ISSN 2686-679X

ВЕСТНИК РГГУ

Серия
«Информатика.
Информационная безопасность.
Математика»

Научный журнал

RSUH/RGGU BULLETIN

"Information Science.
Information Security. Mathematics"
Series

Academic Journal

Основан в 2018 г.
Founded in 2018

4
2021

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

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

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

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

20.00.00 Informatics

81.93.29 Information security, data protection

27.00.00 Mathematics

Objectives and areas of research

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

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

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

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

e-mail: adkozlov@mail.ru

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

Выходит 4 номера печатной версии журнала в год.

Учредитель и издатель – Российский государственный гуманитарный университет (РГГУ)

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

20.00.00 Информатика

81.93.29 Информационная безопасность, защита информации

27.00.00 Математика

Цели и область

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

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

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

Тел: +7 (916) 250-90-85

электронный адрес: adkozlov@mail.ru

Учредитель и издатель
Российский государственный гуманитарный университет (РГГУ)

Ответственный за выпуск:

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

CONTENTS

СОДЕРЖАНИЕ

УДК 004.4
DOI: 10.28995/2686-679X-2021-4-8-29

Разработка и реализация алгоритмов построения точной карты пространства

Тамара М. Волосатова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, tamarav@bmstu.ru

Галина С. Зубова
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, galya.zubova@mail.ru

Светлана Ю. Князева
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, knyazeva@bmstu.ru

Михаил В. Филиппов
Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия, filippov.mike@mail.ru

Аннотация. Построение карты пространства является одной из важнейших задач компьютерного зрения. В статье рассмотрены существующие реализации алгоритма одновременного позиционирования и создания карты местности, основанные на принципах маркерного трекинга. Проанализированы их преимущества и недостатки в рамках решения задачи построения точной карты пространства. Отмечено, что маркерный трекинг требует трудоемких ручных измерений, и, следовательно, больших временных затрат. Поэтому в статье подробно рассмотрены алгоритмы безмаркерного трекинга, не требующие большого количества ручных измерений. На основе проведенного сравнительного анализа выбран базовый алгоритм для решения задачи создания карты пространства – DSO-SLAM, который обладает высокими показателями точности и быстродействия. Отмечены основные недостатки этого алгоритма – отсутствие возможности сохранения карты и коррекции петли. В статье представлен алгоритм, позволяющий устранить указанные недостатки и дающий возможность масштабировать, поворачивать и смещать получаемую карту в пространстве. Показано, что разработанная модификация

существующего алгоритма повышает его точность и надежность работы. Она включает следующие составные части: методы модификации карты, методы сохранения и загрузки карты, алгоритм замыкания петель. Разработан программный комплекс, реализующий рассмотренный алгоритм. Представлены примеры работы данного комплекса, иллюстрирующие особенности замыкания петель и сохранение карты пространства.

Ключевые слова: slam, безмаркерный трекинг, одометрия, дескрипторы, дисторсия, замыкание петель, bugofwords

Для цитирования: Волосатова Т.М., Зубова Г.С., Князева С.Ю., Филиппов М.В. Разработка и реализация алгоритмов построения точной карты пространства // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 8–29. DOI: 10.28995/2686-679X-2021-4-8-29

Design, development and implementation of precision space mapping algorithm

Tamara M. Volosatova
Bauman Moscow State Technical University, Moscow, Russia, tamarav@bmstu.ru

Galina S. Zubova
Bauman Moscow State Technical University, Moscow, Russia, galya.zubova@mail.ru

Svetlana Yu. Knyazeva
Bauman Moscow State Technical University, Moscow, Russia, knyazeva@bmstu.ru

Mikhail V. Filippov
Bauman Moscow State Technical University, Moscow, Russia, filippov.mike@mail.ru

Abstract. Creating the map of a space is one of the most important tasks of computer vision. The article is considering existing implementations for the terrain simultaneous localization and mapping algorithm, based on the principles of marker tracking. Their advantages and disadvantages are analyzed in the framework of solving the problem of constructing an accurate space map. It is noted that the marker tracking requires time-consuming manual measurements, and, therefore, time spending. Therefore, the article discusses in detail markerless tracking algorithms that do not require a large number of manual

measurements. The basic algorithm for solving the problem of creating a space map – DSO-SLAM, having high indicators of accuracy and speed, was selected on the basis of the comparative analysis. The main disadvantages of that algorithm are noted – the inability to save the map and correct the loop. The article presents an algorithm that allows eliminating those shortcomings and makes it possible to scale, rotate and shift the resulting map in space. It is shown that the developed modification of the existing algorithm increases its accuracy and reliability. It includes the following components: methods for modifying a map, methods for saving and loading a map, an algorithm for closing loops. A software package has been developed that implements the considered algorithm. The article presents examples of the operation of such a complex, illustrating the features of the loop closure and saving the space map.

Keywords: SLAM, markerless, tracking, odometry, descriptors, distortion, loop closure, bag of words

For citation: Volosatova, T.M., Zubova, G.S., Knyazeva, S.Yu. and Filippov, M.V. (2021), "Design, development and implementation of precision space mapping algorithm", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 8–29, DOI: 10.28995/2686-679X-2021-4-8-29

Введение

Одной из важнейших задач компьютерного зрения является задача построения карты пространства, которая реализуется путем применения алгоритма одновременного позиционирования и построения карты местности (Simultaneous Localization And Mapping – SLAM) [Bergmann, Wang, Cremers 2018].

Безмаркерный трекинг в последние годы становится все более популярным и исследуемым. В частности, он очень востребован в робототехнике и киноиндустрии. При съемке возникает необходимость в построении карты пространства. Маркерный трекинг требует трудоемких ручных измерений, большого количества маркеров и, соответственно, длительной подготовки съемочных павильонов. Все эти проблемы можно решить путем использования безмаркерного трекинга [Lychkov, Alfimtsev, Sakulin 2018]. Для построения карты в данном случае требуется лишь откалиброванная камера и, возможно, задание положений некоторых точек для масштабирования или ориентации карты в виртуальном пространстве. Однако построить точную карту пространства таким методом не удается.

Для решения проблемы получения точной карты пространства необходимо проанализировать существующие реализации алго-

ритмов безмаркерного трекинга, чтобы модифицировать какую-либо из них или разработать собственную реализацию, позволяющую получать точную карту пространства, сохранять ее, вращать, смещать, масштабировать согласно выбранной системе координат.

Целью публикации является разработка эффективного алгоритма безмаркерного трекинга, позволяющего хранить, модифицировать и корректировать карту изучаемого пространства в процессе ее построения.

Для достижения данной цели поставлены и решены следующие задачи:

1. Провести анализ существующих реализаций алгоритмов безмаркерного трекинга и выбрать наиболее перспективную.

2. Разработать собственную модификацию выбранного алгоритма, включающую:

– методы сохранения и загрузки карты изучаемого пространства;
– методы модификации карты;
– методы коррекции ошибки позиционирования в процессе построения.

Анализ методов. Теоретическая часть

1. Метод SLAM

Метод одновременной локализации и построения карты (SLAM, от *англ.* Simultaneous Localization and Mapping) – метод, используе- мый в мобильных автономных средствах для построения карты в неизвестном пространстве или для обновления карты в заранее известном пространстве с одновременным контролем текущего местоположения и пройденного пути [Ген, Чулин 2017].

Метод SLAM предназначен для решения следующих задач:

– построение карты;
– построение траектории движения.

При этом на алгоритм SLAM накладываются следующие ограничения [Ген, Чулин 2017]:

– метод SLAM не использует данные о среде пространства (метки, предварительная карта);
– среда считается статической (неподвижной) [Lucey 2016].

Работа SLAM может быть представлена как последовательное повторение следующих шагов:

1. Сканирование окружающего пространства.

2. Вычисление ключевых точек каждого нового кадра пространства.

3. Определение смещения на основе сравнения текущего кадра с предыдущим.

4. Сопоставление ключевых точек текущего кадра с точками предыдущих кадров.

5. Обновление на основе этой информации данных предыдущих кадров, оптимизация положения кадров и 3D-позиций точек карты.

На каждом шаге построения карты новый кадр поступает в систему. При этом система хранит ранее сделанные предположения о структуре карты пространства. Вся работа алгоритма разделяется на две части: SLAM-frontend и SLAM-backend.

Задача SLAM-frontend заключается в анализе данных, получаемых от сенсора, и получении на их основе предположения о положении робота в пространстве в данный момент времени, а также передаче этих данных SLAM-backend [Ген, Чулин 2017].

Задача SLAM-backend заключается в оптимизации полученных от SLAM-frontend данных с целью минимизации функции ошибки. Этот этап должен быть независим от метода получения данных от камеры [Ген, Чулин 2017].

1.1. Задача SLAM-frontend

Для выполнения этой задачи необходимо выполнить следующие процедуры:

- получение данных камеры и приведение их к виду, необходимому для работы алгоритма;
- обнаружение ключевых точек;
- получение оценочного положения в пространстве на основе анализа полученных точек и точек, обнаруженных в предыдущих кадрах.

1.2. Задача SLAM-backend

Сравнение данных, полученных в результате предполагаемого локального сдвига камеры, и данных, полученных в результате поиска ключевых точек.

Оптимизация положения камеры и 3D-позиций ключевых точек и обновление данных об изучаемом пространстве.

2. Виды SLAM

Существует два принципиально разных подхода к решению задачи позиционирования в пространстве:

– прямая одометрия;
– непрямая одометрия, базирующаяся на поиске особых объектов [Engel, Schöps, Cremers 2014] [Haynsworth 1968].

Одометрия – метод оценки положения и ориентации робота или иного устройства на основе анализа последовательности изображений, снятых установленной на нем камерой. Базирующаяся на поиске особых объектов, одометрия хранит геометрическую модель карты. Точки в ней представлены своими 3D-координатами, при этом оптимизируется функция, зависящая от трехмерных координат точек в пространстве.

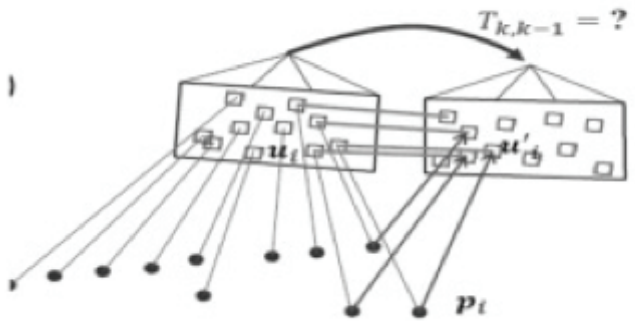

Рис. 1. Схема непрямой одометрии

$$T_{k,k-1} = \arg min_T \sum_i \left\| u'_i - \pi(p_i) \right\|_{\Sigma^2} \quad (1)$$

Здесь u_i – координаты точки первого кадра, а p_i – ее проекции на втором.

В прямой одометрии карта представляет собой набор кадров, в каждом из которых содержится набор особых точек. Каждая точка – это координаты ключевой точки на изображении и ее инверсная глубина. Оптимизируемая функция зависит от интенсивности пикселей изображения [Engel, Koltun, Cremers 2016].

$$I_{k-1}(i) I_k(i') - \sum_i T_{k,k-1} = \arg min_T \quad (2)$$

$$where u'_i = \pi\,(T * (\pi^{-1}(u_i) * d))$$

Здесь I_k – интенсивность одного изображения, а I_{k-1} – другого.

Таким образом, в случае прямой одометрии для получения точки, помимо положения самого кадра, необходимо оптимизировать один параметр, а в непрямой – три [Ген, Чулин 2017].

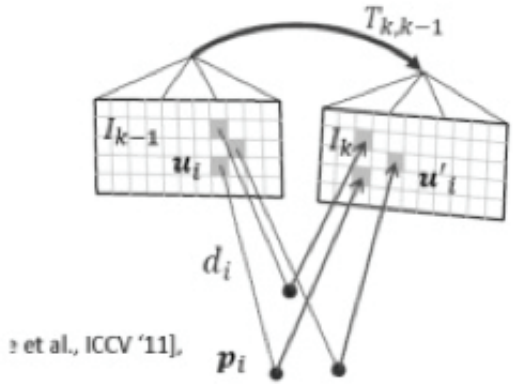

Рис. 2. Схема прямой одометрии

К достоинствам методов, базирующихся на поиске ключевых точек, можно отнести быстродействие и легкое удаление шумов; к недостаткам – неточность при гладкой текстуре, не имеющей углов, и использование малой части информации изображений.

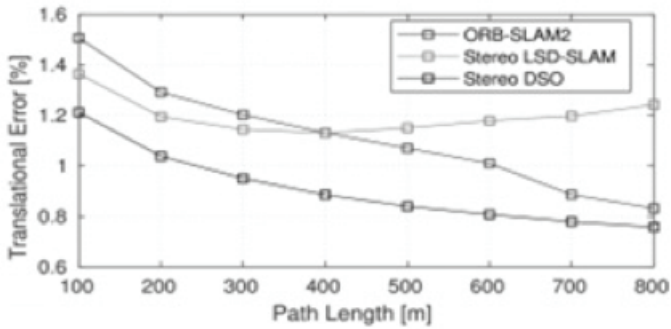

Рис. 3. Погрешность смещения кадров
[Engel, Koltun, Cremers 2018]

Прямые методы

К достоинствам этих методов можно отнести использование более полной информации об изображении, в связи с чем получают точное нахождение ключевых точек и построение карты [Пелевин,

Балясный 2017], а к недостаткам – необходимость хорошей инициализации и невысокую скорость, хотя существует возможность распараллеливания [Ген, Чулин 2017].

На рисунках 3–4 представлено сравнение работы методов прямой и непрямой одометрии в виде графиков зависимости их погрешностей смещения и вращения от количества обработанных кадров:

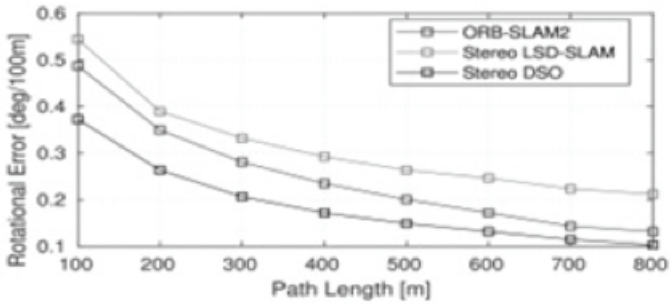

Рис. 4. Погрешность поворота кадров [Engel, Koltun, Cremers 2018]

здесь:
DSO-SLAM – разреженная прямая одометрия, LSD-SLAM – неразреженная прямая одометрия [Engel, Schöps, Cremers 2014], ORB-SLAM – непрямая одометрия [Mur-Artal, Montiel, Tardós 2015]

Для решения поставленной задачи наиболее рациональным можно считать метод прямой разреженной одометрии [Tu, Huang, Zhang, Yu, Xu, Chen 2015]. Это обосновано тем, что данный метод обладает высоким быстродействием и точностью распознавания в связи с используемыми алгоритмами оптимизации глубины ключевых точек.

3. DSO-SLAM

Данная разновидность метода использует достаточно серьезную инициализацию. Для этого производятся геометрическая и фотометрическая калибровки, на основе которых вычисляются параметры камер [Garcia-Fidalgoa, Ortiza 2014]. Отслеживание включает в себя следующие этапы [Engel, Koltun, Cremers 2018]:

1. Инициализация.
   1.1. Обнаружение ключевых точек на кадре.
   1.2. Оптимизация положения второго кадра с учетом точек кадра.
2. Получение следующего кадра, загрузка его в систему, исправление фотометрических и геометрических ошибок.
3. Анализ всех возможных направлений движения, оптимизация, выбор текущего положения кадров.
4. Оптимизация положений и позиций точек предыдущих кадров.
5. Вычисление ключевых точек текущего кадра.

Рассмотрим теоретическую основу этих этапов.

Для инициализации системы необходимо два ключевых кадра. На первом ищутся ключевые точки (механизм поиска будет рассмотрен далее) и задается начальное положение всей карты – ноль глобальной системы координат. Далее определяется второй ключевой кадр. Его позиция получается путем оптимизации целевой функции – преобразования интенсивностей изображений текущего и предыдущего кадров [Engel, Koltun, Cremers 2016].

3.1. Обнаружение ключевых точек

При загрузке изображения в систему высчитываются градиенты интенсивности для каждой точки – пикселя изображения. Для этого необходимо выполнить следующие действия. Изображение разбивается на прямоугольные области. В каждой области суммируются значения градиентов внутренних точек. Затем изображение сжимается в 2 раза, и операция повторяется. Таким образом, строится пирамида гауссиан и разностей гауссиан [Lowe 2004].

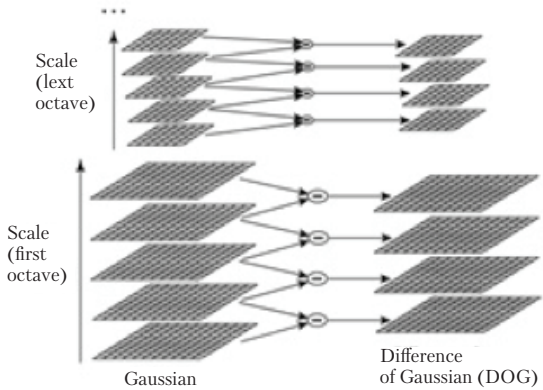

Рис. 5. Пирамида гауссиан [Мясников 2012]

Гауссианом (или изображением, размытым гауссовым фильтром) является изображение, описываемое интегралом свертки значения интенсивности исходного изображения с гауссовым фильтром:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y). \quad (3)$$

Здесь L – значение гауссиана в точке с координатами (x, y), а σ – радиус размытия. G – гауссово ядро, I – значение исходного изображения, $*$ – операция свертки [Lowe 2004].

Разностью гауссиан называют изображение, полученное путем попиксельного вычитания гауссиана исходного изображения из гауссиана с другим радиусом размытия [Lowe 2004].

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) = L(x, y, k\sigma) - L(x, y, \sigma). \quad (4)$$

При помощи пирамиды гауссиан ищутся ключевые точки в так называемом масштабируемом пространстве. Масштабируемым пространством изображения является набор всевозможных версий исходного изображения, сглаженных некоторым фильтром. Доказано, что гауссово масштабируемое пространство является линейным, инвариантным относительно сдвигов, вращений, масштаба, не смещающим локальные экстремумы [Bergmann, Wang, Cremers 2018]. Степень размытия изображения гауссовым фильтром может быть принята за исходное изображение, взятое в некотором масштабе. Таким образом, поиск ключевых точек инвариантен относительно масштаба, если производится на разных уровнях пирамиды гауссиан. Для этого масштабируемое пространство разбивается на несколько участков. Исходное изображение уменьшается в N раз для N-го уровня пирамиды, причем N является степенью двойки. Далее изображение разбивается на ячейки, и в них считается сумма градиентов ключевых точек, а также их направления и дескрипторы. Направление ключевой точки вычисляется исходя из направлений градиентов точек, соседних с особой. Все вычисления градиентов производятся на изображении в пирамиде гауссиан, с масштабом, наиболее близким к масштабу ключевой точки [Супрун 2016].

$$m(x, y) = \sqrt{\left(L(x+1, y) - L(x-1, y)\right)^2 + \left(L(x, y+1) - L(x, y-1)\right)^2},$$

$$\theta(x, y) = tan^{-1}\left(\frac{L(x, y+1) - L(x, y-1)}{L(x+1, y) - L(x-1, y)}\right). \quad (5)$$

Направление ключевой точки находится из гистограммы направлений. Гистограмма состоит из 36 компонент, которые равномерно покрывают промежуток в 360 градусов, и формируется следующим образом: каждая точка окна *(x, y)* вносит вклад, равный *m*G(x, y, sigma)*, в ту компоненту гистограммы, которая покрывает промежуток, содержащий направление градиента $\theta(x, y)$ [Акинин, Никифоров, Таганов 2016]. Направление ключевой точки лежит в промежутке, покрываемом максимальной компонентой гистограммы. Значения максимальной компоненты (*max*) и двух соседних с ней интерполируются параболой, и точка максимума этой параболы берется в качестве направления ключевой точки. Если в гистограмме есть еще компоненты с величинами не меньше *0.8*max*, то они аналогично интерполируются, и дополнительные направления приписываются ключевой точке [Инсаров, Тихонова, Ранкова 2016].

Дескриптор ключевой точки состоит из всех полученных гистограмм. В качестве ключевой точки выбирается та, в которой дескриптор достигает локального максимума в некоторой области – ячейке. Если при поиске ключевых точек результатов получено значительно больше, чем необходимо, действия повторяются, но размеры ячеек берутся большего размера, если не хватает – меньшего. После получения необходимого в некоторых пределах количества ключевых точек часть отбрасывается случайным образом.

3.2. Исправление геометрических ошибок изображений

Геометрическая ошибка изображения, как правило, вызвана дисторсией. Существуют два основных вида дисторсии – радиальная и тангенциальная [Стрелкова, Труфанов, Титов 2019].

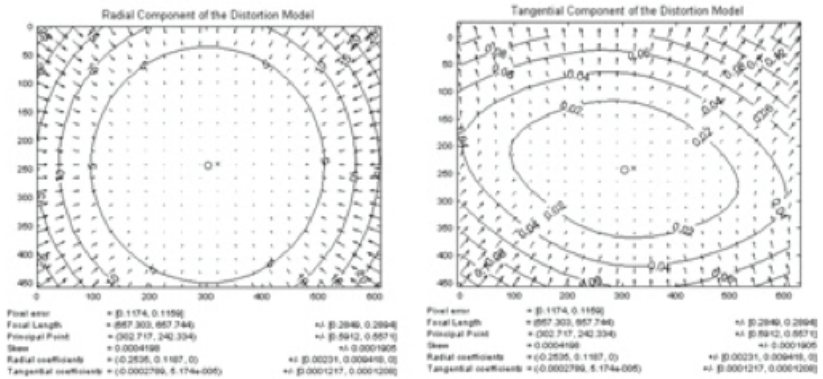

Рис. 6. Дисторсия [Gao 2003]

Радиальная дисторсия – искажение изображения в результате неидеальности параболической формы линзы. Искажения, вызванные радиальной дисторсией, равны нулю в оптическом центре сенсора и возрастают к краям. Как правило, радиальная дисторсия вносит наибольший вклад в искажение изображения [Bergmann, Wang, Cremers, 2018].

Тангенциальная дисторсия – искажения изображения, вызванные погрешностями в установке линзы параллельно плоскости изображения [Пелевин, Балясный, 2017].

Для устранения дисторсии координаты пикселей можно пересчитать с помощью следующего уравнения [Yang, Wang, Gao, Cremers 2018]:

$$u_{corrected} = u(1 + k_1r^2 + k_2r^4 + k_3r^6) + 2p_1uv + (r^2 + 2u^2),$$
$$v_{corrected} = v(1 + k_1r^2 + k_2r^4 + k_3r^6) + 2p_2uv + p_1(r^2 + 2v^2), \quad (6)$$

где (u, v) – первоначальное расположение пикселя;

$(u_{corrected}, v_{corrected})$ – расположение пикселя после устранения геометрических искажений;

k_1, k_2, k_3 – коэффициенты радиальной дисторсии;

p_1, p_2 – коэффициенты тангенциальной дисторсии, $r^2 = u^2 + v^2$. [Gao, Hou, Tang, Cheng 2003].

Точность измерения параметров камеры (коэффициенты дисторсии, матрица камеры) определяется средней величиной ошибки перепроецирования (Reprojection Error, ReEr) – расстояния (в пикселях) между проекцией P' на плоскость изображения точки P на поверхности объекта, и проекцией P'' этой же точки P, построенной после устранения дисторсии с использованием параметров камеры [Belov, Andrianova 2017]. Камера, используемая в системе, должна быть заранее откалибрована [Scaramuzza 2016].

Истинные (идеальные) координаты точки могут быть выражены из реальных (искаженных) координат и величин смещения точек вдоль осей абсцисс и ординат соответственно.

$$x' = x + \delta_x, \quad (7)$$
$$y' = y + \delta_y \quad (8)$$

где (x, y) – реальные координаты точки,

(x', y') – истинные координаты точки,

δ_x, δ_y – величины смещения точек вдоль осей абсцисс и ординат соответственно.

Величины смещения выражаются следующим образом:

$$\delta_x = k_1 x(x^2 + y^2) + p_1(3x^2 + y^2) + 2p_2 xy \quad (9)$$
$$\delta_y = k_1 y(x^2 + y^2) + p_2(3x^2 + y^2) + 2p_1 xy, \quad (10)$$

где $k_1 x(x^2 + y^2)$ и $k_1 y(x^2 + y^2)$ – величина радиальной дисторсии;

$p_1(3x^2 + y^2)+2p_2 xy$ *и* $p_2(3x^2 + y^2) + 2p_1 xy$ – величина тангенциальной дисторсии;

k_1, p_1, p_2 – коэффициенты дисторсии.

3.3. Определение положения кадра в пространстве

Этот процесс моделируется следующим образом. Задаются предположительные смещения нового кадра в пространстве. Для начала задаются варианты изменения координат, основанные на предыдущих смещениях ключевых кадров. Например, делается предположение, что кадр сдвинулся так же, как предыдущий кадр относительно позапрошлого. Предлагаются различные комбинации матриц смещений трех последних кадров системы. Далее выдвигаются предположения о поворотах кадра относительно различных осей на различные углы. Все эти предположения последовательно служат начальными приближениями при оптимизации позиции кадра и его точек в 3D-пространстве [Strasdat, Davison, Montiel, Konolige 2011].

Положение каждого кадра задается его шестью степенями свободы (кватернион [Valigi 2016] и смещение) и двумя фотометрическими параметрами. Фотометрическая ошибка в этом алгоритме задается нелинейной функцией преобразования между двумя последовательными изображениями [Engel, Koltun, Cremers 2018]:

$$I_i(x) = G(t_i V(x) B_i(x)) \quad (11)$$
$$I'_i(x) = t_i B_i(x) = \frac{G^{-1}(I_1(x))}{V(x)} \quad (12)$$

$B(x)$, $V(x)$ – множества значений координат на изображении по осям x и y.

Процесс локализации представляет собой движение некоторого окна по 5–7 кадров. Позиции этих кадров и их точек постоянно оптимизируются и обновляются.

Каждая функция ошибки есть суперпозиция ошибок в восьми точках выбранного шаблона, т. е. помимо ошибки в ключевой точке суммируются ошибки еще в семи окружающих ее точках [Engel, Koltun, Cremers 2018].

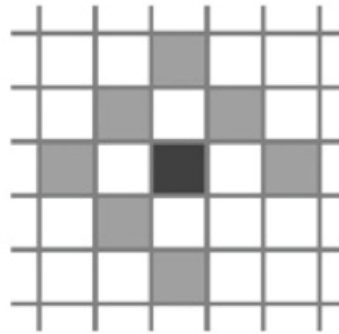

Рис. 7. Пиксельный шаблон
[Engel, Koltun, Cremers2018]

Практическая часть

Базовый DSO-SLAM алгоритм обладает высокими показателями точности и быстродействия, однако имеет ряд недостатков: в нем отсутствует возможность сохранения карты и не реализован механизм коррекции петли. Именно эти недостатки стали задачей при разработке и реализации собственной версии алгоритма DSO-SLAM. В авторской версии недостатки базового алгоритма были устранены.

Алгоритм замыкания петель.

При разработке любого алгоритма важным является достижение максимально возможной точности его работы. Одним из способов решения данной проблемы является алгоритм замыкания петель.

При движении камеры по изучаемому пространству возможны ситуации повторного возвращения в уже пройденную точку. Из-за погрешности позиции кадров в одном и том же месте пространства будут отличаться и карта будет сдвинута относительно самой себя. Такая ситуация корректируется алгоритмом замыкания петель.

Для замыкания петель удобно применять представление информации об изображении в виде так называемой Bug of Words [Valigi 2016], далее BoW. Этот механизм необходим для кластеризации дескрипторов точек. Это упрощает подсчет количества вхождений каждой точки в систему. Таким образом, каждое изображение может быть представлено в виде некоторой гистограммы частот [Gálvez-López, Tardós 2012].

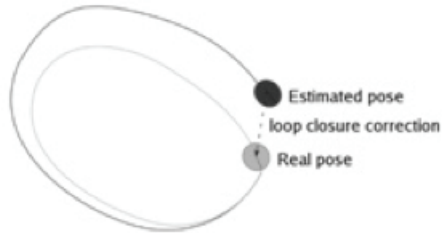

Рис. 8. Петля [Valigi 2016]

Сходство изображений получается из сходства гистограмм, включенных в некоторый словарь. Словарь представляет собой K-D бинарное дерево. При этом на верхних уровнях записаны первые элементы дескрипторов, на вторых – вторые и т. д. Создается индекс дескриптора. Каждый дескриптор имеет вес, отображающий частоту его появления. Приходящее в систему новое изображение добавляется в базу данных BoW и преобразуется в вектор дескрипторов – слов. Для этого в дереве ищется ближайший по расстоянию Хемминга дескриптор к текущему дескриптору ключевой точки изображения [Kejriwal, Kumar, Shibata 2016].

Для каждого слова в базе данных хранится список изображений, где данное слово присутствует. Далее ищутся такие изображения, которые обладают наибольшим количеством сходных слов с текущим исследуемым изображением.

Результат работы алгоритма замыкания петель представлен на рис. 9:

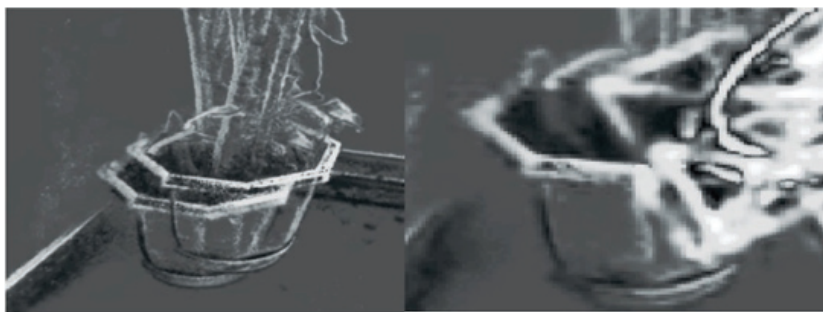

Рис. 9. Результат замыкания петли

3.4. Сохранение облака точек

Для дальнейшей визуализации результата удобно получать карту в виде какого-либо объекта, понятного другим программам – например, облака точек. В таком случае карту можно загружать в любую систему, предназначенную для визуализации, и оценивать результат работы алгоритма [Zhuravlev, Razevig, Chizh, Bugaev 2016]. В системе хранятся положения кадров и точки в этих кадрах. Точка задается своим положением на изображении и инверсной глубиной[1]. Для получения их 3D-позиций в глобальной системе координат необходимо:

1. Получить 3D-точку в системе координат кадра:

$$x = (u * fxi + cxi) * depth; \quad (13)$$
$$y = (v * fyi + cyi) * depth; \quad (14)$$
$$z = depth * (1 + 2 * sqrt(fxi * fxi + fyi * fyi)), \quad (15)$$

где u, v – координаты точки на кадре;
$depth$ – обратная глубина;
fxi, fyi – инверсные фокусные расстояния камеры;
cxi, cyi – инверсные положения центра камеры.

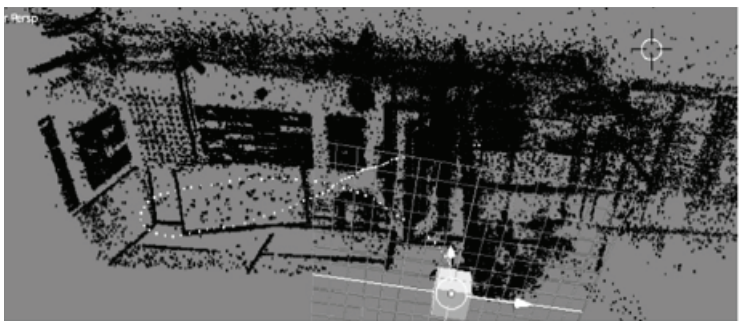

Рис. 10. Сохраненная карта

2. Получить точку в глобальной системе координат:

Для этого необходимо умножить координаты точки в системе координат кадра на матрицу преобразования – [R|t], где R – мат-

[1] Инверсная глубина – значение, обратное глубине точки изображения. Доказано [Yang, Wang, Gao, Cremers 2018], что такое хранение информации наиболее удобно и экономично в контексте решаемой задачи.

рица поворота кадра в глобальной системе координат карты (хранится в виде кватерниона [Зубов, Лапин, Микрин 2013] [Kejriwal, Kumar, Shibata 2016]), t – вектор смещения кадра.

Результаты и дискуссии

В результате проведения теоретических исследований определены алгоритмы безмаркерного трекинга неизвестного пространства и позиционирования мобильного робота.

На основе существующих методов модифицирован собственный DSO-SLAM алгоритм, включающий:

- сохранение карты пространства в различных форматах;
- алгоритм замыкания петель, повышающий точность работы безмаркерного трекинга.

В результате проведенных практических исследований были выявлены следующие проблемы:

- механизм замыкания петель и коррекции карты понижает быстродействие работы алгоритма безмаркерного трекинга. Для повышения быстродействия необходима разработка механизмов распараллеливания программы для реализации алгоритма замыкания петель;
- алгоритм безмаркерного трекинга плохо работает при резких поворотах камеры. Для корректной работы необходимо разработать устройство, осуществляющее плавное движение и повороты камеры со смещением.

В данный момент проводятся работы по решению выявленных проблем.

Литература

Акинин, Никифоров, Таганов 2016 – *Акинин М.В., Никифоров М.Б., Таганов А.И.* Нейросетевые системы искусственного интеллекта в задачах обработки изображений. М.: Горячая линия-Телеком, 2016.

Ген, Чулин 2017 – *Ген К.К., Чулин Н.А.* Алгоритм навигации беспилотного летательного аппарата на основе улучшенного алгоритма одновременной локализации и картографирования с адаптивным локальным диапазоном наблюдения // Вестник МГТУ им. Н.Э. Баумана, серия Приборостроение. 2017. № 3. С. 76–94.

Зубов, Лапин, Микрин 2013 – *Зубов Н.Е., Лапин А.В., Микрин Е.А.* Применение кватернионов в модальном управлении ориентацией космических аппаратов // Инженерный журнал: наука и инновации. 2013. Вып. 10. С. 1–14.

Инсаров, Тихонова, Ранкова 2016 – *Инсаров В.В., Тихонова С.В., Ранкова А.В.* Алгоритмы распознавания объектов из состава наземных сцен в системах технического зрения беспилотных летательных аппаратов // Вестник компьютерных и информационных технологий. 2016. № 11. С. 25–32.

Мясников 2012 – *Мясников В.Д.* Модельно-ориентированный дескриптор поля градиента как удобный аппарат распознавания и анализа цифровых изображений // Компьютерная оптика. 2012. Т. 36. № 4. С. 596–604.

Пелевин, Балясный 2017 – *Пелевин Е.Е., Балясный С.В.* Использование метода Adaptive Threshold в системе технического зрения // Juvenisscientia. Сер. Технические науки. 2017. № 1. С. 4–7.

Стрелкова, Труфанов, Титов 2019 – *Стрелкова А.Н., Труфанов М.И., Титов Д.И.* Способ калибровки дисторсии оптико-электронного устройства [Электронный ресурс]. URL: http://www.findpatent.ru/patent/232/2321888.html (дата обращения 17 мая 2019).

Супрун 2016 – *Супрун Д.Е.* Алгоритм сопоставления изображений по ключевым точкам при масштабируемости и вращении объектов // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2016. № 5. С. 86–98.

Belov, Andrianova 2017 – *Belov A.A., Andrianova O.G.* Robust anisotropy-based control of linear discrete-time descriptor systems with norm-bounded uncertainties // IFAC-Papers On Line. 2017. Vol. 50. Iss. 1. P. 15471–15476.

Bergmann, Wang, Cremers 2018 – *Bergmann P., Wang R., Cremers D.* Online Photometric Calibration of Auto Exposure Video for Realtime Visual Odometry and SLAM // IEEE Robotics and Automation Letters (RA-L). 2018. Vol. 3, no. 2. P. 627–634.

Engel, Koltun, Cremers 2016 – *Engel J., Koltun V., Cremers D.* Direct Sparse Odometry [Электронный ресурс]. URL: https://arxiv.org/pdf/1607.02565.pdf (дата обращения 20 декабря 2021).

Engel, Koltun, Cremers 2018 – *Engel J., Koltun V., Cremers D.* Direct Sparse Odometry // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2018. Vol. 40, no. 3. P. 611–625.

Engel, Schöps, Cremers 2014 – *Engel J., Schöps T., Cremers D.* LSD-SLAM: Large-Scale Direct Monocular SLAM // Proceedings of the 13th European Conference Computer Vision – ECCV 2014, Zurich, Switzerland, September 6–12, 2014. Berlin: Springer, 2014. P. 834–849.

Gao, Hou, Tang, Cheng 2003 – *Gao X.S., Hou X.R., Tang J., Cheng H.F.* Complete solution classification for the perspective-three-point problem // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2003. Vol. 25, no. 8. P. 930–943.

Gálvez-López, Tardós 2012 – *Gálvez-López D., Tardós J.D.* Bags of Binary Words for Fast Place Recognition in Image Sequences // IEEE Transactions on Robotics. 2012. Vol. 28, no. 5. P. 1188–1197.

Garcia-Fidalgoa, Ortiza 2014 – *Garcia-Fidalgoa E., Ortiza A.* Vision-based topological mapping and localization methods: A survey // Robotics and Autonomous Systems. 2014. Vol. 64. P. 1–20.

Haynsworth 1968 – *Haynsworth E.V.* On the Schur Complement // Basel Mathematical Notes. (BMN). 1968. Vol. 20. P. 1–17.

Kejriwal, Kumar, Shibata 2016 – *Kejriwal N., Kumar S., Shibata T.* High performance loop closure detection using bag of word pairs // Robotics and Autonomous Systems. 2016. Vol. 77. P. 55–65.

Lowe 2004 – *Lowe D.G.* Distinctive Image Features from Scale-Invariant Keypoints // International Journal of Computer Vision. 2004. Vol. 60, no. 2. P. 91–110.

Lucey 2016 – *Lucey S.* Direct Visual SLAM. Designing Computer Vision Apps (2016) [Электронный ресурс]. URL: http://16623.courses.cs.cmu.edu/slides/Lecture_19.pdf (дата обращения 20 декабря 2021).

Lychkov, Alfimtsev, Sakulin 2018 – *Lychkov I.I., Alfimtsev A.N., Sakulin S.A.* Tracking of Moving Objects with Regeneration of Object Feature Points // Proceedings of the 2018 Global Smart Industry Conference, GloSIC 2018, 13–15 Nov. 2018, Chelyabinsk, Russia. New York, NY: IEEE, 2018.

Mur-Artal, Montiel, Tardós 2015 – *Mur-Artal R., Montiel J.M.M., Tardós J.D.* ORB-SLAM: A Versatile and Accurate Monocular SLAM System // IEEE Transactions on Robotics. 2015. Vol. 31, no. 5. P. 1147–1163.

Scaramuzza 2016 – *Scaramuzza D.* Visual Odometry and SLAM: past, present, and the robust-perception age. Zurich: University of Zurich; Robotics and Perception Group, 2016.

Strasdat, Davison, Montiel, Konolige 2011 – *Strasdat H., Davison A.J., Montiel J.M.M., Konolige K* Double Window Optimisation for Constant Time Visual SLAM [Электронный ресурс] // Proceedings of the 2011 IEEE International Conference on Computer Vision Workshops (ICCV Workshops), 6–13 Nov. 2011, Barcelona, Spain. New York, NY: IEEE, 2011.

Tu, Huang, Zhang, Yu, Xu, Chen 2015 – *Tu Y., Huang Z., Zhang X., Yu W., Xu Y., Chen B.* The mobile robot SLAM based on depth and visual sensing in structured environment // Robot Intelligence Technology and Applications. 2015. Vol. 3. P. 343–357.

Valigi 2016 – *Valigi N.* Simple bag-of-words loop closure for visual SLAM (2016) [Электронный ресурс]. URL: https://nicolovaligi.com/bag-of-words-loop-closure-visual-slam.html (дата обращения 20 декабря 2021).

Yang, Wang, Gao, Cremers 2018 – *Yang N., Wang R., Gao X., Cremers D.* Challenges in Monocular Visual Odometry: Photometric Calibration, Motion Bias and Rolling Shutter Effect // IEEE Robotics and Automation Letters (RA-L). 2018. Vol. 3, no. 4. P. 2878–2885.

Zhuravlev, Razevig, Chizh., Bugaev 2016 – *Zhuravlev A.V. Razevig V.V., Chizh M.A., Bugaev A.S.* On the use of augmented reality devices for subsurface radar imaging // 2016 Progress in Electromagnetic Research Symposium (PIERS 2016), 8–11 August, Shanghai, China. New York, NY: IEEE, 2016. P. 2132–2136.

References

Akinin, M.V., Nikiforov, M.B. and Taganov, A.I. (2016), *Neirosetevye sistemy iskusstvennogo intellekta v zadachah obrabotki izobrazhenii* [Artificial Intelegence and Neural Networks in Computer Vision Tasks], Goryachaya liniya-Telecom, Moscow, Russia.

Belov, A.A. and Andrianova, O.G. (2017), "Robust anisotropy-based control of linear discrete-time descriptor systems with norm-bounded uncertainties", *IFAC-Papers On Line*, vol. 50, Issue 1, pp. 15471–15476.

Bergmann, P., Wang, R. and Cremers, D. (2018), "Online Photometric Calibration of Auto Exposure Video for Realtime Visual Odometry and SLAM", *IEEE Robotics and Automation Letters (RA-L)*, vol. 3, no. 2, pp. 627–634.

Engel, J., Koltun, V. and Cremers, D. (2016), "Direct Sparse Odometry", [Online], available at: URL: https://arxiv.org/pdf/1607.02565.pdf (Accessed 21 December 2021).

Engel, J., Koltun, V. and Cremers, D. (2018), "Direct Sparse Odometry", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 3, pp. 611–625.

Engel, J., Schöps, T. and Cremers, D. (2014), "LSD-SLAM: Large-Scale Direct Monocular SLAM", *Proceedings of the 13th European Conference Computer Vision – ECCV 2014, Zurich, Switzerland, September 6–12, 2014*, Springer, Berlin, Germany, pp. 834–849.

Gao, X.S., Hou, X.R., Tang, J. and Cheng, H.F. (2003), "Complete solution classification for the perspective-three-point problem", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25. no. 8, pp. 930–943.

Gálvez-López, D. and Tardós, J.D. (2012), "Bags of Binary Words for Fast Place Recognition in Image Sequences", *IEEE Transactions on Robotics*, vol. 28, no. 5, pp. 1188–1197.

Garcia-Fidalgoa, E. and Ortiza, A. (2014), "Vision-based topological mapping and localization methods: A survey", *Robotics and Autonomous Systems*, vol. 64, pp. 1–20.

Geng, K.K. and Chulin, N.A. (2017), "UAV Navigation Algorithm Based on Improved Algorithm of Simultaneous Localization and Mapping with Adaptive Local Range of Observations", *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, no. 3, pp. 76–94.

Haynsworth, E.V. (1968), "On the Schur Complement, Basel Mathematical Notes", *Basel Mathematical Notes. (BMN)*, vol. 20, pp. 1–17.

Insarov, V.V., Tikhonova, S.V. and Rankova, A.V. (2016), "Object Recognition Algorithms to Be Used in the UAV Technical Vision Systems to Recognize Objects on Images of Ground Scenes", *Herald of computer and information technologies*, no. 11, pp. 25–32.

Kejriwal, N., Kumar, S. and Shibata, T. (2016), "High performance loop closure detection using bag of word pairs", *Robotics and Autonomous Systems*, vol. 77, pp. 55–65.

Lowe, D.G. (2004), "Distinctive Image Features from Scale-Invariant Keypoints", *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110.

Lucey, S. (2016), "Direct Visual SLAM. Designing Computer Vision Apps", [Online], available at: http://16623.courses.cs.cmu.edu/slides/Lecture_19.pdf (Accessed 20 December 2021).

Lychkov, I.I., Alfimtsev, A.N. and Sakulin, S.A. (2018), "Tracking of Moving Objects with Regeneration of Object Feature Points", *Proceedings of the 2018 Global Smart Industry Conference, GloSIC 2018, 13–15 Nov. 2018, Chelyabinsk, Russia*, IEEE, New York, NY, USA, 2018.

Mur-Artal, R., Montiel, J.M.M. and Tardós J.D. (2015), "ORB-SLAM: A Versatile and Accurate Monocular SLAM System", *IEEE Transactions on Robotics*, vol. 31, no. 5, pp. 1147–1163.

Myasnikov, V.V. (2012), "Model-Based Gradient Field Descriptor as a Convenient Tool for the Image Recognition and Analysis", *Computer Optics,* vol. 36, issue 4, pp. 596–604.

Pelevin, E.E. and Balyasny, S.V. (2017), "The Usage of Adaptive Threshold Method in the System of Computer Vision", Juvenisscientia, Technical Science, no. 1, pp. 4–7.

Scaramuzza, D. (2016), Visual Odometry and SLAM: past, present, and the robust-perception age, University of Zurich, Robotics and Perception Group, Zurich, Switzerland.

Strasdat, H., Davison, A.J., Montiel, J.M.M. and Konolige, K. (2011), "Double Window Optimisation for Constant Time Visual SLAM", *Proceedings of the 2011 IEEE International Conference on Computer Vision Workshops (ICCV Workshops), 6–13 Nov. 2011, Barcelona, Spain*, IEEE, New York, NY, USA, 2011.

Strelkova, A.N., Trufanov, M.I. and Titov, D.I. (2019), "Sposob kalibrovki distorsii optiko-elektronnogo ustroistva" [Method for calibrating the distortion of an optoelectronic device], [Online], available at: http://www.findpatent.ru/patent/232/2321888.html (Accessed 21 May 2019).

Suprun, D.E. (2016), "Image-Matching Algorithm using Key Points with Scalability and Rotation of Objects", *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, no. 5, pp. 86–98.

Tu, Y., Huang, Z., Zhang, X., Yu, W., Xu, Y. and Chen, B. (2015), "The mobile robot SLAM based on depth and visual sensing in structured environment", *Robot Intelligence Technology and Applications 3*, pp. 343–357.

Valigi, N. (2016), Simple bag-of-words loop closure for visual SLAM, [Online], available at: https://nicolovaligi.com/bag-of-words-loop-closure-visual-slam.html (Accessed 21 December 2021).

Yang, N., Wang, R., Gao, X. and Cremers, D. (2018), "Challenges in Monocular Visual Odometry: Photometric Calibration, Motion Bias and Rolling Shutter Effect", *IEEE Robotics and Automation Letters (RA-L)*, vol. 3, no. 4, pp. 2878–2885.

Zhuravlev, A.V., Razevig, V.V., Chizh, M.A. and Bugaev, A.S. (2016), "On the use of augmented reality devices for subsurface radar imaging", *2016 Progress in Electromagnetic Research Symposium (PIERS 2016), 8–11 August, Shanghai, China,* IEEE, New York, NY, USA, pp. 2132–2136.

Zubov, N.E., Lapin, A.V. and Mikrin, E.A. (2013), "Using quaternions in spacecraft orientation modal control", *Inzhenerny zhurnal: nauka i innovacii*, issue 10, pp. 1–14.

Информация об авторах

Тамара М. Волосатова, кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, tamarav@bmstu.ru

Галина С. Зубова, магистрант, МГТУ им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, galya.zubova@mail.ru

Светлана Ю. Князева, старший преподаватель, МГТУ им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, knyazeva@bmstu.ru

Михаил В. Филиппов, кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, Россия; 105005, Россия, Москва, 2-я Бауманская ул., д. 5, filippov.mike@mail.ru

Information about the authors

Tamara M. Volosatova, Cand. of Sci. (Optical Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; tamarav@bmstu.ru

Galina S. Zubova, graduate student, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; galya.zubova@mail.ru

Svetlana Yu. Knyazeva, senior lecturer, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; knyazeva@bmstu.ru

Mikhail V. Filippov, Cand. of Sci. (Computer Engineering), associate professor, Bauman Moscow State Technical University, Moscow, Russia; bld. 5, 2nd Baumanskaya Str., Moscow, Russia, 105005; filippov.mike@mail.ru

УДК 004.05
DOI: 10.28995/2686-679X-2021-4-30-46

Технология блокчейн: начало, настоящее, будущее

Валерий В. Арутюнов
Российский государственный гуманитарный университет, Москва, Россия, warut698@yandex.ru

Ирина Ю. Авралева
Российский государственный гуманитарный университет, Москва, Россия, avralyova@gmail.com

Аннотация. В начале второго десятилетия XXI в. в мире появилась новая, еще не получившая широкого распространения в России технология блокчейн. В работе рассматривается история ее возникновения, этапы реализации, современное состояние и перспективы развития; приводятся примеры реализации технологии в мире и в различных сферах экономики России, включая запуск цифровой платформы обмена знаниями и управления авторскими правами Минобрнауки России, успешную реализацию технологии блокчейн в Москве и в ряде регионов страны при электронном дистанционном голосовании во время выборов депутатов Государственной Думы 8-го созыва в сентябре 2021 г. и др. Анализируется положительная динамика роста публикационной активности и цитируемости российских исследователей в этой области знаний в 2015–2020 гг. На основе наукометрических показателей выявлены (с использованием системы РИНЦ) перспективные направления исследований российских ученых в данной предметной области; в их числе правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву; блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы; подходы в международном регулировании криптовалют в отдельных иностранных юрисдикциях; криптовалюта и блокчейн-технология в цифровой экономике: генезис развития; блокчейн как технология изменения существующих бизнес-моделей. В заключение выделяются основные проблемы, замедляющие в наши дни активное внедрение технологии блокчейн в России, в число которых входят отсутствие соответствующей полноценной правовой базы в этой области; отсутствие единого арбитра, которому бы доверяли все пользователи технологии, и др.

Ключевые слова: публикационная активность, технология блокчейн, информационная безопасность, перспективные направления исследований, цитируемость, криптовалюта

Для цитирования: Арутюнов В.В., Авралева И.Ю. Технология блокчейн: начало, настоящее, будущее // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 30–46. DOI: 10.28995/2686-679X-2021-4-30-46

Blockchain technology. The beginning, the present, the future

Valery V. Arutyunov
Russian State University for the Humanities, Moscow, Russia, warut698@yandex.ru

Irina Yu. Avraleva
Russian State University for the Humanities, Moscow, Russia, avralyova@gmail.com

Abstract. Since the beginning of the second decade of the 21st century, a new blockchain technology (which has not yet been widely used in Russia) has appeared in the world. The paper considers the history of its origin, the stages of implementation, the current state and prospects of development; it gives examples of implementing the technology in the world and in various spheres of the Russian economy including the example of launching a digital platform for knowledge exchange and copyright management for the Ministry of Education and Science of Russia and that of the successful implementation of blockchain technology in Moscow and in a number of regions of the country with electronic remote voting during the elections of deputies to the State Duma of the 8th convocation in September 2021, etc. The article also analyzes the positive dynamics of the growth in publication activity and citation of Russian researchers in this field of knowledge in 2015–2020. Based on scientometric indicators and using the RSCI system the authors identified promising areas of research for Russian scientists in this subject area among them are legal aspects of the use of smart contracts and blockchain technologies under Russian law; blockchain as a communication basis for the formation of the digital economy: advantages and challenges; approaches to international regulation of cryptocurrencies in certain foreign jurisdictions; cryptocurrency and blockchain technology in the digital economy: the genesis of development; blockchain as a technology for changing existing business models. In conclusion, the paper highlights the main issues that at present slow down the active introduction of blockchain

technology in Russia among them an issue of the lack of an appropriate full-fledged legal framework in this area; the lack of a single arbitrator who would be trusted by all users of the technology, etc.

Keywords: publication activity, blockchain technology, information security, promising areas of research, citation, cryptocurrency

For citation: Arutyunov, V.V. and Avraleva, I.Yu. (2021), "Blockchain technology. The beginning, the present, the future", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 30–46, DOI: 10.28995/2686-679X-2021-4-30-46

Введение

С конца XX в. вопросы защиты информации в информационных системах (ИС) и информационно-телекоммуникационных сетях (ИТС) становятся все более актуальными для российских организаций и коммерческих компаний, когда руководство большинства из них начало приходить к осознанию того факта, что информационные ресурсы организации являются одним из важнейших объектов экономической инфраструктуры, которые необходимо защищать различными методами и средствами от внешних и внутренних злоумышленников. Стало очевидным, что обеспечение информационной безопасности (ИБ) объектов защиты, обладающих значимой для организации ценностью, является серьезной и достаточно сложной задачей, которая требует привлечения комплекса различных ресурсов (людских, программно-технических, организационных и др.) с целью построения необходимой *комплексной системы защиты информации* для функционирующих ИС и ИТС. Это привело в начале XXI в. к развитию ряда направлений в области защиты информации.

В области обеспечения ИБ в последнем десятилетии текущего столетия можно выделить следующие актуальные направления исследований:

- технология блокчейн;
- биометрические методы и средства защиты информации;
- использование облачных технологий при реализации механизмов безопасности;
- применение методов искусственного интеллекта для обеспечения ИБ;
- системы обнаружения и предотвращения вторжений в ИС и ИТС;
- использование технологии Big Data для обеспечения ИБ;

– системы предотвращения утечки информации (DLP-системы);
– современные механизмы обеспечения защиты информации в мобильных системах связи;
– криптографические методы защиты информации (включая квантовую криптографию);
– стеганографические методы защиты информации, обеспечивающие сокрытие самого факта передачи информации, камуфлирование программных модулей и активную защиту определенных видов интеллектуальной собственности;
– кибербуллинг (намеренные агрессивные действия злоумышленника с целью нанесения как минимум психологического вреда человеку, осуществляемые с использованием мобильной связи, различных сервисов Интернет, а также социальных сетей);
– применение методов обфускации для защиты программного обеспечения, в первую очередь предназначенного для защиты ИС и ИТС;
– безопасность Интернета вещей (Internet of Things, IoT).

Блокчейн – это относительно новая технология, которая у многих ассоциируется в основном с криптовалютами. В наши дни, однако, область применения технологии блокчейн далеко не ограничивается только финансовой сферой. Во многих передовых странах мира, активно использующих сервисы Интернет, в наши дни разрабатываются на основе анализируемой в данной работе технологии различные приложения, например, онлайновые системы для голосования, системы для контроля цепочек поставок и др.

При реализации технологии блокчейн каждой совершаемой транзакции (операции) позиционируется соответствующий блок информации. Этот блок содержит ссылку на предыдущий блок, метку времени, сведения об участниках и условиях проведения операции и др.

Копии формируемых цепочек блоков хранятся независимо друг от друга в распределенной базе данных. Для обеспечения целостности базы данных и конфиденциальности информации, хранящейся в ней, используются соответствующие средства криптографической защиты информации, например, средства контроля хеш-функций записей [Лелу 2018].

Существует три основных принципа функционирования блокчейн-технологии:
– защищенность;
– распределенность;
– открытость.

Условие, при котором невозможно подделать записи, не показав факт их изменения, реализуется на основе принципа «защищенность». Основной его смысл следует из названия технологии – «цепочка блоков». Каждый вновь созданный блок содержит в себе набор записей информации о предыдущем блоке, которые зашифрованы, т. е. предыдущий блок связан с новым созданным блоком. При добавлении нового блока он встает строго в конце цепи. При этом в новом блоке уже формируется хеш-функция о предыдущем блоке. В том случае, когда в одном из имеющихся блоков произойдет изменение, его хеш изменится, а следовательно, и в последующих блоках после этого произойдет изменение. Таким образом, достигается реализация принципа «защищенность».

Реализация принципа «распределенность» достигается за счет того, что в процессе осуществления технологии блокчейн обычно участвуют несколько человек одновременно; при этом копия записи определенного действия выдается каждому участнику.

На рис. 1 показан процесс формирования цепочки блоков записи. В верхней части блока располагается хеш предыдущего блока, а под ним – информация о текущем блоке. При переходе к следующему блоку происходит формирование хеша, который затем записывается в верхнюю ячейку блока.

Рис. 1. Формирование цепочки блоков

Принцип «открытость» основан на прозрачности системы. Всегда можно увидеть, например, на какой адрес поступила цифровая валюта и с какого адреса она была отправлена [Киреев, Васильев, Поклонский 2018].

Блокчейн: начало

Идея формирования электронной валюты с использованием технологии блокчейн была описана С. Брэндсом и Д. Чаумом еще в 1983 г.

Однако только в 1997 г. А. Баков внес существенный вклад в формирование концепции цифровых валют. Именно его предложение об использовании системы Hashcash должно было помочь справиться с DoS-атаками и противодействовать отправке спама. В последующем именно эта система была принята за основу при создании блоков в блокчейне; она дала возможность работать с первой криптовалютой в мире.

В 1998 г. была успешно создана первая реализованная цифровая валюта Вэй Дай, которая получила название b-money. Следующая попытка произошла только в 2000 г., когда разработанная Н. Сабом валюта получила название Bit Gold. Обе эти валюты имели один большой недостаток: отмечалось несовершенство системы в принятии решения среди удаленных абонентов.

Далее 1 ноября 2008 г. вышла анонимная статья с названием “Bitcoin: A Peer-to-Peer Electronic Cash System” под псевдонимом Сатоши Накамото [Кернякевич, Чегодаев 2018]. В ней были приведены все теоретические основы создания электронной валюты нового поколения, которая отличалась децентрализованностью, прозрачностью, а также независимостью от Центробанков и регуляторов. Но широкое распространение в первые месяцы она не получила, хотя была обсуждена в широких кругах криптографов, математиков и программистов.

Первое в мире воплощение концепции, описанной в этой статье, было реализовано 3 января 2009 г. на примере валюты Bitcoin (BTC), которая с тех пор уже более 10 лет функционирует в мире.

В 2010 г. Сатоши Накамото отходит от разработки Bitcoin, так и не раскрыв свою личность. А первая в мире транзакция в блокчейне была проведена Сатоши на сумму 10 BTC, когда он отправил ее известному криптографу Гарольду (Хэлу) Финни [Табернакулов 2019].

Блокчейн сегодня

В наши дни при реализации технологии блокчейн формируется в электронном виде значительное число таблиц, которые объединяются в единую базу. Это уникальный инструмент, созданный для создания различных баз данных.

На рис. 2 представлены основные этапы реализации технологии блокчейн.

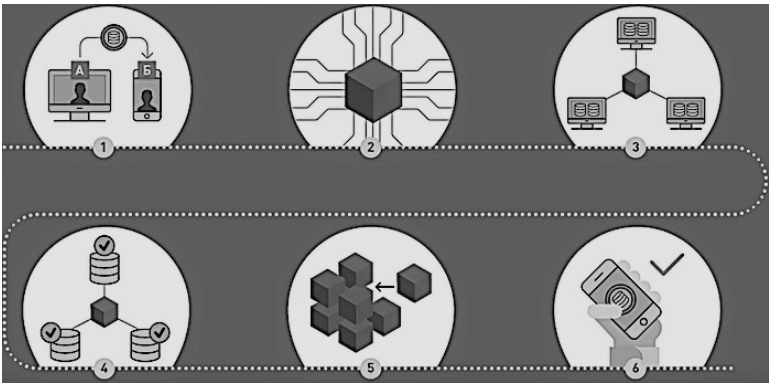

Рис. 2. Основные этапы реализации технологии блокчейн

Когда отправитель А посылает информацию для Б, то его транзакция поступает в сеть в виде блока. Блок распределяется по всей сети блокчейн. Далее участники сети подтверждают сделку; создается новый блок записи о транзакции, который встраивается в сеть, где будет храниться информация об этой записи и всех предыдущих транзакциях; затем информация поступает к Б [Tapscott, Tapscott 2016].

В настоящее время интерес к технологии блокчейн проявляют компании и организации из самых различных сфер экономики и науки [Кузьменко 2018]. В банковском секторе такой интерес проявляют *Visa, Mastercard, Unionpay,* «ВТБ», «Сбербанк». «Альфа-банк» ввел в эксплуатацию блокчейн-платформу автоматизации торговых операций с агентами на базе платформы для создания децентрализованных онлайн-сервисов по технологии блокчейн, работающих на основе «умных» контрактов [Цицкиев 2018].

Блокчейн также способствует решению ряда вопросов, связанных с земельным реестром. Например, в Индии с помощью технологии блокчейн борются с земельным мошенничеством, а Объединённые Арабские Эмираты и Швеция планируют вести земельный реестр с использованием блокчейна.

В настоящее время технология блокчейн начинает активно использоваться системах, удостоверяющих личность. В 2017 г. *Microsoft и Accenture* представили систему цифровых удостоверений личности, основанную на использовании технологии блокчейн [Рязанова 2018].

В Финляндии с помощью блокчейн идентифицируют прибывающих в страну беженцев, а в Эстонии уже не первый год функ-

ционирует блокчейн-система для формирования электронного гражданства.

Правительство Бразилии в 2017 г. начало тестирование системы удостоверений личности с применением блокчейн.

В настоящее время ряд крупных мировых компаний использует блокчейн при управлении распределенной системой с целью распознавания партнеров, работников или пользователей [Мещеряков, Бондарь 2016].

Технология блокчейн также начинает активно применяться при электронном голосовании в регионах, где функционирует сеть Интернет [Зорин, Зорина 2018]. При этом данные о голосах граждан и их подсчете надежно защищаются [Сидоров, Камаева 2019].

Блокчейн в России

К концу второго десятилетия XXI в. в России отмечается все более возрастающий интерес к технологии блокчейн. В стране с использованием этой технологии начинают формироваться различные открытые распределенные реестры, в которых хранится информация о транзакциях, совершаемых торговых сделках, обязательствах и правах и др. Защита вышеназванных реестров при этом обеспечивается специальными подсистемами обеспечения безопасности цифровых платформ [Салабутин, Бабко 2018].

Как отмечается в работе [Шустров 2018], при активном внедрении технологии блокчейн будет возможно увеличить эффективность функционирования многих секторов экономики, а также поддержать развитие малого и среднего бизнеса.

В 2018 г. на Всемирном саммите блокчейна и криптовалют Росреестр (Федеральная служба государственной регистрации, кадастра и картографии) представил Проект по регистрации договоров участия в долевом строительстве с применением технологии блокчейн.

Росреестр в 2018 г. в рамках совместного проекта с Внешэкономбанком зарегистрировал первый договор участия в долевом строительстве в Ленинградской области с применением технологии блокчейн [Петренко, Петренко 2019].

В 2018 г. Государственный комитет Татарстана по архивному делу представил результаты реализации проекта с использованием технологии блокчейн для сохранения архивных документов.

Еще одним примером является запуск цифровой платформы обмена знаниями и управления авторскими правами Министерства образования и науки РФ, реализуемый на основе технологии

блокчейн [Конев, Каминская 2018]. В проекте принимают участие 11 ведущих университетов страны, включая Санкт-Петербургский государственный университет (СПбГУ), Санкт-Петербургский политехнический университет Петра Великого, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (ИТМО), Национальный исследовательский университет «Высшая школа экономики», Российскую академию народного хозяйства и государственной службы при Президенте РФ (РАНХиГС), Сибирский федеральный университет и др.

Для того чтобы повысить в России эффективность функционирования финансовых систем, крупными банками страны вместе с Центральным Банком России была создана платформа «Мастерчейн» [Волконская 2017]. Хотя «Мастерчейн» предназначена для обслуживания прежде всего банковских бизнес-процессов, основным итогом использования этой сети должно стать создание инфраструктуры, которая будет способствовать эффективному взаимодействию финансовых организаций.

На конец 2021 г. одним из примеров успешной реализации технологии блокчейн в России является проект «Активный гражданин», действующий в Москве. С его помощью учитываются на основе голосования мнения граждан, касающиеся улучшения жизни москвичей в столице.

Другим примером использования технологии блокчейн в этом году является успешная реализация в Москве и в ряде регионов России электронного дистанционного голосования при выборе депутатов Государственной Думы 8-го созыва в сентябре 2021 г.

В связи с изложенным несомненный интерес представляет публикационная активность российских исследователей в области технологии блокчейн, отражающая в определенной мере результаты работ в анализируемой предметной области.

Следует отметить, что в литературе в наши дни представлен широкий спектр источников для анализа публикаций в различных отраслях экономики, на основе которых выявляются различные закономерности публикационной активности и востребованности итогов исследований ([Арутюнов 2006], [Арутюнов, Константинов 2006], [Arutyunov 2016], [Маршакова-Шайкевич 2008] и др.) с помощью количественных наукометрических показателей результативности работ исследователей и организаций на основе их публикационной активности P, цитируемости C и индекса Хирша H. Эти наукометрические показатели в России с начала второго десятилетия XXI в. учитываются в качестве основных показателей, определяющих наряду с другими эффективность функционирования научных организаций и высших учебных заведений страны.

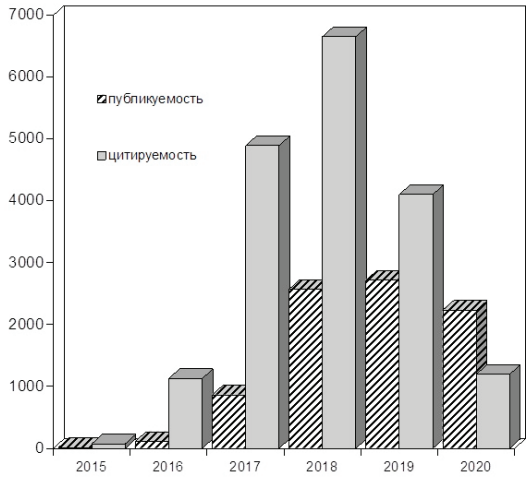

Рис. 3. Динамика публикационной активности
и цитируемости российских ученых в 2015–2020 гг.
в области технологии блокчейн

На рис. 3 представлены динамика публикационной активности в 2015–2020 гг. (определяемая ежегодным числом публикаций *P* в этой области знаний) российских ученых и их цитируемость *C*, отражаемые в базах РИНЦ (Российском индексе научного цитирования) [РИНЦ 2021].

При этом надо отметить, что современный инструментарий для работы с базами РИНЦ, включающий развитой поисковый аппарат, позволяет на основе наукометрических показателей (публикационной активности, цитируемости и ряда др.) определять не только организации-лидеры в создании высоковостребованной научно-технической продукции в той или иной отрасли наук, но и конкретных ученых, создающих эту продукцию, а также те организации, которые активно востребуют данную научно-техническую продукцию.

Как следует из рис. 3, число публикаций в рассматриваемой сфере знаний ежегодно непрерывно росло за последние пять лет, стабилизировавшись в 2018–2020 гг. на отметке, превышающей возросший уровень публикаций 2017 г. практически в три раза.

Что касается показателя цитируемости соответствующих публикаций, который в определенной мере отражает востребованность научного сообщества результатов работ в этой сфере исследований,

то после значительного роста в 2016–2017 гг. и достижения максимума в 2018 г. он начинает уменьшаться.

Невысокое значение в 2020 г. показателя цитирования в сфере технологии блокчейн объясняется, как и для других отраслей естественных наук, известной закономерностью: замедленной реакцией («откликом») научного сообщества на публикации текущего года.

По итогам настоящей работы также удалось выявить с использованием наукометрических показателей РИНЦ перспективные направления исследований российских ученых в рассматриваемой области знаний.

В их числе выделяются следующие основные направления: правовые аспекты использования смарт-контрактов и технологий блокчейн по российскому праву; блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы; подходы в международном регулировании криптовалют в отдельных иностранных юрисдикциях; криптовалюта и блокчейн-технология в цифровой экономике: генезис развития; блокчейн как технология изменения существующих бизнес-моделей.

Необходимо также отметить, что индекс Хирша в области технологии блокчейн, определенный для множества публикаций российских ученых за период 2015–2020 гг. и равный 46 для этой области знаний, практически в три раза превышает минимальный порог мирового уровня научной активности исследователей, равный 16 в соответствии с имеющимися рекомендациями [Ершова 2020].

Этот факт, свидетельствующий о высоком уровне научной активности российских исследователей в области технологии блокчейн, подтверждает также, что и в последующие годы в анализируемой области знаний следует ожидать стабильную высокую публикационную активность российских ученых по результатам их исследований.

Заключение

Стремительное развитие современных технологий, в том числе блокчейн, и их успешная реализация может привести в недалеком будущем к изменению структуры рынка труда, значительному сокращению количества рабочих мест в ряде отраслей экономики и созданию большого числа новых рабочих мест. При этом одной из важных задач государственных организаций и коммерческих компаний в это время будет не только внедрение новых технологий,

включая блокчейн, но и предоставление помощи своим сотрудникам в освоении новых компетенций, быстром наращивании их квалификации для скорейшей адаптации этих новых технологий.

В настоящее время многие эксперты и исследователи из различных стран и сфер экономики приходят к выводу о том, что в наши дни в мире имеется множество потенциальных возможностей применения технологии блокчейн (например, в таких отраслях, как страхование, торговое финансирование, цифровое право, отслеживание активов, патентные заявки и др.).

Большие возможности развития технология блокчейн имеет и в розничной торговле (эта технология, например, уже применяется известной американской сетью Walmart).

Блокчейн возможно также применять в сфере закупок импортного товара. С его помощью контролируется весь маршрут продукта от поставщика до поступления его в супермаркет. При этом можно всегда узнать срок годности этого продукта, требования к условиям хранения и перевозки и т. п., так как эти данные заложены в системе [Валеева, Шипкова 2018].

Технология блокчейн обеспечивает прозрачность и безопасность финансовых потоков компании, а также может облегчить работодателям поиск специалистов с конкретными навыками [Киреев, Васильев, Поклонский 2018].

Блокчейн также позволяет оптимизировать и способ голосования; например, с его применением возможно создать электронную базу для дистанционно голосующих граждан, на основе которой будет намного удобнее подсчитывать итоги голосования. При этом итоги подсчета результатов голосования при использовании технологии блокчейн, как утверждают эксперты, являются более достоверными, чем те, которые будут определены при использовании бумажных бюллетеней, так как принципы функционирования технологии блокчейн практически исключает возможность фальсификации выборов.

Ожидается, что широкое использование технологии блокчейн (при соответствующем государственном регулировании и обеспечении информационной безопасности) практически исключит возможность реализации различного рода нелегальных сделок, особенно в сфере государственных закупок, а также будет способствовать началу выхода из «серой зоны» теневого бизнеса [Силанова 2018].

Исходя из вышесказанного, можно сделать вывод, что к концу второго десятилетия XXI в. в России начала формироваться специализированная децентрализованная система, которая включает неправительственные организации и ассоциации, коммерческие

компании, банковский сектор и в которой реализуются исследования и разработки, связанные с применением технологии блокчейн.

Несмотря на свою новизну и сложности, связанные с ее широким распространением, с помощью технологии блокчейн могут быть переосмыслены подходы к реализации многих бизнес-процессов в экономике и тем самым внесен значительный вклад в развитие цифровой экономики.

При этом необходимо отметить, что периметр использования блокчейна ограничивается лишь профессионализмом и изобретательностью квалифицированных специалистов, которые могут создавать на его основе новые продукты и сервисы. Весьма вероятно, что уже в ближайшем будущем применение технологии блокчейн станет достаточно повседневным явлением (например, при продвижении созданных сервисов или продуктов на рынок), к которому пользователи будет относиться как к чему-то вполне обыденному.

В числе основных проблем, которые в настоящее время в определенной мере замедляют широкое применение технологии блокчейн в России, следует отметить необходимость создания нормативно-правовой базы для использования блокчейн в различных отраслях экономики; отсутствие единого арбитра, которому бы доверяли все пользователи, использующие блокчейн, а также недостаточное правовое регулирование различных подходов к защите информации, применяемых при реализации технологии блокчейн.

Литература

Арутюнов 2006 – *Арутюнов В.В.* Современные проблемы и задачи обеспечения информационной безопасности // Вестник Московского финансово-юридического университета. 2006. № 2. С. 213–222.

Арутюнов, Константинов 2006 – *Арутюнов В.В., Константинов А.С.* Рейтинговый анализ востребованной геологической научно-технической продукции на рубеже XX–XXI веков // Научно-техническая информация. Сер. 1: Организация и методика информационной работы. 2006. № 12. С. 14–19.

Валеева, Шипкова 2018 – *Валеева А.Р., Шипкова Е.А.* Технология блокчейн и ее применение // Научное сообщество студентов: междисциплинарные исследования. Новосибирск: Ассоциация научных сотрудников «Сибирская академическая книга», 2018. С. 119–122.

Волконская 2017 – *Волконская Е.* Блокчейн – что это понятным языком [Электронный ресурс] // Bestinvestpro. URL: http://bestinvestpro.com/blokchejn-chto-eto-ponyatnym-yazykom/#i-11 (дата обращения 15 апреля 2021).

Ершова 2020 – *Ершова С.К.* Инструкция по использованию РИНЦ [Электронный ресурс]. URL: https://rf-gk.ru/profil-avtora-v-rinc-funkcionalnye-vozmozhnosti-rossiiskii/ (дата обращения 15 апреля 2021).

Зорин, Зорина 2018 – *Зорин А. Л., Зорина Н. В.* Применение технологии блокчейн в системе голосования в России // Точная наука. 2018. № 26. С. 104–106.

Кернякевич, Чегодаев 2018 – *Кернякевич П.С., Чегодаев И.В.* Технология блокчейн и ее применение // Вестник современных исследований. 2018. № 5.4 (20). С. 183–185.

Киреев, Васильев, Поклонский 2018 – *Киреев В.С., Васильев М.М., Поклонский А.Ю.* Анализ технологии «блокчейн». Перспективы и области применения // Аллея Науки. 2018. № 5. С. 1–10.

Конев, Каминская 2018 – *Конев А.М., Каминская А.А.* Перспективные направления использования блокчейн-технологий в сфере образования // Вестник современных исследований. 2018. № 6.2 (21). С. 164–165.

Кузьменко 2018 – *Кузьменко Е.К.* Технология блокчейн для банков: перспективы применения в сфере финансового контроля // Проблемы конфигурации глобальной экономики XXI века: идея социально-экономического прогресса и возможные интерпретации. Краснодар: Научно-исследовательский институт экономики Южного федерального округа, 2018. С. 378–382.

Лелу 2018 – *Лелу Л.* Блокчейн от А до Я. Все о технологии десятилетия. М.: Эксмо, 2018.

Маршакова-Шайкевич 2008 – *Маршакова-Шайкевич И.В.* Россия в мировой науке. М.: ИФРАН, 2008.

Мещеряков, Бондарь 2016 – *Мещеряков В.А., Бондарь А.О.* Перспективы применения технологии блокчейн в информационной безопасности и цифровой криминалистике // Охрана, безопасность, связь. 2016. № 1. С. 12–17.

Петренко, Петренко 2019 – *Петренко С.А, Петренко А.С.* Практика применения технологии блокчейн // Материалы II Всероссийской научно-практической конференции. Посвящается 75-летию Гуманитарно-педагогической академии (филиал) ФГАОУ ВО «КФУ им. В.И. Вернадского», 14–15 марта 2019 г., Ялта, Республика Крым, Россия. Симферополь: ООО «Ариал», 2019. С. 330–335.

РИНЦ 2021 – РИНЦ: Российский индекс научного цитирования [Электронный ресурс]. URL: https://elibrary.ru/querybox.asp?scope=newquery (дата обращения 20 сентября 2021).

Рязанова 2018 – *Рязанова А.А.* Технология блокчейн в научно-информационной деятельности // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2018. № 4. С. 8–12.

Салабутин, Бабко 2018 – *Салабутин А.В., Бабко А.Н.* Блокчейн-технологии: перспективы развития в Российской Федерации // Аллея науки. 2018. № 5 (21). С. 554–561.

Сидоров, Камаева 2019 – *Сидоров Д.П., Камаева А.А.* Технология блокчейн и возможности ее применения в учебном процессе // Образовательные технологии и общество. 2019. № 3. С. 94–101.

Силанова 2018 – *Силанова А.С.* О внедрении информационной технологии «блокчейн» в документооборот правоохранительных органов // Теоретические аспекты юриспруденции и вопросы правоприменения. М.: Интернаука, 2018. С. 155–158.

Табернакулов 2019 – *Табернакулов А.* Блокчейн на практике. М.: Альпина Паблишер, 2019.

Цицкиев 2018 – *Цицкиев М.М.* Применение технологии блокчейн в банковском секторе // E-SCIO. 2018. № 4 (19). С. 57–64.

Шустров 2018 – *Шустров Д.* Блокчейн в России [Электронный ресурс] // EX4.ru. URL: https://ex4.ru/blokchejn/blokchejn-v-rossii/ (дата обращения 21 апреля 2021).

Arutyunov 2016 – *Arutyunov V.V.* The results of priority research in the field of information security // Scientific and Technical Information Processing. 2016. Vol. 43, no. 1. pp. 42–46.

Tapscott D., Tapscott A. 2018 – *Tapscott D., Tapscott A.* Blockchain Revolution. New York, NY: Portfolio/Penguin, 2018.

References

Arutyunov, V.V. (2006), *"*Current issues and tasks of information security*", MFUA Bulletin*, vol. 2, pp. 213–222.

Arutyunov, V.V. (2016), "The results of priority research in the field of information security", *Scientific and Technical Information Processing*, vol. 43. № 1, pp. 42–46.

Arutyunov, V.V. and Konstantinov, AS. (2006), "Rating analysis of the demand for geological scientific and technical products of the 20th–21st centuries", *Scientific and technical information*, ser. 1, vol. 12, pp. 14–19.

Tsitskiev, M.M. (2018), "Application of blockchain technology in the banking sector", *E-SCIO*, vol. 4 (19), pp. 57–64.

Ershova, S.K. (2020), "Instructions for using the RSCI", [Online], available at: https://elibrary.ru/querybox.asp?scope=newquery (Accessed 15 April 2021).

Kernyakevich, P.S. and Chegodaev, I.V. (2018), "Blockchain technology and its application", *Vestnik sovremennykh issledovanii*, vol. 5.4 (20), pp. 183–185.

Kireev, V.S., Vasil'ev, M.M. and Poklonskii, A.Yu. (2018), "Blockchain Technology Analysis. Perspectives and Fields of Application", *Alley of Science*, vol. 5, pp. 1–10.

Konev, A.M. and Kaminskaya, A.A. (2018), "Promising uses of blockchain technologies in education", *Vestnik sovremennykh issledovanii*, vol. 6.2 (21), pp. 164–165.

Kuz'menko, E.K. (2018), "Blockchain technology for banks: Perspectives for Financial Supervision", *Issues of Global Economic Design in the 21st Century: The Idea of Economic and Social Progress and Possible Interpretations,* Nauchno-issledovatel'skii institut ekonomiki Yuzhnogo federal'nogo okruga, Krasnodar, Russia. pp. 378–382.

Lelu, L. (2018), "*Blokchejn ot A do Ya. Vse o tekhnologii desyatiletiya*" [Blockchain from A to Z. All about the technology of the decade], Eksmo, Moscow, Russia.

Marshakova-Shaykevich, I.V. (2008), *Rossiya v mirovoi nauke* [Russia in the world science], RAS, Institute of Philosophy, IFRAN, Moscow, Russia, 227 p.

Meshcheryakov, V.A. and Bondar', A.O. (2016), "Perspectives on the use of blockchain technology in information security and digital forensics", *Security, safety, communications*, vol. 1, pp. 12–17.

Petrenko, S.A. and Petrenko, A.S. (2019), "The practice of using blockchain technology", *Materials of the II All-Russian Scientific and Practical Conference. Dedicated to the 75th anniversary of the Humanitarian Pedagogical Academy (branch) Vernadsky CFU, March 14–15, 2019*, Yalta, Republic of Crimea, Russia, LLC "Arial", Simferopol, Republic of Crimea, Russia, pp. 330–335.

RSCI (2021), Russian Science Citation Index [Online], available at: https://elibrary.ru/querybox.asp?scope=newquery (Accessed 20 September 2021).

Ryazanova, A.A. (2018), "Blockchain technology in science and information", *Science and technology information. Series 1: Organization and methodology of information work*, vol. 4, pp. 8–12.

Salabutin, A.V. and Babko, A.N. (2018), "Blockchain technologies. Prospects for development in the Russian Federation", *Alley of Science*, vol. 5 (21), pp. 554–561.

Shustrov, D. (2018), "Blockchain in Russia", *EX4.ru*. [Online], URL: https://ex4.ru/blokchejn/blokchejn-v-rossii/ (Accessed 21 April 2021).

Sidorov, D.P. and Kamaeva, A.A. (2019), "Blockchain technology and its applications in education", *Educational technologies and society,* vol. 3, pp. 94–101.

Silanova, A.S. (2018), "Introduction of information technology "blockchain" in law enforcement documentation", *Teoreticheskie aspekty yurisprudentsii i voprosy pravoprimeneniya* [Theoretical aspects of jurisprudence and the law enforcement issues], Intern, Moscow, Russia, pp. 155–158.

Tabernakulov, A. (2019), *Blokchejn na praktike* [Blockchain in practice], Al'pina Publisher, Moscow, Russia.

Tapscott, D. and Tapscott A. (2018), *Blockchain Revolution*, Portfolio/Penguin, New York, NY, USA.

Valeeva, A.R. and Shipkova, E.A. (2018), "Blockchain technology and its applications", *Nauchnoe soobshchestvo studentov. mezhdistsiplinarnye issledovaniya* [Scientific Community of Students. Interdisciplinary Research], Assotsiatsiya nauchnykh sotrudnikov "Sibirskaya akademicheskaya kniga", Novosibirsk, Russia, pp. 119–122.

Volkonskaya, E. (2017), "Blockchain – that it's understandable", *Bestinvestpro*, [Online], available at: http://bestinvestpro.com/blokchejn-chto-eto-ponyatnym-yazykom/#i-11 (Accessed 15 April 2021).

Zorin, A.L. and Zorina, N.V. (2018), "Application of blockchain technology in the Russian voting system", *Exact science*, vol. 26, pp. 104–106.

Информация об авторах

Валерий В. Арутюнов, доктор технических наук, профессор, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; warut698@yandex.ru

Ирина Ю. Авралева, аспирант, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; pravjik@yandex.ru

Information about the authors

Valery V. Arutyunov, Dr. of Sci. (Computer Science), professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia 125047; warut698@yandex.ru

Irina Yu. Avraleva, postgraduate student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; pravjik@yandex.ru

УДК 003.26
DOI: 10.28995/2686-679X-2021-4-47-57

Криптография: от прошлого к будущему

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

Аннотация. Статья посвящена анализу современных тенденций развития криптографии, имеющих связь с проблемами криптографии прошлого и отражающихся на перспективах развития криптографии в будущем. Выделяются новые тенденции развития криптографии, актуальные в последние десятилетия, к основным из которых можно отнести: осознание математического характера задач шифрования данных, стремительное возрастание объемов обрабатываемой и шифруемой информации, которая распространяется среди неограниченного круга пользователей современных устройств передачи данных, практический и теоретический интерес к криптографии пользователей. Проводится анализ преемственности проблем, стоящих перед криптографией. Среди таких проблем важность человеческого фактора при использовании любых криптографических систем, традиционного участия государства в развитии криптографии, а также теоретического обоснования идей криптографической защиты данных, обобщающих практический опыт применения шифрования. Автор анализирует основные задачи криптографии, к которым относятся идентификация, аутентификация, сохранение целостности, конфиденциальности и доступности информации при ее передаче и хранении, подчеркивая необходимость их решения в рамках проектирования и реализации комплексных систем защиты. В статье на примере развития квантовой криптографии подчеркивается, что развитие новых подходов к криптографической защите данных традиционно приводит к появлению новых факторов уязвимости, а значит, традиционной проблемой криптографии также является работа на опережение потенциальных злоумышленников.

Ключевые слова: криптография, криптографическая защита информации, история криптографии, шифрование, квантовая криптография

Для цитирования: Русецкая И.А. Криптография: от прошлого к будущему // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 47–57. DOI: 10.28995/2686-679X-2021-4-47-57

Cryptography. From the past to the future

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

Abstract. The article is devoted to the analysis of modern trends in the development of cryptography, which are related to the issues of cryptography of the past and are reflected in the prospects for the development of cryptography in the future. New trends in the development of cryptography that are relevant in recent decades are highlighted, the main ones of which include: awareness of the mathematical nature of data encryption problems, the rapid increase in the volume of processed and encrypted information that is distributed among a large unlimited circle of users of the modern data transmission devices, practical and theoretical interest of users in cryptography. It analyzes the continuity of the issues facing cryptography. Among such issues there are: an importance of the human factor in the use of any cryptographic system, the traditional participation of the state in the cryptography development, as well as the theoretical substantiation of ideas of the cryptographic data protection, generalizing the practical experience of using encryption. The author also analyzes the main tasks of cryptography, which include identification, authentication, maintaining the integrity, confidentiality and availability of information during its transfer and storage, emphasizing the need to solve them within the framework of the design and implementation of the complex security systems. Using the development of quantum cryptography as an example, the article emphasizes that the development of new approaches to the cryptographic data protection traditionally leads to the emergence of new vulnerability factors, which means that the traditional issue of cryptography is also to stay ahead of potential attackers.

Keywords: cryptography, cryptographic information protection, history of cryptography, encryption, quantum cryptography

For citation: Rusetskaya, I.A. (2021), "Cryptography. From the past to the future", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 47–57, DOI: 10.28995/2686-679X-2021-4-47-57

Введение

Криптография, возникшая с появлением письменности, является древнейшим направлением обеспечения безопасности информации. На протяжении более 4000 лет и до настоящего времени криптография позволяет решать проблемы безопасной передачи секретных данных. Использование информационных технологий

будущего также нельзя представить без криптографических методов защиты данных.

Целью данной работы является анализ современных тенденций развития криптографии, имеющих связь с проблемами криптографии прошлого и отражающихся на перспективах развития криптографии в будущем.

Поскольку в рамках небольшой работы невозможно осветить все аспекты данной темы, в настоящей статье будут рассмотрены следующие вопросы:

- краткий анализ новых тенденций развития криптографии;
- развитие задач, стоящих перед криптографией в прошлом, настоящем и будущем;
- анализ преемственности проблем, стоящих перед криптографией в прошлом и будущем;
- анализ отдельных перспектив и проблем криптографии будущего, определенных ее историческим развитием.

Развитие основных тенденций криптографической защиты информации: ретроспективный взгляд и проблемы будущего

В настоящее время проблемы криптографической защиты информации занимают важнейшее место в рамках процессов обеспечения информационной безопасности. В последние десятилетия криптография активно развивалась и проявила новые тенденции, к которым, в частности, можно отнести следующие:

1. Осознание математического характера решаемых криптографией задач, цифровизация процесса обмена данными и широкое распространение компьютеров, приведшие к смене ручного шифрования на автоматизированное.

На протяжении разных исторических эпох криптография воспринималась с разных точек зрения: как искусство тайнописи для узкого круга посвященных, практическая помощь при организации секретной связи при личной переписке и ведении военных действий, как раздел натурфилософии и так называемой «естественной магии» [Русецкая 2014]. Криптографические алгоритмы изначально предполагали использование некоторых математических подходов, однако этот аспект на протяжении многих веков не акцентировался исследователями и практиками криптографии. Окончательно математический характер задач, стоящих перед криптографией, был признан после публикации в 1949 г. работы

Клода Шеннона «Теория связи в секретных системах», а к концу 1960-х гг. все шифровальные системы предполагают использование электронных устройств.

2. Возрастание объемов обработки информации, повсеместное распространение криптографии и получение представлений о ней среди широкого круга пользователей информации.

Использование криптографических алгоритмов входит в повседневную жизнь большинства жителей планеты, и, хотя не всеми прямо осознается, сегодня представления о криптографии избавлены от налета тайны, чему способствует поток научно-популярной литературы, посвященной этой теме. Начало широкой популяризации представлений об истории и теории криптографии положила книга Дэвида Кана «Взломщики кодов», опубликованная в 1967 г. и до сих пор пользующаяся интересом публики [Кан 2000]. В России сегодня криптография также является предметом интереса общественности. Одним из примеров этого является открытие в Москве на месте так называемой Марфинской «шарашки» (здания бывшей Марфинской спецтюрьмы № 16 МГБ СССР) Музея криптографии, которое планируется осуществить до конца 2021 г.[1] Организаторы музея руководствуются идеей о том, что проблемы информационной безопасности, в частности криптографии, касаются сегодня каждого человека[2].

3. Перерастание таких проблем доцифровой криптографии, как локальность, замкнутость и доверенность в распределенность, разомкнутость и недоверенность [Щербаков 2020, с. 228].

Информация в современном мире передается не между двумя или несколькими доверенными адресатами, а среди неограниченного круга пользователей. Это поставило новые проблемы организации шифрованной связи.

Однако помимо новых проблем, которые ставят перед криптографией информационной общество и развитие цифровых технологий, очевидно сохраняются общие проблемы криптографии прошлого и настоящего, определяющие преемственность развития теории и особенности практического применения криптографии на протяжении длительного периода. К таким общим проблемам можно отнести следующие:

---

[1] Музей криптографии [Электронный ресурс]. URL: https://cryptography-museum.ru/ (дата обращения 30 октября 2021).

[2] В Москве откроется первый в России музей криптографии [Электронный ресурс] // Интернет-портал «Российской газеты». URL: https://rg.ru/2021/07/27/reg-cfo/kakim-budet-pervyj-v-rossii-muzej-kriptografii.html (дата обращения 30 октября 2021).

1. Человеческий фактор остается одним из ключевых при использовании различных криптографических систем в разное время.

На фоне известных исторических примеров применения подкупа, шантажа и хищения для получения ключей к шифрам не стоит забывать о неосторожных и неразумных действиях современных пользователей, которые сами предоставляют мошенникам доступ к своим аккаунтам, сводя к нулю эффективность криптографических алгоритмов защиты. Большинство современных жителей планеты сталкивается с криптографией ежедневно, вводя пароль от почтового сервиса, сервиса государственных услуг или социальных сетей, узнавая статус покупки в интернет-магазине, делая денежный перевод через мобильное приложение банка и т. п. Рассматриваемые данные защищаются теми или иными криптографическими протоколами. При этом более 80% инцидентов в области информационной безопасности происходят не по вине сбоев и ошибок в алгоритмах защиты информации, а вследствие нарушения самими пользователями мер безопасности.

2. Серьезные импульсы для развития криптографии дает государство.

Исторически шифровальные службы и так называемые «черные кабинеты», в которых проводилась работа по шифрованию и дешифрованию документов, вскрытие корреспонденции противника, подделка печатей и подписей и пр. создавались и совершенствовались государствами в их интересах. Развитие дипломатии, организация посольств при иностранных державах в раннее новое время в Европе и в России привело к созданию организованных спецслужб, ставших прообразом современных органов защиты информации, в которых большое внимание уделялось криптографии.

В XIX–XX вв. основные требования совершенствования криптографии также были связаны с государственной сферой, прежде всего в военной области.

В настоящее время развитие криптографических методов защиты информации происходит при активном участии крупных бизнес-структур, так как отвечает их интересам развития сферы IT-технологий и связанных с ними коммерческих проектов. Однако государства являются ключевыми участниками развития криптографии, поддерживая разработки в этой области. Так, если рассматривать ведущиеся в России исследования в области квантовой криптографии, то следует упомянуть о том, что в 2020–2024 гг. на развитие квантовых коммуникаций, которые предполагают обязательное использование соответствующих средств шифрования, будет потрачено около 11,2 млрд руб. Например, в рамках рассматриваемых проектов в 2020 г. Центр компетенций НТИ «Квантовые

коммуникации» продемонстрировал метод более эффективного обеспечения безопасности квантовой криптографии, а компания «Ростелеком» осенью 2020 г. создала оптическую линию связи с квантовым распределением ключей[3].

2. Практические требования совершенствования криптографической защиты предполагают внедрение новых идей, теоретическое обоснование которых проходит параллельно или позднее.

Исторически сложилось, что различные научно-практические области знания и прикладные научные дисциплины развиваются от частного к общему, то есть на основе успешно применяемых на практике методов обосновываются теоретические положения. Например, так развивалась теория вероятности: на основе использования практических методов, подтвержденных статистикой, к созданию системы аксиом, которое произошло столетием позже. То же можно отнести и к развитию криптографии как научной дисциплины: на протяжении многих веков существовали криптографические алгоритмы, отвечающие потребностям практической деятельности, однако их теоретическое понимание и обоснование происходило позже. И в современной науке не полностью завершено теоретическое осмысление успешно действующих на сегодняшний день механизмов использования алгоритмов шифрования данных, контроля их целостности, применения цифровой подписи и т. п. [Щербаков 2020].

3. Сохраняются основные задачи криптографии: идентификация, аутентификация, сохранение целостности, конфиденциальности и доступности информации при ее передаче и хранении.

Одним из многочисленных подтверждений этого тезиса может служить, в частности, актуальность современного решения классической проблемы криптографии, связанной с распределением ключей. На протяжении всей истории криптографии правильный выбор ключа и исключение его кражи или иного способа попадания к противнику представляли собой важнейшие задачи при организации шифрованной связи. В XX в. эти проблемы стали решаться с помощью создания систем симметричного и ассиметричного шифрования.

Симметричное шифрование (например, алгоритм AES) предполагает, что обе стороны, участвующие в защищенном обмене данными, используют один и тот же ключ для шифрования и дешифрования. Стороны договариваются об общем закрытом ключе

[3] 4 «горячих» направления в сфере шифрования [Электронный ресурс] // CNews. URL: https://safe.cnews.ru/articles/2020-10-13_4_goryachih_napravleniya_v_sfere_shifrovaniya (дата обращения 19 октября 2021).

до начала обмена данными. Симметричные алгоритмы, как правило, применяются для шифрования больших баз данных, файловых систем и хранилищ. Ассиметричное шифрование (например, RSA) связано с использованием двух ключей – открытого и закрытого, которые применяются, соответственно, для шифрования и дешифрования. Используются также гибридные алгоритмы, в рамках которых есть элементы симметричного и асимметричного шифрования.

Решение проблемы распределения ключей важно и для криптографии будущего. Так, применение квантовой криптографии предполагает, что распределение ключей связано с физическими процессами использования поляризованных квантов, перехват которых в рамках оптической связи осуществить не удастся, поскольку характеристики квантов меняются. Невозможность перехвата элементарных частиц, находящихся в неизвестном квантовом состоянии, противоречит законам физики, в частности, теоретическим положениям, сформулированным в 1980-х гг. У. Вуттерсом, В. Зуреком и Д. Диэксом [Позычанюк 2017].

Эффективную защиту при хранении выработанных и распределенных ключей осуществляет квантовый модуль доверенного хранения ключей (QHSM), который отвечает также за осуществление математических преобразований, выдачу собственных ключей и результатов криптографических процедур [Щербаков 2020].

В настоящее время сложность применения квантовых коммуникаций заключается в том, что с помощью наземных кабелей передача ключей с использованием фотонов возможна лишь на сравнительно небольшие расстояния, составляющие несколько десятков километров. На расстояниях более 100 км оптоволоконный кабель поглощает фотоны, что существенно снижает скорость передачи информации. Для решения этой проблемы китайские ученые начали использовать спутниковую связь.

Летом 2020 г. китайским ученым и их коллегам из других стран удалось создать защищенную квантовую линию связи длиной 1120 км. Для этого использовался первый в мире орбитальный зонд «Мо-Цзы» (QUESS), впервые запущенный в 2016 г. [Lu 2020], а также чувствительные наземные телескопы, выступающие в качестве получателей квантовых сигналов. Итоги научной деятельности ученых были представлены в статье в журнале Nature, где отмечено, что удалось достичь скорости передачи информации 0,12 бит в секунду [Yin, Li, Liao 2020].

4. Помимо собственно криптографических алгоритмов большое значение имеют проблемы проектирования и реализации систем защиты.

Современный практический опыт использования криптографии показывает, что уязвимость информации в системах передачи данных обусловлена главным образом не слабостями криптографических алгоритмов, а ошибками и сбоями при проектировании и использовании систем защиты информации. Применяемые криптографические алгоритмы при их грамотном внедрении и использовании позволяют и в будущем создавать устойчивые к атакам системы защиты. С одной стороны, криптографические алгоритмы применяемых во всем мире систем платежей, созданные еще в 1970-х гг. прошлого века, показали свою криптоустойчивость, а мошенники чаще используют скиммеры и накладные клавиатуры в банкоматах, чем взламывают системы шифрования. С другой стороны, в среде специалистов известны многочисленные громкие инциденты в области информационной безопасности, вызванные ошибками и недочетами проектирования и внедрения криптосистем, связанные, например, с протоколами безопасности (WEP и др.), криптографическими библиотеками с открытым исходным кодом (например, OpenSSL), готовыми решениями для безопасности (в частности, шифрованными флеш-накопителями, в которых применялся один общий ключ, установленный на заводе) и т. д.

5. Совершенствование методов криптографической защиты информации приводит к появлению новых методов поиска уязвимостей систем.

На одной из крупных международных конференций в 2018 г. специалисты компании IBM выступили с заявлением, что одной из пяти технологий, которые повлияют на человечество в ближайшие 5 лет, станут квантовые компьютеры, которые возьмут на вооружение в том числе кибермошенники, что приведет к масштабным и практически неотразимым DDoS-атакам. Действительно, с появлением полномасштабного квантового компьютера задачу вскрытия любого шифра можно будет решить за несколько часов. Это прогнозируют результаты теоретической работы, которой занимался исследователь П. Шор в Массачусетском технологическом институте начиная с середины 1990-х гг.

Таким образом, уже сегодня необходимо продумывать пути усиления криптографической защиты данных. Исследователи и специалисты компании IBM утверждают, что в ближайшем будущем необходимо внедрять алгоритмы шифрования, связанные с так называемой криптографией на решетках (lattice-based cryptography), которые являются следующим шагом развития криптоалгоритмов после эллиптических кривых. Эти алгоритмы базируются на методах линейной алгебры и связаны, в частности, с решением задачи нахождения кратчайшего ненулевого вектора.

Задумываться о внедрении так называемой квантово-безопасной криптографии необходимо в настоящее время, поскольку речь может идти о защите уже созданных данных, безопасность которых будет важна в будущем. Возможен и вариант несанкционированного получения информации злоумышленниками в наши дни, а ее расшифровка – после появления соответствующих технических возможностей.

Национальный институт стандартов и технологий США (NIST) в 2016 г. начал исследование по оценке эффективности и стандартизации квантово-устойчивых алгоритмов шифрования с открытым ключом. Предполагается, что первый проект квантово-безопасного стандарта шифрования NIST будет создан в 2022–2024 гг.

Следует отметить, что многие проекты, уже предложенные в NIST, являются лишь модернизацией существующих алгоритмов, не предполагающих принципиально новой схемы шифрования. Применение таких алгоритмов может обеспечить плавный переход к квантово-безопасной криптографии, который является эффективным решением проблемы, поскольку позволит решить две задачи. Во-первых, обеспечит текущую безопасность данных, а во-вторых, обезопасит обладателей информации в будущем при прорыве в квантовых вычислениях [Любашевский 2020].

Заключение

Итак, в данной статье были выделены новые тенденции развития криптографии, актуальные в последние десятилетия, к основным из которых можно отнести: осознание математического характера задач шифрования данных, стремительное возрастание объемов обрабатываемой и шифруемой информации, которая распространяется среди неограниченного круга пользователей современных устройств передачи данных, практический и теоретический интерес пользователей к криптографии.

При этом следует не в меньшей мере учитывать устойчивые проблемы криптографии, проявляющие себя на протяжении длительного периода ее истории. Среди таких задач выделяется важность человеческого фактора при использовании любых криптографических систем, традиционного участия государства в развитии криптографии, а также теоретического обоснования идей криптографической защиты данных, обобщающих практический опыт применения шифрования. Неизменное значение при реализации любых криптографических алгоритмов сохраняют также

основные задачи криптографии, к которым относятся идентификация, аутентификация, сохранение целостности, конфиденциальности и доступности информации при ее передаче и хранении, которые должны решаться в рамках проектирования и реализации комплексных систем защиты. Поскольку развитие новых подходов к криптографической защите данных традиционно приводит к появлению новых факторов уязвимости, то традиционной проблемой криптографии также является работа на опережение потенциальных злоумышленников.

Таким образом, анализ тенденций развития криптографии на протяжении разных исторических периодов показывает неразрывную связь проблем криптографической защиты информации, а главное, путей их решения. Это подчеркивает важность изучения криптографии прошлого для определения подходов к применению эффективных алгоритмов шифрования данных в настоящем и будущем.

Литература

Кан 2000 – *Кан Д.* Взломщики кодов. М.: Центрполиграф, 2000.

Любашевский 2020 – *Любашевский В.* Квантово-безопасная криптография [Электронный ресурс] // Коммерсантъ Наука. 2020. № 6. Март. С. 33. URL: https://www.kommersant.ru/doc/4292008 (дата обращения 25 сентября 2021).

Позывчанюк 2017 – *Позывчанюк В.* Угроза будущего: станет ли квантовое шифрование доступным для каждого [Электронный ресурс] // Технологии и медиа. 2017. № 9 (33). Сент. URL: https://www.rbc.ru/magazine/2017/09/599c07ad9a7947297ed63fa6 (дата обращения 25 сентября 2021).

Русецкая 2014 – *Русецкая И.А.* История криптографии в Западной Европе в раннее новое время. СПб.: Центр гуманитарных инициатив; Университетская книга-СПб., 2014.

Щербаков 2020 – *Щербаков А.Ю.* Перспективы современной криптографии [Электронный ресурс] // Проектирование будущего. Проблемы цифровой реальности: труды 3-й Международной конференции (6–7 февраля 2020 г., Москва). М.: ИПМ им. М.В. Келдыша, 2020. С. 227–233.

Lu 2020 – *Lu D.* China has developed the world's first mobile quantum satellite station [Электронный ресурс] // New Scientist. Space. 2020. Jan. URL: https://www.newscientist.com/article/2229673-china-has-developed-the-worlds-first-mobile-quantum-satellite-station/ (дата обращения 29 октября 2021).

Yin, Li, Liao 2020 – *Yin J., Li Y.H., Liao S.K. et al.* Entanglement-based secure quantum cryptography over 1,120 kilometres // Nature. 2020. No. 582. P. 501–505. DOI: https://doi.org/10.1038/s41586-020-2401-y

References

Kahn, D. (2000), *The Codebreakers*, Tsentrpoligraf, Moscow, Russia.

Lu, D. "China has developed the world's first mobile quantum satellite station", *New Scientist. Space* (January, 2020), [Online], available at: https://www.newscientist.com/article/2229673-china-has-developed-the-worlds-first-mobile-quantum-satellite-station/ (Accessed 29 October 2021).

Lubashevskii, V. (2020) "Quantum secure cryptography", *Kommersant Science*, 2020, no. 6, March, [Online], available at: https://www.kommersant.ru/doc/4292008 (Accessed 25 September 2021).

Pozyvchanyuk, V. (2017), "The threat of the future. Will quantum encryption become available to everyone", *Technology and media*, 2017, no. 9 (33), Sept., [Online], available at: https://www.rbc.ru/magazine/2017/09/599c07ad9a7947297ed63fa6 (Accessed 25 September 2021).

Rusetskaya, I.A. (2014), *History of cryptography in Western Europe in early modern times*, Tsentr gumanitarnykh initsiativ; Universitetskaya kniga-SPb., St. Petersburg, Russia.

Shcherbakov, A.Yu. (2020), "Prospects for modern cryptography", *Designing the future. Issues of Digital Reality: Proceedings of the 3rd International Conference*, February 6–7, 2020, Moscow, KIAM RAS, Moscow, Russia, pp. 227–233.

Yin, J., Li, Y.H., and Liao, S.K. (2020), "Entanglement-based secure quantum cryptography over 1,120 kilometres", *Nature*, vol. 582, pp. 501–505, DOI: https://doi.org/10.1038/s41586-020-2401-y

Информация об авторе

Ирина А. Русецкая, кандидат исторических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; irkom@mail.ru

Information about the author

Irina A. Rusetskaya, Cand. of Sci. (History), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; irkom@mail.ru

УДК 535.1
DOI: 10.28995/2686-679X-2021-4-58-68

Координатное представление рабиевских осцилляций искусственного атома в оптической полости

Надежда Б. Викторова
Российский государственный гуманитарный университет, Москва, Россия, nbvictorova@list.ru

Николай Ю. Сгибнев
Российский государственный гуманитарный университет, Москва, Россия, qwertyalad@yandex.ru

Аннотация. В статье исследована возможность осцилляций электрона в двухъямном потенциале. Гамильтониан системы рассчитывается с учетом формул модели Джеймса-Каммингса. Унитарная динамика проведена с помощью общего решения уравнения Шредингера. Показаны условия на параметры задачи, при которых осцилляция имеет место. Эти условия для точной постановки дискретны. Однако ценность представляет выяснение, при каких параметрах задачи имеют место приближенные осцилляции, при которых наблюдается неполный переход частицы из одной ямы в другую. В стандартных руководствах по квантовой теории одной частицы гамильтониан с самого начала рассматривался без фотонов, то есть предполагалось, что полные осцилляции имеют место всегда. Это приближенное рассмотрение соответствует реальности только при высоком потенциале между ямами. Если потенциал низок, ямы фактически сливаются в одну яму, так что спектр и собственные значения гамильтониана становятся похожими на спектр и собственные значения одноямного потенциала – радикально иной случай. Такое несоответствие происходит из-за игнорирования взаимодействия электрона с электромагнитным полем. Если принять во внимание такое взаимодействие, мы получим динамику, описываемую гамильтонианом Джейнса-Каммингса. При малом потенциале растет энергетическая щель между основным и возбужденным энергетическими состояниями электрона. Поскольку вероятность испускания фотона пропорциональна этой величине, взаимодействие с полем не может быть проигнорировано.

Ключевые слова: квантовая информатика, уравнение Шредингера, рабиевские осцилляции, модель Джейнса-Каммингса, матрица плотности

Для цитирования: Викторова Н.Б., Сгибнев Н.Ю. Координатное представление рабиевских осцилляций искусственного атома в оптической полости // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4 С. 58–68. DOI: 10.28995/2686-679X-2021-4-58-68

Coordinate representation of Rabi oscillations of an artificial atom in an optical cavity

Nadezda B. Victorova
Russian State University for the Humanities, Moscow, Russia, nbvictorova@list.ru

Nikolay Yu. Sgibnev
Russian State University for the Humanities, Moscow, Russia, qwertyalad@yandex.ru

Abstract. The possibility of the electron oscillations in a two-well potential is investigated in the article. The Hamiltonian of the system is calculated taking into account the formulas of the James-Cummings model. The unitary dynamics is carried out using a general solution of the Schrodinger equation. The conditions for the parameters of the problem under which the oscillation takes place are shown. These conditions for the exact formulation are discrete. However, it is valuable to find out at what parameters of the problem there occur approximate oscillations, at which an incomplete transition of a particle from one well to another is observed. In the standard manuals on the quantum theory of a single particle, the Hamiltonian was considered from the very beginning without photons, so it was assumed that complete oscillations always take place. This approximate consideration corresponds to reality only with a high potential between the wells. If the potential is low, the wells actually merge into one well, so that the spectrum and eigenvalues of the Hamiltonian become similar to the spectrum and eigenvalues of a one-dimensional potential – a radically different case. Such a discrepancy occurs due to ignoring the interaction of the electron with the electromagnetic field. If such an interaction is taken into account we get the dynamics described by the Jaynes-Cummings Hamiltonian. At a low potential, the energy gap between the ground and excited energy states of the electron grows. Since the probability of photon emission is proportional to this value, the interaction with the field cannot be ignored.

Keywords: quantum computer science, Schrodinger equation, Rabi oscillations, Jaynes-Cummings model, density matrix

For citation: Victorova, N.B. and Sgibnev, N.Yu. (2021), "Coordinate representation of Rabi oscillations of an artificial atom in an optical cavity", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 58–68, DOI: 10.28995/2686-679X-2021-4-58-68

Введение

Эволюция квантовой частицы в двухъямном потенциале является одной из наиболее распространенных задач квантовой механики. Изучение квантовой динамики такой системы представляет интерес как для фундаментальной, так и прикладной науки, особенно для различных областей физики, биологии и химии. В начале 1990-х годов была предсказана возможность подавления переходов частицы из одной ямы в другую при определенных выбранных параметрах. Это явление называется когерентным разрушением туннелирования, или динамической локализацией, что подразумевало локализацию квантовой частицы в той яме, в которой она находилась в первоначальный момент. Нас же будут интересовать условия и ограничения на параметры, при которых имеют место осцилляции частицы из левой ямы в правую.

Постановка задачи

Задача заключается в исследовании наличия осцилляции электрона из одной ямы в другую в квантовой точке (рис. 1):

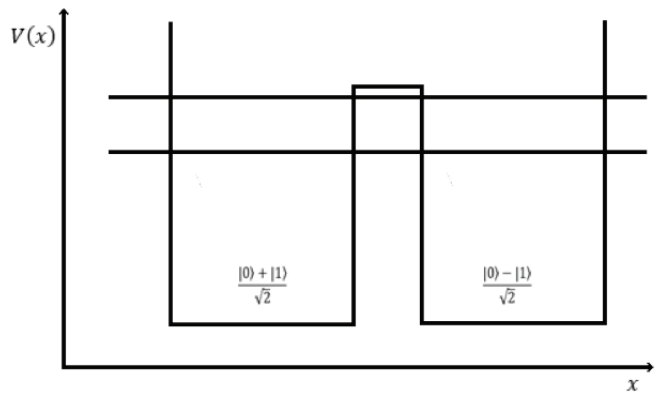

Рис. 1. Квантовая точка

$|\psi\rangle_{\text{баз}} = |ph\rangle|\phi_i\rangle_{c,a}$ – базисные состояния системы, где $i = 0, 1$; $ph = 0, 1$

$|\phi_0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ – невозбужденное состояние электрона (левая яма)

$|\phi_1\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$ – невозбужденное состояние электрона (правая яма)

$|0\rangle_{ph}|\phi_0\rangle = |\theta\rangle_{00}$ – в системе нет фотона, и электрон не возбужден

$|0\rangle_{ph}|\phi_1\rangle = |\theta\rangle_{01}$ – в системе нет фотона, и электрон возбужден

$|1\rangle_{ph}|\phi_0\rangle = |\theta\rangle_{10}$ – в системе есть фотон, и электрон не возбужден

$|1\rangle_{ph}|\phi_1\rangle = |\theta\rangle_{11}$ – в системе есть фотон, и электрон возбужден

Решение задачи

Опишем модель *Джейнса–Каммингса*. Рассмотрим оптическую полость, внутри которой находится двухуровневый атом и фотон. Полость представляет собой оптический резонатор (рис. 2) [Cummings 2013] [Jaynes, Cummings 1963].

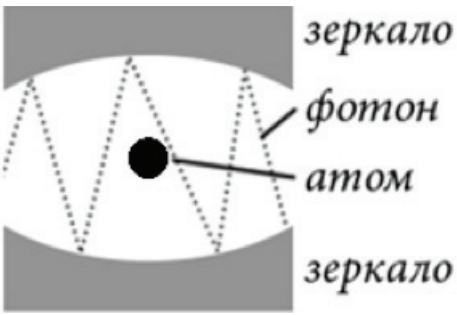

Рис. 2. Устройство оптического резонатора

Имеем двухкубитную систему, в которой за состояние электрона в атоме отвечает правый кубит, а за состояние фотона – левый:

$|00\rangle$ – фотона нет, электрон в невозбужденном состоянии, $|01\rangle$ – фотона нет, электрон в возбужденном состоянии, $|10\rangle$ – фотон есть, электрон в невозбужденным состоянии, $|11\rangle$ – фотон есть, электрон в возбужденном состоянии.

Определим операторы a^+, a^- рождения и уничтожения фотонов, действующих на 1 кубит, формулами

$$a^+a^-|n\rangle = n|n\rangle,\ a^-|n\rangle = \sqrt{n}|n-1\rangle,\ a^+|n\rangle = \sqrt{n+1}|n+1\rangle.$$

Тогда при $n = 1$ a^+, $= \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$, $a^- = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$.

Определим операторы σ+, σ– возбуждения электрона в атоме и уничтожения возбуждения электрона в атоме формулами $\sigma^+|0\rangle = |1\rangle$, $\sigma^+|1\rangle = 0$, $\sigma^-|0\rangle = 0$, $\sigma^-|1\rangle = |0\rangle$.

Тогда $\sigma^+ = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$, $\sigma^- = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$.

Оператор полной энергии (гамильтониан) описанной системы записывается следующим образом [Ожигов 2020] [Ожигов, Викторова, Исупова 2018] [Cummings 2013] [Jaynes, Cummings 1963] [Ozhigov, Skovoroda, Victorova 2016]:

$$H = \left(\hbar w_{ph} a^+ a^-\right) \otimes I + I \otimes (\hbar w_e \sigma^+ \sigma^-) + g(a^+ \otimes \sigma^- + a^- \otimes \sigma^+),$$

где $\hbar$ – постоянная Планка, ω_e – частота электрона, ω_{ph} – частота фотона, g – константа взаимодействия электрона с фотоном.

Пусть $\Delta = \omega_{ph} - \omega_e = 0$, тогда $\omega_{ph} = \omega_e = \omega$ и

$$H = \begin{pmatrix}0 & 0 & 0 & 0\\ 0 & \hbar\omega & g & 0\\ 0 & g & \hbar\omega & 0\\ 0 & 0 & 0 & 2\hbar\omega\end{pmatrix}.$$

Собственные значения матрицы $\lambda_1 = 0$, $\lambda_2 = \hbar\omega - g$, $\lambda_3 = \hbar\omega + g$, $\lambda_4 = 2\hbar\omega$.

Собственные векторы X_1, X_2, X_3, X_4, соответствующие собственным значениям λ_1, λ_2, λ_3, λ_4.

$$X_1 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad X_2 = \begin{pmatrix}0\\-1\\1\\0\end{pmatrix}, \quad X_3 = \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \quad X_4 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Выражая базис через собственные векторы оператора полной энергии, имеем $|00\rangle = X_1, |01\rangle = \frac{1}{2}(X_3 - X_2), |10\rangle = \frac{1}{2}(X_2 + X_3), |11\rangle = X_4$.

Мы хотим проверить наличие осцилляций между левой ямой, задаваемой координатой $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, и правой ямой, задаваемой координатой $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$., используя унитарную динамику вектора

$$|\theta\rangle_{00} = |0\rangle_{ph}\ \frac{|0\rangle+|1\rangle}{\sqrt{2}}.$$

Уравнение Шредингера имеет вид

$$i\hbar\frac{\partial}{\partial t}|\psi\rangle = H|\psi\rangle, \tag{1}$$

где $|\psi\rangle$ – волновой вектор;

$\hbar$ – постоянная Планка;

H – гамильтониан.

Общее решение уравнения Шредингера записывается как

$$|\psi(t)\rangle = \exp\left(-i\frac{Ht}{\hbar}\right)|\psi(0)\rangle. \tag{2}$$

В описываемой задаче

$$\psi(0) = |\theta\rangle_{00} = |0\rangle_{ph}\,\frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle}{\sqrt{2}} = \left(\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}00\right)^{t}.$$

В обозначениях матрицы плотности

$$\rho(t) = |\psi\rangle\langle\psi| \tag{3}$$

имеем

$$\rho(0) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}\frac{1}{\sqrt{2}}(1100) = \frac{1}{2}\begin{pmatrix}1&1&0&0\\1&1&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix} = \begin{pmatrix}\frac{1}{2}&\frac{1}{2}&0&0\\\frac{1}{2}&\frac{1}{2}&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix}.$$

Теперь рассмотрим унитарную динамику вектора $|00\rangle = X_1$.

Поскольку $H X_i = \lambda_i X_i$, то оператор $\exp\left(-i\frac{Ht}{\hbar}\right)$ действует на собственный вектор X_i как

$$\exp\left(-i\frac{Ht}{\hbar}\right) X_i = \exp\left(-i\frac{\lambda_i t}{\hbar}\right) X_i.$$

Отсюда

$$\psi(t) = \exp\left(-i\frac{Ht}{\hbar}\right)|00\rangle = \exp\left(-i\frac{Ht}{\hbar}\right)\mathrm{X}_1 =$$

$$= \exp\left(-i\frac{0\cdot t}{\hbar}\right)\mathrm{X}_1 = \mathrm{X}_1 = |00\rangle.$$

Теперь рассмотрим унитарную динамику вектора $|01\rangle$.

$$|01\rangle = \frac{1}{2}(\mathrm{X}_3 - \mathrm{X}_2), \text{тогда}$$

$$\exp\left(-i\frac{Ht}{\hbar}\right)|01\rangle =$$

$$= \exp\left(-i\frac{Ht}{\hbar}\right)\left(\frac{1}{2}(X_3 - X_2)\right) =$$

$$= \frac{1}{2}\left(\exp\left(-i\frac{Ht}{\hbar}\right)X_3 - \exp\left(-i\frac{Ht}{\hbar}\right)X_2\right) =$$

$$= \frac{1}{2}\left(\exp\left(-i\frac{(\hbar\omega + g)t}{\hbar}\right)X_3 - \exp\left(-i\frac{(\hbar\omega - g)t}{\hbar}\right)X_2\right) =$$

$$= \frac{1}{2}e^{-i\omega t}\left(\exp\left(-i\frac{gt}{\hbar}\right)X_3 - \exp\left(i\frac{gt}{\hbar}\right)X_2\right) =$$

$$= \frac{1}{2}e^{-i\omega t}\left(\exp\left(-i\frac{gt}{\hbar}\right)(|01\rangle + |10\rangle) - \exp\left(i\frac{gt}{\hbar}\right)(|10\rangle - |01\rangle)\right) =$$

$$= e^{-i\omega t}\left(\frac{e^{-i\frac{gt}{\hbar}} + e^{i\frac{gt}{\hbar}}}{2}|01\rangle + i\frac{e^{-i\frac{gt}{\hbar}} - e^{i\frac{gt}{\hbar}}}{2i}|10\rangle\right) =$$

$$= e^{-i\omega t}\left(\cos\left(\frac{gt}{\hbar}\right)|01\rangle - i\sin\left(\frac{gt}{\hbar}\right)|10\rangle\right).$$

Таким образом, мы получили результат

$$\psi(t) = \exp\left(-i\tfrac{Ht}{\hbar}\right)\psi(0) = \quad \psi(t) = \exp\left(-i\tfrac{Ht}{\hbar}\right)|\Theta\rangle_{00} =$$

$$= \frac{|00\rangle + e^{-i\omega t}\left(\cos\left(\frac{gt}{\hbar}\right)|01\rangle - i\sin\left(\frac{gt}{\hbar}\right)|10\rangle\right)}{\sqrt{2}}. \qquad (4)$$

В обозначениях матрицы плотности (3) имеем:

$$\rho(t) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{e^{-i\omega t}\cos\left(\frac{gt}{\hbar}\right)}{\sqrt{2}} \\ \frac{-e^{-i\omega t}i\sin\left(\frac{gt}{\hbar}\right)}{\sqrt{2}} \\ 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{e^{i\omega t}\cos\left(\frac{gt}{\hbar}\right)}{\sqrt{2}} & \frac{e^{i\omega t}i\sin\left(\frac{gt}{\hbar}\right)}{\sqrt{2}} & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{1}{2} & \frac{e^{i\omega t}\cos\left(\frac{gt}{\hbar}\right)}{2} & \frac{e^{i\omega t} i \sin\left(\frac{gt}{\hbar}\right)}{2} & 0 \\ \frac{e^{-i\omega t}\cos\left(\frac{gt}{\hbar}\right)}{2} & \frac{\cos^2\left(\frac{gt}{\hbar}\right)}{2} & \frac{i\cos\left(\frac{gt}{\hbar}\right)\sin\left(\frac{gt}{\hbar}\right)}{2} & 0 \\ \frac{-e^{-i\omega t} i \sin\left(\frac{gt}{\hbar}\right)}{2} & \frac{-i\cos\left(\frac{gt}{\hbar}\right)\sin\left(\frac{gt}{\hbar}\right)}{2} & \frac{\sin^2\left(\frac{gt}{\hbar}\right)}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (5)$$

Напомним, что требуется исследовать осцилляции электрона из левой ямы, задаваемой квантовым состоянием $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, в правую яму, задаваемую квантовым состоянием $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$.. Поэтому требуем обнуления коэффициента амплитуды в (4) при $|10\rangle$, то есть $\sin\left(\frac{gt}{\hbar}\right) = 0$, откуда $t_k = \frac{\hbar\pi k}{g}$, где k = 0, 1, 2 ... Тогда

$$e^{-i\omega t_k}\left(\cos\left(\frac{gt_k}{\hbar}\right)|01\rangle\right) = -1$$

$$(\cos(\omega t_k) - i\sin(\omega t_k))\cos\left(\frac{gt_k}{\hbar}\right) = -1, \text{поэтому}$$

$$\cos\left(\frac{gt_k}{\hbar}\right)\cos(\omega t_k) = -1\,, \cos\left(\frac{gt_k}{\hbar}\right)\sin(\omega t_k) = 0$$

$$\begin{cases} \cos\left(\frac{gt_k}{\hbar}\right) = 1 \\ \cos(\omega t_k) = -1 \\ t_k = \frac{\hbar\pi k}{g} \end{cases} <=> \begin{cases} \frac{g\hbar\pi k}{g\hbar} = 2\pi m\,, m \in Z^+ \\ \frac{\omega\hbar\pi k}{g} = \pi + 2\pi l\,, l \in Z^+ \end{cases} <=>$$

$$<=> \begin{cases} k = 2m, m \in Z^+ \\ \frac{\omega\hbar}{g}k = 1 + 2l, l \in Z^+ \end{cases} <=> \quad \frac{\omega\hbar}{g} = \frac{1+2l}{2m}, l \in Z^+, m \in N <=>$$

$$<=> \omega = \frac{g(1+2l)}{2m\hbar}, l \in Z^+, m \in N \quad (6)$$

$$\begin{cases} \cos\left(\frac{gt_k}{\hbar}\right) = -1 \\ \cos(\omega t_k) = 1 \\ t_k = \frac{\hbar\pi k}{g} \end{cases} <=> \begin{cases} \frac{g\hbar\pi k}{g\hbar} = \pi + 2\pi n\,, n \in Z^+ \\ \frac{\omega\hbar\pi k}{g} = 2\pi q\,, q \in Z^+ \end{cases} <=>$$

$$<=> \begin{cases} k = 1 + 2n\,, n \in Z^+ \\ \dfrac{\omega\hbar}{g} k = 2q, q \in Z^+ \end{cases} <=> \quad \frac{\omega\hbar}{g} = \frac{2q}{1+2n}\ , q \in Z^+, n \in N\ <=>$$

$$<=>\ \omega = \frac{2qg}{\hbar(1+2n)}\ , q \in Z^+, n \in N \tag{7}$$

В итоге

$$\psi(t_k) = \exp\left(-i\frac{Ht_k}{\hbar}\right)|\theta\rangle_{00} = \frac{|00\rangle + e^{-i\omega t_k}\left(\cos\left(\frac{gt_k}{\hbar}\right)|01\rangle\right)}{\sqrt{2}}.$$

Тогда матрица плотности (3) примет вид

$$\rho(t_k) = \begin{pmatrix} \frac{1}{2} & \frac{e^{i\omega t_k}\cos\left(\frac{gt_k}{\hbar}\right)}{2} & \frac{e^{i\omega t_k} i \sin\left(\frac{gt_k}{\hbar}\right)}{2} & 0 \\ \frac{e^{-i\omega t_k}\cos\left(\frac{gt_k}{\hbar}\right)}{2} & \frac{\cos^2\left(\frac{gt_k}{\hbar}\right)}{2} & \frac{i\cos\left(\frac{gt_k}{\hbar}\right)\sin\left(\frac{gt_k}{\hbar}\right)}{2} & 0 \\ \frac{-e^{-i\omega t_k} i \sin\left(\frac{gt_k}{\hbar}\right)}{2} & \frac{-i\cos\left(\frac{gt_k}{\hbar}\right)\sin\left(\frac{gt_k}{\hbar}\right)}{2} & \frac{\sin^2\left(\frac{gt_k}{\hbar}\right)}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{1}{2} & \frac{e^{i\omega t_k}(-1)^k}{2} & 0 & 0 \\ \frac{e^{-i\omega t_k}(-1)^k}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Заключение

В работе исследована динамика заряженной частицы в квантовой точке. Если параметр ω близок к нулю или имеет дискретный спектр вида (6), (7), то имеют место осцилляции заряженной частицы из левой ямы в правую. В других случаях осцилляций нет.

Литература

Ожигов 2020 – *Ожигов Ю.И.* Квантовый компьютер. М.: МАКС Пресс, 2020.

Ожигов, Викторова, Исупова 2018 – *Ожигов Ю.И., Викторова Н.Б., Исупова А.О.* Динамика поля и атома в модели Джейнса-Каммингса // Проблемы вычислительной и прикладной математики. 2018. № 2 (14). С. 106–113.

Cummings 2013 – *Cummings F.W.* Reminiscing about thesis work with E.T. Jaynes at Stanford in the 1950s // Journal of Physics B: Atomic, Molecular and Optical Physics. 2013. Vol. 46. № 22. P. 220–202.

Jaynes, Cummings 1963 – *Jaynes E.T., Cummings F.W.* Comparison of quantum and semiclassical radiation theories with application to the beam maser // Proceedings of the IEEE. 1963. Vol. 51. № 1. P. 89–109.

Ozhigov, Skovoroda, Victorova 2016 – *Ozhigov Y.I., Skovoroda N.A., Victorova N.B.* Quantum revivals of a non-Rabi type in a Jaynes-Cummings model // Theoretical and Mathematical Physics. 2016. Vol. 189. no. 2. P. 1673–1679.

References

Cummings, F.W. (2013), "Reminiscing about thesis work with E.T. Jaynes at Stanford in the 1950s", *Journal of Physics B: Atomic, Molecular and Optical Physics,* vol. 46, no. 22, pp. 220–202.

Jaynes, E.T and Cummings, F.W. (1963), "Comparison of quantum and semiclassical radiation theories with application to the beam maser", *Proceedings* of the *IEEE,* vol. 51, no. 1, pp. 89–109.

Ozhigov, Y.I. (2020), Kvantuvy kompyuter [Quantum computer], MAKS Press, Moscow, Russia.

Ozhigov, Y.I., Skovoroda, N.A. and Victorova, N.B. (2016), "Quantum revivals of a non-Rabi type in a Jaynes-Cummings model", *Theoretical and Mathematical Physics,* vol. 189, no. 2, pp. 1673–1679.

Ozhigov, Y.I., Victorova, N.B. and Isupova, A.O. (2018), "Field and atom dynamics in a Jaynes-Cummings model", *Problemy vychislitelnoi i prikladnoi matematiki*, vol. 2, no. 14, pp. 106–113.

Информация об авторах

Надежда Б. Викторова, кандидат физико-математических наук, доцент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; nbvictorova@list.ru

Николай Ю. Сгибнев, студент, Российский государственный гуманитарный университет, Москва, Россия; 125047, Россия, Москва, Миусская пл., д. 6; qwertyalad@yandex.ru

Information about the authors

Nadezhda B. Victorova, Cand. of Sci. (Physics and Mathematics), associate professor, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia, 125047; nbvictorova@list.ru

Nikolay Yu. Sgibnev, student, Russian State University for the Humanities, Moscow, Russia; bld. 6, Miusskaya Sq., Moscow, Russia 125047; qwertyalad@yandex.ru

УДК 620.22
DOI: 10.28995/2686-679X-2021-4-69-79

Решение проблемы построения представительного блока нагружения с использованием аппарата кластеризации

Ирина В. Гадолина
Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН), Москва, Россия, gadolina@mail.ru

Ирина М. Петрова
Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН), Москва, Россия, impetrova@mail.ru

Аннотация. Принятие обоснованного решения о нагрузке деталей машины во время эксплуатации важно для оценки долговечности как расчетными методами, так и при лабораторных испытаниях. Инженеры должны создать так называемый обобщенный блок нагрузки, основанный на учете распределения времени их работы в процессе эксплуатации. Поскольку нагружение транспортных машин не стационарно, исследование режимов является важной проблемой для принятия решения: список режимов не должен быть ни слишком длинным, ни слишком коротким. Кластерный анализ как один из инструментов машинного обучения использовался в данной работе для выделения похожих на первый взгляд режимов. Поскольку обобщенный блок нагружения создается для оценки долговечности, выбрались те параметры, которые связаны с накоплением усталостных повреждений. По эмпирическим данным был проведен кластерный анализ, который в дальнейшем был проверен «учителем» – т. е. имеющейся в распоряжении исследователей априорной информацией.

Ключевые слова: усталость материалов, случайный процесс нагружения, блок нагрузки, кластерный анализ

Для цитирования: Гадолина И.В., Петрова И.М. Решение проблемы построения представительного блока нагружения с использованием аппарата кластеризации // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 4. С. 69–79. DOI: 10.28995/2686-679X-2021-4-69-79

Solving the issue of constructing a representative loading unit by using the clustering apparatus

Irina V. Gadolina
Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), Moscow, Russia, gadolina@mail.ru

Irina M. Petrova
Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), Moscow, Russia, impetrova@mail.ru

Abstract. Making an informed decision about the loading of machine parts during operation is of importance for assessing durability both by calculation methods and in laboratory tests. Engineers must create a so-called generalized load block based on taking into account the distribution of their work time during operation. Since the loading of transport vehicles is not stationary, the study of modes is an important issue for making a decision: the list of modes should be neither too long nor too short. Cluster analysis, as one of the machine learning tools, was used in this work to distinguish modes, looking similar at first glance. Since the generalized loading block is created to assess the durability, those parameters were chosen that are associated with accumulating the fatigue damage. Based on empirical data, a cluster analysis was carried out, which was later checked by the "teacher" – that is, by the a priori information available to researchers.

Keywords: material fatigue, random loading process, load block, cluster analysis

For citation: Gadolina, I.V. and Petrova, I.M. (2021), "Solving the issue of constructing a representative loading unit by using the clustering apparatus", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, no. 4, pp. 69–79, DOI: 10.28995/2686-679X-2021-4-69-79

Введение

При оценке долговечности транспортных машин по параметру сопротивления усталости [Когаев 1993] необходимо грамотно оценить информацию о нагрузках за весь предполагаемый срок службы, которую характеризует обобщенный блок нагружения, представляющий собой суммарную гистограмму, где некоторым значениям амплитуд ставится в соответствие количество их повто-

рений за характерный период эксплуатации $l_б$ (1 час, 1 км и т. д.). Единицы измерения $l_б$ соответствуют единицам, в которых в дальнейшем, с применением гипотезы накопления усталостных повреждений, рассчитывается ресурс машины.

Как правило, нагружение машин в эксплуатации – нестационарный случайный процесс. В этом случае целесообразно выделить квазистационарные участки и провести схематизацию по методу «Дождя» [Когаев 1993], см., например, [Гадолина, Козлов, Монахова, Серебрякова 2019]. Распределения, полученные на этих квазистационарных участках, суммируются тем или иным способом, описанным в [Петрова, Гадолина 2018]. Некоторая трудность заключается в том, что границы интервалов гистограмм могут быть различными, поэтому одним из перспективных предложенных в [Петрова, Гадолина 2018] способов суммирования является использование метода ядерного сглаживания гистограмм. Ранее в [Петрова, Гадолина 2018] был рассмотрен пример, где по рекомендациям экспертов оценивались режимы, соответствующие различным скоростям движения локомотива. В реальности формирование обобщенного спектра может быть значительно сложнее.

Актуальность

Предлагается метод, который позволит оптимизировать выбор режимов нагружения для составления обобщенного блока нагружения в связи с оценкой долговечности. При этом количество квазистационарных режимов должно быть не слишком мало (для того, чтобы не потерять точность оценивания нагрузок) и не чрезмерно велико (для возможности проведения замеров и вычислений в разумные сроки).

Метод

Разрабатываемый метод на основе многомерного кластерного анализа (пример применения в [Плющенко 2020]) предполагает исследование переменных на последовательных отрезках временной реализации T. Назовем эти k отрезков суб-реализациями, причем их длительности t_i примем постоянными:

$$\sum_{i=1}^{k} t_i = T \,. \qquad (1)$$

На каждом отрезке t_i, $i = 1,2...k$ будут вычисляться определенные параметры, представленные в табл. 1, необходимые для экспериментальной расчетной оценки долговечности. Данная информация используется для установления кластерной принадлежности этих отрезков с последующим их объединением в частные режимы. Наиболее значимыми характеристиками процесса нагружения являются амплитуды напряжений и число их повторения [Когаев 1993]. Поэтому «открывают» табл. 1 эффективная частота f и максимальная амплитуда в суб-реализации σ_{amax}. Там же представлены среднее квадратичное отклонение случайной величины (СКО) и эквивалентная амплитуда спектра

$$\mathrm{VS} = V^{*}\sigma_{amax}, \tag{2}$$

которая в сочетании с f позволяют оценить ресурс при переменном напряжении. В выражении (2) задействована интегральная характеристика распределения амплитуд V, называемая также мерой полноты спектра. V определяется по формуле:

$$V = \sqrt[m]{\frac{1}{n}\sum h_i\left(\frac{\sigma_{ai}}{\sigma\widetilde{amax}}\right)^m} \tag{3}$$

В формуле (3) m – коэффициент угла наклона кривой усталости; n – суммарное число циклов в блоке; h_i – число циклов на i-той ступени; σ_{ai} – текущее значение амплитуды напряжений. Величина V характеризует повреждающее действие напряжений в суб-реализации. Коэффициент нерегулярности случайного процесса I хорошо характеризует сложность случайного процесса и может быть полезен для отслеживания стабильности показателей процесса нагружения на протяжении отрезка временной реализации T.

Таблица 1

Параметры случайного процесса,
ответственные за повреждение от усталости

Эффективная частота	Максимальная амплитуда в суб-реализации	Среднее квадратическое отклонение	Эквивалентная амплитуда спектра	Коэффициент нерегулярности
f	σ_{amax}	*СКО*	*VS*	I

Возможно, некоторые параметры могут оказаться сильно коррелированными, тогда их число возможно сократить.

Для апробации предлагаемого метода были использованы данные, дополнительная информация по которым (а именно, подробные записи временной зависимости напряжений в течение всей реализации) была любезно предоставлена авторами [Benashutti 2007]. График функции напряжения от времени показан на рис. 1.

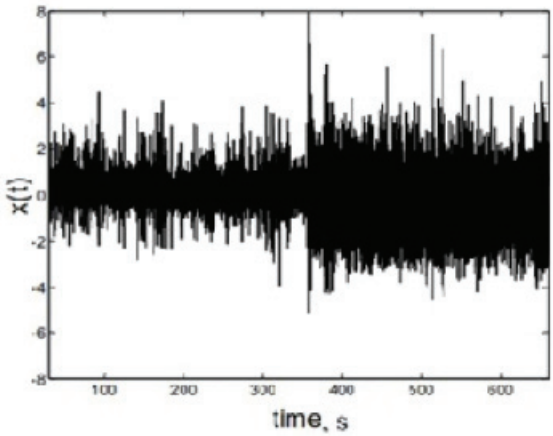

Рис. 1. Напряжения в раме горного велосипеда при движении по смешанной дороге [Benashutti 2007].

Рассматривалась реализация T = 600 сек., которая для целей исследования была разбита на 20 последовательных суб-реализаций длительностью t_i = 30 сек. Для каждой суб-реализации были вычислены параметры, соответствующие перечисленным в табл. 1. На рис. 2 показаны парные корреляции некоторых параметров, а именно: *f*, σ_{amax}, СКО, *VS, I*. На рис. 2 просматривается корреляция *СКО* и σ_{amax} *(Smax* на рис. 2*)* и, в меньшей степени, *VS* и СКО. Связь СКО и σ_{amax} не представляется неожиданной, поскольку обе величины косвенно характеризует интенсивность процесса, что было уже отмечено ранее [Gadolina 2020]. Поскольку случайные величины σ_{amax} и *VS* сильно коррелированы, σ_{amax} была исключена из дальнейшего рассмотрения для упрощения задачи. Параметр широкополосности *I* не влияет на расчетную долговечность и также был отброшен на данном этапе исследования.

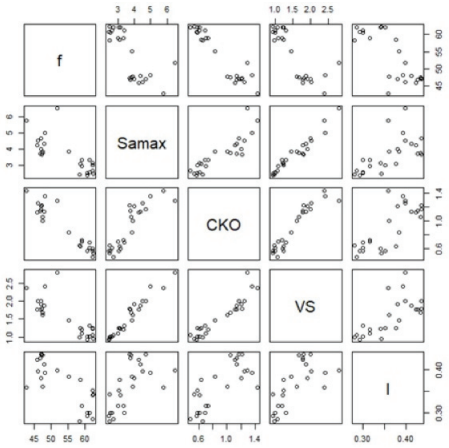

Рис. 2. Парные корреляции параметров
f, σ_{amax}, СКО, *VS, I*

На рис. 3 показаны временные зависимости некоторых параметров, а именно: f, σ_{amax}, СКО, *VS, I*, вычисленных путем осреднения по суб-реализациям.

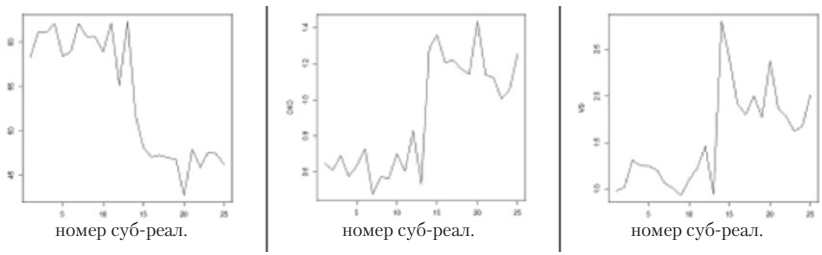

Рис. 3. Временные зависимости параметров частоты,
среднего квадратичного отклонения
и эквивалентной амплитуды спектра по длине реализации T

Для обоснованного суждения о факте принадлежности суб-реализаций к разным режимам нагружения применен кластерный анализ по методу ближайших соседей, *k*-means [R language 2020]. Была использована программа статистического анализа R. Векторы для кластерного анализа составлялись по параметрам из табл. 1. Число

векторов соответствовало числу суб-реализаций, $k = 20$. Результат кластерного анализа показан в табл. 2.

Таблица 2

Результат кластерного анализа по данным [Benashutti 2007]

	Средние значения переменных (средние кластеров)		
Переменная:	СКО	*VS*	*f* [Гц]
Индексы кластеров:			
1	0.63	1.14	60.2
2	1.20	2.0	47.2
Статистические данные	Внутри кластера 54.21	Сумма квадратов в кластере: 46.91	
	Коэффициент детерминации ***D*** (между_*SS* / общее_*SS*) = 91.3 %		

Примечание: коэффициент детерминации — доля дисперсии зависимой переменной, объясняемая рассматриваемой моделью зависимости, т. е. объясняющими переменными.

Распределение кластеров по суб-реализациям показано в табл. 3:

Графическое представление кластеризации в 3*D* показано на рис. 4. На рисунке видно, что точки отчетливо группируются в два множества, что и подтверждает кластерный анализ.

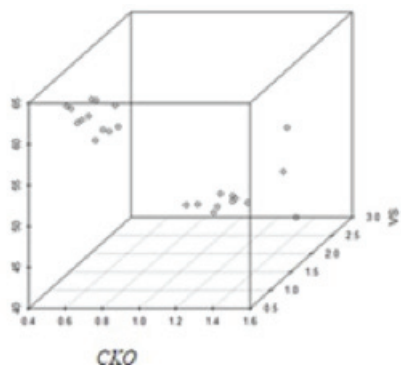

Рис. 4. Графическое представление параметров частоты, среднего квадратичного отклонения и эквивалентной амплитуды в 3*D*

Таблица 3

Принадлежность кластеров по суб-реализациям

Номер суб-реализации	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Принадлежность кластера	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2

Обсуждение

Если вернуться к рис. 1, то можно заметить, что принадлежность кластеров (табл. 3) хорошо характеризует общую картину нагружения. Более того, на основании априорной информации [Benashutti 2007] известно, что примерно в середине записи транспортное средство перешло на другие условия нагружения, а именно, движение по асфальту сменилось движением по грунтовой дороге с переключением передачи. В более общем случае использования машинного обучения для решения задачи о выделении отдельных режимов кластерный анализ с анализом указанных в табл. 1 или дополненным набором параметров поможет решить задачу об оптимизации числа нагрузочных режимов для последующей расчетной или экспериментальной оценки долговечности.

Вывод

Разработан метод, позволяющий провести обоснованное выделение частных режимов нагружения для построения обобщенного блока нагружения, необходимого при оценке усталостной долговечности. Метод опробован на конкретном примере записи эксплуатационной нагруженности детали транспортной машины. Имеющаяся априорная информация позволила подтвердить выводы, сделанные по результатам кластерного анализа.

Литература

Когаев 1993 – *Когаев В.П.* Расчеты на прочность при напряжениях, переменных во времени. М.: Машиностроение, 1993.

Гадолина, Козлов, Монахова, Серебрякова 2019 – *Гадолина И.В., Козлов А.Д., Монахова А.А., Серебрякова И.Л.* Оптимальный способ ЦОС в задачах оценки долговечности // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2019. № 1. С. 78–93.

Петрова, Гадолина 2018 – *Петрова И.М., Гадолина И.В.* Создание обобщенного спектра нагружения при различных вариантах нагружения в эксплуатации // Пром-Инжиниринг: Труды IV Междунар. научно-технической конф. Челябинск: ЮУрГУ, 2018. С. 26–30.

Плющенко 2020 – *Плющенко И.В.* и др. Алгоритм сочетания хромато-масс-спектрометрического ненаправленного профилирования и многомерного анализа для выявления веществ-маркеров в образцах сложного состава // Заводская лаборатория. Диагностика материалов. 2020. Т. 86. № 7. С. 12–19.

Benashutti 2007 – *Benasciutti D., Tovo R.* Frequency-based fatigue analysis of non-stationary switching random loads // Fatigue and Fracture of Engineering Materials and Structures. 2007. Vol. 30 (11). P. 1016–1029. DOI: https://doi.org/10.1111/j.1460-2695.2007.01171.x.

Gadolina 2021 – *Gadolina I.V., Makhutov N.A., Erpalov A.V.* Varied approaches to loading assessment in fatigue studies // International Journal of Fatigue. 2021. Vol. 144, March. 106035. DOI: https://doi.org/10.1016/j.ijfatigue.2020.106035.

Rlanguage 2020 – R Core Team. R: A language and environment for statistical computing [Электронный ресурс] // R Foundation for Statistical Computing, Vienna, Austria, 2020. URL: https://www.R-project.org/ (дата обращения 20 декабря 2021).

References

Kogaev, V.P. (1993), *Raschety na prochnost' pri napryazheniyakh, peremennykh vo vremeni* [Durability calculations at stresses that are variable in time, Mechanical engineering], Moscow, Russia, 364 p.

Gadolina, I.V., Kozlov, A.D., Monakhova, A.A. and Serebryakova, I.L. (2019), "The optimal way of DSP in the problems of assessing durability", *RSUH/RGGU Bulletin. "Information Science. Information Security. Mathematics" Series*, 2019, no. 1, pp. 78–93.

Petrova, I.M. and Gadolina, I.V. (2018), "Creation of a generalized loading spectrum for various loading options in operation", Prom-Engineering: Proceedings of the IV International Scientific and Technical Conference, YuUrGU, Chelyabinsk, Russia, pp. 318–321.

Plyushchenko, I.V. (2020), "Algorithm of combining chromatography mass spectrometry-untargeted profiling and multivariate analysis in samples of complex composition", *Industrial laboratory. Diagnostics of material*, vol. 86, no. 7, pp. 12–19. DOI: https://doi.org/10.26896/1028-6861-2020-86-7-12-19.

Benasciutti, D. and Tovo, R. (2007), "Frequency-based fatigue analysis of non-stationary switching random loads", *Fatigue and Fracture of Engineering Materials and Structures*, vol. 30 (11), pp. 1016–1029. DOI: https://doi.org/10.1111/j.1460-2695.2007.01171.x.

Gadolina, I.V., Makhutov, N.A. and Erpalov, A.V. (2021), "Varied approaches to loading assessment in fatigue studies", *International Journal of Fatigue*, vol. 144, March, 106035, DOI: https://doi.org/10.1016/j.ijfatigue.2020.106035.

R language (2020), R Core Team. R: A language and environment for statistical computing, *R Foundation for Statistical Computing, Vienna, Austria* [Online], available at: https://www.R-project.org/ (Accessed 20 December 2021).

Информация об авторах

Ирина В. Гадолина, кандидат технических наук, старший научный сотрудник, Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН), Москва, Россия; 101000, Россия, Москва, Малый Харитоньевский пер., д. 4; gadolina@mail.ru

Ирина М. Петрова, кандидат технических наук, ведущий научный сотрудник, Институт машиноведения им. А.А. Благонравова Российской академии наук (ИМАШ РАН), Москва, Россия; 101000, Россия, Москва, Малый Харитоньевский пер., д. 4; impetr@mail.ru

Information about the authors

Irina V. Gadolina, Cand. of Sci. (Engineering), senior researcher, Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), Moscow, Russia; Malyi Kharitonievskii lane, bld. 4, Moscow, Russia, 101000; gadolina@mail.ru

Irina M. Petrova, Cand. of Sci. (Engineering), leading researcher, Mechanical Engineering Research Institute of the Russian Academy of Sciences (IMASH RAN), Moscow, Russia; Malyi Kharitonievskii lane, bld. 4, Moscow, Russia, 101000; impetrova@mail.ru

Дизайн обложки
Е.В. Амосова

Корректор
Ж.П. Григорьева

Компьютерная верстка
Н.В. Москвина

Подписано в печать 14.12.2021.
Формат 60×90 1/16.
Уч.-изд. л. 3,4. Усл. печ. л. 5,0.
Тираж 1050 экз. Заказ № 1454

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