analyzed variables were stable enough according to the t-statistics and reliable enough according to the Cronbach's alfa analysis. However, reliability for foreign countries is higher than for Russia due to the fact of a bigger sample.

According to tables 1–3 data about median values can be put into one massive to compare average certification time, life time and development time for new products and new product versions. Comparison data are presented in table 4.

Table 4. Certification time, product life and development time

Country	<i>New version</i>			<i>New product</i>		
	Russia	Product life	Development life	Certification	Product life	Development life
Russia	–	19.0	16.9	11	27.8	27.9
USA	1.9	13.9	11.4	4.1	17.0	23.8
EU	2.0	14.3	11.7	3.4	18.4	25.7
Germany	2.2	14.1	12.8	3.4	17.6	25.4

The data presented in table 4 show that certification time in Russia is about 40% of product life and development time for new products. In contrast, in the USA it is about 24% and 17.2% correspondingly, in European Union – 18.5% and 13.2%, in Germany – 19.3% and 13.3%. Thus, it can be concluded that in Russia the measured variables are significantly higher than in other investigated countries.

For Russia there are no data about certification time for new product versions. However, average coefficient of difference between certification time for a new product and a new product version is 1.8. This variable can be reasonably extended for the certification process in Russia. So, certification time in Russia should be about 6.1 months. This time is 32.1% of new product version life time and 36.1% of new product version development time. For the other investigated countries the following results were calculated: for the USA 13.7% and 16.7%, respectively, for European Union 14% and 17.1%, for Germany 15.6% and 17.2%. Thus, it should be concluded that in Russia average certification time for any process of product creation in the field of industrial cyber security systems is significantly longer in absolute and relative figures than in the USA and Europe.

Discussion

In the research data on product certification time, life and development time for industrial cyber security systems were analyzed. As a result, percentage of certification time in the key process of the IT products in cyber security was found. Previous studies do not cover such kind of statistics. Instead of this they analyze procedures [4–6] and TQM in the field of cyber security [12, 15], specifics of products' technical quality [7, 8], laws in this field and their meaningfulness [9–11].

The key result of the study is that the certification process in absolute and relative measure in Russia is significantly longer than in other investigated countries. This leads to additional slowdown of the new products development in cyber security field. At present, processes of software development in this field are longer than in the USA by 6 months or 1.5 times, and certification procedures take almost 3 times more. Moreover, certification time in the USA is just about 17% of development time both for a new product version and a new product development, whereas in Russia it is 32.1 and 40%, correspondingly.

Conclusion

Both antivirus software and industrial cyber security systems are important for Russia development and security as a country. Moreover, these products can be sold (and are even being sold at present) abroad. At present certification in this field is significantly longer than in other developed countries, which leads to a slowdown in the development of new products and their versions and creates situations where companies are not interested in proper certification of each version. In other words, the certification procedure as a whole for industrial cyber security systems is inefficient. For antivirus software there is no procedure at all, i.e., it is not efficient either. As a result of the article, it can be concluded that reduction of certification time for industrial cyber security system will increase the certification procedure efficiency in product development in this field in Russia.

Moreover, it is important to add that antivirus software and industrial cyber security system are international products. Many countries purchase products that have been created abroad. Therefore, simplification, especially certification process time reduction will lead to extension of Russian cyber security information products abroad.

References:

1. Kabali H.K., Rigoyen M.M., Nunez-Davis R., Budacki J.G., Mohanty S.H., Leister K.P., Bonner R.L. Jr. Exposure and use of mobile media devices by young children. *Pediatrics*. 2015; 136(6): 1044-1050. doi: 10.1542/peds.2015-2151.
2. Schoitsch E., Schmittner C., Ma Z., Gruber Th. The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In: *Advanced Microsystems for Automotive Applications*. Schulze T., Müller B., Meyer G. (eds). Springer, 2015: 251-261.
3. Ni J.Z., Melnyk S., Flynn B.B., Ritchie W. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification. *Int. J. Operat. & Product. Management*. 2016; 36(10): 1161-1181.
4. Gcaza N., Von Solms R. A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries*. 2017; 80(1): 1-17.
5. Mourtzis D., Vlachou E. Cloud-based cyber-physical systems and quality of services. *The TQM Journal*. 2016; 28(5): 704-733.
6. Raisinghani M.S. Can total quality management exist in cyber security: Is it present? Are we safe? In: *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. IGI Global, 2015: 350-359.
7. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*. 2016; 56: 1-27.
8. Kent A.D. Cyber security data sources for dynamic network research. In: *Dynamic Networks and Cyber-Security*. Publisher WSPC, 2016: 37-65.
9. Efremova M.A. Criminal-legal ensuring of cyber security: Problems and ways of their solution. *Pravo i kiberbesopasnost' (Law and Cyber Security)*. 2014; 2: 33-38. (in Russ.)
10. Ziborov O.V., Ivanov M.A., Chekunov I.G. The state of cyber security in modern

information society. *Voprosi kiberbesopasnosti* (Questions of Cyber Security). 2017; 52(20): 15-18. (in Russ.)

11. Kartskhiya A.A. Cybersecurity and intellectual property. Part 1. *Voprosi kiberbesopasnosti* (Questions of Cyber Security). 2014; 1(2): 61-66. (in Russ.)

12. Knowles W., Hutchison D., Prince D., Diss J.P. A survey of cyber security management in industrial control systems. *Int. J. Critical Infrastructure Protection*. 2015; 9: 52-80.

13. Gopalakrishnan S., Zhang H. The link between vendor certification and performance in IT outsourcing: A tale of two stories. *Academy of Management Proceed.* 2018; 1: 129-167.

14. Kantardjieva M. The relationship between total quality management (TQM) and strategic management. *J. Economics, Business and Management*. 2015; 3(5): 537-541.

15. Shin J., Son H., Rahman K.U., Heo G. Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety*. 2015; 134: 208-217.

Литература:

1. Kabali H.K., Rigoyen M.M., Nunez-Davis R., Budacki J.G., Mohanty S.H., Leister K.P., Bonner R.L. Jr. Exposure and use of mobile media devices by young children // *Pediatrics*. 2015. V. 136. № 6. P. 1044–1050. doi: 10.1542/peds.2015-2151

2. Schoitsch E., Schmittner C., Ma Z., Gruber Th. The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles // In: *Advanced Microsystems for Automotive Applications / Schulze T., Müller B., Meyer G. (eds)*. Springer, 2015. P. 251–261.

3. Ni J.Z., Melnyk S., Flynn B.B., Ritchie W. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification // *Int. J. Operat. & Product. Management*. 2016. V. 36. №. 10. P. 1161–1181.

4. Gcaza N., Von Solms R. A strategy for a cybersecurity culture: A South African perspective // *The Electronic Journal of Information Systems in Developing Countries*. 2017. V. 80. №. 1. P. 1–17.

5. Mourtzis D., Vlachou E. Cloud-based cyber-physical systems and quality of services // *The TQM Journal*. 2016. V. 28. № 5. P. 704–733.

6. Raisinghani M.S. Can total quality management exist in cyber security: Is it present? Are we safe? // In: *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance*. IGI Global, 2015. P. 350–359.

7. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems // *Computers & Security*. 2016. V. 56. P. 1–27.

8. Kent A.D. Cyber security data sources for dynamic network research // In: *Dynamic Networks and Cyber-Security*. Publisher WSPC, 2016. P. 37–65.

9. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // *Право и кибербезопасность*. 2014. № 2. С. 33–38.

10. Зиборов О.В., Иванов М.А., Чекунов И.Г. Состояние кибербезопасности современного информационного общества // *Вопросы кибербезопасности*. 2017. № 52(20). С. 15–18.

11. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 1 //

Вопросы кибербезопасности. 2014. № 1(2). С. 61–66.

12. Knowles W., Hutchison D., Prince D., Diss J.P. A survey of cyber security management in industrial control systems // Int. J. Critical Infrastructure Protection. 2015. V. 9. P. 52–80.

13. Gopalakrishnan S., Zhang H. The link between vendor certification and performance in IT outsourcing: A tale of two stories // Academy of Management Proceed. 2018. № 1. P. 129–167.

14. Kantardjieva M. The relationship between total quality management (TQM) and strategic management // J. Economics, Business and Management. 2015. V. 3. № 5. P. 537–541.

15. Shin J. , Son H., Rahman K.U., Heo G. Development of a cyber security risk model using Bayesian networks // Reliability Engineering & System Safety. 2015. V. 134. P. 208–217.

About the authors:

Maxim A. Nazarenko, Ph.D. (Physics and Mathematics), Head of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Alexey I. Gorobets, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Dmitriy V. Miskov, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Vyacheslav V. Muravyev, Senior Lecturer of the Chair KB-9 "Applied and Business Informatics", Institute of Integrated Security and Special Instrumentation, MIREA – Russian Technological University (20, Stromynka St., Moscow 107076, Russia).

Alexandr S. Novikov, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Об авторах:

Назаренко Максим Анатольевич, кандидат физико-математических наук, заведующий кафедрой управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Горобец Алексей Иванович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Миськов Дмитрий Валентинович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Муравьев Вячеслав Викторович, старший преподаватель кафедры KB-9 «Прикладная и бизнес-информатика» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (107076, Россия, Москва, ул. Стромынка, д. 20).

Новиков Александр Серафимович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

For citation: Nazarenko M.A., Gorobets A.I., Miskov D.V., Muravyev V.V., Novikov A.S. Antivirus software and industrial cyber security system certification in Russia. *Rossiyskiy tekhnologicheskii zhurnal* (Russian Technological Journal). 2019; 7(1): 48-56. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-48-56

Для цитирования: Назаренко М.А., Горобец А.И., Миськов Д.В., Муравьев В.В., Новиков А.С. Сертификация антивирусного программного обеспечения и систем кибербезопасности АСУ ТП в России // Российский технологический журнал. 2019. Т. 7. № 1. С. 48–56. DOI: 10.32362/2500-316X-2019-7-1-48-56

УДК 621.37.037

DOI: 10.32362/2500-316X-2019-7-1-57-79

КОНТРЕИНЖИНИРИНГ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

**М.С. Костин[@],
Д.С. Воруничев,
Д.А. Корж**

МИРЭА – Российский технологический университет, Москва 119454, Россия

[@]Автор для переписки, e-mail: kostin_m@mirea.ru

Изложены результаты научно-практических исследований в области спецпроектного реинжиниринга и контрреинжиниринга изделий радиоэлектронных средств. Представлены методы и средства спецпроектного реинжиниринга функциональных модулей многослойных печатных плат и корпусных микросхем. Приведены базисные конструкторско-технологические решения реинжиниринга многослойных печатных плат радиоэлектронных изделий, основанные на физических принципах разрушающего и неразрушающего декомпозиционного исследования: механообработка и химическое травление, стереолазерное структурирование, тепловизионная электротермия, рентгенографический анализ. Сформулированы положения и методология схмотехнического анализа принципиальной архитектуры электрических цепей и сигнальных процессов радиоэлектронных изделий по конфигурации печатного узла, его электронной компонентной базе и их связным топологиям. Рассмотрены методы и средства реинжиниринга радиотехнических цепей и сигналов, позволяющие воспроизвести перечень электронной компонентной базы и принципиальную схмотехнику, а также исследовать основные системотехнические характеристики радиоэлектронного устройства в четырех основных режимах: функциональном, внутрисхемном, периферийном и идентификационной визуализации. Обсуждаются методы и средства аутентичной воспроизводимости радиоэлектронных изделий по ряду конструктивных и радиотехнических идентификаторов. Предложены и сформулированы конструкторско-технологические решения по обеспечению противодействия реинжинирингу изделий радиоэлектронных средств.

Ключевые слова: спецпроектный реинжиниринг, контрреинжиниринг, техническое противодействие, радиоэлектронное изделие, прототипная декомпозиция, сигнальные процессы.

COUNTERREENGINEERING OF ELECTRONIC DEVICES

**M.S. Kostin@,
D.S. Vorunichev,
D.A. Korzh**

MIREA – Russian Technological University, Moscow 119454, Russia

@Corresponding author e-mail: kostin_m@mirea.ru

The paper presents the main results of scientific and practical research in the field of special design reengineering and counterreengineering of radioelectronic devices. Methods and means of special design reengineering of functional modules of multilayer printed circuit boards and case microcircuits are presented. The basic process design for the reengineering of multilayer printed circuits of radioelectronic products is presented. The design is based on the physical principles of destructive and non-destructive decomposing test: mechanical processing and chemical etching, stereolaser structuring, IR imaging electrothermics and X-ray analysis. The article formulates positions and methodology of the circuit analysis of the basic architecture of electrical circuits and signal processes of radio electronic products by the configuration of the printed circuit, its electronic component base and their connected topologies. The article considers methods and techniques for the reengineering of radiotechnical circuits and signals enabling to reproduce the list of the electronic component base and the essential circuit technique, as well as to study the basic circuit characteristics of the appliance in four main modes: functional, in-circuit, peripheral and identification visualization. The methods and means of authentic performance of radioelectronic devices for a number of constructive and radio-technical identifiers are considered. Technical methods and solutions for counterreengineering of radioelectronic devices have been developed.

Keywords: special project reengineering, counterreengineering, technical countermeasures, radio electronic device, prototype decomposition, signaling processes.

Введение

Обеспечение экономической и информационно-технической безопасности (ИТБ) в области радиоэлектронной промышленности и сектора ОПК сегодня является одной из приоритетных задач Государственной программы импортозамещения. При этом доминирующие позиции в сфере обозначенных направлений занимают спецпроектные исследования в области реинжиниринга и контрреинжиниринга радиоэлектронных средств (РЭС). Сегодня реинжиниринговые исследования, позволяющие путем обратного анализа разработать научно-практическую стратегию проектирования и производства изделий РЭС в технически защищенном от копирования исполнении, являются неотъемлемым инструментом конкурентоспособной навигации. Отсюда целью обозначенной стратегии является безошибочный выбор номенклатуры электронной компонентной базы (ЭКБ) и реализация аппаратных и программных средств защиты радиоэлектронного изделия от преднамеренного реинжиниринга.

Таким образом, актуальность и ключевые задачи реинжиниринга заключаются в:

1) техническом противодействии спецпроектным исследованиям поставляемых на экспорт оригинальных РЭС двойного назначения либо импортируемых РЭС, изготовленных иностранными партнерами в рамках программ внешнеэкономической кооперации;

2) исследовании современных методов и средств реинжиниринга РЭС, которые играют ключевую роль в обеспечении ИТБ изделий радиоспецтехники, реализуемых на базе импортной ЭКБ, с целью идентификации элементов и электрических цепей, реализующих программно-аппаратные решения средств РТР и внутрисистемного подавления РЭП;

3) активной модернизации изделий РЭС (принимая во внимание объем морально устаревшего радиоэлектронного оборудования и ЭКБ, находящихся в стадии долгосрочной эксплуатации средств вооружения военной техники, а также допускаемый Главным управлением вооружения ВС перечень импортной ЭКБ, возрастает необходимость активной модернизации для продления жизненного цикла радиоэлектронной аппаратуры; реинжиниринг в таких случаях применяется к оригиналу радиоэлектронного изделия, когда рабочая конструкторская документация на образец утрачена или недоступна);

4) защите изделий РЭС от контрафактного производства в целях поддержания конкурентоспособности и показателей экономического роста от экспортных поставок выпускаемых изделий (рис. 1).

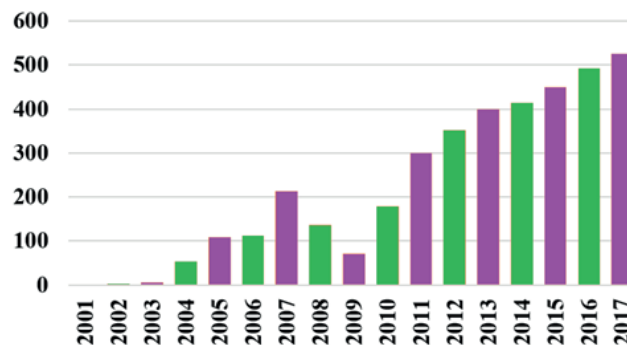


Рис. 1. Ежегодная динамика совокупных убытков мировых компаний радиоэлектронной индустрии от контрафактного производства РЭС средствами реинжиниринга (млрд. USD) [1].

Предметной областью спецпроектного реинжиниринга РЭС являются:

- реинжиниринг конфигурации печатной топологии МПП методами разрушающей (абразивное шлифование, химическое травление, лазерное структурирование, термовоздушное расщепление, фрезерование) и неразрушающей (рентгенографический анализ, ТВЭТ) послойной декомпозиции;
- схемотехнический реинжиниринг многослойных печатных узлов (МПУ): функциональный, внутрисхемный, периферийный (системотехнический);
- реинжиниринг сигнальных и радиофизических процессов МПУ;
- реинжиниринг интегральных устройств ЭКБ (ИМС-логика, ПЛИС, микропроцессоры, цифровые устройства памяти и т. д.).

1. Реинжиниринг многослойных печатных плат

Чтобы разработать комплекс мер противодействия спецпроектному реинжинирингу, необходимо провести исследования методов и средств, позволяющих идентифицировать конструктивные особенности РЭС по топологии печатной платы изделия. При этом особый интерес представляют платы с многослойным распределением печатной топологии – МПП. Как известно, современный реинжиниринг МПП цифровых устройств позволяет

не только восстановить аутентичность спеченой топологии, но и в высоковероятной степени воссоздать принципиальную схему радиоэлектронного изделия в целом [1]. Таким образом, это позволяет выявить номенклатуру интегрированных в МПП электронных радиоэлементов (ЭРЭ). Зная номенклатуру, возможно определить тип микросистемного устройства (как, например, приемопередатчик на ПЛИС) и узнать основные параметры его схемотехнической архитектуры.

Одной из радикальных классификаций методов реинжиниринга МПП является классификация по принципу физического декомпозиции РЭС: разрушающего и неразрушающего воздействия.

Определяющими факторами при выборе того или иного метода и средств реинжиниринга являются:

- 1) конструкция печатного узла;
- 2) материалы, из которых изготовлен печатный узел;
- 3) тип монтажа, примененный в печатном узле.

Стоит отметить, что данные факторы будут определяющими и для выбора технических мер по противодействию реинжинирингу. Так, при проведении послойного топологического анализа появляется возможность слой за слоем воссоздать исследуемый печатный узел и впоследствии создать его прототип с целью модификации в дальнейшем. Кроме того, возможна разработка комплекса мер по защите от спецпроектных исследований, что позволит обеспечить экономическую и интеллектуально-информационную защиту перспективных отечественных РЭС и разработок.

Среди разрушающих способов деструктуризации МПП различают следующие: послойного шлифования, лазерного и химического травления, фрезерования и термовоздушного расщепления [2]. Реинжиниринг разрушающего воздействия не гарантирует отсутствие повреждений топологии МПП повышенной плотности монтажа или трассировки, потому не является прогрессивным. Он применяется только тогда, когда исключается эффективность применения методов неразрушающего прототипирования, позволяющих восстанавливать топологию с применением косвенных методов экспертного анализа: стереолазерное и оптическое сканирование, тепловизионная электротермия, рентгенографический анализ и радиосенсорное исследование, применяемое для контактно-локационного анализа при восстановлении схемотехнической конфигурации печатного изделия [1].

1.1. Прототипирование методом разрушающей декомпозиции печатных узлов

Послойная декомпозиция образца печатного изделия относится к методам разрушающего спецпроектного исследования топологии МПП и является наиболее радикальным техническим решением в области реинжиниринга радиоэлектронных средств, позволяющим получить печатный рисунок, переходя от одного стека топологии к другому. Главной целью данного этапа прототипирования является получение топологии каждого слоя, поэтому после разрушения очередного слоя МПП ее необходимо зафиксировать. Это можно сделать с помощью стереооптического сканирования.

Стереооптическим данный процесс называется благодаря применению лазерно-оптических систем, позволяющих регистрировать как печатную топологию МПП, так и поперечный срез межслойных соединений при помощи специализированных сканеров

и адаптированного ПО, как, например, ScanCAD [3]. Важно отметить, что данный метод теряет свою актуальность, если необходимо исследовать печатные модули со встраиваемыми ЭРЭ, так как при послойной декомпозиции почти во всех случаях будет происходить повреждение встроенных в плату радиодеталей (рис. 2). Заметим, что повсеместное и активное внедрение изготовления печатных узлов со встраиваемой ЭКБ свидетельствует о несостоятельности данного метода при попытке воссоздания прототипа таких печатных узлов.

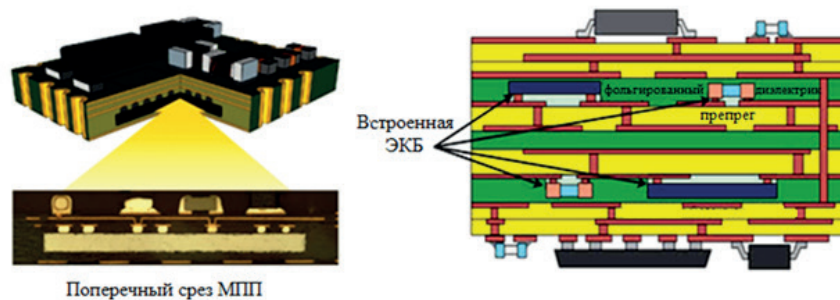


Рис. 2. Поперечный срез конструктивной реализации МПП со встраиваемой ЭКБ.

1.2. Прототипирование методом неразрушающей декомпозиции печатных узлов

Если применение разрушающих методов реинжиниринга невозможно из-за особенностей исследуемого образца, как описано выше, либо других технических ограничений, обычно прибегают к следующим неразрушающим методам:

- 1) рентгенографический анализ;
- 2) тепловизионная электротермия.

Рентгенографический анализ. Метод позволяет – в отличие от разрушающих методов – исследовать топологию и проводить внутрисхемный анализ печатного узла, не прибегая к физическому воздействию, и сохранять его структуру целостной. Однако в классическом варианте нормального (под углом 90°) рентгеновского сканирования рентгенографический анализ не позволяет различить межслойную топологию МПП. Чтобы решить данную проблему, прибегают к режиму углового облучения МПП. Таким способом достигается послойное сканирование топологии медных слоев, а специализированное ПО позволяет получить данные топологии по двум угловым проекциям (рис. 3а, б). Регистрация рентгенограммы изображений слоев топологии МПП происходит посредством компьютерной томографии, которая заключается в получении и наложении с помощью программно-числовой обработки изображений каждого слоя.

Среди специализированного оборудования рентгенографического анализа внутрисхемной топологии печатных плат хорошо зарекомендовала себя установка Nordson DAGE XD7600 NT Ruby X-ray Inspection System [4]. Так, на рис. 3в представлены результаты анализа 4-х-слойной МПП, полученные посредством наложения изображений слоев и их программно-числовой обработки.

Стоит подчеркнуть, что для получения качественной рентгенографической томограммы медной топологии печатной платы необходимо, чтобы исследуемый участок топологии выделялся на контрастном фоне диэлектрика. Отсюда следует, что одним из возможных вариантов противодействия данному методу реинжиниринга является закры-

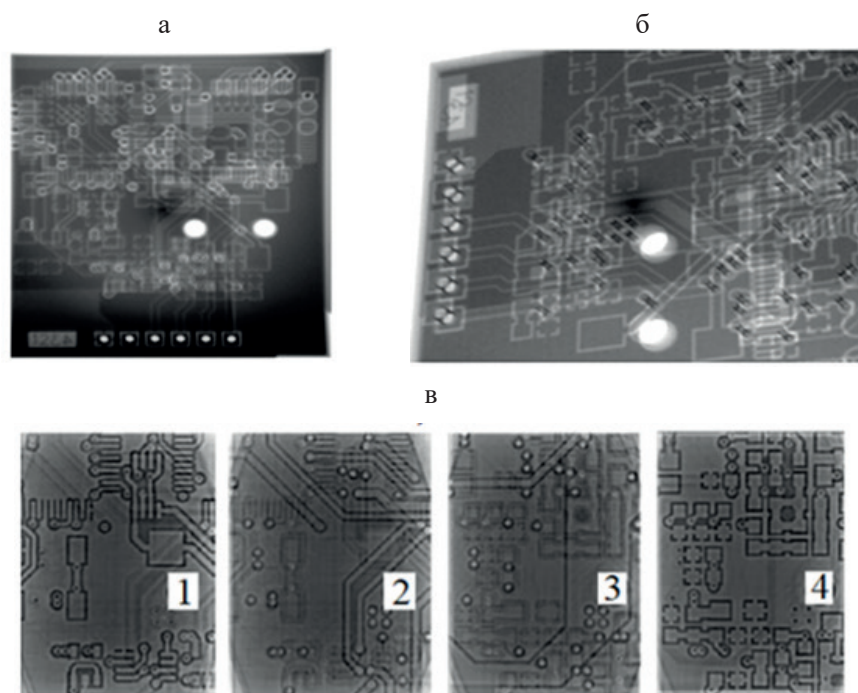


Рис. 3. Рентгенографический анализ многослойной топологии, полученный на установке DAGE XD7500 VR X-ray Inspection System: а) облучение МПП под прямым углом 90°; б) облучение МПП под углом 30°; в) послойная томограмма образца платы.

тие слоя медной топологии от рентгеновских лучей. Действительно, уровень контрастирования находится в прямой зависимости от связанного с ним материала мишени (ЭРЭ, материала проводящего слоя), его физической плотности, физико-химических свойств и атомного числа. В таком случае обеспечивается рентгенографическая блокировка защищаемого участка цепи, позволяющая существенно понизить четкость или вовсе исключить возможность анализа внутрислойной топологии. То есть для создания активных зон рентгенографической блокировки нужно конструктивно использовать в структуре МПП композитные материалы, которые обладают большим атомным числом. Такой блокинг-материал (с атомным числом из диапазона 70–82: вольфрам, тантал, золото, свинец и т. д.) может применяться для нанесения между препергами конструкции МПП в виде фольги или путем напыления на проводники. Его получают путем добавления блокинг-частиц в смолистую основу либо в структуру препергов, путем добавления в припой и др.

Эффективность использования блокинг-материалов показана на рис. 4. Так, на рис.4а изображена рентгенографическая томограмма исследуемой 6-ти-слойной МПП. В отличие от предыдущей (рис. 3), на одном из периферийных слоев данной платы нанесен блокинг-материал (атомное число 73), основанный на припое с примесью тантала, который поглощает рентгеновские лучи.

Важно отметить, что размещение блокинг-материалов на всей площади МПП не является, в принципе, целесообразным. Оно оправдано только в местах коммутации печатных проводников (рис. 4б–д). Правильно подобранное расположение блокинг-материалов и использование встроенной ЭКБ во внутренней структуре МПП делает ее фактически полностью неуязвимой для рентгенографического анализа и разрушающих методов реинжиниринга.

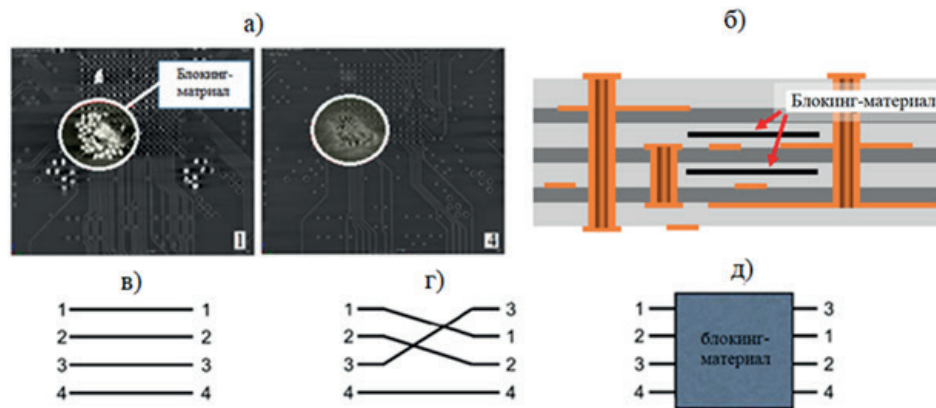


Рис. 4. Использование блокинг-материала в структуре МПП:

- а) образование гамма-шумов в области нанесения блокинг-материала при сканировании МПП методом рентгенографического анализа;
- б) поперечный срез МПП со встроенным блокинг-материалом;
- в) фрагмент узловой топологии оригинала печатного изделия;
- г) неоднозначно структурированная топология;
- д) структурированная топология под слоем блокинг-материала.

Тепловизионная электротермия. Концептуальное решение технологии тепловизионной электротермии (ТВЭТ) заключается в создании индукционного нагрева медных проводников МПП с целью термографического проявления рисунка печатной топологии, скрытой в слоях диэлектрического основания платы, в инфракрасном диапазоне при помощи тепловизора высокого чувствительного и матрично-пиксельного разрешения [5].

Индукционный и диэлектрический электронагревы основаны на выделении тепловой энергии непосредственно в нагреваемом образце МПП при возникновении в нем наведенных вихревых токов Фуко и выделении тепла по закону Джоуля-Ленца в проводниках и токов смещения – в диэлектриках с выделением тепловой энергии вследствие влияния диэлектрических потерь. Основным требованием, предъявляемым к ВЧ-индукторам в ТВЭТ-технологии, является применение конструкций открытого типа с целью нагрева МПП с одной стороны платы и тепловизионной термографии – с противоположной стороны диэлектрического основания. В частности, для реализации тепловизионной электротермии можно использовать два основных конструктива индукторов открытого типа: плоские спиральные и магнитопроводные катушечные.

Поскольку побочный диэлектрический нагрев, создающий тепловой шум, проявляется на частотах свыше 30 МГц, ТВЭТ проводящей топологии МПП осуществляется путем воздействия ближнего поля маломощного плоского ВЧ-индуктора (до 0.5 Вт) и ограничивается частотой 30 МГц. Регистрация ИК-излучения образца МПП осуществляется в среднем диапазоне 8–9.5 мкм с чувствительностью 0.03 °С, что соответствует температурному интервалу +30...+80 °С при среднем нагреве образца около +55 °С, фоновом диэлектрическом нагреве до +26 °С и температуре окружающего пространства +22 °С [5].

Подчеркнем, что ТВЭТ-технология не предусматривает разрушающего воздействия, в чем и состоит ее преимущество. В качестве тепловизора в ТВЭТ-технологии, как правило, применяются инфракрасные камеры среднего спектрального диапазона 7.5–14 мкм, например, RAZ-IR PRO-2 с тепловой чувствительностью менее 0.03 °С [5].

Принцип реализации ТВЭТ-технологии следующий. В результате воздействия магнитных полей, наводимых ВЧ-токами (рис. 5а), происходит индукционный нагрев проводящих слоев на поверхности и внутри диэлектрического основания испытуемого образца МПП. Тепловизионные исследования могут проводиться в двух режимах термографической регистрации: в фоновом и инверсном (рис. 5б–в). Использование инверсного режима является наиболее предпочтительным, поскольку катушка индуктора образует тепловое излучение, которое мешает контрастному восприятию и распознаванию термографического изображения.

Локализуя ВЧ-индуктор в заданной области образца МПП, а также управляя частотой и мощностью ВЧ-генерации, удастся осуществить оптимальную настройку четких очертаний топологии токопроводящего печатного рисунка на тепловизионной камере в заданном слое. Для детального рассмотрения фрагментарных элементов топологии может быть использован способ нагрева печатных проводников контактным методом ВЧ-токами малой мощности.

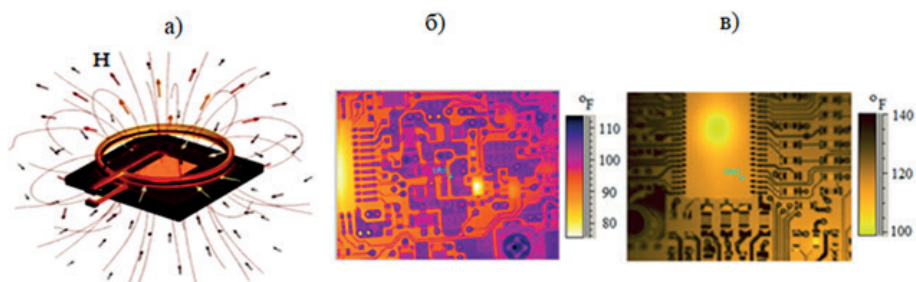


Рис. 5. Образец платы в поле ВЧ-индуктора (а); фоновый (б) и инверсный (в) тепловизионные снимки топологии МПП.

Исследование современных методов и средств реинжиниринга изделий МПП, а также анализ технологии производства и номенклатуры ЭКБ позволяют разработать комплекс технических мер и проектно-конструкторских рекомендаций противодействия спецпроектным исследованиям изделий РЭС, как, например, внедрение в структуру диэлектрической подложки МПП встраиваемых чипов электрорадиоэлементов, исключающих возможность эффективного применения реинжиниринговых средств разрушающей декомпозиции ввиду опасности повреждения ЭКБ. В то же время с целью обеспечения противодействия средствам рентгенографической деструктуризации предлагается применение внутрислойных блокинг-материалов из элементов с высоким атомным числом, препятствующих проникновению рентгеновских лучей в сегментированную область неоднозначно структурированной топологии.

Одним из предложенных в работе способов защиты изделия от исследования методом ТВЭТ является локальное внедрение в структуру диэлектрического основания микрополосковых встречно-бифилярных катушек, закрывающих участки перераспределения коннекции с двух сторон по аналогии с блокинг-материалом и тем самым компенсирующих наводимое поле плоского ВЧ-индуктора. Устойчивость конструкции МПП одновременно к обоим рассматриваемым методам можно достичь комбинированием представленных решений.

Среди прочих находят применение также иные конструкторско-технологические рекомендации контрреинжиниринга РЭС, основанные на принципах визуального измыш-

ления: добавление в печатный узел избыточной активной и пассивной ЭКБ; включение слоев с «холодной» топологией, усложняющих анализ цепей. В качестве компонентов могут быть неработоспособные (непроводящие или всегда открытые) транзисторы, мнимые (непроводящие) вертикальные межсоединения, избыточные проводящие дорожки и т. д.

Противодействием схемотехническому прототипированию может послужить исключение расположения тестовых площадок и/или элементов трассировки на боковых поверхностях МПП. Кроме всего прочего, применение технологий тестирования JTAG, или периферийного схемотехнического анализа, в значительной степени компенсирует недостаток физического доступа, создавая бесконтактную альтернативу тестированию цепей, недоступных для ИСТ-адаптеров.

Анализ и обработка отсканированной топологии МПП требует послойной геометрической векторизации. Используя векторизацию, можно воспроизвести трассировку и изготовить прототип целевой МПП, что затем позволит модифицировать ее топологию и исследовать конфигурацию электрических цепей по ряду идентификаторов. Посредством такой идентификации просто выявить функциональную принадлежность и тип РЭУ. Определяющими идентификаторами способны выступать конкретные выводы шин заземления, а также цепи обвязки ПЛИС, цифровых интерфейсов, микропроцессоров, схем памяти и др.

Среди средств программно-числовой обработки сканированной топологии оригиналов МПП в задачах спецпроектного реинжиниринга находит применение модульный функционал таких специализированных пакетов, как Drupht, Aplite и Phiplastic.

2. Реинжиниринг сигнальных процессов в печатных модулях

Реинжиниринг схемотехнической конфигурации радиоэлектронных цепей печатного узла заключается в воспроизведении перечня ЭКБ, реконструкции электрической принципиальной схемы, а также в параметрическом исследовании сигнальных процессов и основных характеристик и принципов работы радиоэлектронного устройства [2].

Задача реинжиниринга сигнальных процессов решается схемотехническим анализом МПП. Различают следующие виды схемотехнического анализа:

- функциональный;
- внутрисхемный;
- периферийный;
- метод идентификационной визуализации, используемый в качестве вспомогательного при реализации вышеприведенных методов [3].

Целью функционального анализа является исследование и регистрация основных характеристик печатного узла. Функциональный анализ разделен на три этапа:

- 1) на первом этапе МПП рассматривается как многоплюсник;
- 2) на втором этапе исследуются отдельные функциональные узлы и цепи, на которые разбивается МПП;
- 3) на третьем этапе рассматривается ЭКБ, входящая в состав функциональных узлов и цепей МПП.

Для аппаратной реализации функционального анализа МПП необходимо специальное стендовое обеспечение для сигнального моделирования РЭС, в составе которого на-

ходится исследуемый печатный узел. Однако на практике ни один вид анализа не применяется по отдельности. Как правило, это комбинированное исследование: например, комбинация функционального и внутрисхемного анализа или функционального анализа с периферийным.

Внутрисхемный анализ заключается в радиотехнической идентификации цепей или компонентов схемы радиоэлектронного изделия. В качестве аппаратных средств реализации методом внутрисхемного анализа на практике применяют специальное ИСТ-оборудование в составе с внутрисхемным анализатором цепей, оснащенный тестовой контактно-иглочной адаптерной матрицей или подвижным турбопозиционным манипулятором (рис. 6) [6]. Внутрисхемный анализ может применяться не только для анализа печатного узла, но и для анализа отдельных участков и локально расположенных ЭРЭ.

Внутрисхемный анализ, как и функциональный, не предполагает разрушающих воздействий на МПП. При этом для выполнения внутрисхемного анализа, например, по отношению к пассивным цепям исследуемого образца печатного узла исключается необходимость в дополнительном питании компонентной базы, что позволяет произвести локальную идентификацию радиоэлементов, исключая опасность их повреждения [3]. Но есть ограничения. В частности, анализ и исследование активных элементов возможно только при включенном питании. Чтобы компенсировать недостатки матричного доступа ИСТ-адаптера, который для внутрисхемного анализа требует гальванического контакта тестирующих электродов с проводниками печатного узла МПП, можно воспользоваться технологией JTAG-тестирования. Таким образом, применение методов периферийного анализа в схемотехническом реинжиниринге программируемых цифровых устройств является исключительным. Отсюда периферийный анализ печатных узлов, построенных на ядре процессорной или ПЛИС-конфигурации, не нуждается в контакте пробников с внутрисхемной сигнальной топологией печатного узла.

Известно, что программируемые цифровые устройства РЭС отличаются специальными способами криптографической защиты кодировок от внутрисистемного реинжиниринга, как, например, создание динамических псевдослучайных переменных, исключающих открытое чтение машинного кода [7].

Целевой задачей сигнального и схема-архитектурного анализа программируемых цифровых устройств на ПЛИС является также рекомпиляция кода прошивки в схему, через которую возможно восстановить цифровую архитектуру при помощи программно-отладочных сред ISE Web PACK Design Software и Quartus II.

Автоматизация режимов и методов схема-архитектурного анализа сегодня предлагает эффективные технические решения на базе специализированного оборудования: диагностическая система Pin Point или Fault Finder, внутрисхемный матричный адаптер Flex Fixer, автоматизированный пробник Auto Point DT с «летающим щупом» и др. [3].

Матрица тестовых контактных точек МПП служит своеобразным реперным индикатором для удобного и быстрого схемотехнического реинжиниринга и радиотехнического анализа печатного узла. Таким образом, в качестве технических мер обеспечения контрреинжиниринга периферийным исследованиям предлагается исключение с боковой поверхности диэлектрического основания МПП тестовых точек и ключевых сигнальных шин данных. Исключение возможности доступа к JTAG-порту является одним из дей-

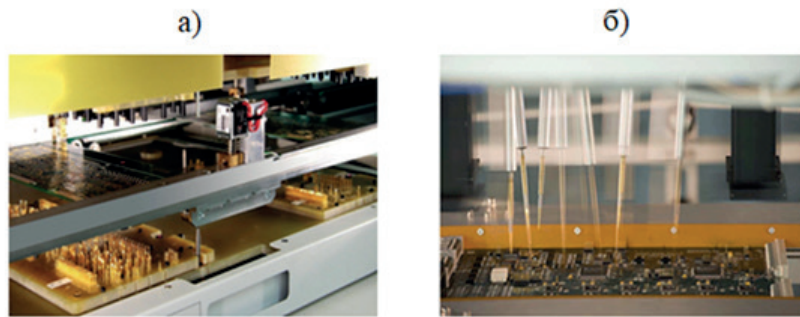


Рис. 6. Внутрисхемный ИСТ-адаптер: а) тестовые щупы матричного типа; б) тестовые щупы «летающего» типа.

ственных способов снижения эффективности периферийного анализа. Это достигается на этапе отладки и прошивки ПЛИС путем его конструктивного устранения.

Реинжиниринг ПЛИС осложняется повышенной степенью технической и криптографической защищенности таких систем. Так, одним из примеров защит является формирование в *Assembler* или скрипте *VHDL* фиктивных и случайных переменных. В то же время одним из наиболее действенных способов контрреинжиниринга программируемых цифровых устройств являются аппаратно-конструктивные решения, поддерживающие, к примеру, технологию токового выжигания сигнальных конвекторов *JTAG*-интерфейсов.

3. Прототипная декомпозиция интегральных микросхем

Если при реинжиниринге МПП возможно использование и разрушающих, и неразрушающих методов, то при спецпроектном исследовании топологии интегральных микросхем (ИМС) применяют только разрушающие методы. К ним относятся:

- 1) механическое фрезерование ИМС;
- 2) послойное химическое травление ИМС;
- 3) комбинированный метод (последовательное сочетание 1-го и 2-го методов);
- 4) лазерная декапсуляция ИМС.

Выбор того или иного метода и средства декапсуляции во многом будет зависеть от конструкции, материалов кристалла, корпуса и типа реализации технологии интегральной сборки: полупроводниковая, пленочная, гибридная или смешанного типа [8].

3.1. Прототипная декапсуляция корпусных микросхем

Химическая декапсуляция. Главной целью исследования в процессе реинжиниринга является кристалл ИМС, препятствием к которому является корпус чипа. Следовательно, чтобы получить доступ к кристаллу, необходимо произвести химическое травление корпуса, которое осуществляется с помощью концентрированной азотной или серной кислоты.

Рынок профессионального оборудования для декапсуляции чипа достаточно широк, однако среди прочих зарекомендовал себя программируемый установочный комплекс декапсуляции *PS103S (PS105)*. Данный комплекс обеспечивает выбор из 25 режимов травления пластика и применяется для декапсуляции чипа в процессе анализа отказов ИМС (рис. 7).

Основной проблемой данного метода является слабо контролируемая длительность воздействия кислот, так как длительное воздействие разрушает не только корпус ИМС,

но и может повредить сам кристалл и его соединительные проводники. Проблема решается применением плазмохимического и сухого химического травления.

На практике находят применение установки плазмохимической декапсуляции типа Е373 и Е401.

Механическая декапсуляция. Помимо метода химической декапсуляции, широко применяется механический метод. Он используется в качестве подготовительного этапа перед химическим травлением, а также самостоятельно при декапсуляции корпуса ИМС. Стоит отметить, что данный метод подходит не только для ИМС с полимерным корпусом, но и для ИМС с керамическим и металлокерамическим корпусами.

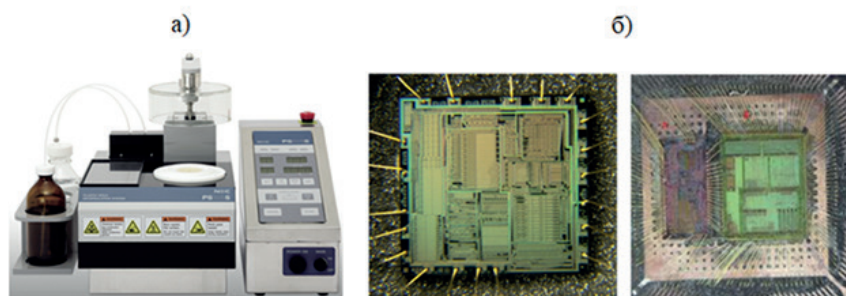


Рис. 7. Установки декапсуляции для сухого травления ИМС с ЧПУ PS 103S (PS105) (а) и снимки кристаллов ИМС после химической декапсуляции полимерного корпуса (б).

Сущность механического метода заключается в физическом воздействии на корпус ИМС с помощью фрез. Производители предлагают широкий спектр современного оборудования, которое с помощью микрофрез осуществляет прецизионное и быстрое удаление материала корпусов ИМС. Характерно, что декапсуляция корпуса ИМС может осуществляться как на самой печатной плате, так и в процессе предварительного демонтажа ИМС с ее поверхности при помощи паяльной станции. Такую комбинацию операций можно провести, например, с помощью фрезерно-шлифовального станка с ЧПУ LY-1001 и паяльной установки RW-SV520 (рис. 8).

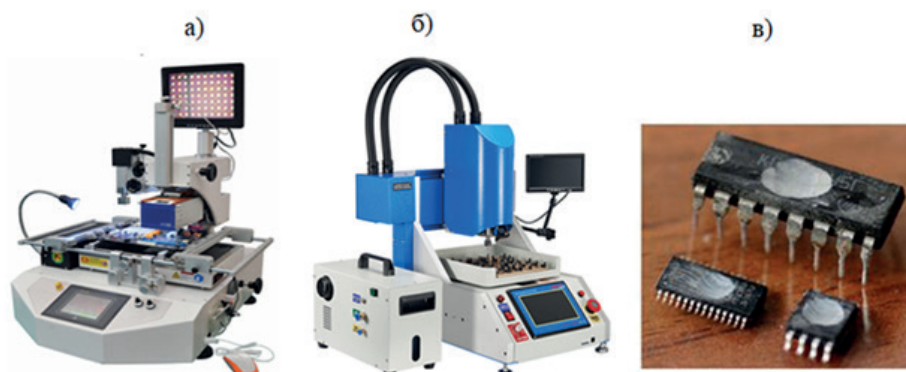


Рис. 8. Установки демонтажа и механической декапсуляции ИМС: паяльная микровизионная станция RW-SV520 (а); прецизионный микровизионный фрезерно-шлифовальный станок LY-1001 (б); образцы ИМС, прошедшие фрезерную обработку (в).

Термическая (лазерная) декапсуляция. Технология лазерной декапсуляции заключается в удалении слоя полимерного, или керамического, или металлокерамического материалов корпуса ИМС. Метод эффективен при вскрытии корпусов с медными и серебряными проводниками, его можно использовать также и для полимеров, практически не растворимых в кислотах (рис. 9).

Лазерный метод, как и метод механообработки, в технологическом цикле декапсуляции ИМС часто предшествует химическому или плазмохимическую травлению в качестве подготовительной операции, оставляя надкристалльный слой материала корпуса около 100 мкм [9]. Метод применяется также самостоятельно. Подобно методу механической декапсуляции, он подходит для полимерных, керамических и металлических корпусов ИМС типа BGA. Для решения задач реинжинирига ИМС методом лазерной декапсуляции наиболее эффективной оказалась установка Falit и ее модификация PL101i (PL121i).

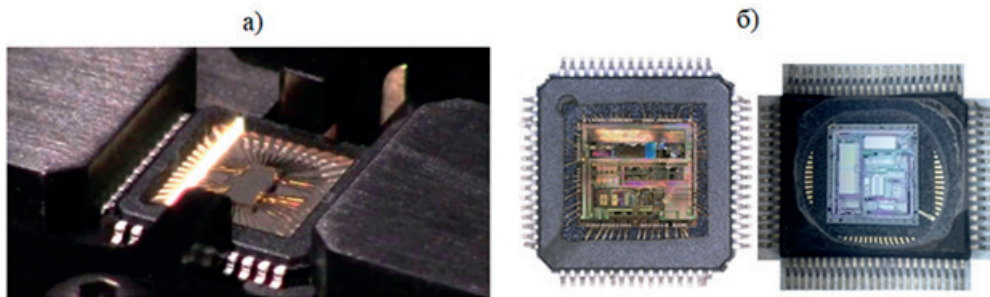


Рис. 9. Фрагмент процесса лазерной декапсуляции чипа (а); декапсулированные образцы микросхем (б).

3.2. Анализ кристалльной топологии микросхем

Неотъемлемым инструментом для изучения и анализа топологии ИМС в реинжиниринге является микровизор. Микровизоры – это новое поколение микроскопов, имеющих аппаратно-программный комплекс для регистрирования и обработки изображений, для решения задач микровизионного атомно-силового анализа. Существует несколько видов микровизоров, отличающихся по функционалу и своим возможностям. Допустим, для простого оптического исследования топологии ИМС с постобработкой изображений можно эффективно использовать цифровые микровизоры серии μ Vizo (рис. 10а). Однако, если появляется потребность в разрешении 0.5 мкм, целесообразно использовать электронный микроскоп. Например, электронный микроскоп серии JEOL JIB-4601F в отличие от конкурентов обладает ионной пушкой, что позволяет применять его как универсальный инструмент для реинжиниринга ИМС разрушающим методом (рис. 10б). Учитывая уже приведенные недостатки разрушающих методов, нельзя исключить и применение атомно-силовой микроскопии (АСМ), основанной на взаимодействиях Ван-дер-Ваальса.

Используют сканирующие зондовые и оптические микроскопы, например, серию Certus Optic, главным достоинством которой является разрешающая сила, позволяющая получать изображения с разрешением от 0.1 до 10 нм (рис. 10в).

На основании изложенных методов и средств предлагаются следующие методы противодействия спецпроектным реинжиниринговым исследованиям ИМС на различных уровнях:

- на уровне чипа:

- 1) использование фиктивной ЭКБ. В качестве компонентов могут быть неработоспособные (непроводящие или всегда открытые) транзисторы, мнимые (непроводящие) вертикальные межсоединения, избыточные проводящие дорожки, то есть элементы, которые никак не влияют на характеристики изделия в целом;

- 2) использование избыточных слоев топологии в ИМС;



Рис. 10. Установки микровизионной, растрово-электронной и атомно-силовой микроскопии: микровизоры μ Vizo-101 (а); электронные микроскопы типа JEOL JIB-4601F (б); зондооптический микроскоп Certus Optic U (в).

3) использование в структуре ИМС «скрытых» (не видимых микровизионными способами) функциональных компонентов;

- на уровне защитных покрытий и физико-химической структуры корпуса:

1) изготовление корпуса ИМС из материалов, устойчивых к методам механического, химического и термического разрушающих воздействий;

2) использование встраиваемых электронных систем защищенного доступа самоуничтожения. Так, например, в структуру корпуса ИМС вводят пьезокристалл, который под воздействием механической деформации индуцирует высоковольтный разряд, разрушительно действующий на элементы КМОП-логики;

3) использование химических примесей в структуре корпуса ИМС (как правило, полимерного). Так, при попытке химического травления корпуса данная примесь вступает в реакцию с кислотой, что приводит к экзотермической реакции, и кристалл уничтожается.

- на уровне аппаратной блокировки:

1) блокировка доступа к интерфейсу ввода/вывода данных ПЗУ [10, 11]. Реализовать механизм можно следующим способом: выполнить выжигание одного или нескольких выводов микросхемы, предназначенных для чтения/записи данных в ПЗУ, подав на порт ИМС предельно допустимый ток;

- на системно-технологическом уровне:

1) использование специализированной ячейки памяти – бита защиты, отвечающего за отключение доступа к данным. В простейшем варианте этот бит контролирует функцию чтения программного интерфейса;

2) криптографические средства защиты;

3) размещение специальной сетки в корпусе чипа, на которой непрерывно контролируется изменение емкости [2, 12], что позволяет идентифицировать и блокировать сигнальное тестовое или деструктурирующее воздействие путем затирания ключевых кодовых данных;

4) применение технологии стохастической аутентификации на базе технологии физически неклонируемых функций [13]. Так, на производстве изделие ИМС получается уникальным за счет неконтролируемых факторов (погрешностей и случайностей). Эти особенности можно регистрировать и использовать как уникальный идентификатор.

4. Методы и средства высокоточного стереолазерного сканирования элементов с многопрофильной геометрией

Для получения трехмерных моделей объектов в реинжиниринге используется метод обратного моделирования по физическим объектам. Первым этапом обратного моделирования обычно является процесс 3D-сканирования, т. е. процесс определения координат точек, принадлежащих поверхностям проектируемых изделий. Полученные модели могут быть экспортированы в CAD-системы и в дальнейшем модифицироваться. В промышленном производстве с помощью 3D-сканирования может осуществляться:

- контроль точности изготовления – устанавливается степень отличия от проектной документации;
- раскрытие дизайна, функционирования и способа производства продукции конкурентов;
- цифровое архивирование для воспроизводства устаревших компонентов, изделий с утерянной конструкторской документацией, а также геометрических моделей из устаревших систем проектирования без необходимости повторного проектирования;
- разработка компонентов для существующих товаров и изделий, разработка упаковки по форме физического объекта (переоборудование и вторичный рынок);
- репродукция в масштабе существующих объектов (модели и макеты);
- производство оснастки для ремонта, обновления и замены изношенных деталей [14].

4.1. Методы получения трехмерных моделей

В настоящее время существуют различные бесконтактные оптические методы получения геометрических моделей (рис. 11).



Рис. 11. Бесконтактные оптические методы для получения трехмерных моделей.

Бесконтактные оптические методы получения трехмерных моделей делятся на две группы: активные и пассивные. Активные 3D-сканеры излучают на объект сканирования свет, луч лазера, ультразвук или рентгеновские лучи и считывают отражение. Действие пассивных 3D-сканеров (не содержащих источники излучения) основано на принципе обнаружения отраженного окружающего излучения.

Бесконтактные 3D-сканеры также можно разделить по принципу работы на три основные технологии сканирования:

- триангуляции;
- структурированного освещения;
- стереоскопии.

Триангуляция основана на проецировании лазерного луча на объект сканирования. Все искажения воспринимаются измерительной камерой, которая отслеживает положе-

ние лазерного луча; полученные данные передаются на компьютер.

Сканирование на основе структурированного света заключается в проецировании на объект линий, образующих уникальный узор, каждое изменение которого сканируется приемной камерой.

Стереоскопия представляет собой фотографирование исходного объекта с различных ракурсов и воссоздание на основе полученных изображений трехмерной модели, координаты точек получают в результате компьютерной обработки.

4.2. Сканирование изделий РЭС методом триангуляции

Системы триангуляционного сканирования используются для воссоздания трехмерной структуры объектов с использованием структурированной подсветки. В основе принципа работы лазерных триангуляционных измерителей лежит метод определения расстояния между лакируемым объектом контроля и приемником излучения канала регистрации.

Эта технология названа триангуляцией, потому что лазерная точка, камера и сам лазерный излучатель образуют своеобразный треугольник. Известна длина одной стороны АВ этого треугольника – расстояние между камерой и лазерным излучателем (рис. 12а). Известен также угол лазерного излучателя α . А вот угол камеры β можно определить по расположению лазерной точки в поле обзора камеры [15]. Эти три показателя полностью определяют форму и размер треугольника (рис. 12б) и указывают на расположение угла лазерной точки.

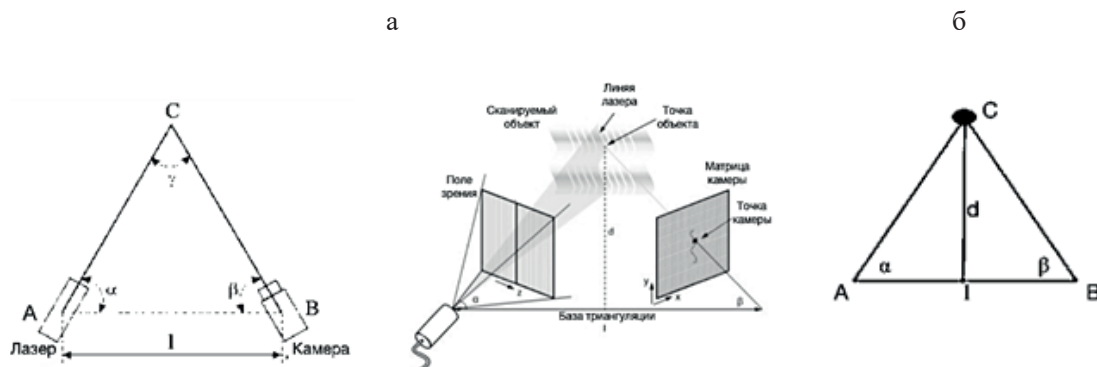


Рис. 12. Геометрия построения триангуляционных систем.

В большинстве случаев, чтобы ускорить процесс получения данных, вместо лазерной точки пользуются лазерной полосой.

Для определения координат точки на плоскости необходимо найти высоту d (расстояние от точки С до базы триангуляции) в треугольнике ABC (рис.12б), для чего воспользуемся формулой определения катетов в полученных прямоугольных треугольниках:

$$d = \frac{l \cdot \sin(\alpha) \cdot \sin(\beta)}{\sin(\alpha + \beta)} \quad (1)$$

Чтобы построить 3D-модель объекта, необходимо знать пространственные координаты. Получить их можно, рассмотрев модель на рис. 13.

Зная координаты на плоскости, можно найти координаты для построения 3D-модели по следующим формулам:

$$X = \frac{\tan(\alpha) \cdot l \cdot x}{f + x \cdot \tan(\alpha)} \quad (2)$$

$$Y = \frac{\tan(\alpha) \cdot l \cdot y}{f + x \cdot \tan(\alpha)}, \quad (3)$$

$$Z = \frac{\tan(\alpha) \cdot l \cdot f}{f + x \cdot \tan(\alpha)}, \quad (4)$$

Дальность действия сканеров такого типа составляет от 10 см до 25 м, ошибки в измеряемых углах, вызванные влиянием атмосферы (рефракцией и затуханием электромагнитных колебаний), практически не оказывают влияния на результаты измерений. Точность получения пространственных координат точек объекта триангуляционными сканерами составляет от 50 мкм до 0.3 мм и в основном зависит от величины измеряемого расстояния, инструментальных ошибок прибора, методических ошибок, связанных с точностью математических решений, положенных в основу управляющего программного продукта сканера, а также от материала, текстуры и формы сканируемого объекта.

Идеальными для сканирования триангуляционным сканером являются однородные отражающие поверхности, так как это позволяет избежать ошибок при определении углов.

Если объект или сканер переместится в пространстве, то результаты сканирования будут ложными. Поэтому так важно устанавливать и объект, и сканер на фиксированной платформе и свести возможность вибрации к минимуму. Следовательно, сканирование объектов в движении практически невыполнимо.

4.3. Сканирование структурированным светом

3D-сканеры, работающие по технологии структурированного света, как правило, состоят из источника структурированного света – проектора и нескольких видеокамер. Проектор проецирует на сканируемый объект световую сетку, форма и искажения которой фиксируются видеокамерами. Алгоритмы обработки изображений и триангуляции преобразуют эти искажения в облако 3D-точек. Облако точек можно использовать непосредственно для анализа объекта или легко экспортировать в различные форматы моделирования САПР.

Для каждой камеры необходимо определить, будет ли данный пиксель непосредственно подсвечиваться проектором в каждом отображаемом изображении (рис. 14).

Преимуществами 3D-сканера, использующего структурированный свет, является скорость и точность работы.

Вместо сканирования одной точки в один момент времени структурированные сканеры сканируют одновременно несколько точек или все поле зрения сразу. Сканирование всего поля зрения занимает долю секунды, а сгенерированные профили являются более точными, чем лазерные триангуляции. Это полностью решает проблему искажения данных, вызванную движением. Кроме того, некоторые существующие системы способны сканировать даже движущиеся объекты в режиме реального времени.

4.4. Сканирование методом стереоскопии

Рассмотрим пассивный бесконтактный метод сканирования – стереоскопию. Сканеры, работающие по данному методу, не имеют источника света, используется отраженный свет из окружающей среды. Стереоскопические системы предусматривают использова-

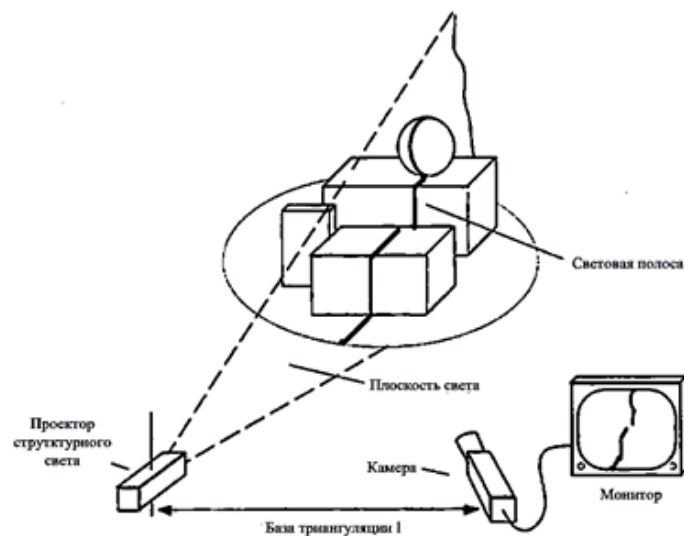


Рис. 14. Построение системы сканирования структурированным светом.

ние нескольких видеокамер. Камеры должны быть сонаправлены, но могут находиться в разных местах. Получая снимки с каждой из камер, определяют расстояние z (рис. 15а) до каждой точки изображения и затем вычисляют их координаты [16].

Для определения z (расстояния до точки P сканируемого объекта) нужно воспользоваться соотношениями подобия треугольников PNC_r , PMC_r , $p_l LC_l$ и $p_r RC_r$ (рис. 15б). Проекция точки P (сканируемого объекта) лежит в левой и правой плоскостях изображения в точках p_l и p_r . Установим за начало координат левый центр линзы:

$$z = \frac{b \cdot f}{(x'_l - x'_r)} \quad (5)$$

Таким образом может быть установлена глубина в различных точках сканируемого объекта. Из-за дискретности цифровых изображений значения неравенства являются це-

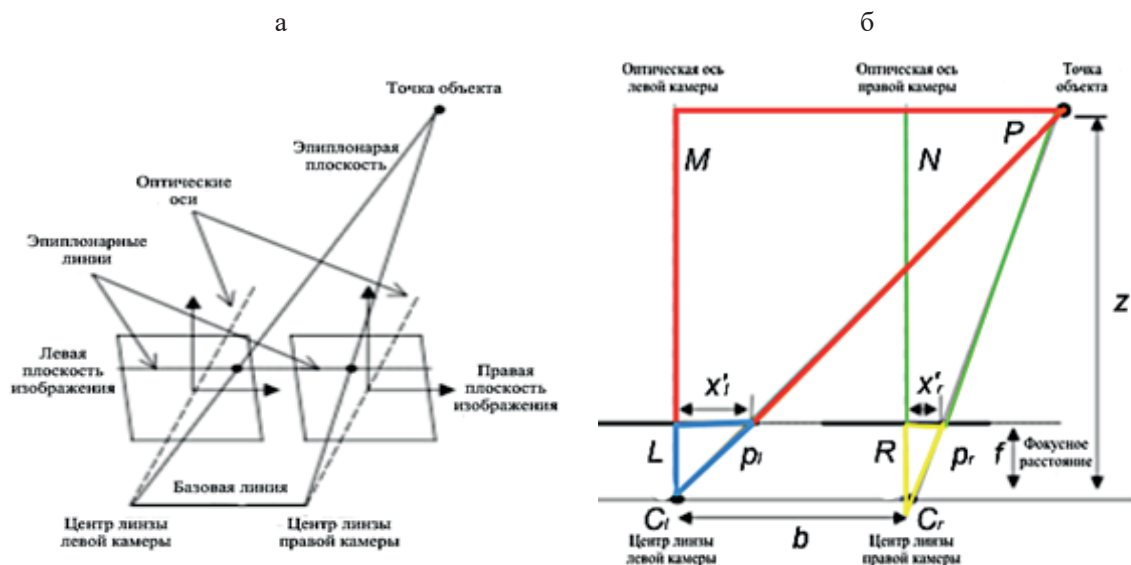


Рис. 15. Геометрия построения стереоскопических систем.

лыми числами. Точность вычисления глубины для заданной точки повышается за счет увеличения базового расстояния b . Однако такие широкоугольные методы стереоскопии создают другие проблемы. Например, когда базовое расстояние увеличивается, уменьшается доля всех точек облака, которые наблюдаются на обеих камерах. Более того, даже те области, которые видны обеими камерами, скорее всего, будут выглядеть по-разному на одном изображении по сравнению с соответствующими областями другого изображения из-за искажений, создаваемых перспективной проекцией, что затрудняет идентификацию сопряженных пар.

4.5. Прототипирование радиоэлектронных изделий

Рассмотрим процесс прототипирования (рис. 16). В общем случае процесс включает следующие этапы: визуальный анализ конструкции изделия; сканирование; создание и редактирование триангуляционной модели (при использовании бесконтактных методов сканирования, основанных на технологиях структурированного белого света и лазерного луча); построение базовых поверхностей; контроль базовых поверхностей; создание прототипа посредством 3D-печати; построение 3D-модели; контроль 3D-модели и ее доработка (при необходимости).

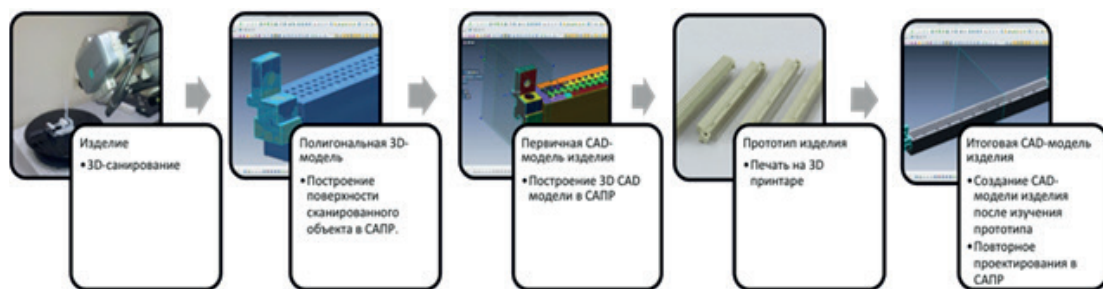


Рис. 16. Процесс прототипирования радиоэлектронных изделий.

Сначала происходит процесс сканирования объекта и создания облака точек, которые с помощью САПР моделируются в поверхности объекта через неоднородный рациональный В-сплайн, NURBS (математическая форма, применяемая в компьютерной графике для генерации и представления кривых и поверхностей) или же редактируемые CAD-модели (также известные, как объемные (монокитные) модели) (рис. 17).



Рис. 17. Этапы получения CAD-модели.

Существует несколько подходов, позволяющих получить параметрическую САПР-модель. Одни предполагают только экспорт NURBS-поверхности, оставляя САПР инженеру, чтобы завершить моделирование. Другие – используют данные сканирования для создания редактируемой функциональной модели.

Таким образом, комплекс технических мер противодействия стереолазерному и инфракрасному прототипированию может быть представлен следующими предложенными

техническими рекомендациями: создание шероховатой поверхности, использование отражающих материалов и использование полупрозрачных покрытий.

Действительно, одной из причин расходимости пучка лазера является шероховатость (неоднородность) поверхности. Когда лазерный луч попадает на край объекта, луч разделяется на две части. Одна часть луча отражается от края поверхности, а другая часть движется дальше, чтобы попасть на следующую поверхность (рис. 18а). В результате информация от одного лазерного импульса, который отправляется обратно в приемник (камеру), поступает из двух разных мест в пространстве. Координаты для такой точки относительно положения сканера будут вычисляться на основе среднего числа возвращенных сигналов, и поэтому координаты точки не будут соответствовать действительности.

При использовании сканирования высокого разрешения увеличивается вероятность попадания луча на край, и полученные данные будут показывать шум сразу за краями объекта. Сканеры с меньшей шириной луча помогают решить эту проблему, но остается ограничение по дальности действия, так как при ее увеличении увеличивается ширина луча.

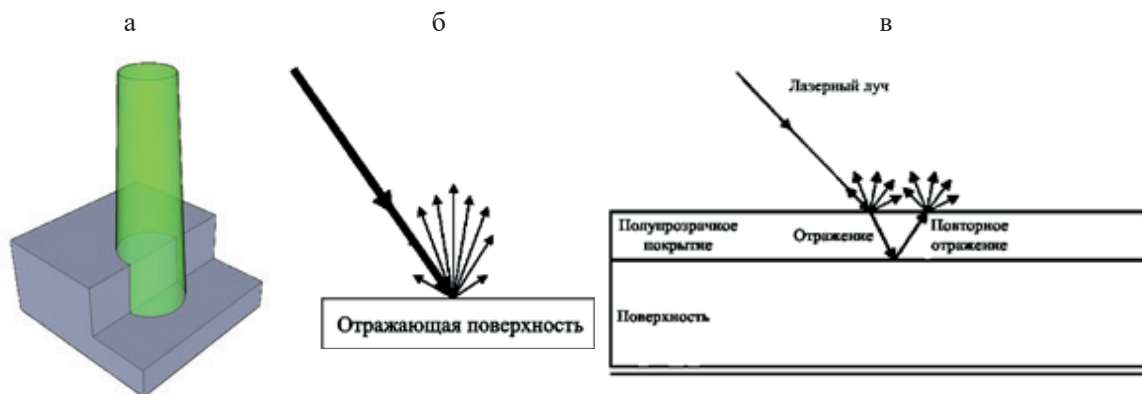


Рис. 18. Попадание луча лазера на поверхность объекта.

Поскольку сканеры регистрируют отражение лазерного луча от поверхности, необходимо учитывать физические законы отражения и оптические свойства материалов. Лучи монохроматического света обычно отражаются во многих направлениях (рис. 18б).

На лазерный луч влияет поглощение сигнала, проходящего через воздух, отражение материала сканируемого объекта и угол между лазерным лучом и нормалью к поверхности. Это означает, что для очень темных (черных) поверхностей, поглощающих большую часть видимого спектра, отраженный сигнал будет очень слабым, поэтому точность координат точки исказится. Поверхности с высокой отражательной способностью (т. е. яркие поверхности) дают более надежные и точные измерения диапазона. Однако, если отражательная способность объекта слишком высока (металлическая поверхность, светоотражающая лента и др.), лазерный луч полностью отклоняется в направлении зеркального отражения и попадает на другую поверхность. Отклонение приводит к тому, что получаемые координаты не являются координатами точки, на которую указывает лазер, или точка вообще не принадлежит сканируемой поверхности.

Помимо эффектов отражения, ряд материалов имеет полупрозрачное покрытие, которое позволяет лазерному лучу преломлять и отражать в самом материале. Эти эффекты приводят к сложению констант при измерении расстояния, что необходимо учитывать при вычислении (рис. 18в).

Заключение

Конструкторско-технологические решения производства печатных модулей и интегральных микросборок усложняются, приобретая комплексную направленность реализации оригинальных технических предложений с внедрением перспективных материалов и разработок, что усиливает спрос на специфическую деятельность, связанную с развитием процесса разработки новых методов спецпроектного реинжиниринга – параметрического прототипирования изделий РЭС. Одной из стратегий спецпроектных реинжиниринговых исследований является создание нового прототипного изделия и параметрическое исследование и диагностика с целью повышения его качества и надежности и т. д. Однако без знаний способов реинжиниринга невозможна организация противодействия ему, поэтому проводимые исследования в этой области имеют ключевую роль в обеспечении информационно-технической безопасности радиоэлектронной аппаратуры.

Рассмотренные в работе методы и средства спецпроектного прототипирования конструкций радиоэлектронных изделий и особенности технологий производства позволяют выработать комплекс технических мер противодействия спецпроектным исследованиям.

Литература:

1. Костин М.С., Воруничев Д.С. Реинжиниринг радиоэлектронных средств: монография. М.: Московский технологический университет (МИРЭА), 2018. 132 с.
2. Костин М.С., Воруничев Д.С., Марков Д.В. Реинжиниринговые исследования печатных плат с многослойной топологией в аспектах обеспечения технического противодействия // Оборонный комплекс – научно-техническому прогрессу России. 2018. № 1. С. 47–56.
3. Keng Tiong Ng. The art of PCB reverse engineering (standard edition): Unravelling the beauty of the original design. USA: Create Space Independent Publishing Platform, 2015. 372 p.
4. Asadizanjani N., Shahbazmohamadi S., Tehranipoor M., Forte D. Non-destructive PCB reverse engineering using X-ray micro computed tomography // Proceed. of the 41st International Symposium for Testing and Failure Analysis, ASM. Oregon, USA: ASM Int., 2015. P. 1–5.
5. Костин М.С., Воруничев Д.С. Тепловизионная электротермия топологии печатных плат в магнитном поле плоского ВЧ-индуктора // Журнал радиоэлектроники [электронный журнал]. 2017. № 9. URL: <http://jre.cplire.ru/jre/sep17/7/text.pdf> (дата обращения 09.11.2018).
6. Bukroyd A. In-Circuit Testing. USA: Butterworth-Heinemann, 2015. 168 p.
7. Костин М.С., Воруничев Д.С., Марков Д.В., Латышев К.В. Реинжиниринг радиоэлектронных цепей и сигналов печатных узлов с многослойной топологией в аспектах обеспечения технического противодействия // Оборонный комплекс – научно-техническому прогрессу России. 2018. № 3. С. 49–56.
8. Castillo-León J., Svendsen W. Lab-on-a-Chip devices and micro-total analysis systems: a practical guide. USA: Springer, 2015. 243 p.
9. Flich J., Bertozzi D. Designing Network On-Chip Architectures in the Nanoscale Era. USA: Chapman and Hall/CRC, 2010. 528 p.
10. Li W., Wasson Z., Seshia S. Reverse engineering circuits using behavioral pattern mining

// In: Hardware-Oriented Security and Trust (HOST), International Symposium on IEEE. USA: IEEE, 2012. P. 83–88.

11. Guin U., DiMase D., Tehranipoor M. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead // J. Electronic Testing. 2014. V. 30. № 1. P. 9–23.

12. Curtis S.K., Harston S.P., Mattson C.A. The fundamentals of barriers to reverse engineering and their implementation into mechanical components // Res. Eng. Design. 2011. V. 22. № 4. P. 245–261.

13. Böhm Ch., Hofer M. Physical Unclonable Functions in Theory and Practice. USA: Springer Science & Business Media, 2012. 270 p.

14. Середович В.А., Комиссаров А.В., Комиссаров Д.В., Широкова Т.А. Наземное лазерное сканирование: монография. Новосибирск: СГГА, 2009. 261 с.

15. Akyol O., Duran Z. Low-cost laser scanning system design // J. Russ. Laser Res. 2014. V. 35. № 3. P. 244–251.

16. Torrance R., James D. The State-of-the-Art in IC Reverse Engineering // In: Cryptographic Hardware and Embedded Systems (CHES) // Lecture Notes in Computer Science. Berlin: Springer, 2009. V. 5747. P. 363–381.

References:

1. Kostin M.S., Voronichev D.S. Reengineering of radio electronic equipment: monograph. Moscow: Moscow Technological University (MIREA), 2018. 132 p. (in Russ.)

2. Kostin M.S., Voronichev D.S. Reengineering study of PCB with multi-layer topology in aspects ensuring technical counteraction. *Oboronnyy kompleks – nauchno-tekhnicheskomu progressu Rossii* (Defense complex – for scientific and technical progress of Russia). 2017; 1: 47-56. (in Russ.)

3. Keng Tiong Ng. The art of PCB reverse engineering (standard edition): Unravelling the beauty of the original design. USA: Create Space Independent Publishing Platform, 2015. 372 p.

4. Asadizanjani N., Shahbazmohamadi S., Tehranipoor M., Forte D. Non-destructive PCB reverse engineering using X-ray micro computed tomography. *Proceed. of the 41st International Symposium for Testing and Failure Analysis, ASM*. Oregon, USA: ASM Int., 2015. P. 1-5.

5. Kostin M.S., Voronichev D.S. Thermal vision electrothermia of the topology of PCB in the magnetic field of the flat HF-inductor. *Zhurnal radioelektroniki* (Electronic network journal) [electronic network journal]. 2017; 9. URL: <http://jre.cplire.ru/jre/sep17/7/text.pdf>. (in Russ.)

6. Bukroyd A. In-Circuit Testing. USA: Butterworth-Heinemann, 2015. 168 p.

7. Kostin M.S., Voronichev D.S., Markov D.V., Latyshev K.V. Reengineering of electronic circuits and signals of node PCB with multi-layer topology in aspects ensuring technical counteraction. *Oboronnyy kompleks – nauchno-tekhnicheskomu progressu Rossii* (Defense complex – for scientific and technical progress of Russia). 2018; 3: 49-56. (in Russ.)

8. Castillo-León J., Svendsen W. Lab-on-a-Chip devices and micro-total analysis systems: a practical guide. USA: Springer, 2015. 243 p.

9. Flich J., Bertozzi D. Designing Network On-Chip Architectures in the Nanoscale Era. USA: Chapman and Hall/CRC, 2010. 528 p.

10. Li W., Wasson Z., Seshia S. Reverse engineering circuits using behavioral pattern mining. In: Hardware-Oriented Security and Trust (HOST), International Symposium on IEEE.

USA: IEEE, 2012. P. 83-88.

11. Guin U., DiMase D., Tehranipoor M. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *J. Electronic Testing*. 2014; 30(1): 9-23.

12. Curtis S.K., Harston S.P., Mattson C.A. The fundamentals of barriers to reverse engineering and their implementation into mechanical components. *Res. Eng. Design*. 2011; 22(4): 245-261.

13. Böhm Ch., Hofer M. Physical Unclonable Functions in Theory and Practice. USA: Springer Science & Business Media, 2012. 270 p.

14. Seredovich V.A., Komissarov A.V., Komissarov D.V., Shirokova T.A. Terrestrial laser scanning: monograph. Novosibirsk: SGGa (Siberian State Academy of Geodesy) Publ., 2009. 261 p. (in Russ.)

15. Akyol O., Duran Z. A low-cost laser scanning system design. *J. Russ. Laser Res.* 2014; 35(3): 244-251.

16. Torrance R., James D. The State-of-the-Art in IC Reverse Engineering. Crypto-graphic Hardware and Embedded Systems (CHES). *Lecture Notes in Computer Science*. Berlin: Springer, 2009; 5747: 363-381.

Об авторах:

Костин Михаил Сергеевич, кандидат технических наук, доцент кафедры конструирования и производства радиоэлектронных средств Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Воруничев Дмитрий Сергеевич, заместитель директора Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Корж Дмитрий Алексеевич, инженер кафедры конструирования и производства радиоэлектронных средств Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

About the authors:

Mikhail S. Kostin, Ph.D. (Engineering), Associate Professor of the Chair of Design and Production of Radio Electronic Equipment, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Dmitriy S. Vorunichev, Deputy Director of the Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Dmitriy A. Korzh, Engineer of the Chair of Design and Production of Radio Electronic Equipment, Institute of Radio Engineering and Telecommunications Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Для цитирования: Костин М.С., Воруничев Д.С., Корж Д.А. Контрреинжиниринг радиоэлектронных средств // Российский технологический журнал. 2019. Т. 7. № 1. С. 57–79. DOI: 10.32362/2500-316X-2019-7-1-57-79

For citation: Kostin M.S., Vorunichev D.S., Korzh D.A. Counterreengineering of electronic devices. *Rossiyskiy tekhnologicheskij zhurnal* (Russian Technological Journal). 2019; 7(1): 57-79. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-57-79

**ПРОТОТИПИРОВАНИЕ СВЧ-УСТРОЙСТВ С ЗАДААННЫМИ
ЭЛЕКТРОДИНАМИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ
ПО ТЕХНОЛОГИИ АДДИТИВНОЙ 3D-ПЕЧАТИ**

**С.В. Харалгин^{1,2,@},
Г.В. Куликов¹,
А.Б. Котельников³,
М.В. Снастин⁴,
Е.М. Добычина⁴**

¹МИРЭА – Российский технологический университет, Москва 119454, Россия

²Центральный научно-исследовательский радиотехнический институт имени академика А.И. Берга, Москва 107078, Россия

³Московский педагогический государственный университет, Москва 119991, Россия

⁴Московский авиационный институт (Национальный исследовательский университет), Москва 125993, Россия

@Автор для переписки, e-mail: hsvl92@mail.ru

Целью настоящего исследования является оценка и изучение возможностей технологии 3D-печати, применяемой для производства СВЧ-приборов, и сравнение характеристик полученных устройств с характеристиками электродинамической модели. Печатаение металлических деталей является чрезмерно дорогостоящим процессом в мелкосерийном производстве, причем и с точки зрения стоимости оборудования, и применительно к используемым материалам. Детали микроволновых устройств изготовлены нами из пластика. Относительно дешевые полимеры, используемые в 3D-печати, являются диэлектриками, и чтобы ограничить распространение электромагнитной волны во всех направлениях, потребовалось создание проводящего слоя на поверхности печатных моделей. В статье определены параметры печати FFF, которые в наибольшей степени влияют на распространение электромагнитной волны, описан процесс и проблемы, возникающие при печати и гальванизации деталей, обсуждаются этапы моделирования устройств и измерения их параметров. Для реализации проводящего слоя на поверхности моделей использовали метод гальванизации. В статье исследованы адгезионные свойства полученных металлических покрытий, приведены результаты электромагнитного моделирования, определены параметры, которые в наибольшей степени влияют на качество реализованных устройств. Исследованы характеристики микроволновых приборов, выполненных по технологии 3D-печати. Проведена оценка возможностей изготовления антенн и коаксиально-волноводных переходов с использованием этой технологии. Проведены лабораторные измерения характеристик изготовленных приборов. Результаты моделирования рассмотренных устройств хорошо согласуются с экспериментальными.

ми характеристиками изготовленных моделей с использованием технологии 3D-печати. Проведен полный цикл производства микроволновых устройств: проектирование, моделирование, производство образцов и валидация характеристик. Перспективы дальнейшего развития описанной технологии включают в себя изменение типов пластмасс, используемых в качестве субстрата, применение отделочных декоративных и функциональных покрытий, улучшение адгезионных свойств нанесенного слоя меди с подложкой.

Ключевые слова: технология 3D-печати, рупорная антенна, коаксиально-волноводный переход, аддитивные технологии, гальванизация.

PROTOTYPING OF MICROWAVE DEVICES WITH SPECIFIED ELECTRODYNAMIC CHARACTERISTICS USING ADDITIVE 3D PRINTING TECHNOLOGY

**S.V. Kharalgin^{1,2,@},
G.V. Kulikov¹,
A.B. Kotelnikov³,
M.V. Snastin⁴,
E.M. Dobychina⁴**

¹*MIREA – Russian Technological University, Moscow 119454, Russia*

²*Academician A.I. Berg Central Scientific Research Radio Engineering Institute, Moscow 107078, Russia*

³*Moscow Pedagogical State University, Moscow 119991, Russia*

⁴*Moscow Aviation Institute (National Research University), Moscow 125993, Russia*

@Corresponding author e-mail: hsvl92@mail.ru

The technology of additive 3D printing is widely used in various branches of science and industry. The purpose of the research presented in the article is to evaluate and study the possibilities of 3D printing technology applied to the manufacture of microwave devices and to compare the characteristics of the devices obtained with the characteristics used in the electrodynamic model. Printing metal parts is an overly expensive process in small-scale production, both in terms of the cost of equipment and in relation to the materials used. In this work, parts for microwave devices were made of plastic with the aim of cheapening. Relatively cheap polymers used in 3D printing are dielectrics. Therefore, to limit the propagation of an electromagnetic wave in all directions it was necessary to create a conductive layer on the surface of printed models. The article: identifies the FFF print parameters that affect to the maximum extent the propagation of an electromagnetic wave; describes the process and problems encountered when printing and galvanizing parts; discusses the steps of modeling devices and measuring their parameters. The characteristics of microwave devices made by 3D printing technology were investigated. An assessment of the possibilities of manufacturing antennas and coaxial-waveguide transitions using this technology was carried out. To implement the conductive layer on the surface of the models, the method of galvanization was used. The adhesion properties of the obtained metallic coatings were investigated. The results of electromagnetic modeling are given. The parameters that affect to the maximum extent the quality of the implemented devices were determined.

Laboratory measurements of the characteristics of produced devices were conducted. The simulation results of the examined devices are in good agreement with the experimental characteristics of the made models using 3D printing technology. A complete production cycle of microwave devices was carried out: design, simulation, sample production, and validation of characteristics. Prospects for the further development of the described technology include a variation of the types of plastics used as a substrate, the application of finishing decorative and functional coatings, an improvement in the adhesion properties of the applied copper layer with the substrate.

Keywords: 3D printing technology, horn antenna, coaxial-waveguide transition, additive technologies, galvanization.

Введение

В настоящее время технология аддитивной 3D-печати находит широкое применение в различных отраслях науки и производства. При этом печать цельнометаллических деталей до сих пор является чрезмерно дорогостоящим процессом с точки зрения мелкосерийного производства как в плане стоимости оборудования, так и в отношении расходных материалов.

Целью представленных в статье исследований являлась оценка и проработка возможностей технологии 3D-печати применительно к изготовлению устройств СВЧ и сравнение характеристик полученных устройств с характеристиками, закладываемыми в электродинамической модели.

Заготовки для реализованных устройств СВЧ с целью удешевления изготавливали из пластика. Поскольку относительно дешевые полимеры, используемые в 3D-печати, являются диэлектриками, для ограничения распространения электромагнитной волны во всех направлениях потребовалось создание проводящего слоя на поверхности распечатанных моделей. В настоящей работе определяются параметры 3D-печати, которые в наибольшей степени влияют на распространение электромагнитной волны, описан процесс и проблемы, возникшие при печати и гальванизации деталей, рассмотрены этапы моделирования устройств и измерения их параметров.

1. Технологии, оборудование и материалы, используемые при прототипировании

Виды технологий 3D-печати. Среди существующих технологий 3D-печати можно выделить следующие: масочная стереолитография (SGC), технология многоструйного моделирования (MJM), цветная струйная печать (CJP), цифровая светодиодная проекция (DLP), струйная трехмерная печать (3DP), выборочное лазерное спекание (SLS), выборочная лазерная плавка (SLM), стереолитография (SLA), выборочное тепловое спекание (SHS), изготовление объектов методом ламинирования (LOM), электронно-лучевая плавка (EBM), прямое лазерное спекание металлов (DMLS), производство электронно-лучевой плавкой (EBF₃), моделирование методом послойного наплавления (FFF), технология ламинирования методом селективного осаждения (SDL) [1].

Низкая цена и широкая доступность оборудования и расходных материалов на российском рынке обусловили выбор для реализации моделей метода послойного наплавления (*Fused Filament Fabrication*, FFF). Процесс FFF-печати заключается в последова-

тельном нанесении слоев расплавленного пластика, подаваемого в место печати. Каждый слой наносимого пластика повторяет контуры соответствующего слоя исходной трехмерной модели, область внутри контуров может либо заполняться пластиком – при этом деталь получается монолитной, либо заполняться частично вплоть до печати пустотелой детали. Принтеры, используемые для такого типа печати, состоят из холодной или нагреваемой подвижной платформы (ПП), на которую наносится первый слой, а также печатающей головки, разогревающей поступающий в нее пластик (филамент). Остальные составляющие принтера определяются его конструкцией. Для перемещения печатающей головки и ПП применяют винтовые и ременные передачи, приводимые в движение шаговыми двигателями или серводвигателями. Линейность перемещения ПП и печатающей головки обеспечивают стальные направляющие рельсы.

Оборудование, используемое для 3D-печати. В рамках данной работы использовали принтер конструкции Prusa i3, представленный на рис. 1. Некоторые характеристики принтера приведены в табл. 1.

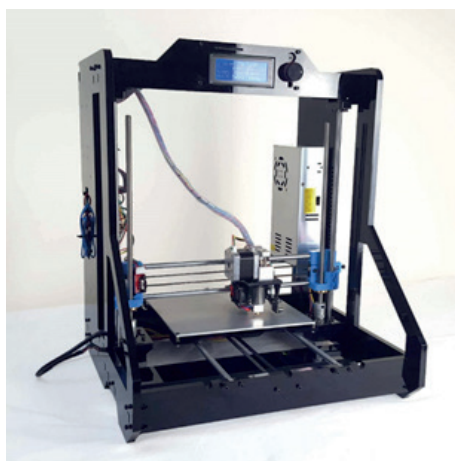


Рис. 1. 3D-принтер конструкции Prusa i3.

Таблица 1. Характеристики 3D-принтера

Характеристика	Значение
Размер печатной области, мм	210×210×230
Диаметр сопла печатающей головки, мм	0.2–0.6*
Минимальная высота слоя, мкм	100

* В настоящей работе использовано сопло диаметром 0.4 мм.

Исходная конструкция принтера доработана путем замены пластиковых составляющих на металлические, что повысило жесткость и обеспечило возможность поместить принтер в закрытую камеру. Размещение принтера в закрытой камере позволило создать при печати повышенную температуру воздуха внутри (около 65 °С), вследствие чего появилась возможность печати ABS-пластиком, уменьшилась усадка печатаемых моделей и устранилась деламинация от поверхности платформы. Из-за высокой температуры внутри камеры при печати ABS-пластиком плата управления, а также шаговые двигатели, подающие пластик в печатающую головку, вынесены на внешнюю часть печатной камеры. Печатная камера оборудована также вытяжной вентиляцией для увеличения обдува

¹ABS-пластик – термопластическая смола, сополимер акрилонитрила с бутадиеном и стиролом.

воздухом моделей, печатаемых из PLA-пластика². В принтере произведена замена печатающей головки с одним соплом на печатающую головку с двумя соплами для печати одновременно двумя типами пластика. Установлена зеркальная основа поверх ПП для увеличения адгезии. Перед печатью на поверхность зеркальной основы наносится слой лака, чтобы исключить деламинацию первого слоя модели.

Характеристики деталей, получаемых методом FFF-печати. Характеристики получаемых деталей зависят от параметров выбранного для печати материала и от настроек печати. В настоящей работе использовали PLA-пластик, характеристики которого приведены в табл. 2³ [2].

Таблица 2. Характеристики PLA-пластика

Характеристика	Значение
Температура плавления, °С	173–178
Температура размягчения, °С	50
Твердость (по Роквеллу)	R70–R90
Относительное удлинение при разрыве, %	3.8
Прочность на изгиб, МПа	55.3
Прочность на разрыв, МПа	57.8
Модуль упругости при растяжении, ГПа	3.3
Модуль упругости при изгибе, ГПа	2.3
Температура стеклования, °С	60–65
Плотность, г/см ³	1.23–1.25
Минимальная толщина стенок, мм	1
Усадка при изготовлении изделий	Нет
Влагопоглощение, %	0.5–50

С целью повышения прочности детали печатали со 100-процентным межслойным заполнением. Перед печатью в настройках принтера задавали условие, чтобы каждый последующий слой наносился так, что линии, по которым проходит печатающая головка, были повернуты на 90° относительно предыдущего слоя. В результате деталь печатается послойно, и полимер подается в сопло под давлением. Это приводит к тому, что расплавленный пластик накладывается на модель с бочкообразным профилем и внешняя поверхность распечатываемых изделий обладает ребристостью, как представлено на рис. 2.

Последующая абразивная обработка распечатанных деталей позволила выровнять поверхности, однако при исходном проектировании моделей пришлось учитывать усадки и изменения габаритных размеров в результате обработки.

Погрешности, возникающие при 3D-печати. Сегодня на рынке существует множество материалов для 3D-печати, обладающих различными характеристиками. Влияние вида материала на точность изготовления заключается в различной степени усадки материала в процессе остывания распечатанной модели. Выбор PLA-пластика обусловлен тем, что он обладает меньшим коэффициентом усадки.

Следующая погрешность определялась качеством сборки конструкции 3D-принтера. Отклонения от перпендикулярности различных направляющих ПП и печатающей

²PLA-пластик – термопластичный алифатический полиэфир.

³PLA-пластик для 3D-печати [Электронный ресурс]. URL: http://3dtoday.ru/wiki/PLA_plastic/ (дата обращения: 11.01.2019).

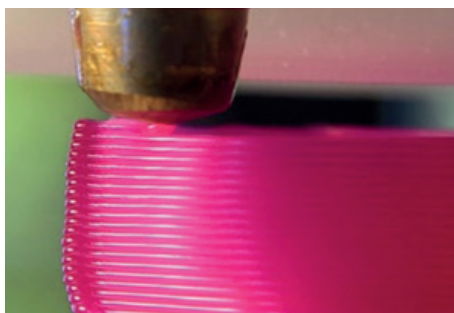


Рис. 2. Эффект ребристости при 3D-печати.

головки приводили к перекосам изготавливаемой модели. Подобную погрешность нивелировали путем калибровки области печати. На высоких скоростях печати инерционность ПП и печатающей головки приводила к погрешностям типа «волна» (рис. 3а) на внешних поверхностях деталей. Для печати изначально с помощью САД-программ разрабатывали компьютерную модель, которую переводили в сеточную модель, за счет чего и возникала погрешность, зависящая от степени детализации модели (рис. 3б).

Так как модель печатается послойно, а высота слоя конечна, то наблюдался тот же эффект, что и при цифровом преобразовании аналогового сигнала – погрешность дискретизации и квантования: гладкие наклонные поверхности компьютерной 3D-модели распечатывались ступенчато. Реализация полусферы при различной минимальной высоте слоя представлена на рис. 3в.

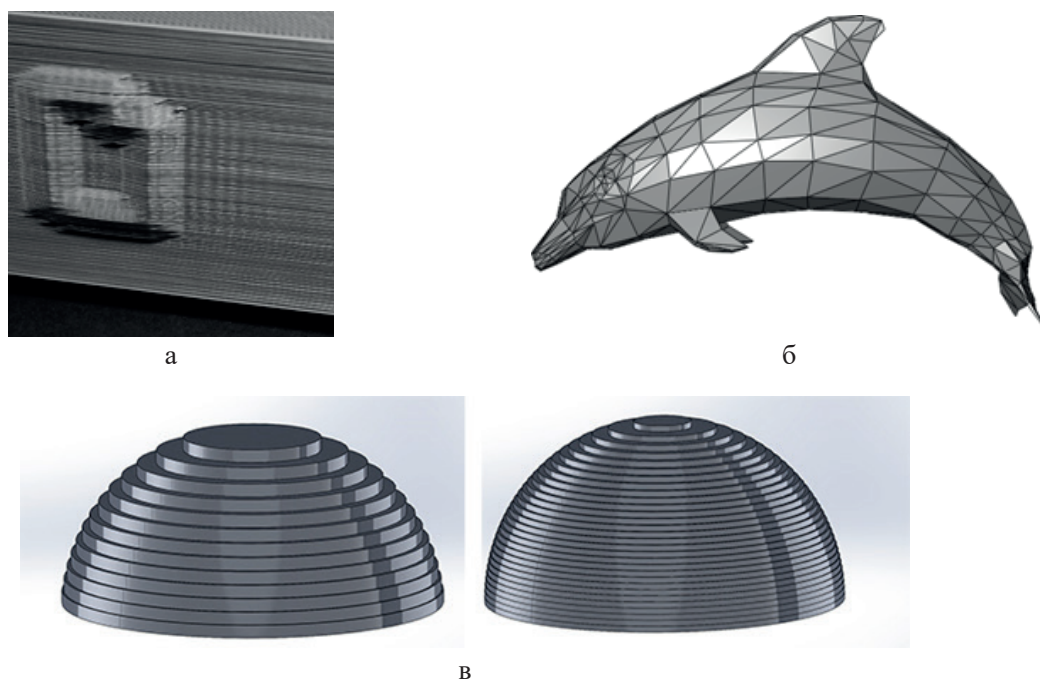


Рис. 3. Типовые источники погрешности при 3D-печати:

а – вследствие инерционности ПП; б – конечность детализации сеточной модели;
в – эффект ступенчатости при различной высоте слоя печати.

Минимальная высота слоя при печати дает еще одну погрешность: если требовалось распечатать некоторый выступ высотой 50 мкм, то при минимальной высоте слоя в 100 мкм возникала погрешность высоты выступа на 50 мкм.

Точность позиционирования печатающей головки зависит от значения минимального угла, на который могли повернуться валы шаговых двигателей, отвечающих за перемещение сопла.

Стабильность температуры печатающей головки существенно влияет на качество и точность печати. При температуре, превышающей оптимальную, повышается текучесть пластика, и ширина печатаемых линий увеличивается, что может привести к увеличению площади печатаемых линий. При пониженной температуре текучесть уменьшается, при этом также уменьшается толщина печатаемых линий, что может привести к неполному заполнению слоев и к худшей межслойной адгезии.

2. Моделирование и изготовление СВЧ-элементов

Реализация рупорного излучателя X-диапазона длин волн. Основой для реализации рупорного излучателя послужила публикация [3]. В нашей работе изначально повторяется реализация антенны X-диапазона с более подробным исследованием характеристик.

Первым этапом проектирования рупорного излучателя явилось создание модели в одной из систем электродинамического моделирования. При моделировании оценивались коэффициент стоячей волны по напряжению, диаграмма направленности и поверхностные токи. Определение силовых линий поверхностных токов в рупоре – это непростая задача, поскольку весьма трудоемко оклеивание алюминиевым скотчем полученной антенны с запитывающим волноводом сечением 23×10 мм. Чтобы упростить оклеивание, было решено изготавливать излучатель из отдельных частей с их металлизацией по отдельности.

Определение плоскости, по которой возможно разделить антенну на две части с наименьшим влиянием на характеристики распространяющейся волны, возможно с помощью анализа картины силовых линий поверхностных токов. Из теории щелевых антенн известно, что щель, прорезанная в волноводе, излучает только тогда, когда она пересекает силовые линии токов. Щель, прорезанная по центру широкой стенки прямоугольного волновода с основным типом волны H_{10} , не излучает, так как токи обтекают щель.

В дальнейшем предстояла проверка: изменится ли структура силовых линий токов на поверхности рупора, так как электромагнитная волна H_{10} претерпевает ряд изменений при распространении в рупоре.

Толщина алюминиевого скотча составляет 55 мкм. В связи с этим обстоятельством возникает ограничение по нижней граничной частоте. Из определения скин-эффекта известно, что плотность тока в металлическом проводнике убывает по экспоненциальному закону. Частота, для которой плотность тока уменьшилась на 20 дБ при толщине алюминиевого покрытия 55 мкм, составила 50 МГц. Снижение нижней граничной частоты достигается при применении медного скотча, имеющего большую проводимость. Наклеивание нескольких слоев скотча не имеет смысла в связи с тем, что клеевая основа скотча является диэлектриком.

Ограничение по верхней граничной частоте связано с шероховатостью поверхности, получаемой в процессе печати. Полученные в результате печати неровности приводят к увеличению фактической длины протекания тока и появлению диффузного рассеяния. Печать антенны выполняли с высотой слоя, равной 0.1 мм, и среднее значение высоты неровностей взято приблизительно равным значению высоты слоя. Из [4] известна связь

между неровностью поверхности устройства СВЧ и длиной волны. При условии, что рассеиваемая мощность не превышает 10% от аналогичного зеркального отражения, получаем:

$$\sigma_r \leq 0,025\lambda_b, \quad (1)$$

где σ_r – среднеквадратическое значение случайных неровностей, мм;

λ_b – длина волны в волноводе, мм.

Следовательно, для волновода, работающего в диапазоне частот 32.9–50 ГГц, технологическая неровность поверхности должна составлять 0.15 мм. Отсюда следует вывод, что изготовление устройств СВЧ при помощи 3D-печати без последующего выравнивания внутренних поверхностей и при оклеивании алюминиевым скотчем возможно в диапазоне частот 0.05–50 ГГц при условии рассеяния мощности в 10%.

После изготовления антенны последовал этап измерения характеристик. Измерения диаграммы направленности производили в антенном измерительно-вычислительном комплексе (АИВК) на базе безэховой камеры (БЭК) ФГБОУ ВО «Московский авиационный институт (Национальный исследовательский университет)». Лабораторный комплекс обеспечивает проведение автоматизированных измерений радиотехнических характеристик антенн, антенных систем и СВЧ-устройств в ближней и дальней зоне. Основные характеристики комплекса сведены в табл. 3.

Таблица 3. Параметры безэховой камеры

Характеристика	Значение
Частотный диапазон, ГГц	0.8–40
Коэффициент ослабления (экранирования) БЭК и дверей БЭК на частотах от 400 МГц до 40 ГГц, дБ, не менее	90
Коэффициент безэховости (уровень отраженного сигнала) при нормальном падении плоской волны и при падении плоской волны под углом 45°, дБ, не более	-30 дБ (на частотах от 1 до 40 ГГц); -20 дБ (на частотах от 0.8 до 1 ГГц)
Электрогерметичный экран	состоит из стальных панелей, соединенных методом сварки

При помощи стандартного коаксиально-волноводного перехода (КВП) рупор был подключен к векторному анализатору цепей с последующим съемом характеристик излучения в дальней зоне.

Амплитудную диаграмму направленности по углу α и ее нормированную величину рассчитывали следующим образом:

$$A(\alpha) = \sqrt{\mathbf{E}_x^2(\alpha) + \mathbf{E}_y^2(\alpha)} \sim \sqrt{S_{rt\ co}^2(\alpha) + S_{rt\ cx}^2(\alpha)},$$

$$A_{\text{норм}}(\alpha) = A(\alpha) / A_{\text{max}}, \quad (2)$$

где $\mathbf{E}_x$, $\mathbf{E}_y$ – ортогональные в пространстве компоненты вектора $\mathbf{E}$ напряженности электрической компоненты для произвольно поляризованной антенны;

$S_{rt\ co}^2, S_{rt\ cx}^2$ – коэффициенты передачи между приемной и передающей антеннами при их согласованной и кросс-поляризации, соответственно.

Согласно формуле идеальной радиопередачи [5, 6], коэффициент передачи между приемной и передающей антеннами равен:

$$S_{rt}^2 = G_r G_t \left(\frac{\lambda}{4\pi R} \right)^2, \quad (3)$$

где G_r, G_t – коэффициенты усиления приемной и передающей антенн;

λ – длина волны, м;

R – расстояние между фазовыми центрами антенн, м.

Сравнительные диаграммы направленности в двух сечениях модели и макета представлены на рис. 4. Штриховыми линиями обозначены диаграммы модели, сплошными – диаграммы макета.

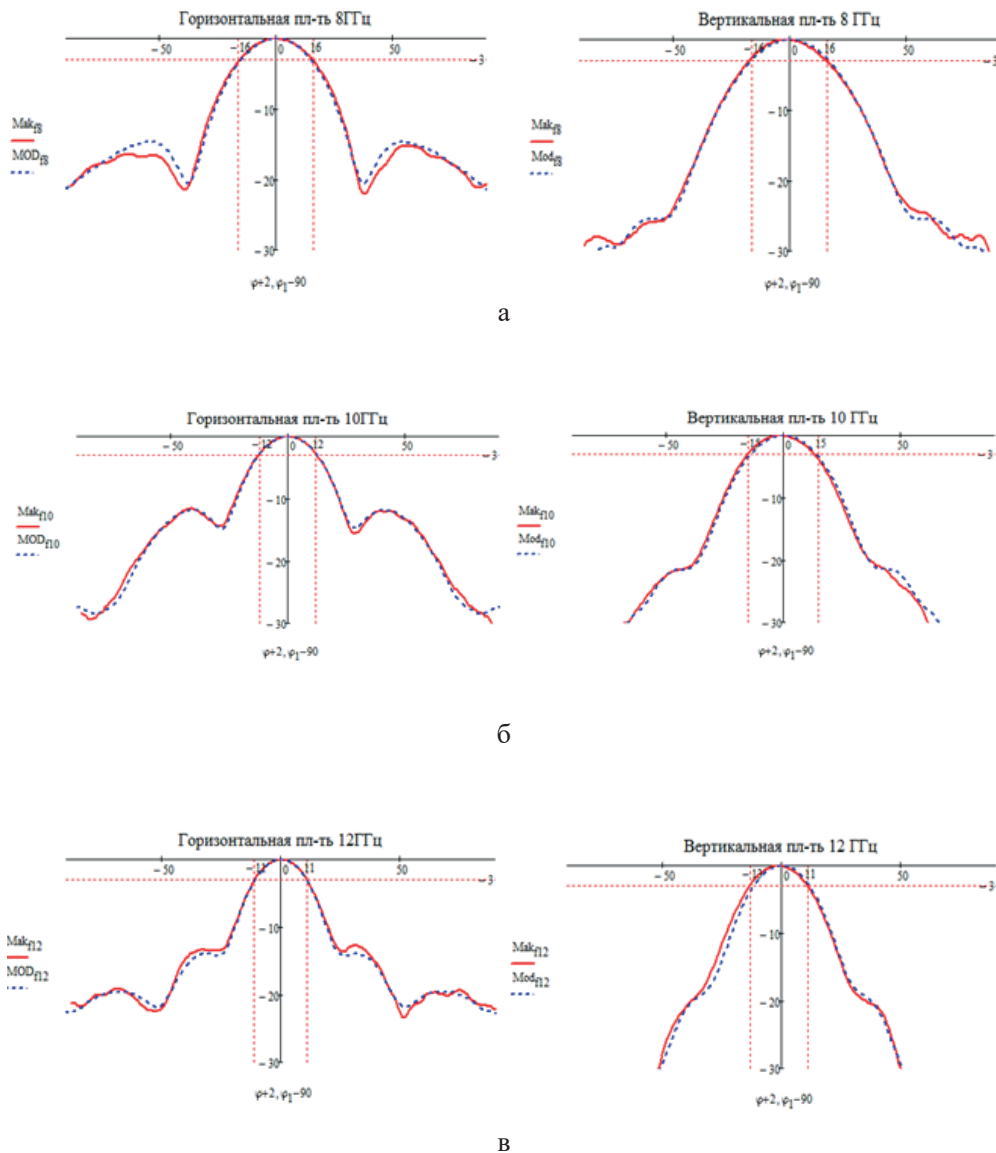


Рис. 4. Сравнительные диаграммы направленности модели и макета на частоте:
а – 8 ГГц; б – 10 ГГц; в – 12 ГГц.

Из представленных диаграмм следует, что модель и макет имеют очень хорошую сходимость.

Моделирование сверхширокополосного излучателя и коаксиально-волнового перехода.

Для изготовления сверхширокополосной антенны нами выбран хорошо зарекомендовавший себя в измерительной технике тип рупорной антенны, представленный на рис. 5.

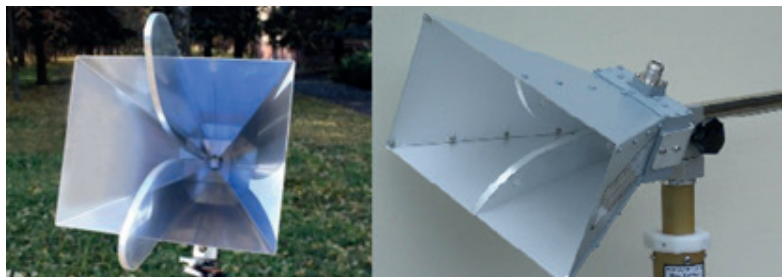


Рис. 5. Измерительные сверхширокополосные антенны.

Конструктивно подобные антенны состоят из комбинации рупора и экспоненциального перехода (ЭП). Разрез изготавливаемого излучателя представлен на рис. 6а.

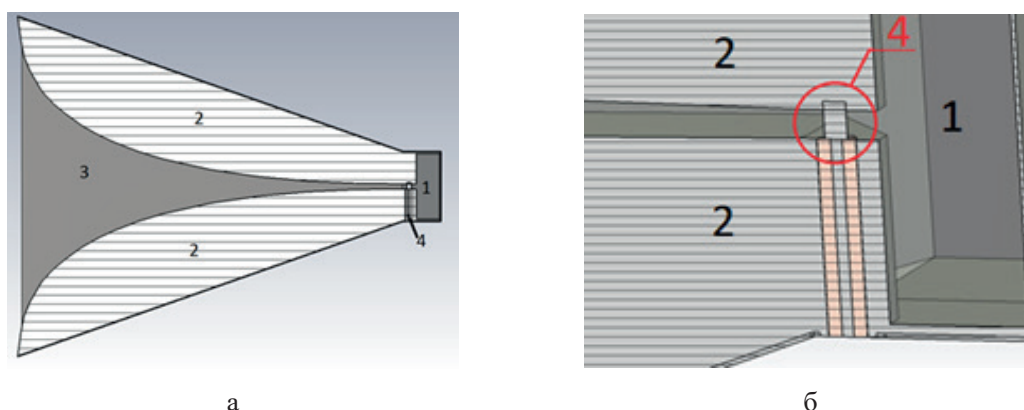


Рис. 6. Разрез модели сверхширокополосного излучателя:
а – излучатель; б – реализация ввода СВЧ (обозначения в тексте).

Антенна состоит из резонатора 1, двух ЭП 2, рупора 3, коаксиального СВЧ-ввода 4. Резонатор представляет собой Н-волновод, закороченный с одной стороны. Н-волновод имеет более широкую полосу пропускания, доходящую до нескольких октав. Однако увеличение полосы частот в этих волноводах сопровождается снижением электропрочности и заметным возрастанием коэффициента затухания [6]. Поскольку Н-волновод имеет меньшее в сравнении с прямоугольным волновое сопротивление, согласование свободного пространства с коаксиальной линией (50 Ом) осуществляется более просто. При этом в резонаторе степенями свободы при оптимизации являются расстояние до короткого замыкания, высота и ширина ступени Н-волновода. Экспоненциальные переходы представляют собой две пластины определенной ширины, расположенные по центру широкой стенки волновода. Ввод энергии СВЧ производится при помощи коаксиального кабеля, расположенного перпендикулярно оси рупора. Оплетка коаксиального кабеля соединяется с первым ЭП, центральная жила – с противоположным (рис. 6б).

В процессе электродинамического моделирования в одной из систем автоматизированного проектирования проводили оптимизацию структуры в диапазоне частот 1.5–18 ГГц. В результате моделирования получен график зависимости коэффициента стоячей волны по напряжению (КСВн) от частоты (рис. 7). Резкое повышение КСВн на частоте 14.5 ГГц связано со структурой поля в резонаторе, как показано на рис. 8. Цветовым градиентом проекций поля обозначено абсолютное значение напряженности.

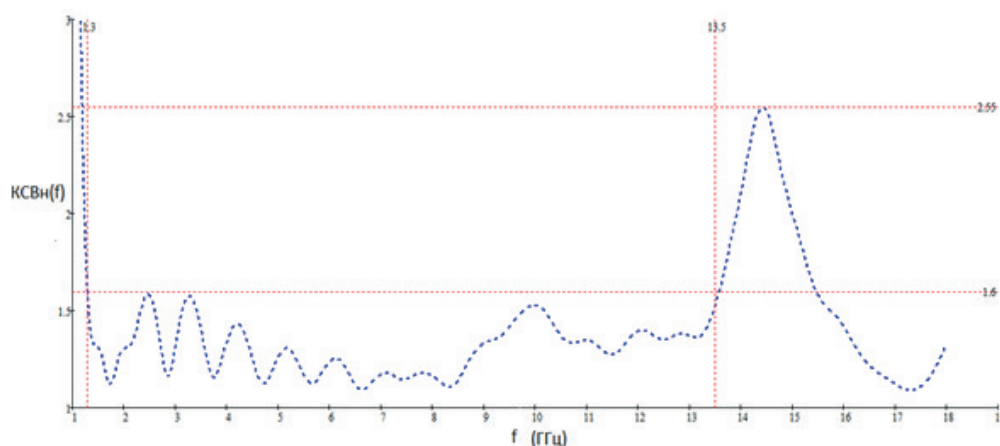


Рис. 7. График зависимости КСВн антенны от частоты, полученный в результате моделирования.

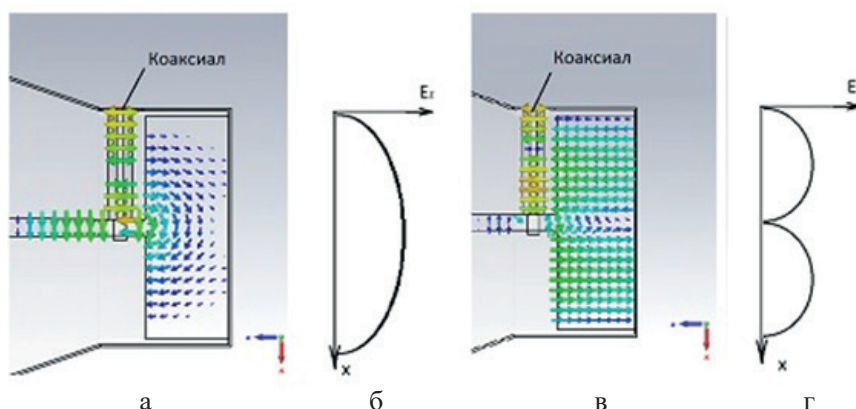


Рис. 8. Проекция силовых линий и распределение электрического поля по оси x : а, б — на частоте 7.0 ГГц; в, г — на частоте 14.5 ГГц, соответственно.

В диапазоне частот 1.3–13.5 ГГц распределение поля по оси x имеет вид, близкий к одному полупериоду косинуса. Данный тип волны имеет достаточно простую структуру и собственную частоту, синфазную с волной, распространяющейся между экспоненциальными переходами. На частоте выше 13.5 ГГц происходит усложнение конфигурации поля (в распределении поля по оси x присутствуют два максимума). Помимо изменения типа волны, происходит повышение собственной частоты резонатора, и волна, отраженная от КЗ резонатора, оказывается несинфазной волне, распространяющейся в рупоре, что, в свою очередь, приводит к возрастанию КСВн. В области частот ниже 1.3 ГГц резкое возрастание КСВн связано с тем, что существование любых типов мод в резонаторе на частотах ниже критической невозможно. Указанное обстоятельство обуславливает смещение плоскости короткого замыкания ближе к коаксиальному вводу и резкое по-

вышение КСВн. Расстояние до короткого замыкания в резонаторе подобрано примерно равным четверти длины волны в волноводе на центральной частоте. В результате оптимизации получен излучатель с размерами раскрыва 109×156 мм и длиной 173 см.

КВП в реализованной конструкции является частным случаем перехода, выполненного в сверхширокополосном излучателе. ЭП заменен упрощенным ступенчатым переходом. Общий вид ступенчатого перехода, распечатанного на принтере, представлен на рис. 9. При моделировании КВП выполнялась оптимизация характеристик отражения. Целевой функцией при оптимизации стала минимизация КСВн в Ку-диапазоне длин волн, при этом варьировались следующие параметры: высоты отдельных ступеней и общая ширина ступенчатого перехода.

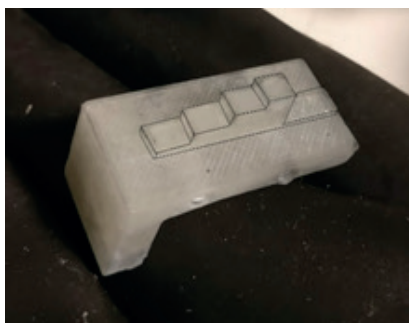


Рис. 9. Ступенчатый переход КВП.

После этапа электродинамического моделирования исходные модели были разбиты на отдельные части для последующей печати на 3D-принтере. Важным с точки зрения электродинамики является электрический контакт центральной жилы к первому ЭП и оплетки коаксиала ко второму ЭП.

Из-за наличия сложных поверхностей (типа ЭП) оклеивание скотчем с учетом поверхностных токов (а в случае КВП Ку-диапазона – наличие мелких частей) было бы весьма трудоемким, поэтому для последующей металлизации поверхностей выбран метод гальванизации.

Нанесение металлических покрытий методом гальванизации. Принципиально важной характеристикой при нанесении металлических покрытий на распечатанную модель является химическая стойкость, возможность механической обработки, а также стойкость к кратковременному локальному нагреву в случае пайки металлических поверхностей. Выбранный PLA-пластик не соответствует лишь третьему из этих требований, так как температура плавления пластика составляет $173\text{--}178$ °С, температура размягчения – 50 °С. Это накладывает ограничения на пайку нанесенного слоя металла. В настоящей работе в качестве решения применяли сплав Вуда, обладающий температурой плавления 68.5 °С. При этом предлагаемая нами технология нанесения металлических покрытий позволяет выбрать произвольный инженерный пластик с разной температурой плавления, который бы подходил в большей мере для различных нужд. Недостаток таких материалов – высокая стоимость и труднодоступность на российском рынке.

В настоящее время методы нанесения металла на поверхность пластиковых деталей сводятся к технологиям химического и гальванического осаждения. Согласно [7], химическое меднение позволяет получать покрытия толщиной вплоть до 20 мкм.

Кроме того, химическое меднение позволяет наносить покрытие на детали сложной формы без необходимости их разделения на элементы более простой геометрии. Образующееся покрытие обладает при этом большей равномерностью. В случае гальванического нанесения деталь должна обладать простой геометрией, желательно без острых выступов и внутренних углов, чтобы получаемое покрытие было равномерным и не образовывались водородные карманы в местах углублений [7]. На рис. 10 приведено распределение электрического поля для П-образной детали, полученное численным моделированием в программе ELCUT.

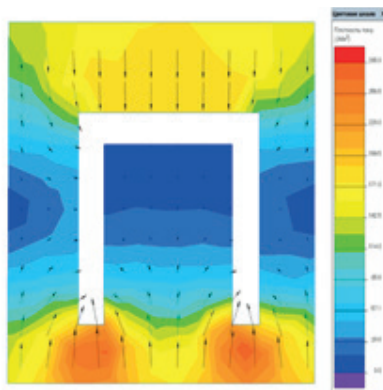


Рис. 10. Распределение напряженности электрического поля у П-образного профиля.

Как можно видеть из рис. 10, во внутренних углах напряженность поля минимальна, в местах с наименьшей длиной сторон напряженность поля максимальна. Именно здесь осаждение металла будет происходить с большей интенсивностью, однако, несмотря на это, за счет гальванизации возможно получение покрытий с толщиной, значительно превосходящей 20 мкм. В данной работе нами используется технология нанесения металлических покрытий методом гальванического осаждения, вследствие большей простоты и невысокой цены оборудования, а также по причине необходимости получения толщины покрытия более 20 мкм.

В соответствии с рекомендациями⁴ использовали алгоритм подготовки деталей к нанесению металла, представленный на рис. 11. Все операции, если это не оговорено специально, осуществляли при нормальных условиях.

Механическая обработка заключалась в выравнивании шлифованием наждачной бумагой поверхностей, к которым имеются требования к плоскостности и шероховатости. Остальные поверхности также обрабатывались наждачной бумагой для образования сетки мелких штриховых рытвин, за счет которых достигается увеличение адгезии осадка с субстратом. Выполнялось также снятие фасок с ребер и стачивание острых вершин для исключения мест с повышенной плотностью тока, что может привести к неравномерности толщины металлического слоя. Кроме того, выполнялась очистка распечатанных моделей от любых артефактов, образующихся в процессе печати.

Промывку проводили в дистиллированной воде вручную, после каждой промывки раствор заменяли на чистую воду. Сушку вели принудительно под струей атмосферного

⁴Королева Г.В. Химическое меднение – что это такое? [Электронный ресурс]. URL: <http://blog.tep-nn.ru/?p=1206> (дата обращения: 11.01.2019).

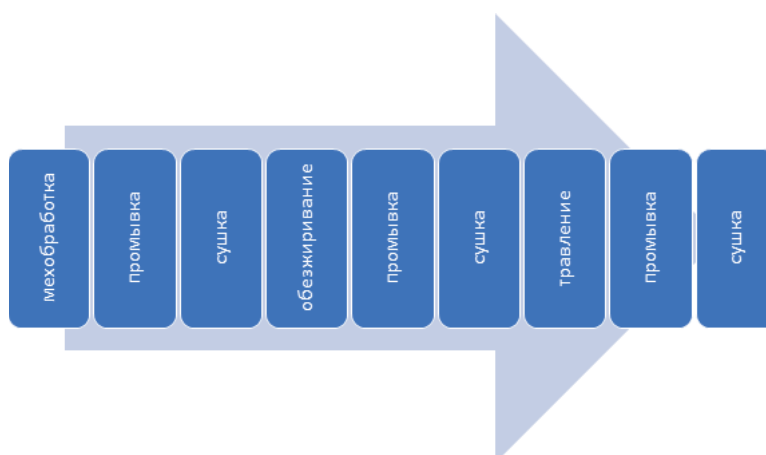


Рис. 11. Алгоритм подготовки деталей перед металлизацией.

воздуха. Обезжиривание осуществляли в растворе этанола, затем в растворе 10 г/л гидроксида натрия, 40 г/л гидрокарбоната натрия, 40 г/л фосфата натрия. Состав раствора для травления: 100 г серной кислоты и 30 г хромового ангидрида на 1 л раствора, экспонирование 1–5 мин при 60 °С. В результате травления на поверхности деталей образовывался белый налет, который ухудшает адгезию осадка с поверхностью, поэтому после травления поверхность очищали щеткой. На рис. 12 изображена деталь после травления.



Рис. 12. Общий вид детали после травления.

Очевидно, что, несмотря на промывку и чистку, внутри детали, распечатанной со 100%-ным заполнением, можно видеть присутствие небольшого количества раствора для травления (зеленоватого цвета). Не исключено, что это может привести к образованию полостей и излишнему протравливанию поверхностей. Для получения токопроводящего покрытия используют медь: она является относительно недорогим металлом, причем медные покрытия наносят на самые разные основы, и технологические проблемы не возникают.

Среди достоинств медного покрытия можно выделить следующие [7]:

- хорошо полируется, легко деформируется, пластична;
- непосредственно после осаждения легко паяется;
- имеет высокие адгезионные свойства почти со всеми металлами;
- имеет самую высокую, наряду с серебром, удельную электропроводность, пригодна для изготовления печатных плат и волноводов;
- незаменима в качестве компонентов многослойных покрытий, особенно медь-никель-хром;

- имеет низкие внутренние напряжения, допускает получение очень толстых ненапряженных покрытий.

К недостаткам следует отнести:

- покрытия химически малостойки, в том числе в обычной атмосфере, не обеспечивают электрохимической защиты, в качестве самостоятельного финишного покрытия может применяться только с последующим применением лака;

- мало подходит для герметичных соединений, например, для покрытия сварных швов;

- легко диффундирует в другие металлы, требует нанесения барьерных слоев, особенно в условиях высоких температур;

- покрытия, хотя и пригодны под пайку, могут образовывать интерметаллиды, ухудшающие паяемость;

- медь нестойка в контакте со многими органическими веществами.

Для меднения печатных плат с металлизированными отверстиями рекомендуется применение электролита с пониженным содержанием сульфата меди и большой концентрацией серной кислоты состава [8]: медь сернокислая 60–80 г/л; серная кислота 180–200 г/л; температура 18–25 °С; плотность тока 1–4 А/дм²; желательно присутствие хлоридов ~30 мг/л и органических добавок.

Для гальванического меднения диэлектрических деталей требуется создать на поверхности детали токопроводящий слой. Рассмотрены два варианта создания проводящего слоя: печать деталей с помощью токопроводящих пластиков и покрытие напечатанных деталей токопроводящим лаком. Сначала для тестирования был выбран токопроводящий ABS-пластик⁵. Удельное электрическое сопротивление пластика составляет 14559 кОм·мм²/м, но оно оказалось чрезмерно большим сопротивлением для осаждения медного покрытия в гальванической ванне: после 8 ч гальванизации при токе 1 А/дм² детали не покрылись слоем меди. Безусловно, существуют пластики, обладающие существенно меньшим удельным сопротивлением⁶, но такие материалы недоступны на российском рынке. В связи с этим нанесение токопроводящего покрытия на диэлектрические детали осуществляли токопроводящим лаком Cramolin Graphite⁷ с заявленной удельной проводимостью покрытия 1000–2000 Ом/м². Лак наносили на детали в три слоя после этапа травления деталей в растворе серной кислоты и хромового ангидрида. После нанесения графитового покрытия проводили гальванизацию: детали подвешивали на катодной штанге на медные провода, которые пропускались через отверстия деталей или обматывались вокруг деталей в случае отсутствия отверстий. Важно подчеркнуть, что в местах, расположенных под медным проводом, толщина покрытия получалась меньше, чем в остальных местах. Детали, подвешенные на катодную штангу, загружались в электролит под напряжением, согласно [7].

Чтобы характеристики изготавливаемых СВЧ-изделий соответствовали предъявляемым требованиям, необходимо соответствие геометрии деталей, покрытых металлом, геометрии исходной компьютерной модели. Поэтому требуется контролировать толщи-

⁵Токопроводящий (Conductive) ABS-пластик [Электронный ресурс]. URL: <http://rusabs.ru/blogs/blog/tokoprovodyaschiy-conductive-abs-plastik/> (дата обращения: 11.01.2019).

⁶Токопроводящий филамент для 3D-печати Electrifi вышел в продажу [Электронный ресурс]. URL: <http://3dtoday.ru/blogs/news3dtoday/conductive-filament-for-3d-printing-electrifi-went-on-sale-/> (дата обращения: 11.01.2019).

⁷GRAPHITE Cramolin графитовый токопроводящий лак [Электронный ресурс]. URL: <http://cramolin.info/catalog/cramolin-laki/cramolin-graphite/> (дата обращения: 11.01.2019).

ну наносимого слоя металла и остановить гальванизацию в тот момент, когда толщина металла станет равной расчетной. Изъятие деталей из ванны в процессе гальванизации недопустимо, поскольку это может привести к отслаиванию металла. Таким образом, простой контроль непосредственным замером в течение гальванизации недопустим.

Чтобы определить время, необходимое для протекания процесса гальванизации, целесообразно использовать аналитическую формулу для толщины покрытия [8]:

$$h = itQ, \quad (4)$$

где $i = I/S$ – плотность тока при электролизе, А/см²;

I – общий ток в цепи, А;

t – время экспозиции, ч;

S – площадь покрываемой поверхности, см²;

Q – электрохимический эквивалент, см³/А·ч.

В случае меди(II) электрохимический эквивалент будет равен 0.1326 см³/А·ч [8].

На практике толщина металлизации оказывается больше, чем расчетная, поэтому была произведена контрольная гальванизация для получения поправочного коэффициента, который можно было бы внести как множитель в выражение (4). Формула с поправочным коэффициентом позволила бы более точно контролировать время экспозиции для получаемого электролита.

В качестве субстрата был напечатан шар диаметром 20 мм со штангой. Форма шара выбрана для получения более равномерного распределения напряженности поля по его поверхности. Осаждение производили при постоянном токе в цепи в 150 мА без перемешивания электролита при температуре 21 °С в течение 13 ч. Площадь поверхности детали ~1256 мм², следовательно, ток цепи по отношению к площади сферы равен

$$I = i / S = 0,15 / 0,1256 = 1,194 \text{ А/дм}^2.$$

Замеры диаметра шара после покрытия лаком были произведены в трех точках, соответствующие значения составили 20.0, 20.07 и 20.08 мм. Масса шара до гальванизации составляла 4.34 г, после гальванизации – 7.13 г; разница в массе составила 2.79 г. В соответствии с ГОСТ 9.302-88 для определения толщины покрытия h_{cp} (в мкм) по гравиметрическому методу необходимо воспользоваться соотношением:

$$h_{cp} = \frac{m_1 - m_2}{S\rho} 10^4,$$

где m_1 – масса деталей после нанесения покрытия, г;

m_2 – масса деталей до нанесения покрытия или после растворения покрытия, г;

S – площадь покрытия, см²;

ρ – плотность материала покрытия, г/см³.

Соответственно, толщина покрытия равна 38.27 мкм.

Измерения диаметра гальванизированного шара в трех местах дали значения 20.8, 20.9 и 20.66 мм.

Третий тип измерения толщины покрытия подразумевал разрушающее воздействие в виде отрыва части металлизированного слоя от субстрата. В результате измерения тол-

щины металлизации получено значение 0.32 мм. Усредненное значение толщины получившегося покрытия равно 0.375 мм. Используя (4), можно рассчитать теоретическое значение толщины покрытия, которое составило 206 мкм. Отсюда найден поправочный коэффициент как отношение контрольной толщины к теоретической:

$$K_1 = 0,375 / 0,206 = 1,82.$$

Для повышения точности был проведен повторный цикл контрольной гальванизации. Детали экспонировались 19 ч 45 мин под током 500 мА, площадь поверхности 81.9 см². В результате получен слой толщиной 240 мкм. Теоретическая толщина слоя составила 0.16 мм, и поправочный коэффициент равен

$$K_2 = 0,24 / 0,16 = 1,5.$$

При последующих процессах гальванизации также возможно уточнение данного поправочного коэффициента, для чего достаточно измерять получаемые покрытия неразрушающими методами. Итоговый коэффициент выбран нами равным 1.66 – средним от полученных замеров. Итоговое выражение для толщины покрытия:

$$h = 1,66itQ.$$

Необходимо учитывать, что в дальнейшем при замене электролита требуется соответствие по составу нового электролита тому, для которого были рассчитаны поправочные коэффициенты.

Изготовленные сверхширокополосная антенна и КВП представлены на рис. 13.



Рис. 13. Устройства СВЧ, изготовленные методом 3D-печати с последующей гальванизацией.

3. Экспериментальное исследование характеристик антенны

Результатами экспериментального исследования характеристик антенны измерений являются главные сечения амплитудной диаграммы направленности (АДН) на интересующих частотах в рабочем диапазоне длин волн, а также зависимость КСВн от частоты и координаты фазового центра. Типовой стенд для измерений в дальней зоне представлен на рис. 14.

При измерении АДН антенны исследуемая антенна располагалась на опорно-поворотном устройстве (ОПУ), а измерительный зонд – в дальней зоне на расстоянии порядка 6 м. При вращении измеряемой антенны на ОПУ по азимуту регистрировали коэффициент передачи между антеннами. Для определения координат фазового центра антенны

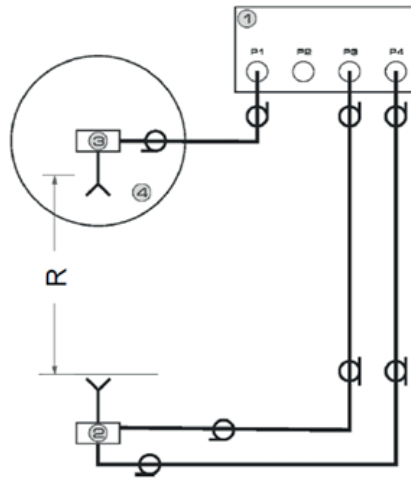


Рис. 14. Схема стенда для измерения характеристик в дальней зоне:

1 – векторный анализатор цепей; 2 – измерительный зонд;
3 – исследуемая антенна; 4 – ОПУ.

применялся математический аппарат [8]. В общем случае фазовый центр антенны вынесен относительно оси вращения поворотного стола. Данный параллакс влияет как на измеряемую амплитудную диаграмму направленности (ДН), так и на фазовую ДН. Определение координат фазового центра возможно осуществить после измерения основных сечений ДН и анализа их фазовых составляющих.

Результатами измерений явились главные сечения амплитудной диаграммы направленности, зависимость КСВн от частоты и координаты фазового центра. Сравнительные результаты расчета модели и измерения макета представлены на рис. 15–17.

Из результатов сравнения моделей и макетов, изготовленных с применением технологии 3D-печати, следует хорошее совпадение параметров изготовленных антенн с изначальными моделями. Можно утверждать, что вследствие высокой скорости прототипирования в сочетании с низкой ценой технология 3D-печати применительно к устройствам СВЧ обладает рядом преимуществ по сравнению со стандартными методами изготовления.

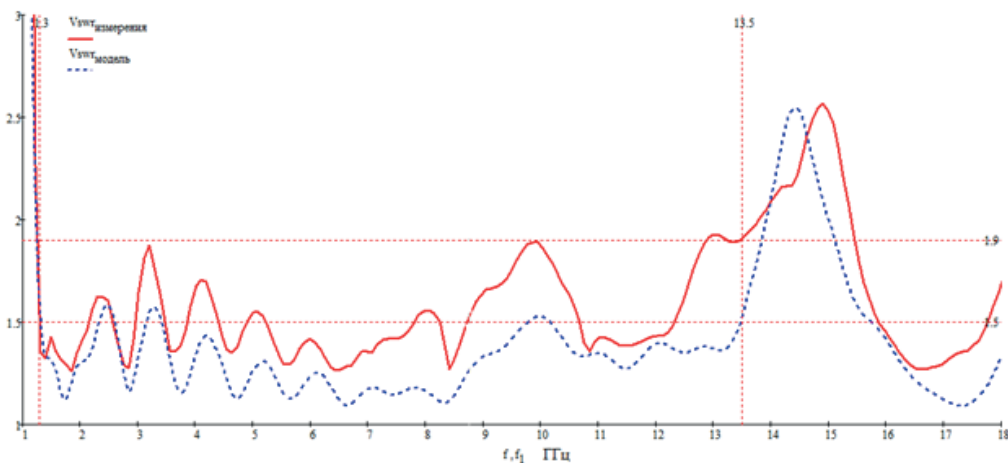
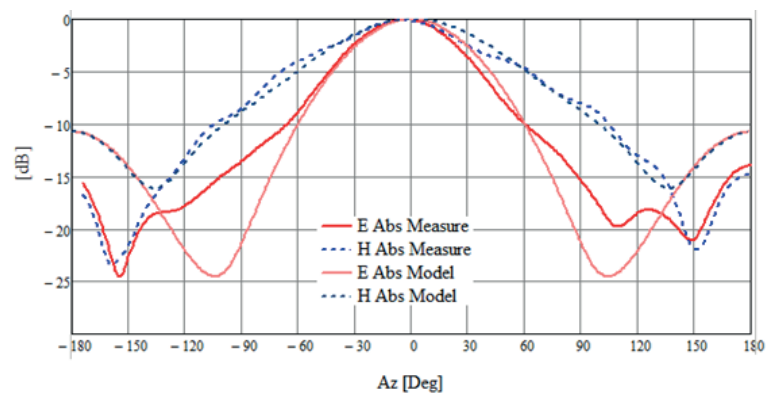
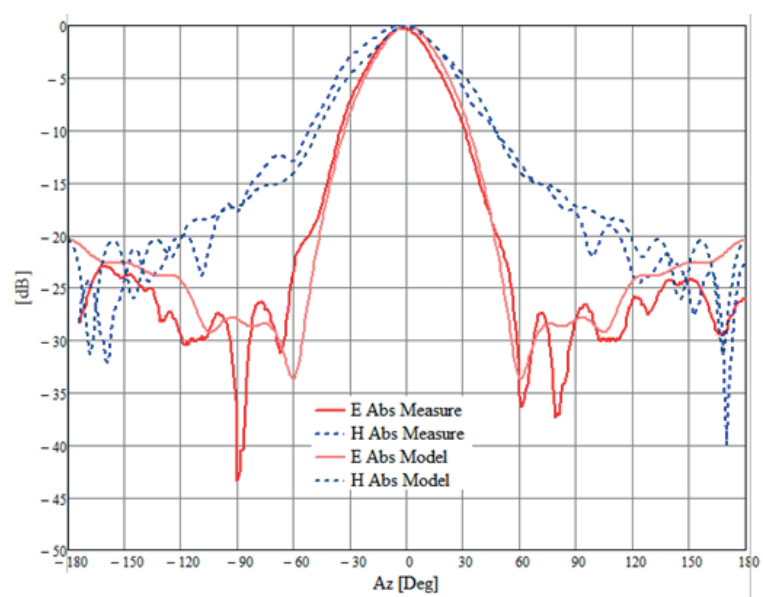


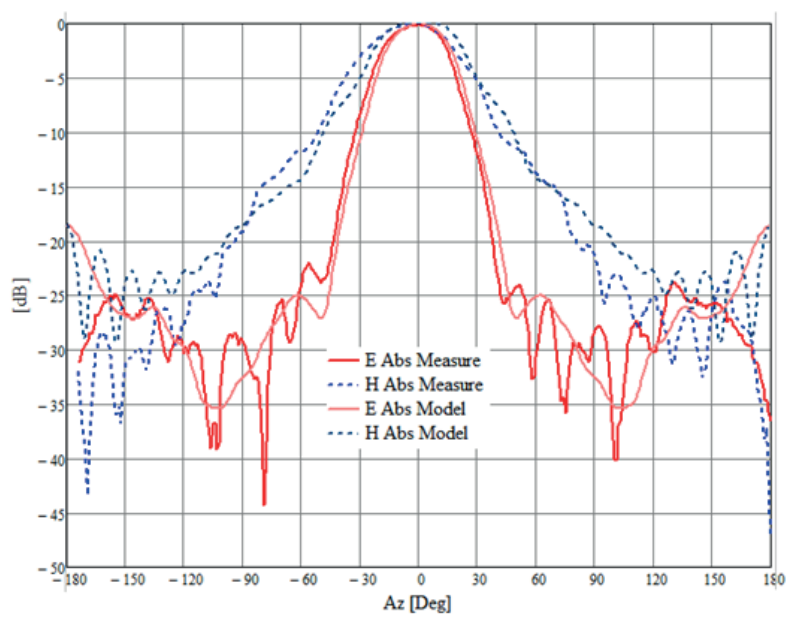
Рис. 15. Сравнительные графики КСВн модели и макета.



а



б



в

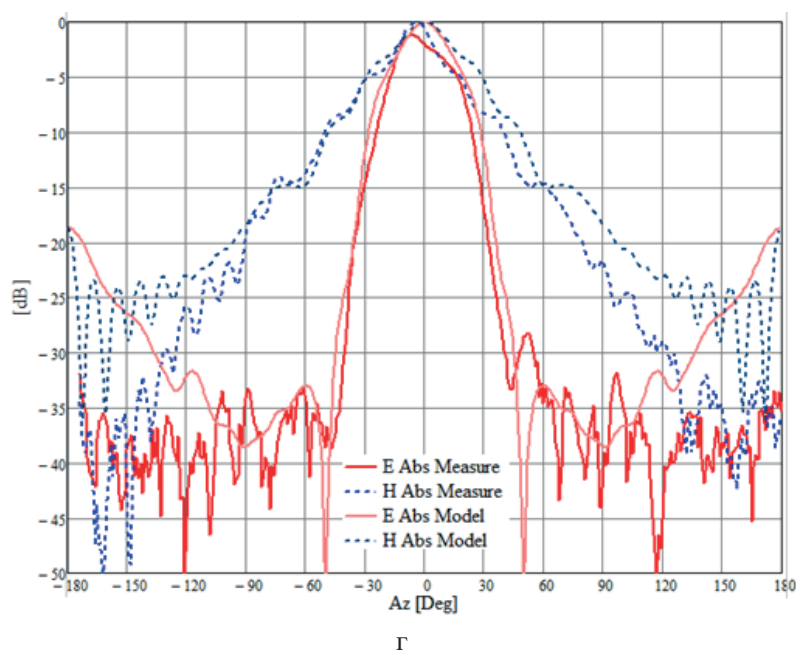


Рис. 16. Сравнение главных сечений диаграммы направленности с моделью на частоте: а – 1.5 ГГц; б – 6 ГГц; в – 9 ГГц; г – 12 ГГц.

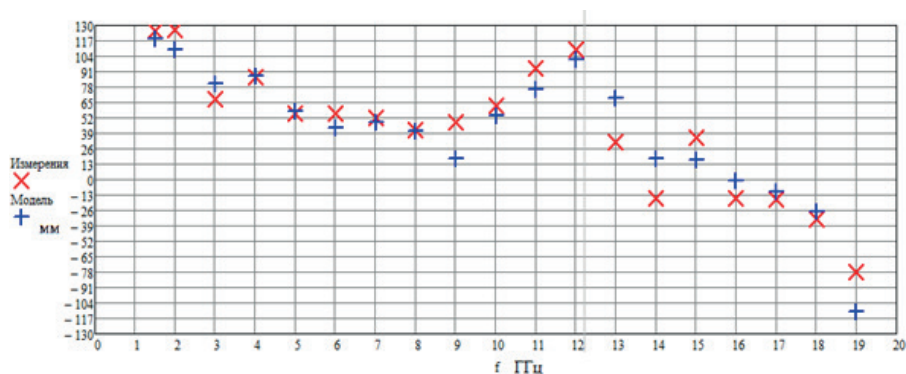


Рис. 17. Сравнительные результаты вычисления фазового центра модели и макета в зависимости от частоты.

Заключение

Рассмотренная технология изготовления устройств СВЧ может найти широкое применение для прототипирования и создания мелкосерийных деталей, требующих наличия проводимого металлического слоя на их поверхности. Стоимость получаемых деталей значительно ниже стоимости аналогичных деталей, полученных методом фрезерования или литья – при учете, что к деталям, получаемым описанным способом, не выдвигаются требования высокой механической прочности. Следует отметить лучшие массогабаритные характеристики получаемых деталей в сравнении с цельнометаллическими. Сама технология FFF-печати подразумевает возможность создания цельных деталей без сборки, что не только уменьшает время производства, но и дополнительно снижает массу изделий из-за меньшего количества винтовых соединений. В результате исследований проведен полный цикл производства устройств СВЧ: проектирование, моделирование, изготовление образца и валидация характеристик. Результаты моделирования рассмотренных

устройств хорошо согласуются с экспериментальными характеристиками изготовленных макетов с применением технологии 3D-печати.

Выполнена оценка влияния шероховатости поверхности, получаемой в результате 3D-печати, на ограничения по частотным свойствам изготавливаемых устройств. Проведен анализ полосовых свойств сверхширокополосной антенны.

Перспективы дальнейшего развития описанной технологии включают вариацию типов пластиков, используемых в качестве субстрата, нанесение финишных декоративных и функциональных покрытий, увеличение адгезионных свойств наносимого слоя меди с субстратом. Представляет интерес и переход на технологию SLA-печати для расширения номенклатуры производимых изделий за счет улучшения качества печатных деталей.

Литература:

1. Лысыч М.Н., Шабанов М.Л., Качурин А.А. Обзор современных технологий 3D-печати // Современные наукоемкие технологии. 2015. № 6. С. 26–30. URL: <http://www.top-technologies.ru/ru/article/view?id=35053> (дата обращения: 25.11.2018).
2. Лысыч М.Н., Шабанов М.Л., Воронцов Р.В. Материалы, доступные в рамках различных технологий 3D-печати // Современные наукоемкие технологии. 2015. № 5. С. 20–25. URL: <http://www.top-technologies.ru/ru/article/view?id=35031> (дата обращения: 23.11.2018).
3. Yunus C.T., Peyman Mahouti, Filiz Güneş. Design and manufacturing of an X-band horn antenna using 3-D printing technology // Proceed. of the 8th International Conference on Recent Advances in Space Technologies - RAST 2017. Istanbul, Turkey, 2017. P. 195–198.
4. Воробьев Е.А. Расчет производственных допусков устройств СВЧ. Л.: Судостроение, 1980. 148 с.
5. Gregson S.F., McCormick J., Parini C.G. Principles of planar near-field antenna measurements. IET Electromagnetic Waves, series 53. Stevenage: The Institution of Engineering and Technology, 2007. 424 p.
6. Сазонов Д.М. Антенны и устройства СВЧ. М.: Высшая школа, 1988. 432 с.
7. Гамбург Ю.Д. Гальванические покрытия. Справочник по применению. М.: Техносфера, 2006. 220 с.
8. Shang I.-P., Fu D.-M., Deng Y.-B., Jiang S. Measurement of phase center for antenna with the method of moving reference point // Proceed. of the 8th International Symposium on Antennas, Propagation and EM Theory (ISAP) 2008. Kunming, 2008. P. 114–117.

References:

1. Lysych M.N., Shabanov M.L., Kachurin A.A. Review of modern technologies of 3D printing. *Sovremennyye naukoymkiye tekhnologii* (Modern High Technologies). 2015; 6: 26-30. Available at: <http://www.top-technologies.ru/ru/article/view?id=35053>. Date of access: 11/25/2018. (in Russ.)
2. Lysych M.N., Shabanov M.L., Vorontsov R.V. Materials available in various 3D printing technologies. *Sovremennyye naukoymkiye tekhnologii* (Modern High Technologies). 2015; 5: 20-25. Available at: <http://www.top-technologies.ru/ru/article/view?id=35031>. Date of access: 11/23/2018. (in Russ.)
3. Yunus C.T., Peyman Mahouti, Filiz Güneş. Design and manufacturing of an X-band horn

antenna using 3-D printing technology. *Procced. of the 8th International Conference on Recent Advances in Space Technologies - RAST 2017*. Istanbul, Turkey, 2017: 195-198.

4. Vorobiev E.A. Production tolerances calculation for microwave devices. Leningrad: Sudstroyeniye Publ., 1980. 148 p. (in Russ.)

5. Gregson S.F., McCormick J., Parini C.G. Principles of planar nearfield antenna measurements. IET Electromagnetic Waves, series 53. Stevenage: The Institution of Engineering and Technology, 2007. 424 p.

6. Sazonov D.M. Antennas and Microwaves Devices. Moscow: Vysshaya shkola Publ., 1988. 432 p. (in Russ.)

7. Gamburg Yu.D. Electroplated Coatings. Handbook for applying. Moscow: Tekhnosfera, 2006. 220 p. (in Russ.).

8. Shang I.-P., Fu D.-M., Deng Y.-B., Jiang S. Measurement of phase center for antenna with the method of moving reference point. *Proceed. of the 8th International Symposium on Antennas, Propagation and EM Theory (ISAP) 2008*. Kunming, 2008: 114-117.

Об авторах:

Харалгин Сергей Владимирович, сотрудник научно-производственного предприятия АО «ЦНИРТИ им. академика А.И. Берга» (107078, г. Москва, ул. Новая Басманная, д. 20); аспирант кафедры радиоэлектронных систем и комплексов Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Куликов Геннадий Валентинович, профессор, доктор технических наук, профессор кафедры радиоэлектронных систем и комплексов Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Котельников Андрей Борисович, аспирант кафедры теоретической информатики и дискретной математики ФГБОУ ВО «Московский педагогический государственный университет» (119991, Россия, Москва, ул. Малая Пироговская, д. 1).

Снастин Михаил Владимирович, сотрудник научно-производственного центра радиоинформационной метрологии ФГБОУ ВО «Московский авиационный институт (Национальный исследовательский университет)» (125993, Россия, Москва, Волоколамское шоссе, д. 4).

Добычина Елена Михайловна, кандидат технических наук, доцент, профессор кафедры «Радиофизика, антенны и микроволновая техника» ФГБОУ ВО «Московский авиационный институт (Национальный исследовательский университет)» (125993, Россия, Москва, Волоколамское шоссе, д. 4).

About the authors:

Sergey V. Kharalgin, Employee, Academician A.I. Berg Central Scientific Research Radio Engineering Institute (20, Novaya Basmannaya st., Moscow 107078, Russia); Postgraduate Student of the Chair of Radio Electronic Systems and Complexes, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Gennady V. Kulikov, Professor, D.Sc. (Engineering), Professor of the Chair of Radio Electronic Systems and Complexes, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia).

Andrey B. Kotelnikov, Postgraduate Student of the Chair of Theoretical Informatics and Discrete Mathematics, Moscow Pedagogical State University (1, Malaya Pirogovskaya st., Moscow 119991, Russia).

Mikhail V. Snastin, Employee, Center of Radio Information Metrology, Moscow Aviation Institute (National Research University) (4, Volokolamskoe highway, Moscow 125993, Russia).

Elena M. Dobychina, Ph.D. (Engineering), Associate Professor, Professor of the Chair of Radiophysics, Antennas and Microwave Technology, Moscow Aviation Institute (National Research University) (4, Volokolamskoe highway, Moscow 125993, Russia).

Для цитирования: Харалгин С.В., Куликов Г.В., Котельников А.Б., Снастин М.В., Добычина Е.М. Прототипирование СВЧ-устройств с заданными электродинамическими характеристиками по технологии аддитивной 3D-печати // Российский технологический журнал. 2019. Т. 7. № 1. С. 80–101. DOI: 10.32362/2500-316X-2019-7-1-80-101

For citation: Kharalgin S.V., Kulikov G.V., Kotelnikov A.B., Snastin M.V., Dobychina E.M. Prototyping of microwave devices with specified electrodynamic characteristics using additive 3D printing technology. *Rossiyskiy tekhnologicheskii zhurnal* (Russian Technological Journal). 2019; 7(1): 80-101. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-80-101

РАЗДЕЛЕНИЕ ДИФРАКЦИОННЫХ СПЕКТРОВ МЕТОДОМ ГЛАВНЫХ КОМПОНЕНТ НА ПРИМЕРЕ ЛЕКАРСТВЕННОГО СРЕДСТВА АРИФОН

**Р.В. Чехова^{1,@},
В.М. Пышный¹,
Л.А. Пьянкова²,
В.А. Елохин²**

¹МИРЭА – Российский технологический университет, Москва 119454, Россия

²АО «Научные приборы», Санкт-Петербург 190103, Россия

@Автор для переписки, e-mail: chekhova.r@gmail.com

В статье рассматриваются результаты экспериментальных исследований по статистической обработке дифракционных спектров твердых лекарственных средств (ЛС) с целью их разделения и возможностью идентификации. Для исследования были использованы дифрактограммы оригинального и фальсифицированного ЛС Арифон, полученные на настольном дифрактометре Дифрей-401 производства АО «Научные приборы» (Санкт-Петербург, Россия). Исследования проводились в распространяемой по свободной лицензии среде Scilab. Отснятые дифракционные спектры обработаны с помощью процедуры сглаживания, которая позволила устранить влияние случайной составляющей в исходных данных. Анализ результатов сглаживания методом скользящего среднего показал, что алгоритм сглаживания с окном 41 точка наиболее предпочтителен. Приведены результаты статистической обработки дифрактограмм исследуемых ЛС методом главных компонент (МГК) в графической и числовой форме, которые показали хорошую сходимость и работоспособность данного метода при разделении дифракционных спектров. Проведенные исследования дают возможность создания методики, позволяющей идентифицировать твердые лекарственные препараты методом рентгеновской дифракции.

Ключевые слова: дифракционный спектр, лекарственное средство, метод главных компонент, собственное число, собственный вектор.

SEPARATION OF DIFFRACTION SPECTRA BY PRINCIPAL COMPONENT METHOD BY THE EXAMPLE OF ARIFON DRUG

**R.V. Chekhova^{1,@},
V.M. Pyshniy¹,
L.A. Pyankova²,
V.A. Elokhin²**

¹MIREA – Russian Technological University, Moscow 119454, Russia

²Scientific Instruments Inc., St. Petersburg 190103, Russia

@Corresponding author e-mail: chekhova.r@gmail.com

The article deals with the results of experimental studies on statistical processing of diffraction spectra of solid drugs for the purpose of their separation and identification. Diffractograms of the original and falsified drugs Arifon were used for the study. They were obtained on a desktop diffractometer Difray 401 produced by Scientific Instruments Inc. (Saint Petersburg, Russia). The research was conducted in the Scilab environment distributed under a free license. The captured diffraction spectra were processed using a smoothing procedure that eliminated the influence of a random component in the original data. Analysis of the results of smoothing by the moving average method showed that the smoothing algorithm with the window 41 point is most preferable. The results of statistical processing of diffractograms of the drugs investigated by the principal component analysis (PCA) in graphical and numerical form, which showed good convergence and efficiency of this method in the separation of diffraction spectra, are presented. The conducted studies make it possible to create a technique that allows identifying solid drugs by X-ray diffraction.

Keywords: diffraction spectrum, drug, principal component analysis, eigenvalue, eigenvector.

Предотвращение обращения на территории Российской Федерации недоброкачественных и фальсифицированных препаратов является одной из приоритетных задач государства¹. В соответствии со Стратегией национальной безопасности Российской Федерации 2010–2020 г., утвержденной в 2009 г., стратегическими целями национальной безопасности в сфере здравоохранения являются совершенствование стандартов медицинской помощи и контроль качества, эффективности и безопасности лекарственных средств (ЛС).

В настоящее время мировое фармацевтическое сообщество проявляет повышенный интерес к рентгеновской дифрактометрии как мощному инструменту для фармацевтического анализа [1]. Метод дифракции рентгеновских лучей на порошковом образце вследствие простоты и информативности имеет хорошую практическую возможность для исследования поликристаллических субстанций лекарственных веществ, полиморфизма, сольватоморфизма, изучения переходов состояний «кристаллическое – аморфное» и оценки степени кристалличности твердых лекарственных форм [2].

Распознавание (идентификацию) непосредственно лекарственного средства возможно осуществлением сопоставлением дифрактограмм исследуемого образца ЛС и его референтного образца с использованием методов хемометрики [3–5]. Наиболее широко хемометрический подход разделения спектров отработан и используется для анализа лекарственных форм в методе БИК-спектрометрии в сочетании со статистической обработкой результатов при исследовании многофакторных зависимостей, при этом обработка спектров производится методом главных компонент (МГК) [6, 7]. На практике МГК для БИК-спектрометрии реализован в программном обеспечении спектрометров фирмы «Bruker Optik GmbH»² (Германия). Необходимо отметить, что если для БИК-спектрометрии метод МГК хорошо отработан, то в рентгеновской дифрактометрии этому методу только начинают уделять внимание, публикаций по хемометрической обработке дифракционных спектров немного [8].

¹Федеральный закон Российской Федерации № 61-ФЗ от 12.04.2010 г. «Об обращении лекарственных средств» (с изменениями, внесенными в соответствии с Федеральным законом № 425-ФЗ от 28.12.2017 г.).

²<http://www.brukeroptics.com/mpa.html>

Для моделирования процедуры распознавания образцов ЛС были использованы дифрактограммы оригинального и фальсифицированного ЛС Ариффон, предоставленные АО «Научные приборы» (Санкт-Петербург, Россия). Дифрактограммы Ариффона получены на настольном дифрактометре «Дифрей-401» производства АО «Научные приборы». Набор данных составлял 4 и 8 спектров оригинального и фальсифицированного ЛС, соответственно. Для исследования были предоставлены данные, которые в процессе измерения не подвергались статистической обработке, в том числе процедуре сглаживания, поэтому каждый снятый дифракционный спектр был обработан с помощью процедуры сглаживания, которая позволила устранить влияние случайной составляющей в регистрации рентгеновских квантов, убрать шумы в дифракционной картине.

Исследование проводилось в лицензионной среде Scilab³, поскольку результаты работы предполагалось использовать в учебном процессе. Однако первоначально все результаты с использованием стандартных функций были получены в среде Matlab, которая по сравнению с Scilab обладает гораздо большими функциональными возможностями. Применение Scilab дало практически полностью аналогичные результаты (расхождения лишь после четвертого знака после запятой). Одним из наиболее часто используемых алгоритмов сглаживания является алгоритм арифметического скользящего среднего. Однако в Scilab нет подходящих функций для сглаживания данных, поэтому был разработан собственный программный код, реализующий алгоритм скользящего среднего, который дает результаты, сопоставимые с данными, полученными с помощью функции Smooth в Matlab.

Метод арифметического скользящего среднего заключается в замене фактических значений членов ряда средним арифметическим значений нескольких ближайших к нему членов. Набор усредняемых значений образует так называемое окно сглаживания. Сглаживание осуществляется по следующей формуле⁴:

$$\bar{x}(k) = \frac{1}{n} \sum_{t=k}^{n+k} X(t), \quad (1)$$

где $X(t)$ – исходные данные,

$\bar{x}(k)$ – сглаженные значения,

n – размер окна (период сглаживания),

k – номер члена ряда, значение которого заменяется средним.

Для определения размера окна n , позволяющего эффективно сглаживать данные, произведен сравнительный анализ сглаживания с окнами 21, 41 и 61 точка.

Чтобы дать количественную оценку эффективности сглаживания с различными окнами, было определено среднее квадратичное отклонение (S_i) между каждой точкой исходных и сглаженных данных. Эти значения составили:

$$S_1 = 0.154, \text{ для } n = 21;$$

$$S_2 = 0.181, \text{ для } n = 41;$$

$$S_3 = 0.238, \text{ для } n = 61.$$

Разность между $n = 21$, $n = 41$ и $n = 41$, $n = 61$ точка составила:

$$\Delta_{12} = 0.027; \Delta_{23} = 0.057.$$

³<http://www.scilab.org>

⁴<http://www.poznayka.org>

Наблюдается меньшее отклонение Δ_{12} , чем Δ_{23} , что свидетельствует о меньшем различии в степени сглаживания для $n = 21$ и $n = 41$, а также большей степени сглаживания данных для окна 61 точка. При сглаживании методом скользящего среднего с окном 21 точка наблюдается неполное сглаживание шумов, а при окне 61 точка происходит более сильное сглаживание, которое может привести к некоторой потере информации, содержащейся в исходных данных. Поэтому для дальнейшего анализа были использованы данные, сглаженные с окном 41 точка.

На рис. 1 представлены исходный (синий) и сглаженный (красный) дифракционные спектры ЛС Арифон. Из рис. 1 видно, что наблюдается достаточно сильное подавление шумовой составляющей исходных данных.

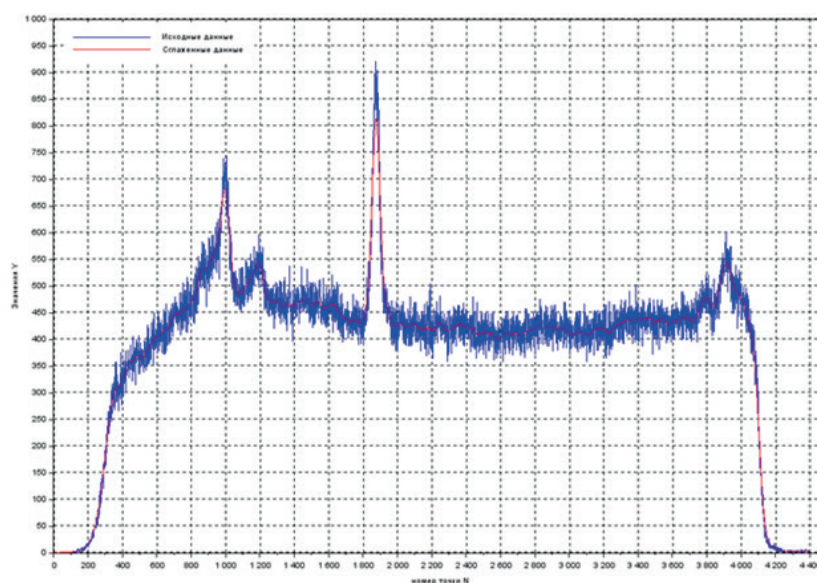


Рис. 1. Исходные и сглаженные дифракционные спектры ЛС Арифон.

После проведения процедуры сглаживания каждого набора данных проводилось слияние и усреднение серии обработанных спектров для каждого из окон по формуле:

$$Y = \frac{\sum_{i=1}^N X[i]}{N}, \quad (2)$$

где Y – канал результирующего спектра,

X – канал составляющего спектра,

N – количество спектров, участвующих в усреднении.

В качестве референтного образца (эталона) был принят усредненный по формуле (2) спектр, образованный слиянием четырех сглаженных дифракционных спектров оригинального ЛС Арифон (обозначение на рисунках «Арифон оригинал»).

За анализируемые образцы приняты сглаженный первый дифракционный спектр оригинального ЛС Арифон (обозначение на рисунках «Арифон 1 оригинал»), а также усредненный по формуле (2) спектр, образованный слиянием восьми сглаженных дифракционных спектров фальсифицированного ЛС Арифон (обозначение на рисунках «Арифон фальсификат»).

В настоящей работе для статистической обработки дифракционных спектров с целью их разделения и распознавания выбран метод главных компонент, поскольку он лежит в основе целого класса проекционных методов, используемых для сжатия исходных данных и эффективен в задачах разделения [9]. МГК (в англоязычной литературе – *principal component analysis*, PCA) – один из наиболее распространенных методов факторного анализа, позволяющий выделить ведущие факторы вариации исследуемых случайных величин. Метод основан на нахождении собственных чисел и собственных векторов ковариационной матрицы с последующим взвешиванием компонентов собственных векторов. Эти компоненты после соответствующего взвешивания дают значения коэффициентов корреляции с независимыми факторами, представленными через линейную комбинацию значений исследуемых случайных величин. Комбинации находятся таким образом, что представляют собой оси ортогональной системы координат и являются независимыми друг от друга. Метод имеет большие перспективы в минералогии, геохимии, палеонтологии и т. п. во всех случаях, когда можно предполагать, что значения случайной величины флуктуируют под воздействием ограниченного числа причин, и эти причины могут быть выражены через исследуемые случайные величины⁵.

Метод применяется к данным, записанным в виде прямоугольной матрицы X размером i строк и j столбцов. В нашем случае каждый столбец матрицы содержит дифракционные спектры различных образцов.

С математической точки зрения МГК – это представление исходной матрицы X в следующем виде [10]:

$$X = T \cdot P^T + E, \quad (3)$$

где T – матрица счетов (*scores*),

P – матрица нагрузок (*loadings*),

E – матрица остатков.

В основе анализа главных компонент лежит математический метод нахождения собственных значений и собственных векторов ковариационной матрицы исходных данных X , являющихся дифракционными спектрами. При этом нагрузки P являются матрицей собственных векторов, содержащей координаты главных компонент (ГК).

МГК реализован в среде Scilab с помощью стандартной функции:

$$[P, T, L] = \text{princomp}(X); \quad (4)$$

где X – исходная матрица данных,

P – матрица нагрузок,

T – матрица счетов,

L – собственные значения ковариационной матрицы X .

Следует учитывать, что собственные значения являются дисперсиями ГК, и первая компонента всегда объясняет как можно больше общей дисперсии и имеет максимальное собственное число. Основная доля информации содержится именно в ней [10].

⁵https://dic.academic.ru/dic.nsf/enc_geolog/

На рис. 2 представлены сглаженные дифракционные спектры референтного (синий) и исследуемого (красный) образцов оригинального ЛС Арифон. Из рис. 2 видно, что эти спектры практически идентичны.

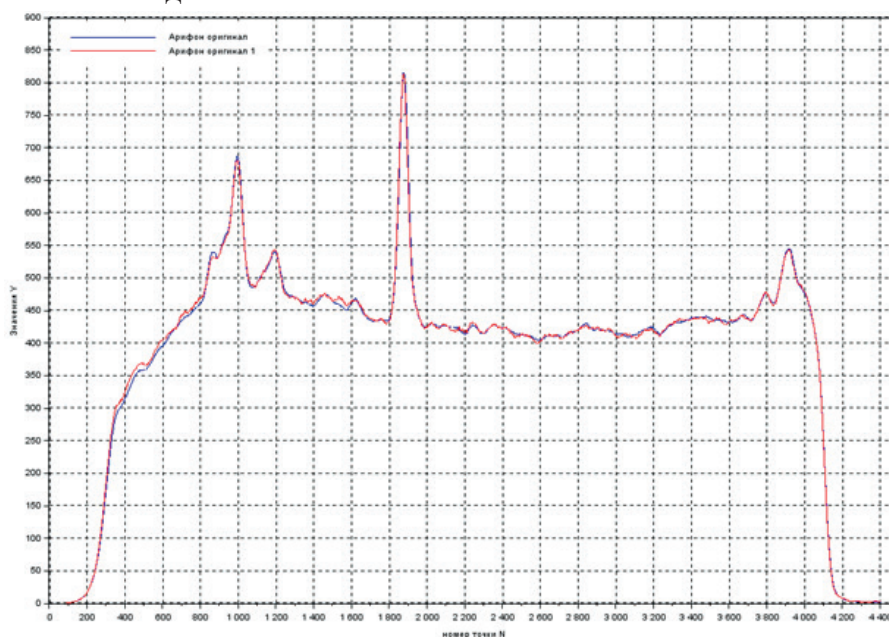


Рис. 2. Сглаженные дифракционные спектры референтного (синий) и исследуемого (красный) образцов оригинального ЛС Арифон.

На рис. 3 представлена матрица исходных данных сглаженных дифракционных спектров референтного (синий) и исследуемого (красный) образцов оригинального ЛС Арифон в координатах $X_{j,2}, X_{j,1}$ и $X_{j,1}, X_{j,2}$, где по оси абсцисс откладываются данные первого столбца матрицы X , а по оси ординат – второго, затем наоборот. На рис. 3 также изображена ГК Р2. ГК Р1 располагается строго перпендикулярно ГК Р2, но ее значение по оси ординат отрицательно, и она на рисунке не отображена.

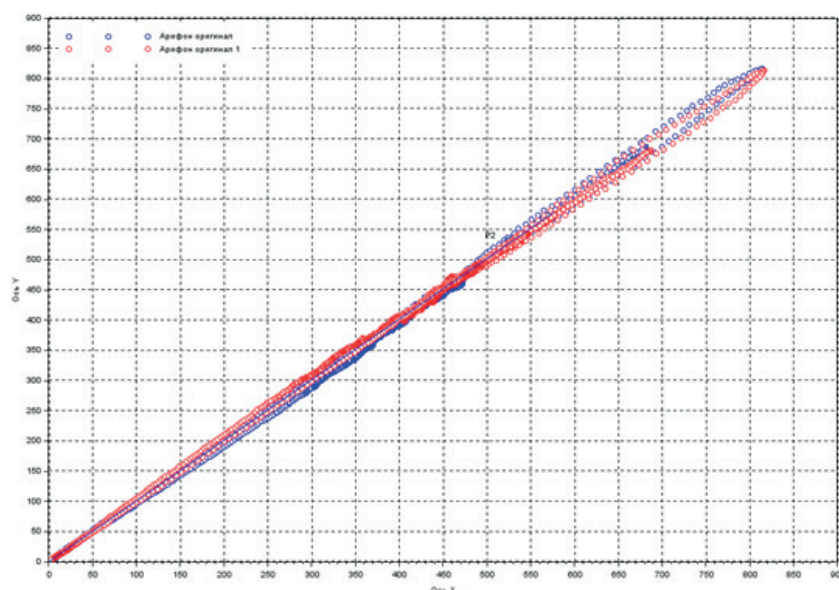


Рис. 3. Матрица исходных данных сглаженных дифракционных спектров референтного (синий) и исследуемого (красный) образцов оригинального ЛС Арифон в координатах $X_{j,2}, X_{j,1}$ и $X_{j,1}, X_{j,2}$ с изображением ГК Р2.

На рис. 4 представлена матрица счетов T с изображением ГК P1 и P2. Построение матрицы T выполнено аналогично рис. 3.

Для анализа эффективности применения МГК выполнен анализ фальсифицированного ЛС Арифон по алгоритму, описанному выше для оригинального ЛС Арифон.

На рис. 5 представлены сглаженные дифракционные спектры референтного (синий) и фальсифицированного (красный) ЛС Арифон. Из дифракционных картин видно сильное расхождение образцов.

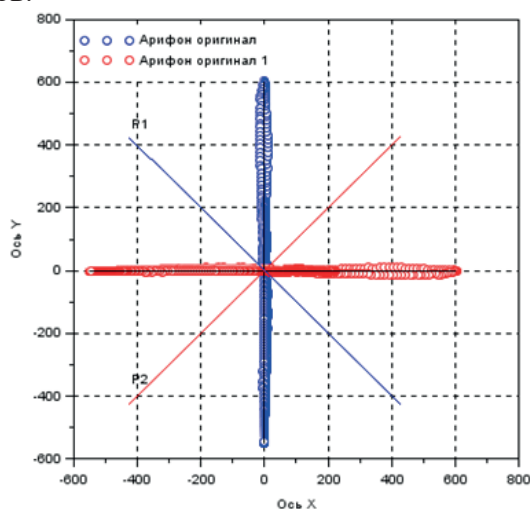


Рис. 4. Матрица счетов T с изображением ГК P1 и P2.

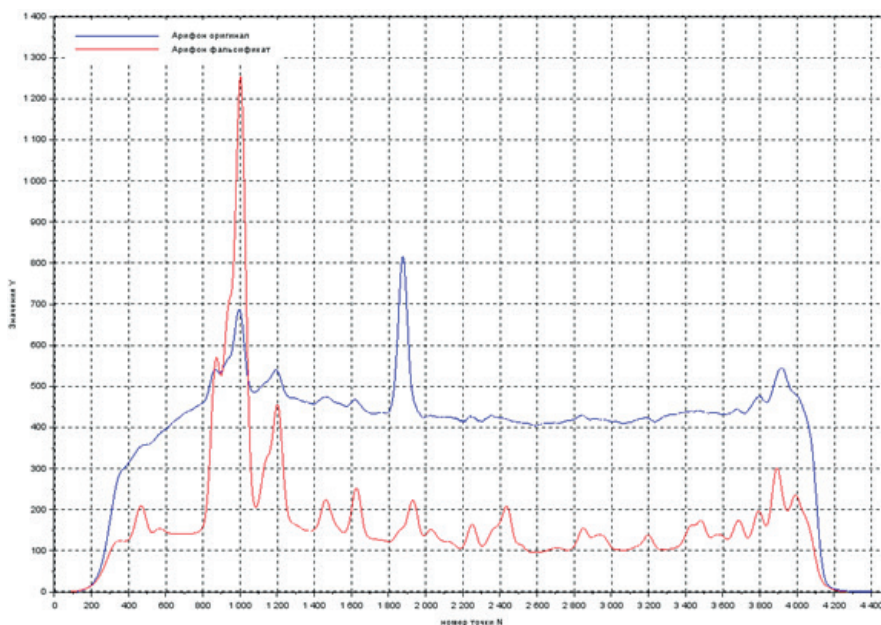


Рис. 5. Сглаженные дифракционные спектры референтного (синий) и фальсифицированного (красный) ЛС Арифон.

На рис. 6 представлена матрица исходных данных сглаженных дифракционных спектров референтного (синий) и фальсифицированного (красный) ЛС Арифон в координатах $X_{j,2}$, $X_{j,1}$ и $X_{j,1}$, $X_{j,2}$, также на рисунке изображена ГК P1. Вторая ГК P2 должна располагаться строго перпендикулярно первой, но ее значение по оси ординат отрицательно, и она на рисунке не отображена, что закономерно проявляется из исходных данных.

На рис. 7 приведена матрица счетов T с изображением ГК P1 и P2.

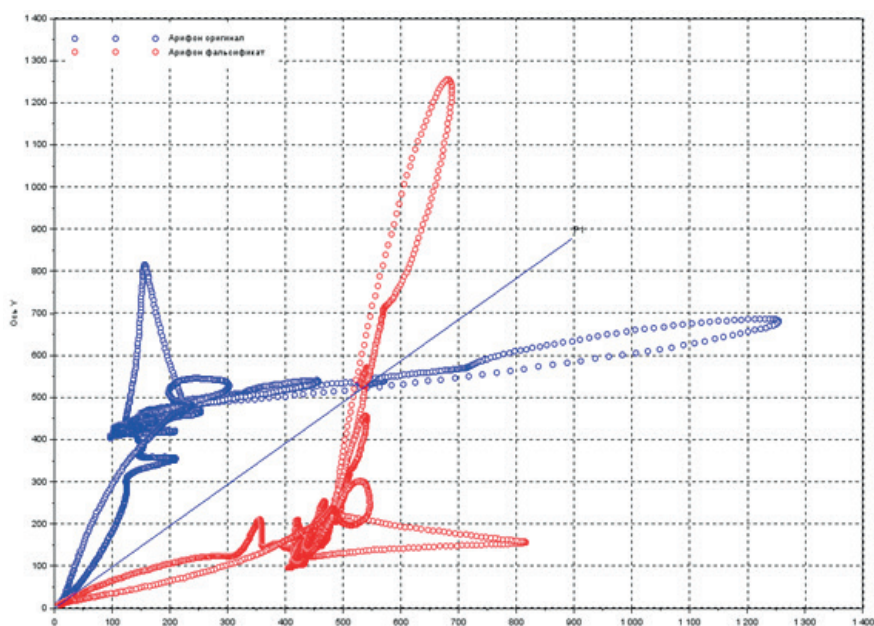


Рис. 6. Матрица исходных данных smoothed дифракционных спектров референтного (синий) и фальсифицированного (красный) ЛС Арифон в координатах $X_{j,2}, X_{j,1}$ и $X_{j,1}, X_{j,2}$ с изображением ГК P1.

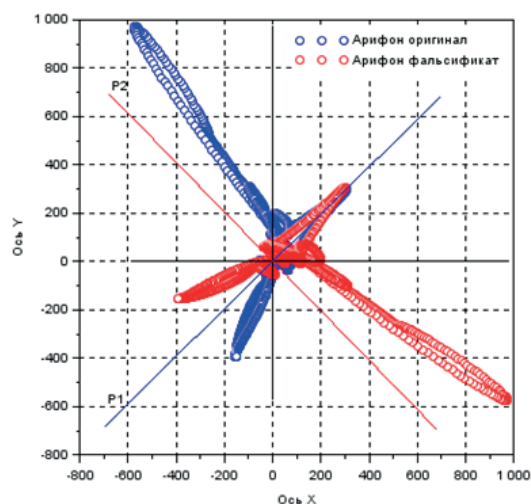


Рис. 7. Матрица счетов T с изображением ГК P1 и P2.

Результаты анализа образцов оригинального и фальсифицированного ЛС Арифон, преобразованные с помощью функции (4), сведены в таблицу, дополнительно в ней указано соотношение собственных чисел в процентах, то есть процент от общей дисперсии для каждого компонента⁶:

$$\begin{aligned} d_1 &= \lambda_1 \cdot 100 / (\lambda_1 + \lambda_2) \\ d_2 &= \lambda_2 \cdot 100 / (\lambda_1 + \lambda_2), \end{aligned} \quad (5)$$

где λ_1, λ_2 – собственные числа ковариационной матрицы исходных данных;
 d_1, d_2 – процент от общей дисперсии для каждого компонента.

⁶[http:// www.statsoft.ru/home/textbook/modules/stfacan.html](http://www.statsoft.ru/home/textbook/modules/stfacan.html)

Результаты исследований оригинального и фальсифицированного ЛС Арифон

ЛС	Матрица нагрузок, P		Вектор собственных значений, L		Соотношение вектора L , в %	
	ГК P1, X, Y	ГК P2, X, Y	λ_1	λ_2	d_1 , %	d_2 , %
Арифон оригинал	0.7084, -0.7058	0.7058, 0.7084	50379.53	9.4503	99.98	0.02
Арифон фальсификат	0.7146, -0.6996	-0.6996, -0.7146	39450.24	10509.27	78.96	21.04

Из таблицы видно, что в первом случае (оригинальный препарат) собственное число λ_1 более, чем в 5000 раз превышает λ_2 и объясняет 99.98 % общей дисперсии, при этом различие обоих данных составляет 0.02%. Это указывает на то, что отличие образцов незначительно, то есть исследуемое ЛС Арифон является оригинальным.

В случае фальсифицированного препарата собственные числа λ_1 и λ_2 отличаются всего лишь в 4 раза, и различие обоих образцов составляет 21.04%. Это указывает на то, что исследуемый образец не является оригинальным ЛС Арифон.

При обработке спектральных данных методом главных компонент нужно иметь некий образцовый набор данных (образец), наиболее точно отражающий спектр исследуемого вещества. Применение МГК сводится к сравнению исследуемого вещества с образцом, и в зависимости от полученных данных принимается решение о его соответствии образцу. В распоряжении авторов помимо дифрактограмм оригинального ЛС Арифон были дифрактограммы оригинальных ЛС Левомецетина, Метронидазола и Парацетамола, а также дифрактограммы фальсифицированного ЛС Арифона, поэтому сравнительному исследованию подвергался исключительно ЛС Арифон. Для дополнительной проверки работоспособности метода МГК было предложено провести сравнительный анализ заведомо разных ЛС – Арифона и Парацетамола, который показал, что различие образцов составляет порядка 30%. Такой результат (70% схожести) объясняется тем, что в состав этих ЛС входят одинаковые наполнители, а активные вещества разные.

Проведенные экспериментальные исследования показали работоспособность алгоритма МГК (с предварительным сглаживанием дифракционных спектров методом скользящего среднего) в разделении дифрактограмм для имеющейся выборки: 4 спектра оригинальных ЛС и 8 спектров фальсифицированных ЛС. Проведенная модельная процедура распознавания дифракционных спектров показала явную принадлежность оригинального ЛС Арифон к оригиналу, а фальсифицированного ЛС – к фальсификату. Данная методика может быть использована в учебных процессах по направлениям «Криминалистика» и «Промышленная фармацевтика». Для создания методики, позволяющей идентифицировать твердые лекарственные препараты методом рентгеновской дифракции, необходимо провести исследования на большом количестве выборок и проверку на различных лекарственных средствах.

Литература:

1. Елохин В.А., Архипов С.Н., Пьянкова Л.А., Петров А.В., Чехова Р.В., Пышный В.М. Рентгеновская дифрактометрия в фармацевтическом анализе: практика применения настольных дифрактометров «Дифрей» // Научное приборостроение. 2018. Т. 28. № 1. С. 61–68.

2. Государственная фармакопея РФ. Общая фармакопейная статья. Рентгеновская порошковая дифрактометрия. ОФС. URL: <http://pharmacopoeia.ru/ofs-1-2-1-1-0011-15-rentgenovskaya-poroshkovaya-difraktometriya/>
3. Болл С.В., Елохин В.А., Соколов В.Н. Фальсифицированные лекарственные средства и роль государства в борьбе с ними. М.: Инновационный фонд "РОСИСПЫТАНИЯ", 2009. 96 с.
4. Архипов С.Н., Болл С.В., Елохин В.А., Николаев В.И., Протопопов С.В., Пьянкова Л.А., Соколов В.Н. Рентгенодифракционный способ идентификации партий фармацевтической продукции: пат. 2452939 Рос. Федерация. № 2011102329/28; заявл. 18.01.2011; опубл. 10.06.2012. Бюл. № 16.
5. Родионова О.Е., Померанцев А.Л. Хемометрика в аналитической химии: обзор. М.: ИХФ им. Н.Н. Семенова РАН, 2016. 60 с. URL: http://www.chemometrics.ru/materials/articles/chemometrics_review.pdf
6. Соболева О.В., Елизарова Т.Е., Арик Ю.А., Колдина А.М., Морозова М.А. Ретроспективный обзор методологических основ новой ОФС «Спектрометрия в ближней инфракрасной области» // Ведомости Научного центра экспертизы средств медицинского применения. 2016. № 2. С. 58–64.
7. Safwan M. Obeidat, Ban Al-Tayyem. Spectroscopic and chemometric analysis of illegally manufactured formulations of selected medicines // Oriental Journal of Chemistry. 2012. V. 28. № 2. P. 795–801.
8. Caliendo R. Static and dynamical structural investigations of metal-oxide nanocrystals by powder X-ray diffraction: Colloidal tungsten oxide as a case of study // Chemistry Department / Brookhaven National Laboratory USA. March 2016. 30 p. URL: <https://www.bnl.gov/isd/documents/93116.pdf>
9. Родионова О.Е. Интервальный метод обработки результатов многоканальных экспериментов: дис. ... д-ра физ.-мат. наук. Москва, 2009. 272 с.
10. Эсбенсен К. Анализ многомерных данных / Сокр. пер. с англ. под ред. О. Родионовой. Черноголовка: ИПХФ РАН, 2005. 160 с.

References:

1. Elokhin V.A., Arkhipov S.N., Pyankova L.A., Petrov A.V., Chekhova R.V., Pyshniy V.M. X-ray diffractometry in pharmaceutical analysis: practices of using «Difray» benchtop diffractometers. *Nauchnoe priborostroenie* (Scientific Instrument Engineering). 2018; 28(1): 61-68. (in Russ.)
2. State Pharmacopoeia of the Russian Federation. General Pharmacopoeia Article. X-ray powder diffractometry. GPhA 1.2.1.1.0011.15. (in Russ.). URL: <http://pharmacopoeia.ru/ofs-1-2-1-1-0011-15-rentgenovskaya-poroshkovaya-difraktometriya/>
3. Boll S.V., Elokhin V., Sokolov V.N. Counterfeit medicines and the role of the state in combating them. Moscow: Innovation Fund "ROSISPYTANIYA", 2009. 96 p. (in Russ.)
4. Arkhipov S.N., Ball S.V., Elokhin V.A., Nikolaev V.I., Protopopov S.V., Pyankova L.A., Sokolov V.N. X-ray diffraction method for identifying batches of pharmaceutical products: Pat. 2452939 RU. No. 2011102329/28; filled 01/18/2011; publ. 06/10/2012. (in Russ.)
5. Rodionova O.E., Pomerantsev A.L. Chemometrics in analytical chemistry: Review. Moscow: N.N. Semenov Institute of Chemical Physics of the Russian Academy of Sciences, 2016. 60 p. (in Russ.). URL: http://www.chemometrics.ru/materials/articles/chemometrics_review.pdf

6. Soboleva O.V., Elizarova T.E., Arik Yu.A., Goldin A.M., Morozova M.A. A retrospective review of the methodological foundations of the new GPhA "Spectrometry in the near infrared region". *The Bulletin of the Scientific Centre for Expert Evaluation of Medicinal Products*. 2016; (2): 58-64.

7. Safwan M. Obeidat, Ban Al-Tayyem. Spectroscopic and chemometric analysis of illegally manufactured formulations of selected medicines. *Oriental Journal of Chemistry*. 2012; 28(2): 795-801.

8. Caliandro R. Static and dynamical structural investigations of metal-oxide nanocrystals by powder X-ray diffraction: Colloidal tungsten oxide as a case of study. Chemistry Department; Brookhaven National Laboratory USA. March 2016. 30 p. URL: <https://www.bnl.gov/isd/documents/93116.pdf>

9. Rodionova O.E. Interval method of processing the results of multichannel experiments: dissertation ... D.Sc. (Physics and Mathematics). Moscow, 2009. 272 p. (in Russ.)

10. Esbensen K.H. Multivariate Data Analysis – In Practice. 5-th ed. CAMO, 2004. 587 p.

Об авторах:

Чехова Регина Владимировна, кандидат химических наук, доцент кафедры «Приборы и информационно-измерительные системы» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Пышный Вячеслав Михайлович, кандидат технических наук, доцент кафедры «Приборы и информационно-измерительные системы» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (107996, Россия, Москва, ул. Стромынка, д. 20).

Пьянкова Любовь Алексеевна, кандидат геолого-минералогических наук, ведущий специалист КТО РТ АО «Научные приборы» (190103, Санкт-Петербург, Рижский пр., д. 26).

Елохин Владимир Александрович, кандидат физико-математических наук, генеральный директор АО «Научные приборы» (190103, Санкт-Петербург, Рижский пр., д. 26).

About the authors:

Regina V. Chekhova, Ph.D. (Chemistry), Associate Professor of the Chair “Devices and Information Measuring Systems”, Institute of Complex Security and Special Instrument Engineering, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Vyacheslav M. Pyshniy, Ph.D. (Engineering), Associate Professor of the Chair “Devices and Information Measuring Systems”, Institute of Complex Security and Special Instrument Engineering, MIREA – Russian Technological University (20, Stromynka st., Moscow 107996, Russia).

Lyubov A. Pyankova, Ph.D. (Geology and Mineralogy), Leading Specialist of Design and Technology Department, Scientific Instruments Inc. (26, Rzhskiy pr., St. Petersburg, 190103, Russia).

Vladimir A. Elokhin, Ph.D. (Physics and Mathematics), General Director of Scientific Instruments Inc. (26, Rzhskiy pr., St. Petersburg, 190103, Russia).

Для цитирования: Чехова Р.В., Пышный В.М., Пьянкова Л.А., Елохин В.А. Разделение дифракционных спектров методом главных компонент на примере лекарственного средства Арифон // Российский технологический журнал. 2019. Т. 7. № 1. С. 102–112. DOI: 10.32362/2500-316X-2019-7-1-102-112

For citation: Chekhova R.V., Pyshniy V.M., Pyankova L.A., Elokhin V.A. Separation of diffraction spectra by principal component method by the example of Arifon drug. *Rossiyskiy tekhnologicheskii zhurnal* (Russian Technological Journal). 2019; 7(1): 102-112. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-102-112

Свидетельство о регистрации СМИ Эл № ФС 77-74578 от 14 декабря 2018 г.

Дата опубликования 31 января 2019 г.

МИРЭА - Российский технологический университет

119454, Москва, пр. Вернадского, 78

<http://rtj.mirea.ru>