16+

ISSN 2074-1707

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ В. Н. ТАТИЩЕВА

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 3 (59)

Журнал включен в перечень рецензируемых научных изданий, рекомендованных ВАК России для публикации основных научных результатов диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук по следующим научным специальностям.

Группа специальностей 1.2 «Компьютерные науки и информатика»:

1.2.2 – Математическое моделирование, численные методы и комплексы программ (технические науки).

Группа специальностей 2.2 «Электроника, фотоника, приборостроение и связь»:

2.2.4 – Приборы и методы измерения (по видам измерений) (технические науки);

2.2.11 – Информационно-измерительные и управляющие системы (технические науки);

2.2.12 – Приборы, системы и изделия медицинского назначения (технические науки).

Группа специальностей 2.3 «Информационные технологии и телекоммуникации»:

2.3.1 – Системный анализ, управление и обработка информации (технические науки);

2.3.4 – Управление в организационных системах (технические науки);

2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей (технические науки);

2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки).

Журнал входит в базу данных Ulrich’s Periodicals Directory.

Астрахань
Астраханский государственный университет имени В. Н. Татищева
2022

ББК 30
П75

Рекомендовано к печати редакционно-издательским советом
Астраханского государственного университета имени В. Н. Татищева

ПРИКАСПИЙСКИЙ ЖУРНАЛ: управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 3 (59)

Журнал выходит 4 раза в год
Все материалы, поступающие в редколлегию журнала,
проходят независимое рецензирование

ISSN 2074-1707

ASTRAKHAN STATE UNIVERSITY
NAMED AFTER V. N. TATISHCHEV

PRIKASPIYSKIY ZHURNAL:
Upravlenie i Vysokie Tekhnologii

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2022
No. 3 (59)

The journal is included in the list of the reviewed scientific journals recommended by VAK of Russia for the publication of the main scientific results of theses for the candidate of science degree, for the doctor of science degree on the following scientific specialties.

Group of specialties 1.2 "Computer science and informatics":
1.2.2 – Mathematical modelling, numerical methods and complexes of programms (technical sciences).

Group of specialties 2.2 "Electronics, photonics, instrument engineering and communication":
2.2.4 – Instruments and methods of measurement (by type of measurement) (technical sciences);
2.2.11 – Information-measuring and control systems (technical sciences);
2.2.12 – Medical devices, systems and products (technical sciences).

Group of specialties 2.3 "Information technologies and telecommunications":
2.3.1 – System analysis, information control and processing (technical sciences);
2.3.4 – Management in organizational systems (technical sciences);
2.3.5 – Mathematical software and software for computing systems, complexes and computer networks (technical sciences);
2.3.6 – Information security methods and systems, information security (technical sciences).

The journal is included into the database Ulrich's Periodicals Directory.

Astrakhan
Astrakhan State University named after V. N. Tatishchev
2022

Recommended by the Editorial and Publishing Board
of Astrakhan State University named after V. N. Tatishchev

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2022
No. 3 (59)

The journal is published four times a year
All materials that come to the Editorial Board of the journal
are subject to independent peer-review

СОДЕРЖАНИЕ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УПРАВЛЕНИЕ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

CONTENTS

INFORMATICS, COMPUTER TECHNIQUE AND CONTROL

SYSTEM ANALYSIS, CONTROL AND INFORMATION PROCESSING

MANAGEMENT IN ORGANIZATIONAL SYSTEMS

MATHEMATICAL MODELLING, NUMERICAL METHODS AND PROGRAM SYSTEMS

MATHEMATICAL SOFTWARE AND SOFTWARE FOR COMPUTING MACHINES, COMPLEXES AND COMPUTER NETWORKS

METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

INSTRUMENT ENGINEERING, MEASUREMENT SCIENCE, INFORMATION AND MEASURING DEVICES AND SYSTEMS

INFORMATION-MEASURING AND CONTROL SYSTEMS

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УДК 004.827

СИСТЕМНЫЙ АНАЛИЗ ИНСТРУМЕНТОВ РАЗВИТИЯ ИНТРАПРЕНЁРСТВА НА ОСНОВЕ КРИТЕРИЕВ ПРИНЯТИЯ РЕШЕНИЙ

Статья поступила в редакцию 24.05.2022, в окончательном варианте – 31.05.2022.

Иванов Сергей Александрович, Санкт-Петербургский государственный университет им. С.М. Кирова, 194021, Российская Федерация, г. Санкт-Петербург, Институтский пер., 5, литер У; Санкт-Петербургский университет технологий управления и экономики, 190103, Российская Федерация, г. Санкт-Петербург, Лермонтовский пр., 44а,

кандидат технических наук, ORCID: 0000-0002-0243-3104, e-mail: kemsit@mail.ru

Щипанов Евгений Фёдорович, Санкт-Петербургский университет технологий управления и экономики, 190103, Российская Федерация, г. Санкт-Петербург, Лермонтовский пр., 44а,

кандидат экономических наук, доцент, ORCID: 0000-0001-6431-033X, e-mail: schipanov.ef@gmail.com

Земенцкий Юрий Владимирович, Санкт-Петербургский государственный университет им. С.М. Кирова, 194021, Российская Федерация, г. Санкт-Петербург, Институтский пер., 5, литер У; ВШТЭ Санкт-Петербургский государственный университет промышленных технологий и дизайна, 198095, Российская Федерация, г. Санкт-Петербург, ул. Ивана Черных, 4,

кандидат экономических наук, доцент, ORCID: 0000-0003-1717-9310, e-mail: olygerd@yandex.ru

Настоящее исследование направлено на разработку метода работы системы поддержки принятия решений при выборе инструмента развития внутреннего предпринимательства для корпоративных структур. Цель исследования заключается в повышении эффективности при решении многокритериальной задачи выборы инструментария развития внутреннего предпринимательства организации. Для достижения поставленной цели можно выделить следующие задачи: провести анализ существующих инструментов развития внутреннего предпринимательства для корпоративных структур; разработать теоретико-множественную модель как концептуальное описание информационной системы поддержки принятия решений; разработать метод ранжирования инструментов развития внутреннего предпринимательства на основе критериев принятия решений. Для решения поставленных задач использованы методы системного анализа, методы моделирования. Был проведен анализ инструментов развития внутреннего предпринимательства, определены основные практики, ориентированные на адаптацию под специфику системы управления различных корпораций. Разработано концептуальное описание системы поддержки принятия решений, представленное теоретико-множественной моделью. Разработан метод ранжирования альтернатив на основе критериев Вальда, Гурвица и Сэвиджа. На данном этапе исследования разработан метод ранжирования инструментов развития внутреннего предпринимательства на основе критериев принятия решений. Обоснована актуальность исследования, проведён анализ существующих инструментов развития внутреннего предпринимательства. Предложена теоретико-множественная модель – концептуальное описание системы поддержки принятия решений.

Ключевые слова: системный анализ, система поддержки принятия решений, многокритериальная задача выбора, выбор в условиях неопределенности, минимизация затрачиваемых ресурсов, внутреннее предпринимательство, интрапренерство, инновации

SYSTEM ANALYSIS OF INTRAPRENEURSHIP DEVELOPMENT INSTRUMENTS BASED ON DECISION-MAKING CRITERIA

The article was received by the editorial board on 24.05.2022, in the final version – 31.05.2022.

Ivanov Sergey A., Saint-Petersburg State University named after S.M. Kirov, letter U, 5 Institutsky per., St. Petersburg, 194021, Russian Federation; Saint-Petersburg University of Management Technologies and Economics,44 Lermontovsky prospect, Saint-Petersburg, 190103, Russian Federation,

Cand. Sci. (Engineering), ORCID: 0000-0002-0243-3104, e-mail: kemsit@mail.ru

Shchipanov Evgeniy F., Saint-Petersburg University of Management Technologies and Economics, 44 Lermontovsky prospect, Saint-Petersburg, 190103, Russian Federation,

Cand. Sci. (Economics), Associate Professor, ORCID: 0000-0001-6431-033X, e-mail: schipanov.ef@gmail.com

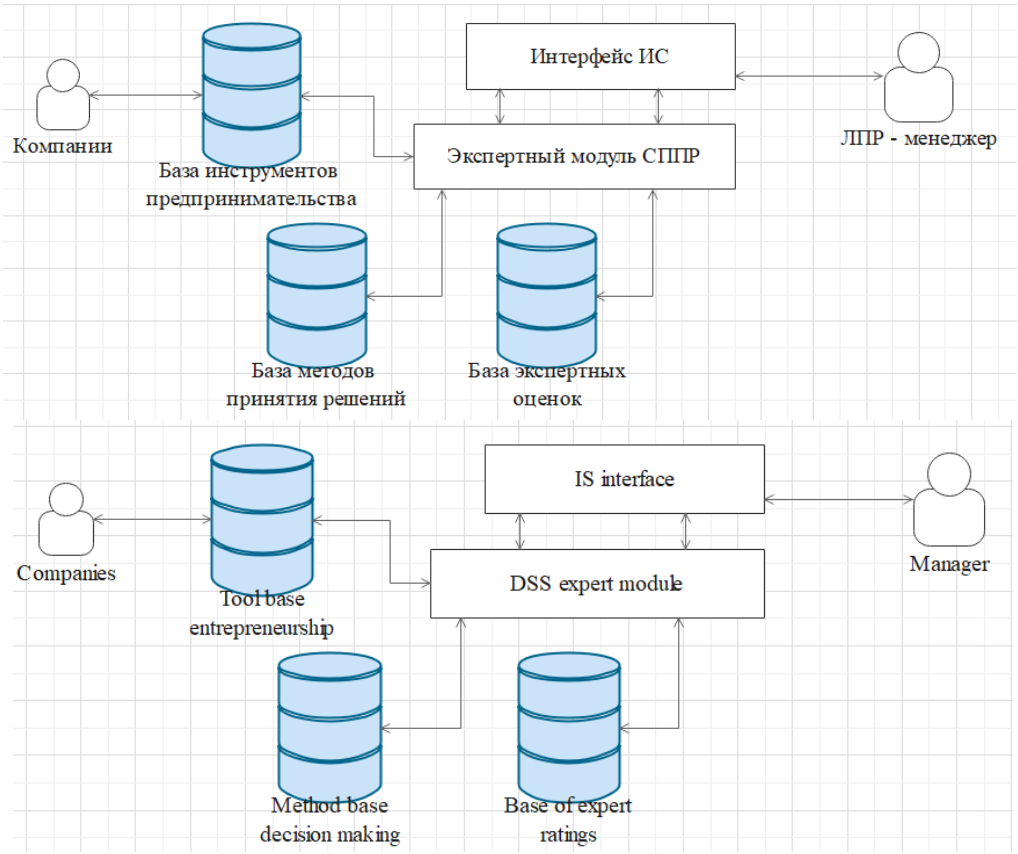
Zementckii Iurii V., Saint-Petersburg State University named after S.M. Kirov, letter U, 5 Institutsky per., Saint-Petersburg, 194021, Russian Federation; Higher School of Technology and Energy (HSTE) of the Saint Petersburg State University of Industrial Technologies and design, 4 ul. Ivana Chernykh, Saint-Petersburg, 198095, Russian Federation,

Cand. Sci. (Economics), Associate Professor, ORCID: 0000-0003-1717-9310, e-mail: olygerd@yandex.ru

This study is aimed at developing a method of operation of the decision support system when choosing a tool for the development of intrapreneurship for corporate structures. The purpose of the study is to increase efficiency in solving the multi-criteria problem of choosing tools for the development of intrapreneurship. To achieve this goal, the following tasks can be distinguished: to analyze the existing tools for the development of intrapreneurship for corporate structures; to develop a set-theoretical model as a conceptual description of an information DSS; to develop a method for ranking instruments for the development of intrapreneurship based on decision-making criteria. To solve the tasks set, methods of system analysis, modeling methods were used. An analysis was made of tools for the development of intrapreneurship, and the main practices focused on adaptation to the specifics of the management system of various corporations were identified. A conceptual description of the DSS, represented by a set-theoretic model, has been developed. A method for ranking alternatives based on the criteria of Wald, Hurwicz and Savage has been developed. At this stage of the study, a method has been developed for ranking the instruments for developing intrapreneurship based on decision-making criteria. The relevance of the study is substantiated, the analysis of existing tools for the development of intrapreneurship is carried out. A set-theoretic model is proposed - a conceptual description of a DSS.

Keywords: system analysis, decision support system, multicriteria choice problem, choice under uncertainty, resource minimization, intrapreneurship, innovations

Graphical annotation (Графическая аннотация)



Введение. Устойчивое развитие современной экономики разных иерархических уровней невозможно без реализации инновационно-ориентированных стратегий и проектов. Однако помимо объективных сложностей, обусловленных замедлением темпов роста глобальной и национальной экономик, на пути инновационного пути развития встают проблемы субъективного характера (человеческий фактор). Сам термин «инновация» с момента первого своего применения в 1911 г. претерпел значительную эволюцию.

С точки зрения российского законодательства (ФЗ № 127 «О науке и государственной научно-технической политике» от 23.08.1996 г. с изменениями и дополнениями) инновации – это введенный в употребление новый или значительно улучшенный продукт (товар, услуга) или процесс, новый метод продаж или новый организационный метод в деловой практике, организации рабочих мест или во внешних связях [8].

Современная Россия одновременно обладает значительным инновационным потенциалом и целым рядом системных проблем в его реализации. С 2011 года в РФ действовала «Стратегия инновационного развития Российской Федерации на период до 2020 года», создавалась соответствующая инфраструктура [1].

К сожалению, большинство плановых показателей так и не были достигнуты. В качестве одной из важнейших проблем ее реализации можно выделить недостаточное внимание инновационным процессам внутри компаний.

Внутрифирменные инновационные процессы можно обозначить с помощью термина «интрапренёрство» (от англ. Intrapreneurship – внутреннее предпринимательство), под которым понимается система, позволяющая сотруднику действовать как предприниматель в рамках компании (организации). Интрапренёры – это целеустремленные, инициативные и ориентированные на действия люди, которые проявляют инициативу в продвижении инновационного продукта или услуги [2].

В России интрапренёрство – относительно новая категория, поэтому одновременно в источниках встречаются: интрапренёрство, интрапредпринимательство, внутреннее (внутрикорпоративное/внутрифирменное) предпринимательство.

Внутреннее предпринимательство – это, прежде всего, система отношений, требующих регламентации и однозначных трактовок, чтобы все участники инновационного процесса были заинтересованы в успешном и взаимовыгодном сотрудничестве. Это является глобальной проблемой даже для тех стран, где интрапренёрство уже является привычной практикой. На сегодняшний день по итогам опроса глобального мониторинга предпринимательства в России всего 0,7 % населения вовлечено в предпринимательский процесс внутри корпораций. Для сравнения: в Германии – 5,2 %, а США – 8 % [3].

Развитию внутреннего предпринимательства в РФ мешают как объективные трудности, так и проблемы, которые могут быть решены организационными мерами, которые в свою очередь требуют понимания проблемы руководством компании и системного подхода. Передовой мировой опыт уже имеет развитый инструментарий реализации интрапренёрства, что порождает задачу оптимального выбора наиболее подходящего инструмента для каждой конкретной организации. Системный анализ на основе критериев принятия решений может стать ключом к решению этой проблемы.

Анализ инструментов развития внутреннего предпринимательства. В современной зарубежной и российской практике формирования организационных структур стимулирования инновационной активности корпорации можно выделить шесть основных инструментов реализации внутреннего предпринимательства [4]:

- конкурсы/хакатоны;
- бизнес-акселераторы;
- инкубаторы;
- лаборатории инноваций;
- программы внутреннего предпринимательства;
- стартап-студии.

Хакатон (англ. hackathon, от hacker «хакер» + marathon «марафон») – форум для разработчиков, во время которого специалисты из разных областей разработки программного обеспечения (программисты, дизайнеры, менеджеры) решают какую-либо проблему на определенное время (от нескольких дней до недели). Обычно в результате хакатонов создаётся MVP (минимально жизнеспособный продукт). При этом тематика хакатонов чрезвычайно широка, они часто используются для стимулирования свободной генерации идей и формирования внутреннего сообщества, ориентированного на инновационную и предпринимательскую культуру.

Внутренний бизнес-акселератор – краткосрочная программа для сотрудников по ускоренной разработке и тестированию продукта с привлечением ресурсов корпорации. Акселератор помогает компании ускоряться, когда у нее уже есть основа для развития: поток проектов, инициатив, гипотез. Смысл акселерационной программы – недорого и быстро сформулировать новые инновационные идеи и собрать команды исполнителей. Скорость и относительная лёгкость не подразумевает того, что акселератор работает как разовое внешнее событие, в идеале он становится постоянным бизнес-процессом внутри компании.

Внутренний инкубатор нацелен на индивидуальную и более длительную поддержку инициативных сотрудников и команд. Для инкубационных программ чаще всего характерен меньший поток проектов, но при этом более высокая конверсия – доля успешно реализованных кейсов.

В инкубатор чаще всего подбираются идеи, проекты, стратегии, комплементарные текущим направлениям деятельности компании, хотя могут быть и исключения. Продолжительность инкубации не фиксирована и зависит от типа проектов.

Корпоративная инновационная лаборатория – это особое независимое подразделение компании, предназначенное для проведения экспериментов и определения возможностей, которые можно развить внутри организации. Лаборатории инноваций занимаются не только разработкой продукта и поиском новых ниш, но и реализацией проектов и выводом новых продуктов на рынок.

Программа внутреннего предпринимательства состоит из набора взаимосвязанных инструментов и мероприятий по организации системной работы с идеями – от их подачи до превращения в готовый продукт. Программа доступна в любое время при наличии идеи, а не периодически, что позволяет массово вовлечь сотрудников.

Цель стартап-студии/corporate Venture Builder («венчурное строительство», «фабрика стартапов») – серийное воспроизводство новых стартапов. Для неё характерны высокие показатели выживаемости проектов и высокая скорость их вывода на рынок. Студия оказывает полный цикл услуг: формулирование идей и проверка гипотез внутри корпорации, подбор команд, поддержка управления внутренних стартапов и их масштабирование. Стартап-студия вкладывается в первую очередь не деньгами, а компетенциями и ресурсами (например, доступ к данным, помощь в поиске разработчика и пр.) [5].

В итоге можно констатировать тот факт, что все шесть инструментов имеют свои достоинства и недостатки, в некоторых случаях они могут дополнять друг друга. Выбор одного из них не является очевидным, в связи с этим лицу, принимающему решение (ЛПР), требуется поддержка в виде соответствующей системы, а появление новых инструментов развития внутреннего предпринимательства только усилит роль этой системы.

Системный анализ ключевых параметров. Все указанные инструменты развития внутрикорпоративного предпринимательства можно представить как множество альтернатив, из которых система поддержки принятия решений (СППР) выбирает наиболее эффективную для ЛПР:

$$A = \{a_1, a_2, \dots, a_q\}, \quad (1)$$

где a_q – альтернатива; q – количество альтернатив. Выбор альтернатив осуществляется из шести основных инструментов развития внутреннего предпринимательства, представленных в таблице 1.

Таблица 1 – Выбранные альтернативы

a_1	a_2	a_3	a_4	a_5	a_6
Конкурс/ хакатон	Акселератор	Инкубатор	Лаборатория инноваций	Программа внутреннего предпринимательства	Стартап-студия

Каждая из альтернатив обладает набором свойств:

$$W = \{w_1, w_2, \dots, w_n\}, \quad (2)$$

где n – количество свойств. В первом приближении выделяется три основных свойства: инвестиции в создание соответствующего инструмента, получаемый экономический эффект и эффект, направленный на развитие корпоративной культуры. Оценки, данные в качественном формате, необходимо перевести в количественные показатели при помощи вербально-числовой шкалы Харрингтона [7] (при интервале оценки [0; 1], шаг 0,3), представленные в таблице 2.

Таблица 2 – Вербально-числовая шкала Харрингтона для W

Свойство/оценка	**Высокий**	**Средний**	**Низкий**
Инвестиции в создание	0,8	0,5	0,2
Экономический эффект	0,8	0,5	0,2
Эффект на развитие корпоративной культуры	0,8	0,5	0,2

Оценку альтернатив возможно произвести по приведенной шкале. Результаты оценки представлены в таблице 3.

Таблица 3 – Оценка альтернатив

Свойство/альтернатива	a_1	a_2	a_3	a_4	a_5	a_6
Инвестиции в создание	0,2	0,5	0,2	0,8	0,5	0,8
Экономический эффект	0,2	0,5	0,5	0,8	0,5	0,8
Эффект на развитие корпоративной культуры	0,5	0,8	0,8	0,2	0,8	0,2
∑	**0,9**	**1,8**	**1,5**	**1,8**	**1,8**	**1,8**

Наравне со свойствами каждой из альтернатив необходимо ввести набор ключевых метрик:

$$M = \{m_1, m_2, \dots, m_t\}, \quad (3)$$

где t – количество метрик, характеризующих альтернативы.

Данные, показывающие соответствие альтернативы/метрики, можно привести в следующем виде.

Таблица 4 – Соответствие альтернативы/метрики

Метрика/альтернатива	a_1	a_2	a_3	a_4	a_5	a_6
Количество команд	+	+	+	–	–	–
Количество рабочих прототипов	+	–	–	–	–	–
Доля вовлеченных сотрудников	+	–	–	–	+	–
Количество успешных пилотов (внедренных решений)	–	+	+	–	+	–
Количество итоговых проектов	–	–	+	–	–	–
Количество коммерциализированных продуктов	–	–	–	+	–	+
Скорость разработки продукта	–	–	–	+	–	–
Количество идей	–	–	–	–	+	–

Также необходимо определить множество основных задач, которые решает для компании та или иная альтернатива, в виде:

$$Z = \{z_1, z_2, \dots, z_p\}, \quad (4)$$

где p – количество задач. Для определения задач использованы материалы из доклада агентства инноваций города Москвы «Развитие предпринимательства внутри корпораций: международный опыт и российская практика» (табл. 5).

Таблица 5 – Решаемые задачи

a_1	a_2	a_3	a_4	a_5	a_6
Быстро найти новые идеи под конкретную задачу, сформировать внутреннее сообщество интрапренёров	Ускорить разработку продукта/сервиса, найти новых клиентов, развить предпринимательские компетенции	Доработать идею развития предпринимательских компетенций, превратив в продукт,	Быстро выводить на рынок прорывные продукты, чаще всего смежных и новых рынков	Создать новый внутренний бизнес-процесс по работе с инновациями	Запустить серийное производство внутренних стартапов

Концептуальное описание системы можно представить в виде теоретико-множественной модели:

$$X = < A, W, M, Z, f_q(w_i, m_j, z_p) >, \quad (5)$$

где набор свойств W – это качественные характеристики множества альтернатив A (представленные в виде весовых коэффициентов); набор ключевых метрик M – это количественные характеристики множества альтернатив A; множество Z – задачи, которые решают альтернативы A. Каждая альтернатива в таком случае представима в виде [8]:

$$a_q = \{f_q(w_i, m_j, z_p)\}, \quad (6)$$

где $i = \overline{1,n}$; $j = \overline{1,t}$; $p = \overline{1,q}$; $f_q(w_i, m_j, z_p)$ – характеристическая функция, определяющая подмножество $A^* \subseteq A$, где A^* – все возможные альтернативы, подходящие компании.

Метод ранжирования альтернатив. Для решения многокритериальной задачи выбора инструмента для развития внутреннего предпринимательства необходимо разработать метод ранжирования инструментов – альтернатив. Данный метод направлен на решение задачи выбора организациями вне зависимости от формы собственности на основании выделенных ранее критериев. Метод можно разделить на несколько этапов.

Этап 1. Формирование базы альтернатив и обработка входной информации.

1.1. Создание базы альтернатив, в которую включены все варианты инструментов развития внутреннего предпринимательства: конкурс/хакатон, акселератор, инкубатор, лаборатория инноваций, программа внутреннего предпринимательства, стартап-студия. Базу данных можно представить в виде массива:

$$BDA = [\beta b_{nq}, \upsilon b_{tq}, \varphi b_{pq}], \quad (7)$$

где βb_{nq} – оценка каждой альтернативы с точки зрения характеристик экспертом;

υb_{tq} – оценка каждой альтернативы с точки зрения ключевых метрик экспертом;

φb_{pq} – оценка каждой альтернативы с точки зрения задач экспертом.

1.2. При сборе входной информации пользователю предлагается выбрать параметры, являющиеся важными для него при выборе альтернативы. В таком случае набор входных данных со стороны пользователя представим в виде массива:

$$BDM = [\beta c_{nq}, \upsilon c_{tq}, \varphi c_{pq}], \quad (8)$$

где βc_{nq} – оценка каждой альтернативы с точки зрения характеристик пользователем;

υc_{tq} – оценка каждой альтернативы с точки зрения ключевых метрик пользователем;

φc_{pq} – оценка каждой альтернативы с точки зрения задач пользователем.

Этап 2. Получение результирующей матрицы, выбор критерия принятия решения.

Для принятия решения необходимо получить результирующий массив, который объединит в себе потребности пользователя (на основании входных данных) и мнение эксперта по каждой из альтернатив. Результирующий массив можно представить как

$$RES = BDA \cap BDM, RES = [\beta r_{nq}, \upsilon r_{tq}, \varphi r_{pq}]. \quad (9)$$

Для решения многокритериальной задачи выбора необходимо определить соответствующий критерий принятия решения. Предлагается три сценария поведения системы поддержки принятия решения: критерий крайнего пессимизма (критерий Вальда), критерий золотой середины (критерий Гурвица), критерий, позволяющий с наибольшей вероятностью избежать максимального риска (критерий Сэвиджа). Рассмотрим указанные критерии.

Критерий Вальда

Основывается на понятии «рассчитывай на худшее», определяется параметром эффективности:

$$K_1 = \max_{\lambda} \min_{\rho} e_{\lambda\rho}, \quad (10)$$

где $e_{\lambda\rho}$ – поведение среды при использовании конкретной альтернативы.

Этот критерий ориентирует лицо, принимающее решение (ЛПР), которым является пользователь системы, на наихудшие условия. В более благоприятныхусловиях этот критерий приводит к потере эффективности.

Критерий Гурвица

Этот критерий предписывает руководствоваться «золотой серединой», то есть случаем, когда $0 \le ak \le 1$, и избегать как пессимистичного, так и оптимистичного варианта. В таком случае решение выглядит следующим образом:

$$K_2 = \max_{\lambda}[ak \min_{\rho} e_{\lambda\rho} + (1 - ak) \max_{\rho} e_{\lambda\rho}], \quad (11)$$

где *ak* – некий коэффициент субъективности, выбираемый из интервала от 0 до 1. Использование этого критерия вносит в решение задачи дополнительный субъективизм.

Критерий Сэвиджа

Данный критерий используется для того, чтобы с наибольшей вероятностью избежать максимального риска. В таком случае критерий Сэвиджа обеспечивается наименьшим значением максимального риска:

$$K_3 = \max_{\lambda} \min_{\rho} r_{\lambda\rho}, \quad (12)$$

где $r_{\lambda\rho}$ определяется выражением $\beta k - e_{\lambda\rho}$, где $\beta\kappa$ – максимально возможный выигрыш.

Этап 3. Определение полученных решений, представление их ЛПР.

На данном этапе на основании полученного результирующего массива в соответствии с тремя определенными критериями конечному пользователю представляется результат ранжирования альтернатив.

Решение, согласно критерию Вальда, представимо как:

$$A_1^* = \left[\max_{n} \min_{q} \beta r_{nq}, \max_{t} \min_{q} \upsilon r_{tq}, \max_{p} \min_{q} \varphi r_{pq}\right]. \quad (13)$$

Решение, согласно критерию Гурвица, представимо как:

$$A_2^* = [k_1, k_2, k_3], \quad (14)$$

где

$$k_1 = \max_{n}[ak \min_{q} \beta r_{nq} + (1 - ak) \max_{q} \beta r_{nq}],$$
$$k_2 = \max_{t}[ak \min_{q} \upsilon r_{tq} + (1 - ak) \max_{q} \upsilon r_{tq}],$$
$$k_3 = \max_{p}[ak \min_{q} \varphi r_{pq} + (1 - ak) \max_{q} \varphi r_{pq}].$$

Решение, согласно критерию Сэвиджа, представимо как:

$$A_3^* = [\max_{n} \min_{q}(\beta k - \beta r_{nq}), \max_{t} \min_{q}(\beta k - \upsilon r_{tq}), \max_{p} \min_{q}(\beta k - \varphi r_{pq})]. \quad (15)$$

В таком случае результирующее множество, которое будет представлено пользователю, можно представить как:

$$A^* = \{A_1^*, A_2^*, A_3^*\}. \quad (16)$$

Выводы. В итоге на данном этапе исследования разработан метод ранжирования инструментов развития внутреннего инновационного предпринимательства на основе критериев принятия решений.

Обоснована актуальность исследования, проведён анализ существующих инструментов развития внутреннего предпринимательства. Предложена теоретико-множественная модель – концептуальное описание СППР. Для решения поставленных задач использованы методы системного анализа, методы моделирования.

На следующем этапе исследования следует разработать набор универсальных качественных ключевых показателей, учесть фактор неопределённости и ограничения – минимальный объём ресурсов, необходимых для реализации того или иного пути внутрикорпоративного инновационного развития.

Отдельно следует отметить значимость отраслевой специфики организаций, которая серьёзным образом влияет на выбор формы, в которой будет развиваться интрапренёрство. Учёт отраслевой специфики также является одной из будущих задач.

Итогом исследования станет создание базы знаний, проектирование СППР и реализация её в виде специального программного продукта.

Библиографический список

1. Стратегия инновационного развития Российской Федерации на период до 2020 года. – Режим доступа: https://ac.gov.ru/files/attachment/4843.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.02.2022).

2. Irbe, M. Research on Transdisciplinary Entrepreneurship Training. Intellectual Output 2. ERASMUS+ KA2 – Cooperation for Innovation and Exchange of Good Practices KA203 – Strategic Partnerships for higher education European Entrepreneurship Training Community Reference No. 2018-1-LV01-KA203-046974 / M. Irbe, M. Ozolins, M. Nemilentsev, M. Priem, M. Smits, A. Van Der Zouwen, L. Martin, et al. – 2020. – Режим доступа: https://goodpractices.eu/research-results, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 18.02.2022).

3. Евстигнеева, Е. Е. Инновационное развитие России: стратегия, барьеры и способы их преодоления / Е. Е. Евстигнеева, Ю. В. Махрова // Молодой ученый. – 2018. – № 22 (208). – С. 399–402. – Режим доступа: https://moluch.ru/archive/208/50842/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.02.2022).

4. Сайт «Стартап Лаборатория». – Режим доступа: https://startup-lab.ru (дата обращения: 20.02.2021)

5. Доклад агентства инноваций города Москвы «Развитие предпринимательства внутри корпораций: международный опыт и российская практика». – Октябрь 2020. – Режим доступа: https://innoagency.ru/files /Corporate_entrepreneurship_2020_Moscow_Agency_of_innovations.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.02.2022).

6. Иванов, С. А. Методы морфологического анализа при исследовании сложных систем / С. А. Иванов // Роль интеллектуального капитала в экономической, социальной и правовой культуре общества XXI века : тезисы докладов на Международной научно-практической конференции. – Санкт-Петербург, 2018. – С. 346–348.

7. Иванов, С. А. Постановка многокритериальной задачи выбора комплектующих для автоматизированной теплицы / С. А. Иванов // Роль и место информационных технологий в современной науке : сборник статей Международной научно-практической конференции. – Магнитогорск, 2017. – С. 55–57.

8. Квятковская, А. Е. Информационная технология поиска компаний-аналогов для оценки стоимости бизнеса, использующая интеллектуальных агентов / А. Е. Квятковская, Е. В. Чертина, А. О. Полумордвинова, И. Ю. Квятковская // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2019. – № 1. – С. 99–106.

References

1. *Strategiya innovatsionnogo razvitiya Rossiyskoy Federatsii na period do 2020 goda* [Strategy for Innovative Development of the Russian Federation for the period up to 2020]. Available at: https://ac.gov.ru /files/attachment/4843.pdf (accessed 20.02.2022).

2. Irbe, M., Ozolins, M., Nemilentsev, M., Priem, M., Smits, M., Van Der Zouwen, A., Martin, L., et al. Research on Transdisciplinary Entrepreneurship Training. European Entrepreneurship Training Community Reference. Report number: 2018-1-LV01-KA203-046974. 2020. Available at: https://goodpractices.eu/research-results (accessed 20.02.2022).

3. Evstigneeva, E. E., Makhrova, V. Innovatsionnoe razvitie Rossii: strategiya, barery i sposoby ikh preodoleniya [Innovative development of Russia: strategy, barriers and ways to overcome them]. *Molodoy uchenyy* [Young scientist], 2018, no. 22 (208), pp. 399–402. Available at: https://moluch.ru/archive/208/50842/ (accessed 21.02.2022).

4. *Sayt "Startap Laboratoriya"*. Site "Startup Laboratory". Available at: https://startup-lab.ru (accessed 20.02.2022).

5. *Doklad agentstva innovatsiy goroda Moskvy "Razvitie predprinimatelstva vnutri korporatsiy: mezhdunarodnyy opyt i rossiyskaya praktika"* [The Moscow Innovation Agency Report "Development of Entrepreneurship within Corporations: International Experience and Russian Practice], October 2020. Available at: https://innoagency.ru/files/Corporate_entrepreneurship_2020_Moscow_Agency_of_innovations.pdf (accessed 20.02.2022).

6. Ivanov, S. A. Metody morfologicheskogo analiza pri issledovanii slozhnykh sistem [Methods of morphological analysis in the study of complex systems]. *Rol intellektualnogo kapitala v ekonomicheskoy, socialnoy i pravovoy kulture obshchestva XXI veka : tezisy dokladov na mezhdunarodnoy nauchno-prakticheskoy konferentsii* [The role of intellectual capital in the economic, social and legal culture of society in the XXI century : proceedings of the international scientific-practical conference]. St. Petersburg, 2018, pp. 346–348.

7. Ivanov, S. A. Postanovka mnogokriterialnoy zadachi vybora komplektuyushchikh dlya avtomatizirovannoy teplicy [Statement of the multi-criteria problem of choosing components for an automated greenhouse]. *Rol i mesto informatsionnykh tekhnologiy v sovremennoy nauke : sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [The role and place of information technology in modern science : proceedings of the International Scientific-Practical Conference]. Magnitogorsk, 2017, pp. 55–57.

8. Kvyatkovskaya, A. E., Chertina, E. V., Polumordvinova, A. O., Kvyatkovskaya, I. Ju. Informatsionnaya tekhnologiya poiska kompaniy-analogov dlya otsenki stoimosti biznesa, ispolzuyushchaya intellektualnykh agentov [Information technology of searching for analogous companies for assessing the value of a business, using intellectual agents]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Engineering and Informatics], 2019, no. 1, pp. 99–106].

УПРАВЛЕНИЕ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ

УДК 371.39: 37.042

МЕТОДИКА ИНДИВИДУАЛИЗАЦИИ ЦИФРОВОЙ СРЕДЫ НА ОСНОВЕ ДИАГНОСТИКИ ПСИХОЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ ОБУЧАЮЩЕГОСЯ[1]

Статья поступила в редакцию 15.06.2022, в окончательном варианте – 03.08.2022.

Ажмухамедов Искандар Маратович, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

доктор технических наук, декан факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности, ORCID: 0000-0001-9058-123X, e-mail: aim_agtu@mail.ru

Хайтул Анастасия Всеволодовна, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

бакалавр, ORCID: 0000-0003-2112-8145, e-mail: khaaaytul@icloud.com

Статья посвящена описанию методики индивидуализации цифровой среды обучения в рамках разработки индивидуальной образовательной траектории на основе диагностирования психоэмоционального состояния обучающегося. Анализ имеющихся методик определения психоэмоционального состояния позволил сделать вывод о том, что для решения поставленной задачи наиболее подходящим является цветовой тест Люшера. При этом для интерпретации результатов прохождения теста предложено использовать так называемый «вегетативный коэффициент». Далее в соответствии с различными значениями указанного коэффициента, а также с учётом построенного на основе методики «7 радикалов» психологического портрета, подбираются различные наборы тем и практических заданий для изучения и закрепления материала, имеющие различную сложность и трудоёмкость выполнения. Также приведена проектная диаграмма и описана структура разработанного в среде PyCharm программного обеспечения, реализующего предложенную методику. Апробация данного программного продукта преподавателями нескольких общеобразовательных средних учебных заведений, а также его использование при изучении отдельных предметов студентами факультета цифровых технологий и кибербезопасности в Астраханском государственном университете позволили сделать вывод о целесообразности использования предложенной методики и соответствующего программного обеспечения для повышения эффективности процесса обучения.

Ключевые слова: цифровая образовательная среда, психоэмоциональное состояние обучающегося, цветовой тест Люшера, подбор учебного материала

METHODOLOGY FOR INDIVIDUALIZATION OF THE DIGITAL ENVIRONMENT BASED ON DIAGNOSIS OF THE PSYCHO-EMOTIONAL STATE OF THE LEARNER

The article was received by the editorial board on 15.06.2022, in the final version – 03.08.2022.

Azhmukhamedov Iskandar M., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

Doct. Sci. (Engineering), Dean of the Faculty of Digital Technologies and Cybersecurity, Professor of the Department of Information Security, ORCID: 0000-0001-9058-123X, e-mail: aim_agtu@mail.ru

Khaytul Anastasia V., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

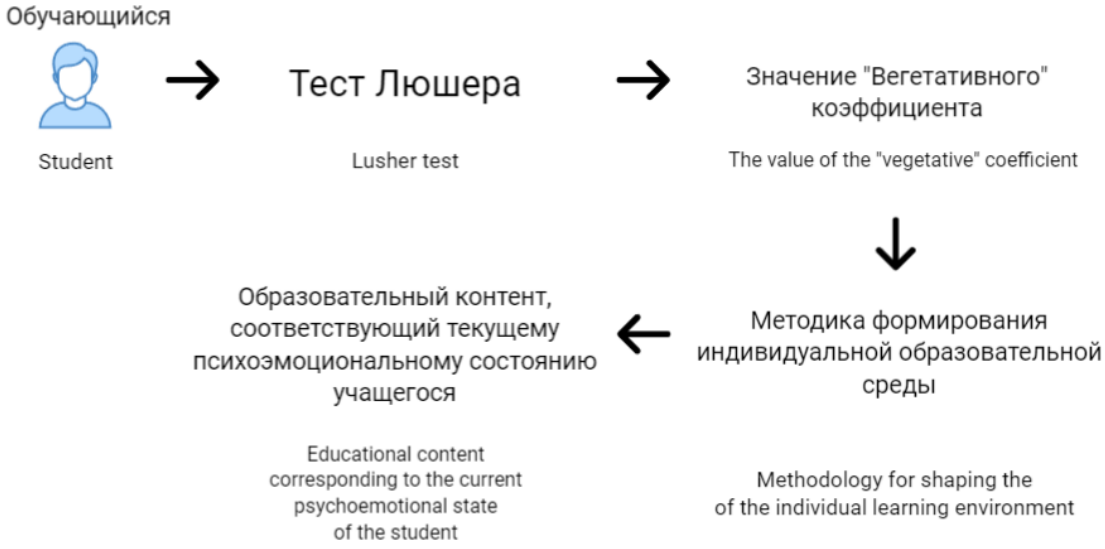
undergraduate student, ORCID: 0000-0003-2112-8145, e-mail: an_khaaaytul@icloud.com

The article is devoted to describing the methodology of individualization of the digital learning environment in the development of an individual educational trajectory based on the diagnosis of psycho-emotional state of the learner. The analysis of the available methods for determining the psycho-emotional state allowed us to conclude that the Lusher color test is the most suitable for solving the task. At the same time, it is proposed to use the so-called "vegetative coefficient" to interpret the test results. Further, in accordance with the different values of this coefficient, as well as considering the psychological portrait based on the "7 radicals" methodology, various sets of topics and practical tasks are selected for studying and fixing the material, having different complexity and complexity of execution. The design diagram is also given and the structure of the software developed in the PyCharm environment implementing the proposed methodology is described. The testing of this software product by teachers of several general secondary educational institutions, as well as its use in the study of individual subjects by students of the Faculty of Digital Technologies and Cybersecurity at Astrakhan State University allowed us to conclude that it is advisable to use the proposed methodology and appropriate software to improve the effectiveness of the learning process.

Keywords: digital educational environment, psychoemotional state of the student, Lusher color test, selection of educational material

[1] Статья выполнена при поддержке гранта РФФИ, проект № 19-29-14007 мк «Оценка влияния цифровизации образовательного и социального пространства на человека и разработка системы безопасной коммуникативно-образовательной среды».

Graphical annotation (Графическая аннотация)



Введение. Несмотря на постоянное совершенствование методов и методик обучения, задача повышения эффективности усвоения учебного материала до сих пор остаётся весьма актуальной. Это связано с резким, лавинообразным увеличением информационного потока, быстрым изменением требований к знаниям и компетенциям, которые необходимо выработать у обучающегося, а также с появлением новых форм обучения (дистанционное обучение с использованием информационно-коммуникационных технологий; самостоятельное изучение материалов, размещенных в среде интернета и т.д.). При этом в процессе обучения необходимо учитывать индивидуальные особенности каждого ученика. Для этого, в свою очередь, необходимо предварительно построить его психологический портрет. Исследованию данного вопроса, в том числе с целью минимизации рисков при использовании дистанционного формата обучения, была посвящена работа [1]. Было предложено построить психологический портрет обучающегося на основе методики В.В. Пономаренко [2]. Однако необходимо учесть, что даже один и тот же человек, находясь в разных психоэмоциональных состояниях, совершенно по-разному способен усваивать учебный материал.

Об этом свидетельствует ряд работ как отечественных [3–6, 8], так и зарубежных [7, 9, 10] исследователей, посвященных проблеме взаимосвязи психоэмоционального состояния человека с его способностью воспринимать и обрабатывать поступающую информацию.

Так, например, для отображения важности влияния настроения на продуктивность человека американские исследователи Нэнси Ротбард из школы менеджмента Wharton и Стеффани Уилк из бизнес-школы Fisher при университете Огайо провели эксперимент, в котором в течение трёх недель 29 сотрудников call-центров из разных городов должны были совершить не менее 64 звонков в день. В течение всего эксперимента исследователи фиксировали настрой сотрудника и его производительность в начале рабочего дня. Эксперимент показал, что испытуемые, пришедшие на работу в хорошем настроении, имели более высокую производительность и больше проводили времени погружаясь в рабочий процесс, в отличие от испытуемых, начавших рабочий день в плохом психоэмоциональном состоянии [6]. Таким образом, эксперимент подтвердил важность учета начального психоэмоционального состояния человека и его вклад в результативность рабочего процесса.

В работе [8] изложены результаты исследования, проведенного с использованием методик А.Б. Леоновой «Методика интегральной диагностики и коррекции стресса (ИДИКС)» и М.П. Мороза «Экспресс-диагностика работоспособности и функционального состояния человека», в котором в качестве респондентов выступили студенты Кисловодского государственного училища олимпийского резерва. В результате проведения исследования был сделан вывод о том, что «чем выше показатели стресса, тем ниже работоспособность спортсменов» [8].

Научные работники Гентского университета в ходе изучения влияния позитивного настроения на широту внимания доказали, что эмоции человека влияют на аналитическую активность его мозга [9]. Учёные выявили, что люди в «приподнятом» настроении проявляют большую концентрацию и лучше обращают внимание на то, что происходит вокруг них. Данные результаты обусловлены связью работы коры головного мозга с деятельностью его лимбической системы.

Американские исследователи из школы медицины Икана Медицинского центра Маунт-Синай провели эксперимент на животных (обезьянах), где устанавливали, каким образом повышенное возбуждение влияет на принятие решений. В ходе работы был сделан вывод о том, что при перевозбужденном состоянии «количество нейронов, участвующих в процессе принятия решений, уменьшалось, в то время как количество нейронов в дорсальной передней поясной коре мозга животных немного увеличивалось. Измененные функции нейронов свидетельствуют о том, что нейронные сигналы, участвующие в принятии решений, блокируются из-за повышенного возбуждения» [10].

Таким образом, можно сделать вывод о том, что способность эффективно воспринимать информацию и находить нужные решения в значительной степени зависит от психоэмоционального состояния (ПЭС), в котором человек находится.

Следовательно, при выстраивании индивидуальной образовательной траектории (ИОТ) обучающегося необходима индивидуализация образовательной среды, учитывающая его текущее психоэмоциональное состояние.

Сравнительный анализ методик определения психоэмоционального состояния. Существует достаточно большой список методик, применение которых позволяет оценить различные аспекты ПЭС человека.

Так, например, методика Л.В. Куликова [11] определяет актуальное психоэмоциональное состояние человека, его доминирующие чувства и то, какую общую оценку даёт испытуемый событиям, происходящим в его субъективном настоящем. Методика предусматривает использование опросника, состоящего из 38 несложных, подразумевающих внимательное прочтение, но не требующих долгого обдумывания вопросов, ответы на которые занимают в среднем около 5–6 минут.

Также широко известен «Личностный опросник» Г.Ю. Айзенка, состоящий из 57 вопросов [12]. Прохождение анкетирования позволяет определить, к какому из темпераментов (холерик, меланхолик, сангвиник, флегматик) ближе всего подходит личность тестируемого. Однако использование данного подхода не даёт возможности судить о текущем психоэмоциональном состоянии испытуемого.

Кроме тестов, основанных на анкетировании, существуют также методики, предусматривающие выбор определенных изображений. Типичным представителем этого класса методик является «Проективный тест Маркерта» [13], в рамках прохождения которого испытуемому необходимо из восьми фигур выбрать сначала наиболее приятную, а после этого выбрать наименее приятную фигуру. Преимущество данного подхода в его простоте и минимальной трудоёмкости. Однако на его основе можно получить лишь очень ограниченный объём информации о ПЭС человека (только информацию о том, что он «спокоен», «раздражён» или «возбужден»).

Ещё одним широко распространённым тестом определения ПЭС является цветовой тест Люшера [14]. При его прохождении испытуемым последовательно предлагается из восьми карточек с разными цветами выбрать карточки от наиболее приятного цвета к наименее приятному. Указанная выборка производится дважды. При этом результаты, полученные на основе анализа первого выбора, свидетельствуют «о желаемом» состоянии, а результаты второй выборки характеризуют текущее «реальное» психоэмоциональное состояние человека. Прохождение теста Люшера не занимает много времени и не требует длительных размышлений. Более того, для правильного прохождения тестирования нужно как можно меньше задумываться о выбираемом ответе и принимать решения на интуитивном уровне. Интерпретация теста Люшера хорошо разработана и функциональна, она позволяет получить обширную детализацию ПЭС испытуемого.

Результаты сравнительного анализа рассмотренных выше методик приведены в таблице 1.

Таблица 1 – Сравнительный анализ методик определения психоэмоционального состояния человека

Название методики	Время прохождения	Степень детализации ПЭС после интерпретации результатов тестирования	Степень применимости для индивидуализации образовательной среды
Определение актуального состояния (Л.В. Куликов)	5–6 минут	Средняя	Средняя
Личностный опросник (Г.Ю. Айзенк)	12–18 минут	Выше среднего	Ниже среднего
Проективный тест Маркерта	1–2 минуты	Ниже среднего	Средняя
Тест Люшера (М. Люшер)	2–3 минуты	Выше среднего	Высокая

Таким образом, исходя из проведенного анализа, был сделан вывод о том, что наиболее подходящим для выявления психоэмоционального состояния обучающегося с целью индивидуализации образовательной среды является тест Люшера.

Формирование индивидуальной образовательной среды на основе ПЭС. Следующей задачей после определения ПЭС является формирование учебно-методического контента, соответствующего психологическому профилю учащегося и его текущему психологическому состоянию.

Вопросы построения психологического профиля и рекомендация по снижению рисков, в частности при использовании ДОТ, были рассмотрены раннее в работах [1, 15].

Для учета же психоэмоционального состояния, установленного с использованием цветового теста Люшера, необходимо прежде всего выбрать наиболее значимые с точки зрения возможностей усвоения предлагаемого учебного материала характеристики из интерпретации результатов прохождения теста. При этом желательно, чтобы указанные характеристики можно было отобразить в одном интегральном критерии, в соответствии которому в дальнейшем можно было бы сопоставить уровень предлагаемых для изучения учебных материалов.

Анализ многочисленных работ, посвященных интерпретации результатов цветового теста Люшера (ЦТЛ), показал, что наиболее подходящим для использования является так называемый «Вегетативный коэффициент», предложенный в работе А.О. Прохорова [16]. Данный коэффициент, по мнению его автора, отражает стремление «к затрате энергии» или «к её сбережению или накоплению».

Для подсчёта значения вегетативного коэффициента (ВК) А.О. Прохоровым на основе большого числа экспериментальных данных была выведена формула 1:

$$\text{ВК} = (18 - \text{К} - \text{Ж}) \ / \ (18 - \text{С} - \text{З}), \tag{1}$$

где *К, Ж, С, З* – порядковые номера цветов (красный, жёлтый, синий, зелёный), выбранные испытуемым на втором этапе тестирования (так как текущее («актуальное») состояние человека отражается результатами второй выборки при прохождении ЦТЛ).

В этой же работе А.О. Прохоров отметил, что при низких значениях вегетативного коэффициента в диапазоне от 0,2 до 0,4 у человека наблюдается: «истощенность, установка на бездействие; хроническое переутомление. В связи с этим характерны пассивность в реагировании на трудности, неготовность к напряжению и адекватным действиям в стрессовых ситуациях». Обозначим такое состояние *S1*.

При значении ВК, находящемся в диапазоне от 0,5 до 0,8 включительно (состояние *S2*), у испытуемого наблюдается «установка на оптимизацию расходования сил, умеренная потребность в восстановлении и отдыхе. Энергетический потенциал невысок, но вполне достаточен для успешной деятельности в привычных спокойных условиях. В экстремальной ситуации вероятно запаздывание с ориентировкой и принятием решений».

В диапазоне вегетативного коэффициента от 0,9 до 1,9 (состояние *S3*) человек ощущает «мобилизованность, установку на активное действие; оптимальную мобилизованность физических и психических ресурсов. В экстремальной ситуации наиболее вероятна высокая скорость ориентировки и принятия решений, целесообразность и успешность действий».

При значениях ВК от 2,0 до 3,2 (состояние *S4*) у тестируемых отмечается «избыточное возбуждение, суетливость, уровень возбуждения избыточно высок. Нередки случаи, когда испытуемый что-либо делает не ради самого дела, а лишь для того, чтобы разрядиться. В сложных ситуациях легко формируются лихорадочные реакции: импульсивность, нетерпеливость, снижение эмоционального самоконтроля, необдуманные поступки. В экстремальных ситуациях наиболее вероятна низкая эффективность действий, панические реакции. Необходимы разноплановые релаксирующие и успокаивающие процедуры» [17].

Таким образом, с ростом ВК работоспособность сначала возрастает, достигая максимума в диапазоне изменения ВК от 0,9 до 1,9 (состояние *S3*), затем она резко снижается (состояние *S4*). Аналогичное поведение описывается вторым законом Йеркса – Додсона (см., например, [18]): по мере увеличения интенсивности мотивации качество деятельности изменяется по колоколообразной кривой: сначала повышается, затем, после перехода через точку наиболее высоких показателей успешности, постепенно снижается.

Для определения степени принадлежности ПЭС испытуемого к одному из значений из термножества $S = \{S1; S2; S3; S4\}$ предлагается ввести в рассмотрение трапецеидальные функции принадлежности μ(ВК) следующим образом:

$$\text{для } S1\text{: } \mu = \begin{cases} 0, \text{при ВК} \le 0{,}2 \\ 1, \text{при } 0{,}2 \le \text{ВК} \le 0{,}4 \\ \frac{0{,}5 - \text{ВК}}{0{,}1}, \ 0{,}4 \le \text{ВК} \le 0{,}5 \\ 0, \text{при } 0{,}5 \le \text{ВК} \end{cases} \tag{2}$$

$$\text{для } S2\text{: } \mu = \begin{cases} 0, \text{при } ВК \le 0{,}5 \\ \frac{ВК-0{,}4}{0{,}1}, \text{при } 0{,}4 \le ВК \le 0{,}5 \\ 1, \text{при } 0{,}5 \le ВК \le 0{,}8 \\ \frac{0{,}9-ВК}{0{,}1}, \ 0{,}8 \le ВК \le 0{,}9 \\ 0, \text{при } 0{,}9 \le ВК \end{cases} \quad (3)$$

$$\text{для } S3\text{: } \mu = \begin{cases} 0, \text{при } ВК \le 0{,}9 \\ \frac{ВК-0{,}8}{0{,}1}, \text{при } 0{,}8 \le ВК \le 0{,}9 \\ 1, \text{при } 0{,}9 < ВК \le 1{,}9 \\ \frac{1{,}9-ВК}{0{,}1}, \ 1{,}9 \le ВК \le 2{,}0 \\ 0, \text{при } 2{,}0 \le ВК \end{cases} \quad (4)$$

$$\text{для } S4\text{: } \mu = \begin{cases} 0, \text{при } ВК \le 1{,}9 \\ \frac{ВК-1{,}9}{0{,}1}, \text{при } 1{,}9 \le ВК \le 2{,}0 \\ 1, \text{при } 2{,}0 \le ВК \le 3{,}2 \\ 0, \text{при } 3{,}2 \le ВК \end{cases} \quad (5)$$

Графическое представление различных состояний приведено на рисунке 1.

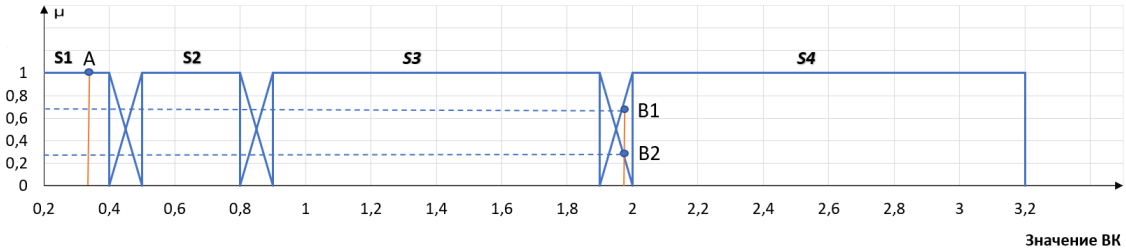


Рисунок 1 – Трапецеидальные функции принадлежности μ(ВК) к различным состояниям из множества S

После вычисления ВК необходимо установить, согласно формулам (2–5), степени принадлежности ПЭС обучающегося к тому или иному состоянию. В дальнейшем их можно интерпретировать как соответствующую долю подходящих по сложности для этого состояния заданий.

Например, если ВК тестируемого равен 0,35, то мы полностью уверены (μ = 1), что его психоэмоциональное состояние соответствует *S1* (точка А на рисунке 1) и обучающемуся необходимо предложить только задания низкого уровня сложности.

Если же, например, значение ВК равно 1,95 (точки В1, В2 на рисунке 1), то степень принадлежности обучающегося к состоянию *S3* равна 0,3, а степень принадлежности к *S4* равна 0,7. В этом случае в состав учебного контента для изучения целесообразно включить 70 % материалов, имеющих низкую степень сложности, с последующим переходом изучения 30 % материалов с высоким уровнем сложности.

Таким образом, для формирования набора индивидуальных учебных заданий для прошедшего ЦТЛ обучающегося необходимо из базы учебных материалов отобрать в необходимых пропорциях такие задания, которые соответствуют текущему ПЭС ученика.

Для этого необходимо, чтобы учебный контент перед его помещением в базу данных был соответствующим образом «маркирован» преподавателем (желательно с участием психолога). Маркировка должна учитывать наличие у обучающегося различных радикалов, полученных ранее при построении его психологического профиля по методике «7 радикалов», и соответствовать различным диапазонам изменения ВК.

Таким образом, задания в базе данных должны храниться в виде кортежа:

$$< Nz;\ Z;\ R1;\ R2;\ F;\ D >, \quad (6)$$

где *Nz* – уникальный номер учебного материала; *Z* – содержимое учебного материла; *F* – форма представления задания, зависящая от значения радикалов; *R1* и *R2* – основные радикалы, при наличии которых обучаемому предлагается задание *Z* в форме *F*; *D* – сложность задания.

Обобщая все вышесказанное, методику формирования индивидуальной образовательной среды можно представить следующим образом:

1. Преподаватель заполняет базу данных учебным контентом по своей дисциплине с указанием элементов, входящих в кортеж 6.

2. Преподаватель регистрирует учащихся в системе и заносит в нее данные, позволяющие с помощью методики «7 радикалов» построить их психологические профили (выявить два основных, «ведущих» радикала *R1* и *R2* в их характерах). Вся информация сохраняется в базе данных «Учащиеся».

3. Обучающийся проходит ЦТЛ, в результате которого по формуле 1 вычисляется ВК.

4. Согласно формулам (2–5) определяется степень принадлежности ПЭС обучающегося к тому или иному состоянию из множества *S*.

5. Система, с учётом ведущих радикалов обучающихся *R1* и *R2*, а также на основании вычисленной в п. 4 степени принадлежности к различным состояниям ПЭС, формирует из базы данных набор соответствующих заданий для изучения учебного материала.

6. Результаты выполнения фиксируются и заносятся в базу данных «Учащиеся».

Разработка программного продукта. Для создания программного обеспечения [19], реализующего предложенную выше методику, были разработаны соответствующие проектные диаграммы. В качестве примера на рисунке 2 приведена так называемая диаграмма вариантов использования (Use Case – диаграмма).

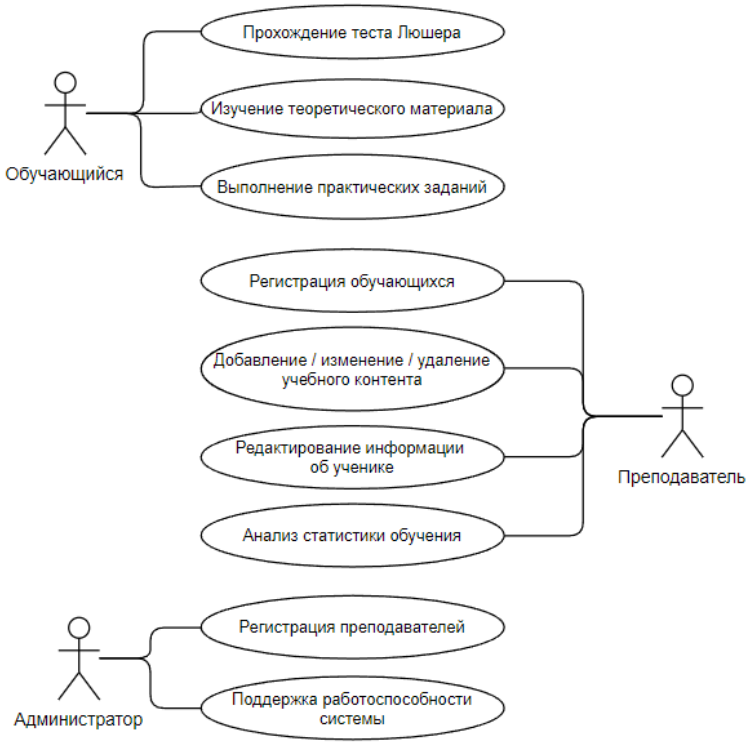


Рисунок 2 – Диаграмма вариантов использования (Use case)

Предусматривается три роли: администратор системы, преподаватель и обучающийся. В таблице 2 приведен их основной функционал.

Таблица 2 – Функционал пользователей ПО

Роль	Функционал
Администратор	Администратор для поддержания работоспособности системы имеет полный контроль над ней: регистрирует преподавателей, имеет доступ к файлам с заданиями и данным учеников и преподавателей.
Преподаватель	Преподаватель имеет возможность регистрировать обучающихся и вводить в систему информацию об их «ведущих» радикалах, просматривать статистику выполненных ими заданий, может добавлять/редактировать и удалять учебный контент.
Обучающийся	Обучающийся проходит цветовой тест Люшера, изучает теоретический материал и выполняет практические задания в соответствии с текущим значением «Вегетативного» коэффициента

Приложение имеет серверную часть, настроенную при помощи программного обеспечения Nginx. Фронтенд разработан на языке Python версии 3.9 с использованием фреймворка Djanga, бэкенд написан в среде PyCharm на языке Python версии 3.9.

Заключение. Предложенная в данной работе методика и реализующее её программное обеспечение прошли апробацию в нескольких средних образовательных учреждениях г. Астрахани и на факультете цифровых технологий и кибербезопасности в Астраханском государственном университете. Апробация показала возможность применения предложенной методики для повышения эффективности конструирования ИОТ, в том числе при использовании дистанционных образовательных технологий.

Накопленные в БД «Учащиеся» данные могут в дальнейшем позволить использовать для более точного подбора заданий метод претендентов. Согласно этому методу при регистрации в системе нового ученика в базе данных находится ученик, наиболее близкий к «новичку» по «ведущим» радикалам и текущему ПЭС, и ему предлагается набор учебных материалов, который был наиболее успешно освоен предыдущим учащимся, профиль которого оказался наиболее близким к «новичку».

Библиографический список

1. Ажмухамедов, И. М. Оценка восприимчивости участника образовательного процесса к рискам цифрового обучения в зависимости от его психологического профиля / И. М. Ажмухамедова, В. Ю. Кузнецова // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 2 (54).

2. Пономаренко, В. В. Практическая характерология. Методика 7 радикалов / В. В. Пономаренко. – Москва : АСТ, 2019. – 224 с.

3. Парыгин, Б. Д. Социальная психология. Проблемы методологии, истории и теории / Б. Д. Парыгин. – Санкт-Петербург : ИГУП, 1999. – 592 с.

4. Поршнев, Б. Ф. Социальная психология и история / Б. Ф. Поршнев ; АН СССР. – Москва : Наука, 1979. – 236 с.

5. Рубинштейн, С. Л. Основы общей психологии / С. Л. Рубинштейн. – Санкт-Петербург : Питер, 2000 – 712 с.: ил. – (Серия «Мастера психологии»).

6. Как настроение влияет на результаты работы. – Режим доступа: https://klerk-ru.turbopages.org /klerk.ru/s/boss/articles/55238/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 24.05.2022).

7. Хайдеггер, М. Бытие и время / М. Хайдеггер ; пер. с нем. В. В. Бибихина. – Харьков : Фолио, 2003. – 503, [9] с. – (Philosophy).

8. Гавриков, В. А. Изучение взаимосвязей работоспособности и характеристик психоэмоционального стресса у студентов-спортсменов / В. А. Гавриков, О. Н. Боровик // Достижения вузовской науки. – 2014. – № 9. – С. 76–79. – EDN SAWNLZ.

9. Grol, Maud. Effects of positive mood on attentional breadth for emotional stimuli / Grol Maud and Rudi De Raedt // FRONTIERS IN PSYCHOLOGY 5. – 2014. – DOI: 10.3389 / fpsyg.2014.01277.

10. Телесное возбуждение влияет на процесс принятия решений. – Режим доступа: https://fb.ru/post/stress-management/2021/9/3/326558, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.05.2022).

11. Методика: Доминирующие состояния (ДС-8) (Л.В. Куликов). – Режим доступа: https://www.sites.google.com/site/test300m/ds8, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.05.2022).

12. Личностный опросник EPI (методика Г.Айзенка) // Альманах психологических тестов. – М., 1995. – С. 217–224.

13. Проективный тест Маркерта. – Режим доступа: https://pandia.org/text/80/285/1317.php, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.05.2022).

14. Тест Люшера — описание и интерпретация. Режим доступа: http://pfmethod.psy.spbu.ru/Praktikum/lusher.htm, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 26.05.2022).

15. Ажмухамедов, И. М. Программный продукт для управления рисками при использовании цифровой образовательной среды / И. М. Ажмухамедова, В. Ю. Кузнецова, А. В. Станишевская // Прикаспийский журнал: управление и высокие технологии. – 2021. – №3 (55).

16. Методики диагностики и измерения психических состояний личности / автор и составитель А. О. Прохоров. – Москва : ПЕР СЭ, 2004. – 176 с.

17. Математика Люшера. – Режим доступа: http://monatkodenis.blogspot.com/2018/08/luscher.html?m=1, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.05.2022).

18. Горбатков, А. А. Закон Йеркса-Додсона: проблема содержания переменных / А. А. Горбатков // Вопросы психологии. – 2009. – Т. 2. – С. 63–81.

19. Ажмухамедов, И. М. Диагностика психоэмоционального состояния обучающегося для индивидуализации цифровой среды обучения : свидетельство о регистрации программы для ЭВМ RU 2022660740, 08.06.2022. – Заявка № 2022619786 от 27.05.2022 / И. М. Ажмухамедов, Т.М. Ишкин, А. В. Станишевская, А. В. Хайтул.

References

1. Azhmuhamedov, I. M., Kuznetsova, V. Ju. Otsenka vospriimchivosti uchastnika obrazovatelnogo protsessa k riskam tsifrovogo obucheniya v zavisimosti ot ego psihologicheskogo profilya [Assessment of the susceptibility

of a participant in the educational process to the risks of digital learning depending on his psychological profile]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2021, no. 2 (54).

2. Ponomarenko, V. V. *Prakticheskaya kharakterologija. Metodika 7 radikalov* [Practical characterology. Method of 7 radicals]. Moscow, AST Publ., 2019. 224 p.

3. Parygin, B. D. *Sotsialnaya psikhologiya. Problemy metodologii, istorii i teorii* [Social psychology. Problems of methodology, history and theory]. Saint Petersburg, IGUP, 1999. 592 p.

4. Porshnev, B. F. *Sotsialnaya psikhologiya i istoriya* [Social psychology and history]. Moscow, Nauka Publ., 1979. 236 p.

5. Rubinshteyn, S. L. *Osnovy obshchey psikhologii* [Fundamentals of general psychology]. Saint Petersburg, Piter Publ., 2000. 712 p.: il. (Seriya «Mastera psikhologii»).

6. *Kak nastroenie vliyaet na rezultaty raboty* [How mood affects the results of work]. Available at: https://klerk-ru.turbopages.org/klerk.ru/s/boss/articles/55238/ (accessed 24.05.2022).

7. Khaydegger, M. Bytie i vremya [Being and time]; transl. from German V. V. Bibikhina. Kharkov, Folio Publ., 2003. 503 [9] p. (Philosophy).

8. Gavrikov, V. A., Borovik, O. N. Izuchenie vzaimosvyazey rabotosposobnosti i kharakteristik psikhoemotsionalnogo stressa u studentov-sportsmenov [Studying the relationship of working capacity and characteristics of psycho-emotional stress in student-athletes]. *Dostizheniya vuzovskoy nauki* [Achievements of high school science], 2014, no. 9, pp. 76–79. EDN SAWNLZ.

9. Grol Maud and Rudi De Raedt. 2014. Effects of positive mood on attentional breadth for emotional stimuli. *Frontiers in psychology 5.* DOI: 10.3389 / fpsyg.2014.01277.

10. *Telesnoe vozbuzhdenie vliyaet na protsess prinyatiya resheniy* [Bodily arousal affects the decision-making process]. Available at: https://fb.ru/post/stress-management/2021/9/3/326558 (accessed 26.05.2022).

11. *Metodika: Dominiruyushchie sostoyaniya (DS-8) (L.V. Kulikov)* [Methodology: Dominant states (DS-8) (L.V. Kulikov)]. Available at: https://www.sites.google.com/site/test300m/ds8 (accessed 26.05.2022).

12. Lichnostnyy oprosnik EPI (metodika G. Ayzenka) EPI Personality Questionnaire (G. Eysenck's method). *Almanakh psikhologicheskikh* testov [Almanac of psychological tests]. Moscow, 1995, pp. 217–224.

13. *Proektivnyy test Markerta* [Markert's projective test]. Available at: https://pandia.org/text/80/285/1317.php (accessed 26.05.2022).

14. *Test Lyushera – opisanie i interpretatsiya* [Luscher test – description and interpretation]. Available at: http://pfmethod.psy.spbu.ru/Praktikum/lusher.htm (accessed 26.05.2022).

15. Azhmuhamedov, I. M., Kuznetsova, V. Ju., Stanishevskaya A. V. Programmnyy produkt dlya upravleniya riskami pri ispolzovanii tsifrovoy obrazovatelnoy sredy [Software product for risk management when using a digital educational environment]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2021, no. 3 (55).

16. Prokhorov, A. O. *Metodiki diagnostiki i izmereniya psikhicheskikh sostoyaniy lichnosti* [Methods for diagnosing and measuring the mental states of a person]. Moscow, PER SE Publ., 2004. 176 p.

17. *Matematika Lyushera* [Luscher's Mathematics]. Available at: http://monatkodenis.blogspot.com/2018 /08/luscher.html?m=1 (accessed 21.05.2022).

18. Gorbatkov, A. A. Zakon Jerksa-Dodsona: problema soderzhaniya peremennykh [The Yerkes-Dodson law: the problem of the content of variables]. *Voprosy psikhologii* [Problems of psychology], 2009, vol. 2, pp. 63–81.

19. Azhmukhamedov, I. M., Ishkin, T. M., Stanishevskaja, A. V., Haytul A. V. *Diagnostika psikhoemotsionalnogo sostoyaniya obuchayushchegosya dlya individualizatsii tsifrovoy sredy obucheniya : svidetelstvo o registratsii programmy dlya EVM RU 2022660740* [Diagnostics of the psycho-emotional state of a student for the individualization of the digital learning environment : certificate of registration of a computer program RU 2022660740], 08.06.2022. Application no. 2022619786 dated 27.05.2022.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ,
ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

DOI 10.54398/20741707_2022_3_25
УДК 004.896

МЕТОД РАСПРЕДЕЛЕНИЯ И ПЛАНИРОВАНИЯ ВЫПОЛНЕНИЯ ЗАДАЧ АГЕНТАМИ РОЕВЫХ РОБОТОТЕХНИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ НЕДЕТЕРМИНИРОВАННОЙ СРЕДЫ[1]

Статья поступила в редакцию 10.08.2022, в окончательном варианте – 10.08.2022.

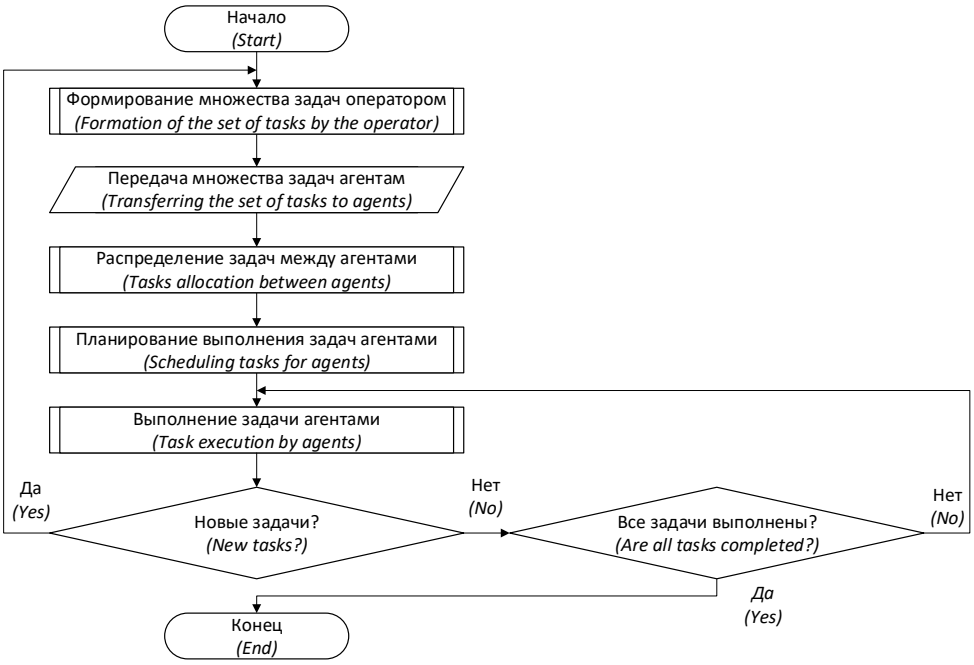
Петренко Вячеслав Иванович, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
кандидат технических наук, заведующий кафедрой, ORCID: 0000-0003-4293-7013, e-mail: vipetrenko@ncfu.ru
Тебуева Фариза Биляловна, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
доктор физико-математических наук, заведующий кафедрой, ORCID: 0000-0002-7373-4692, e-mail: fbtebueva@ncfu.ru
Павлов Андрей Сергеевич, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
старший преподаватель, ORCID: 0000-0002-8413-8706, e-mail: losde5530@gmail.com
Гурчинский Михаил Михайлович, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
аспирант, ORCID: 0000-0002-1739-2624, e-mail: gurcmikhail@gmail.com

Применение роевых робототехнических систем в условиях недетерминированной среды актуализирует вопросы разработки соответствующих методов и алгоритмов распределения и планирования выполнения задач. Под условиями недетерминированной среды в работе понимается такая ситуация, когда максимальное количество задач лимитировано, а сразу после выполнения первой из них появляется новая задача, то есть происходит динамическое изменение списка задач в процессе функционирования роевых робототехнических систем. При функционировании роевых робототехнических систем в условиях недетерминированной среды существующие методы и алгоритмы не позволяют оптимально распределить задачи между всеми роботами системы и запланировать последовательность выполнения задач, закрепленных за каждым из роботов. Помимо этого, известные методы распределения и планирования задач не учитывают ограничения сенсорных и вычислительных возможностей робототехнических устройств, используемых в составе роевых робототехнических систем (например, малый объем оперативной памяти, низкая тактовая частота процессора, малая емкость аккумуляторной батареи, низкая производительность бортовых датчиков и сенсоров и т.д.). Также стоит отметить, что не все известные методы, направленные на решение указанной задачи, учитывают специфику децентрализованного управления роевыми робототехническими системами, заключающуюся в ограниченной области видимости, в результате чего их применение в реальных сценариях использования роевых робототехнических систем сопряжено со значительными проблемами. Целью работы является повышение эффективности распределения и планирования выполнения задач в роевых робототехнических системах в условиях недетерминированной среды с учетом ограниченных возможностей элементов роевых робототехнических систем и специфики децентрализованного управления. Решение задачи выполнено с использованием методов системного анализа, аналитической геометрии и искусственных нейронных сетей. Элементом научной новизны являются предложенные алгоритмы сортировки задач и поиска транзитных задач, обеспечивающие повышение эффективности планирования и распределения задач в роевых робототехнических системах в условиях недетерминированной среды с учетом ограниченных возможностей элементов роевых робототехнических систем. Предложенный метод отличается от известных методов алгоритмом сортировки приоритета выполнения задач в виде связного списка, что дает возможность осуществлять масштабирование численности агентов роевых робототехнических систем при динамическом изменении списка актуальных задач. Еще одним отличием является процедура распределения задач между агентами роевых робототехнических систем, позволяющая искать промежуточные задачи для выполнения, что обеспечивает уменьшение общего времени выполнения задач по сравнению с аналогичными решениями. На основе предложенного метода в работе представлена нейросетевая модификация этого метода, отличающаяся учетом специфики децентрализованного управления. Представленное решение программно реализовано на языке Python и может быть использовано при моделировании децентрализованных систем управления роевых робототехнических системами.

Ключевые слова: роевые робототехнические системы, распределение задач, планирование последовательности выполнения задач, искусственные нейронные сети

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90026.

Графическая аннотация (Graphical annotation)



METHOD FOR TASKS ALLOCATION AND PLANNING THE SEQUENCE OF PERFORMING TASKS BY AGENTS OF SWARM ROBOTIC SYSTEMS UNDER UNCERTAINTY

The article was received by the editorial board on 10.08.2022, in the final version – 10.08.2022.

Petrenko Vyacheslav I., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

Cand. Sci. (Engineering), Head of Department, ORCID: 0000-0003-4293-7013, e-mail: vipetrenko@ncfu.ru

Tebueva Fariza B., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

Doct. Sci. (Physics and Mathematics), Head of Department, ORCID: 0000-0002-7373-4692, e-mail: fbtebueva@ncfu.ru

Pavlov Andrey S., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

Senior Lecturer, ORCID: 0000-0002-8413-8706, e-mail: losde5530@gmail.com

Gurchinskiy Mikhail M., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

postgraduate student, ORCID: 0000-0002-1739-2624, e-mail: gurcmikhail@gmail.com

The use of swarm robotic systems in a non-deterministic environment actualizes the issues of developing appropriate methods and algorithms for distributing and scheduling tasks. Under the conditions of a non-deterministic environment, we mean such a situation when the maximum number of tasks is limited, and immediately after the first task is completed, a new task appears, that is, the list of tasks changes dynamically during the operation of the swarm robotic systems. When swarm robotic systems operate in a non-deterministic environment, the existing methods and algorithms do not allow optimal distribution of tasks between all robots of the system and plan the sequence of tasks assigned to each of the robots. In addition, the known methods of task distribution and scheduling do not take into account the limitations of the sensory and computing capabilities of robotic devices used in the swarm robotic systems (for example, a small amount of RAM, low processor clock frequency, low battery capacity, low performance of onboard sensors and sensors, etc.). It is also worth noting that not all known methods aimed at solving this problem take into account the specifics of the decentralized control of swarm robotic systems, which consists in a limited scope, because of which their use in real scenarios of using swarm robotic systems is associated with significant problems. The aim of the work is to increase the efficiency of distribution and planning of tasks in the swarm robotic systems in a non-deterministic environment, taking into account the limited capabilities of the elements of the swarm robotic systems and the specifics of decentralized control. The problem was solved using the methods of system analysis, analytical geometry and artificial neural networks. An element of scientific novelty is the proposed algorithms for sorting tasks and searching for transit tasks, which provide an increase in the efficiency of planning and distribution of tasks in swarm robotic systems

in a non-deterministic environment, taking into account the limited capabilities of swarm robotic systems elements. The proposed method differs from the known methods by the sorting algorithm of task execution priority in the form of a linked list, which makes it possible to scale the number of swarm robotic systems agents with a dynamic change in the list of urgent tasks. Another difference is the procedure for distributing tasks between swarm robotic systems agents, which makes it possible to search for intermediate tasks to be performed, which reduces the total task execution time compared to similar solutions. Based on the proposed method, the paper presents a neural network modification of this method, which differs by taking into account the specifics of decentralized control. The presented solution is programmatically implemented in Python and can be used in modeling decentralized control systems of swarm robotic systems.

Keywords: swarm robotic systems, task allocation, task scheduling, artificial neural networks

Введение. В настоящее время в групповой робототехнике доминируют системы управления, построенные по принципу централизованной стратегии управления [1]. Данная стратегия предполагает, что каждому роботу (далее «агенту») центральное вычислительное устройство назначает задачи, а также в каждый дискретный момент времени формирует управляющее воздействие для исполнительных устройств агента. Типичным примером приложения групповой робототехники, в том числе роевых робототехнических систем (РРТС), является автоматизированный склад. Схематическое представление централизованной системы управления РРТС представлено на рисунке 1.

Достоинством централизованных систем управления является высокая эффективность выполнения задач агентами при их ограниченном количестве, а также при функционировании в строго детерминированной среде. Однако увеличение численности используемых агентов РРТС требует увеличения ресурсов каналов связи, что уменьшает эффективность выполнения задач. Также стоит отметить, что масштабирование существующей системы управления требует привлечения дополнительных вычислительных ресурсов, способных обеспечить требуемый объем расчетов для поддержания возможности формирования управляющих инструкций для каждого агента в режиме реального времени.

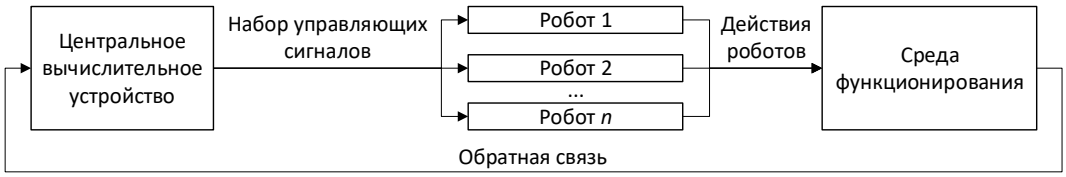


Рисунок 1 – Схема централизованной стратегии управления

Представленные недостатки централизованных систем управления группой роботов привели к переходу исследователей и разработчиков к частичному или полному автономному управлению. Ярким примером такого перехода является автоматизированный склад компании Alibaba, Китай [2]. В основу системы управления агентами положена смешанная стратегия управления, включающая в себя элементы децентрализации. Так, часть функционала системы управления выполняется на центральном вычислительном устройстве, например, формирование списка актуальных задач, мониторинг выполнения задач и т.д. Другая часть функционала системы управления переносится на вычислительные устройства агентов, например, распределение задач, планирование пути и траектории движения и т.д. Представленный подход существенно уменьшает нагрузку на каналы связи, а также позволяет распределить вычисления между всеми узлами системы. Схематическое представление смешанной системы управления представлено на рисунке 2.

Рисунок 2 – Схема смешанной стратегии управления

Одной из сложнейших задач в смешанных и децентрализованных системах управления является оптимальное распределение задач между всеми агентами системы [3–6]. Большинство известных методов и алгоритмов распределения задач предназначены для использования в детерминированной среде с ограниченным количеством задач. В рассмотренном примере автоматизированного склада Alibaba среда функционирования агентов является недетерминированной, так как одновременно функционирует множество агентов и людей, а список задач изменяется динамически в процессе функционирования РРТС.

В данных условиях интенсификация исследований в области решения задачи распределения задач позволит увеличить эффективность выполнения задач по транспортировке груза агентами в недетерминированной среде с учетом таких показателей эффективности, как время выполнения задачи, длина пути, энергоэффективность, функциональная безопасность и т.д. Дополнительно стоит отметить необходимость разработки таких решений, которые позволят не только оптимальным образом распределить актуальные задачи между агентами, но и оптимизировать последовательность их выполнения.

Таким образом, наблюдается противоречие в науке и практике, которое заключается в необходимости комплексного подхода для повышения эффективности функционирования робототехнической системы с одной стороны и недостаточным уровнем развития научно-методического аппарата распределения и планирования задач с другой стороны, чем и определяется актуальность исследований в данной области.

Социально-экономический эффект от решения представленной задачи состоит в том, что оптимальное распределение и планирование выполнения задач группой роботов позволит увеличить количество транспортировок посылок за один цикл работы от аккумуляторной батареи робота путем уменьшения суммарного пройденного расстояния каждым роботом системы.

С точки зрения автоматизированного склада решение рассмотренной задачи позволит снизить экономические издержки за счет следующих аспектов:

- отсутствие необходимости в покупке и обслуживании высокопроизводительных средств связи и центральных вычислительных устройств для управления робототехнической системой;
- увеличение объема выполненной работы при сохранении уровня издержек на обслуживание и ремонт робототехнических устройств и их компонентов.

1. Актуальное состояние проблемы. Анализ работ в области распределения задач позволяет говорить о большом многообразии теоретических методов распределения задач, особенно при равном количестве агентов и подзадач. Среди множества методов можно выделить эвристические алгоритмы [7], аналитические алгоритмы [8], алгоритмы на основе моделей рыночной экономики [9, 10], методы на основе потенциальных полей [11, 12], вероятностные алгоритмы [13, 14], методы на основе машинного обучения и искусственных нейронных сетей [15, 16], методы нечеткой логики [17], муравьиные алгоритмы [18, 19], методы динамического и целочисленного программирования [20, 21], генетические алгоритмы [22], смешанные алгоритмы [23].

В работе [24] представлен централизованный алгоритм распределения задач между агентами РРТС с целью автоматизации логистических работ на автоматизированном складе. Основной упор авторы сделали на обеспечении возможности масштабируемости количества задач, исходя из чего, в работе предложен эвристический обобщенный алгоритм, включающий в себя алгоритмы кластеризации и маршрутизации (планирования пути). Аналогичный подход применили авторы работы [25], но для децентрализованного распределения задач. В работе [26] рассматривается задача распределения задач при транспортировке объектов в автоматизированном складе. Авторы предложили централизованный эвристический алгоритм, позволяющий оптимизировать как длину траектории движения агентов, так и время их перемещения с учетом возможных коллизий (столкновений) с другими агентами. Недостатком данного алгоритма является необходимость наличия центрального устройства, на котором осуществляются все расчеты по распределению задач, а также устойчивый канал связи между всеми агентами и центральным вычислительным устройством, что не всегда можно обеспечить в реальных условиях. В работе [27] представлен модифицированный алгоритм распределения задач на основе алгоритма пчелиной колонии [28], предназначенный для минимизации времени выполнения задания в условиях отсутствия информации о задачах. Основным недостатком данного алгоритма является допущение авторов о стационарности агентов, из-за чего его применение без дальнейшей модификации существенно ограничено.

Методом-аналогом можно считать работу [29], в которой предложен эвристический метод планирования выполнения задач по принципу минимизации штрафа за просроченное выполнение задач. В основе принципа минимизации штрафа лежит идея разделения множества задач на два подмножества: первое подмножество включает те задачи, которые могут быть назначены одному из агентов РРТС и выполнены в срок. Во второе подмножество задач входят все те задачи, которые не удовлетворяют данному условию, то есть результат их выполнения неизбежно приведет к получению штрафа. Данный метод состоит из двух этапов. На первом этапе выполняется распределение первого подмножества задач между всеми агентами системы по критерию минимального остатка времени до дедлайна (метка времени, до которой задача должна быть выполнена без получения штрафа). Вторым этапом является оценка штрафа для каждой задачи второго подмножества (формула (8) оригинальной работы) и назначение приоритета этой задачи. Далее на основе рассчитанных приоритетов задач они назначаются агентам системы для выполнения. Таким образом, в результате

распределения и планирования задач каждый агент имеет список закрепленных за ним задач в виде очереди, то есть первая закрепленная задача будет выполнена первой.

Необходимо отметить, что данный метод предназначен для централизованных систем, то есть все вычисления и назначение списка задач агентам выполняются на центральном вычислительном устройстве. Данный факт делает неприменимым этот метод для РРТС в классическом его понимании [30], либо требует модификации метода путем добавления элементов децентрализации. С другой стороны, авторами оригинальной работы упоминается, что в результате выполнения второго этапа метода один или несколько агентов могут быть «перегружены», то есть время выполнения списка закрепленных за такими агентами задач существенно больше среднего времени выполнения списка задач другими агентами. Описанная ситуация требует дополнительного перераспределения задач между агентами, в результате чего может быть получена неоптимальная последовательность выполнения задач по одному из критериев оценки эффективности функционирования РРТС.

Исходя из проведенного обзора, повышение эффективности распределения задач в РРТС в условиях недетерминированной среды является актуальной и своевременной задачей.

2. Постановка задачи. Дано: РРТС численностью n агентов r_i, $R = r_1, r_2, \dots, r_n$; O – множество, содержащее m элементарных задач m (далее просто «задач»), $O = o_1, o_2, \dots, o_m$; Y – множество выходных параметров (количество выполненных задач агентами РРТС); Z – множество внутренних параметров РРТС (текущая позиция, заряд батареи, скорость, ускорение и т.д.); E – множество параметров среды; Q – множество показателей качества функционирования РРТС, например, время выполнения множества задач O, длина пути, пройденная агентами, суммарный расход аккумуляторной батареи агентов и т.д.

Целью данной работы является повышение эффективности планирования задач в РРТС в условиях неполноты информации о задании с учетом ограниченных возможностей элементов РРТС и специфики децентрализованного управления. Содержательная (вербальная) постановка научной задачи: разработать метод M повышения качества/эффективности функционирования РРТС R по показателям $q_1, \dots, q_k$ в диапазоне значений входных и выходных параметров (T, Y) системы за счет варьирования значений ее внутренних параметров Z и при ограничениях на значения параметров среды $E \subseteq E_{доп}$. Формальная постановка научной задачи: найти метод M такой(-ую), что

$$M : \langle R, T, Y, Z, E, Q \rangle \rightarrow \{\Delta q_1, \dots, \Delta q_k\} \mid \forall \Delta q_i > 0,\ q_i \in Q,\ i = \overline{1,k}, \quad (1)$$

при этом $\Delta q_i = q_i^{п} - q_i^{д}$, $i = \overline{1,k}$, где индекс «д» значит «до использования метода», индекс «п» – «после использования метода».

3. Методы и материалы. Каждая задача $o_j \in O, j = \overline{1,m}$ представляет собой вектор $\left[x_j, y_j, \widehat{x_j}, \widehat{y_j}, t_j, f_j\right]$, где x_j, y_j – координаты задачи o_j; $\widehat{x_j}, \widehat{y_j}$ – координаты места, куда необходимо транспортировать груз; t_j – метка времени, к которой задача должна быть выполнена (дедлайн); f_j – коэффициент для расчета штрафа за выполнение задачи после дедлайна. Значение штрафа F_j за невыполнение задачи в срок может быть вычислено следующим образом:

$$F_j = \left(c_j - t_j\right) f_j, \quad (2)$$

где c_j – время завершения выполнения задачи o_j. Соответственно, агенты РРТС получат штраф только в том случае, если задача o_j будет выполнена после дедлайна, то есть $c_j > t_j$.

В качестве среды функционирования РРТС рассматривается автоматизированный склад. На рисунке 3 представлен пример среды для проведения последующих экспериментов с 5 задачами. Цветные круги определяют исходные позиции задач, а крестики – позиции, в которые необходимо переместить товар в рамках выполнения задачи. Вся карта разделена на ряд областей:

- область получения товаров (ПТ). Предполагается, что здесь осуществляется разгрузка и прием товаров, а также их первоначальное размещение на стеллажах;
- область сортировки товаров (СТ). Эта область содержит ряды со стеллажами, на которых размещены товары;
- область комплектации заказов (КЗ). В данной области оператор собирает заказ, поочередно собирая нужные товары со стеллажей;
- область отгрузки заказов (ОЗ). В эту область осуществляется перемещение уже собранных заказов для дальнейшей их передачи курьерской службе.

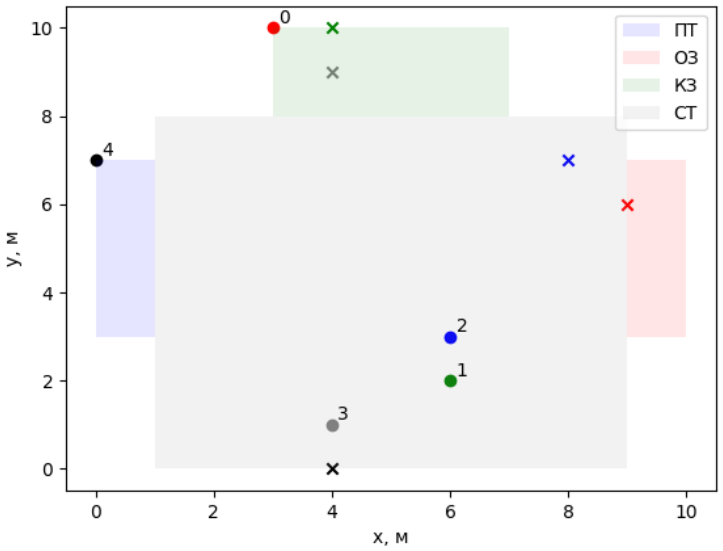


Рисунок 3 – Пример исходных данных для проведения эксперимента

В каждой из представленных областей положения стеллажей являются фиксированными, так как в противном случае проезд агента со стеллажом может быть перекрыт. Исходя из этого, начальные и конечные координаты задач также являются детерминированными (пример разметки автоматизированного склада представлен на рисунке 4).

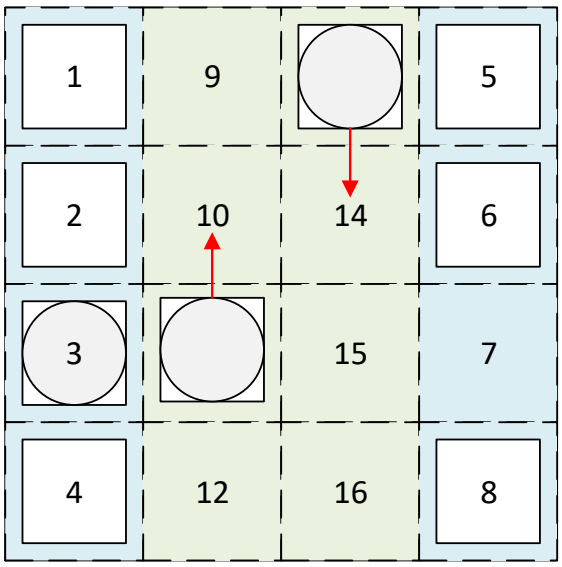


Рисунок 4 – Пример разметки автоматизированного склада

На рисунке 4 представлен пример организации расположения стеллажей (клетки 1–8 голубого цвета) для хранения продукции и дорожек для перемещения агентов (клетки 9–16 зеленого цвета). Подобные обозначения позиций для размещения стеллажей могут использоваться при оборудовании штрих-кодами, RFID-метками и т.д. для идентификации нужной позиции стеллажа. Движение агентов может быть организовано двухполосным (красными стрелками показано направление движения агентов), для того чтобы не создавать заторы, а агенты имели достаточно места для маневра при захвате и отгрузке стеллажей. Также стоит отметить, что если некоторый агент не функционирует, например, на момент его запуска, то его позиция также является строго детерминированной (специально выделенные позиции для зарядных станций, пункта обслуживания и ремонта и т.д.). Таким образом, всю карту автоматизированного склада можно представить в виде поля, разбитого на клетки, где совокупность этих клеток представляет собой множество P, содержащее как позиции задач $p_j = x_j, y_j, j = \overline{1, m}$, так и m' позиций перемещения агентов РРТС $p_r = x_r, y_r, r = \overline{m+1, m'}$ (приведенные координаты x_j, y_j и x_r, y_r являются координатами центров клеток).

3.1. Аналитический метод планирования последовательности выполнения задач агентами РРСТ. В работе [29] предложен централизованный метод планирования выполнения задач на основе итерационного эвристического алгоритма. Однако применение этого метода невозможно в случае гибридной архитектуры системы управления автоматизированного склада, что требует модификации этого решения путем внедрения элементов децентрализации. Помимо этого, как отмечалось ранее, один или несколько агентов РРТС в результате распределения задач могут быть «перегружены». Такая ситуация, с одной стороны, требует непрерывного мониторинга результатов распределения задач на центральном вычислительном устройстве, а с другой стороны, вызывает необходимость повторения процедуры распределения и планирования выполнения задач. Аналогичная ситуация возникает и в том случае, если происходит увеличение численности агентов – для каждого нового агента системы потребуется перераспределение задач, что может занимать достаточно времени, особенно при значительном количестве новых агентов.

Исходя из этого, в данной работе предлагается идея разработки итерационного алгоритма для планирования ограниченного количества задач (не более двух для каждого агента). Аналогично методу-аналогу предлагаемый метод может быть разделен на два этапа: первый предполагает предобработку исходного множества задач, а второй – распределение задач между агентами.

3.1.1. Алгоритм предобработки исходного множества задач. Согласно вышеописанной идее работы, последовательность задач, закрепленных за агентом r_i, должна состоять не более чем из 2 задач. Процедуру попарного планирования задач предлагается реализовать по аналогии со связным списком, т.е. текущий элемент списка явно указывает на следующий. Для этого сначала предлагается осуществить на стороне центрального вычислительного устройства предобработку списка задач путем их сортировки по возрастанию по значению дедлайна t_j. Т.е. необходимо выполнить перестановку элементов множества O в таком порядке, при котором для заданной функции упорядочения S справедливо соотношение:

$$S(t_1) \le S(t_2) \le \cdots \le S(t_m). \quad (3)$$

В результате выполнения сортировки будет сформирован список L, в самом начале которого расположен ряд задач, которые должны быть выполнены в первую очередь. С учетом того, что количество агентов РРТС n ограничено, то первые n задач списка L могут быть распределены между агентами РРТС таким образом, чтобы минимизировать значение штрафа за просроченное выполнение задач или избежать его совсем. Назовем первые n задач списка L «горящими».

Следующим шагом предобработки списка задач является поиск для каждой задачи o_j списка L ближайшей задачи в геометрическом пространстве и добавление ее в качестве «указателя» o_j^{ptr} к задаче o_j. При этом в качестве указателя o_j^{ptr} могут рассматриваться только те задачи, которые располагаются в списке L после задачи o_j, для того, чтобы соблюдать порядок выполнения задач в соответствии с их дедлайнами:

$$\forall o_j : \min\left(D\left(o_j, o_l\right)\right) \Rightarrow o_j^{ptr} = o_l;\ l = \overline{j+1, m}; j = \overline{1, m}, \quad (4)$$

где $D\left(o_j, o_l\right)$ – функция вычисления расстояния между двумя задачами.

Таким образом, список задач L преобразуется в связный список, в результате чего каждый агент r_i при распределении задач будет выбирать только одну горящую задачу. А после ее выполнения – перейдет к выполнению задачи-указателя. Согласно выражению (4), последняя задача o_m списка L не будет иметь указателя, что должно быть предусмотрено на следующем этапе предлагаемого метода. После того как связный список L сформирован, оператор передает его по каналу связи агентам РРТС для дальнейшего распределения задач.

Блок-схема этапа предобработки списка задач представлена на рисунке 5.

Таким образом, отличием первого этапа предложенного метода от метода-аналога является то, что:

- выполняется обработка только исходного множества задач без их распределения между агентами со стороны центрального вычислительного устройства;
- обработка исходного множества задач предполагает не только их сортировку в порядке возрастания по дедлайну, но и формирование связного списка по принципу геометрической близости задач;
- при необходимости предложенная реализация вычисления близости задач может включать в себя множество критериев, которые позволят достигнуть требуемых значений показателей эффективности функционирования РРТС.

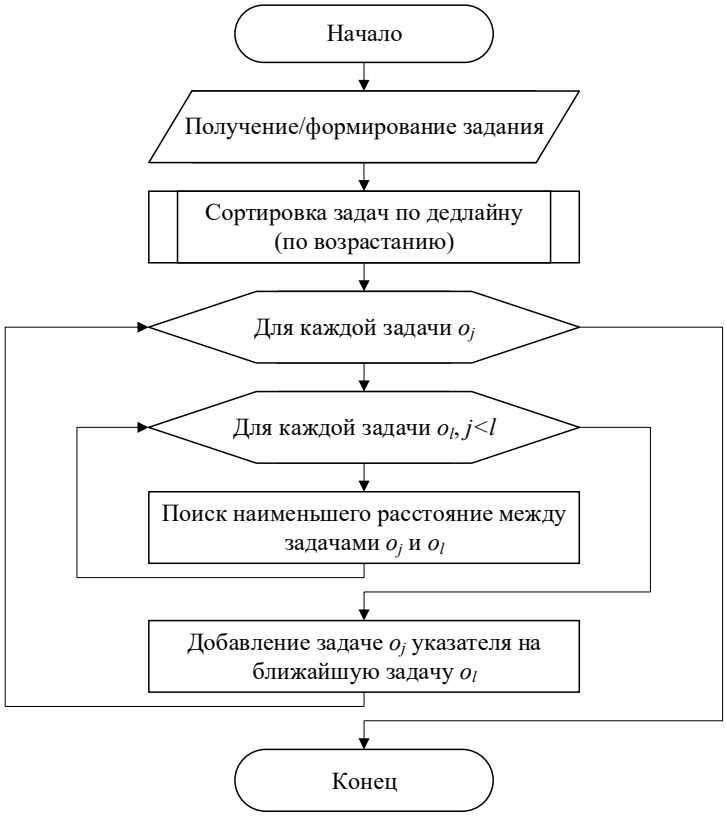


Рисунок 5 – Блок-схема этапа предобработки исходного множества задач

3.1.2. Алгоритм распределения и планирования последовательности выполнения задач агентами PPTC. Распределение задач между агентами предлагается реализовать на основе жадного алгоритма [31]. Каждый агент r_i выбирает для выполнения такую горящую задачу o_j, которая находится ближе всего к агенту. Необходимо отметить, что этап распределения задач выполняется децентрализовано, и соответственно, после выбора той или иной задачи каждый агент должен оповестить соседних агентов о том, что эта задача уже занята. Информацию о занятой задаче агенты заносят в собственную память для того, чтобы в последующем не возникало коллизий (выбор одной и той же задачи несколькими агентами).

После выполнения горящей задачи каждый агент оповещает других агентов о завершении текущей задачи. Соответственно, после этого агент готов приступить к выполнению задачи-указателя. Однако необходимо отметить следующую особенность. На этапе предобработки списка задач предполагалось, что задачей-указателем может быть только самая ближайшая задача. При этом дедлайн задачи-указателя t_j^{ptr} может быть настолько велик, что целесообразно отложить выполнение этой задачи, если поблизости есть невыполненные задачи с меньшим дедлайном, чем у задачи-указателя. Таким образом, в работе предлагается использование термина «транзитная» задача для любых задач, которые могут быть выполнены «по пути» к выполнению задачи-указателя без получения штрафа агентом. Выбор транзитной задачи может быть представлен следующим выражением:

$$\min\left(\left(c_l + c_j^{ptr}\right) \le t_j^{ptr}\right), l = \overline{1,m}, \tag{5}$$

где $\left(c_l + c_j^{ptr}\right)$ – время завершения выполнения задачи-указателя после выполнения транзитной задачи.

Аналогично процедуре распределения горящих задач, после выбора транзитной задачи агент оповещает остальных агентов о своем выборе и приступает к выполнению задачи.

Возможна ситуация, когда после выполнения транзитной задачи агентом r_i задача-указатель уже будет закреплена за другим агентом. Тогда выбор следующей задачи осуществляется непосредственно по основным узлам связного списка.

Преимуществом предлагаемого решения является простота реализации и низкая вычислительная сложность. Также необходимо отметить, что численность агентов PPTC может быть уменьшена и это не потребует перепланирования последовательности выполнения задач (увеличится только продолжительность выполнения текущего списка задач). Аналогично при увеличении количества

агентов любой новый агент выбирает свободную задачу согласно связного списка L. Блок-схема этапа распределения задач представлена на рисунке 6а, а блок-схема процедуры поиска транзитной задачи показана на рисунке 6б.

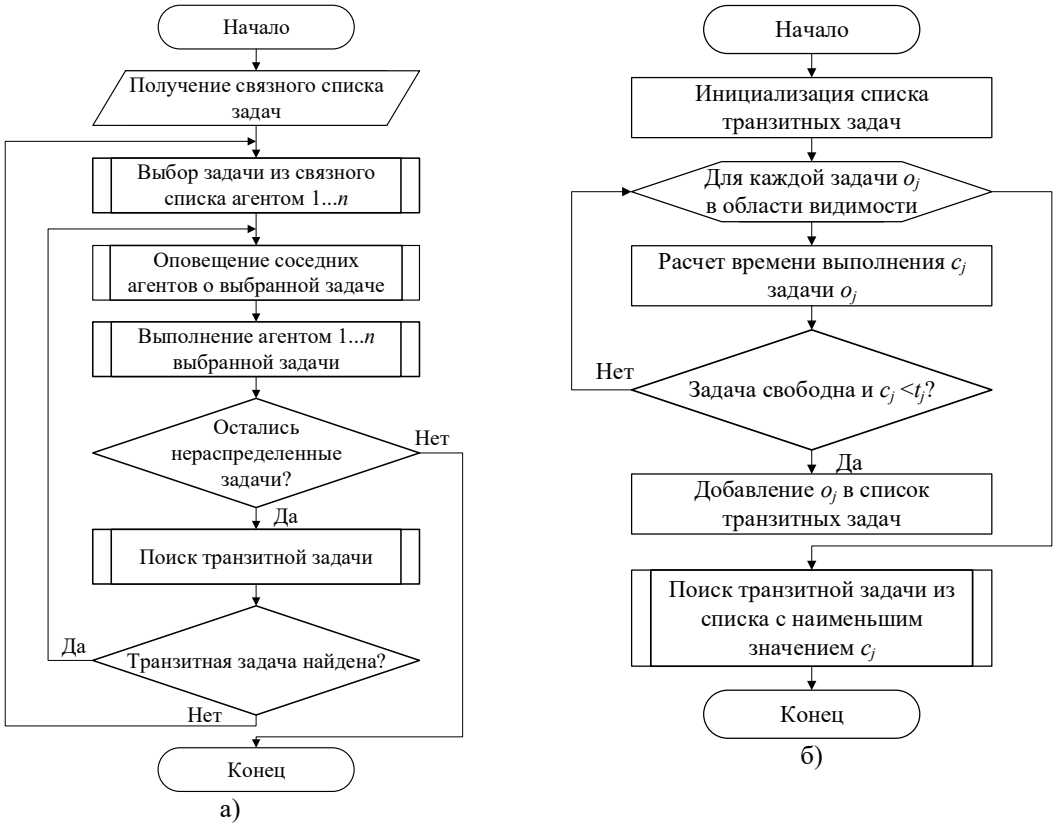


Рисунок 6 – Блок-схемы: а) этапа распределения задач в РРТС; б) поиска транзитных задач

В данном решении достижение консенсуса между агентами наиболее значимо на самой первой итерации этапа распределения задач, когда каждый агент РРТС выбирает горящую задачу. В том случае, если несколько агентов n_c выбирают одну и ту же задачу o_j (такую ситуацию здесь и далее будем называть «коллизией»), алгоритм достижения консенсуса будет следующим. Каждый из n_c агентов рассчитывает расстояние d_i от текущей позиции p_i до позиции начала выполнения задачи p_j. Функция вычисления расстояния будет аналогична представленной в выражении (4), т.е. $d_i = D(p_j, p_i), i = \overline{1, n_c}$. Далее путем информационного обмена агенты, попавшие в коллизию, обмениваются полученными значениями d_i и сравнивают их между собой. В результате этого задачу o_j закрепляет за собой тот агент, у которого значение d_i оказалось наименьшим. В том случае, если у агентов значения d_i оказались равны, то описанная последовательность действий повторяется только между этими агентами с той разницей, что значение d_i не рассчитывается, а выбирается случайно из некоторого диапазона чисел $[0, N]$. Как и ранее, задачу o_j закрепляет за собой агент с минимальным значением d_i. А все остальные агенты продолжают поиск подходящей горящей задачи по связному списку.

Все последующие итерации для агентов РРТС будут асинхронными. В случае повторной коллизии агентов на k-й итерации работы алгоритма, выбор того или иного агента также будет осуществляться на основе метрики расстояния до задачи или случайно, если показатели равны.

Блок-схема процедуры достижения консенсуса между агентами РРТС представлена на рисунке 7.

Необходимо отметить, что при появлении каждой новой задачи связный список L формируется заново на центральном вычислительном устройстве и передается по каналу связи агентам РРТС. При этом каждая задача $o_j \in O$ остается закрепленной за тем агентом, который ее выбрал ранее или уже выполняет. Таким образом, функционирование агентов РРТС при динамическом изменении множества задач O продолжается в штатном режиме.

Рисунок 7 – Блок-схема процедуры достижения консенсуса между агентами РРТС при планировании выполнения задач

Таким образом, отличием второго этапа предложенного метода от метода-аналога является то, что:

- агенты РРТС выполняют итеративное распределение задач децентрализовано, при этом каждая следующая задача i-го агента априори известна (без учета транзитных задач);
- в предложенном методе реализуется концепция выполнения транзитных задач, если дедлайн следующей задачи связного списка позволяет выполнить транзитную задачу без получения штрафа;
- в отличие от метода-аналога и других известных методов планирование выполнения задач ограничено только двумя задачами (текущей задачей и задачей-указателем), что позволяет учитывать специфику РРТС, а также позволяет выбирать агентам наиболее оптимальные планы выполнения задач в текущий момент времени с учетом собственного состояния агента;
- в результате масштабирования численности агентов РРТС нет необходимости осуществлять перераспределение задач между агентами – каждый новый агент гибко интегрируется в процесс функционирования РРТС.

3.2. Нейросетевой метод планирования последовательности выполнения задач агентами РРТС. К недостаткам аналитического метода, предложенного в пункте 3.1, можно отнести его декомпозицию на два отдельных этапа: предобработка множества задач на стороне центрального вычислительного устройства и распределение задач между агентами с выбором транзитных задач. На каждом из этапов предложенного метода выполняется полный перебор задач в глубину. Количество вычислений можно уменьшить, если использовать предложенный метод для обучения искусственной нейронной сети (ИНС), а обученную ИНС – для распределения и планирования выполнения задач с использованием вычислительных платформ агентов РРТС. Такой вариант реализации предложенного решения будет полностью децентрализованным, что может быть полезным, если множество задач изменяется непрерывно. С одной стороны, такой подход уменьшает нагрузку на центральное вычислительное устройство, а с другой стороны, использование ИНС для распределения задач позволит учесть те скрытые зависимости при выборе задач, которые аналитический метод не позволяет увидеть явно. Основной идеей реализации нейросетевого метода распределения и планирования последовательности выполнения задач агентами РРТС является использование метода Word2Vec [32] для выбора следующих задач (задачи), которые будут выполнены,

на основе меры их сходства. В отличие от предложенного в пункте 3.1 аналитического метода, этот подход позволит при выборе следующей задачи агентом РРТС найти компромисс между срочностью выполнения задач и расстоянием, которое необходимо пройти в процессе их выполнения, что в конечном итоге повысит эффективность функционирования РРТС.

Метод Word2Vec может быть реализован на основе двух алгоритмов обучения: «непрерывный мешок со словами» (CBOW, continuous bag-of-words model) и «скип-граммы» (skip-gram). Первый алгоритм предназначен для подбора наиболее вероятной задачи на основе представленного контекста (последовательности задач), а второй – для предсказания контекста по исходной задаче. Более наглядно различия в схемах реализации алгоритмов CBOW и skip-gram показаны на рисунке 8, где o обозначает задачу, а значение в скобках – порядок следования этой задачи в последовательности задач.

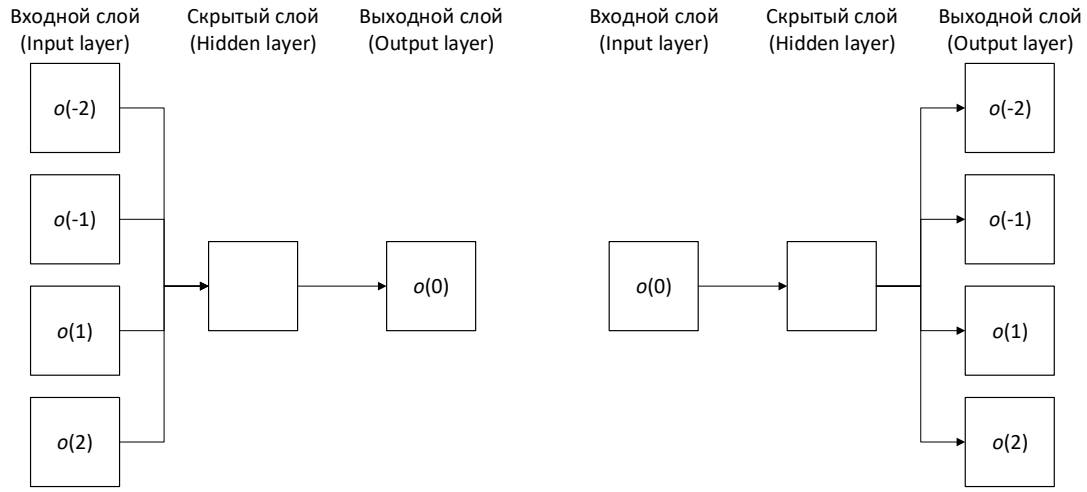


Рисунок 8 – Обобщенные схемы реализации алгоритмов CBOW и skip-gram

В процессе обучения ИНС получает на вход «one-hot» вектор $h = (h_1, h_2, \dots, h_m)$, где $h_j = 1$, если элемент h_j соответствует позиции задачи o_j, и $h_j = 0$ в противном случае, $j = \overline{1, m}$. Задача обучения ИНС заключается в том, чтобы осуществить распределение вероятностей каждой задачи оказаться в контексте входной задачи. В соответствии с оригинальной работой [32] основы процесса обучения ИНС могут быть описаны следующим образом. Вектор h исходной задачи подается на вход ИНС, которая пытается предсказать выходную задачу. После сравнения предсказанной задачи и той задачи, которая на самом деле находится в контекстном окне, вычисляется функция потерь, которая вместе со стохастическим градиентным спуском используется для оптимизации ИНС.

Для рассматриваемой задачи распределения и планирования задач наиболее подходящим является алгоритм skip-gram, так как на вход ИНС может быть подана текущая позиция p_i агента r_i, а на выходе получено распределение вероятностей выбора следующей задачи согласно их позициям. При этом количество выбираемых задач может быть не ограничено. Однако такая реализация соответствует только второму этапу аналитического метода, предложенного в пункте 3.1, так как фактически выбор следующих задач основывается на метрике расстояния между задачами без учета их дедлайна.

Для того чтобы учесть дедлайн выполнения задач, предлагается подавать на вход ИНС не «one-hot» вектор, а вектор h', содержащий индекс текущей позиции агента $p_i \in P$ и множество значений потенциального штрафа за нарушение дедлайна при выполнении задачи $z = (z_1, z_2, \dots, z_m)$. Расчет значения потенциального штрафа за нарушение дедлайна при выполнении задачи o_j основывается на формуле (2), при этом отличие будет заключаться в том, что время завершения задачи c_j рассчитывается «грубо» в зависимости от расстояния от позиции завершения выполнения текущей задачи b_c (или позиции агента) до позиции начала выполнения следующей задачи a_n, а также расстояния от позиции начала выполнения текущей задачи a_n до позиции завершения выполнения задачи b_n. Под грубым расчетом в данном случае понимается допущение о равномерном движении агента с постоянной скоростью, для более точного расчета можно воспользоваться методами планирования пути перемещения агента или траектории его движения [33–35]. Таким образом, расчет потенциального штрафа z_j за нарушение дедлайна при выполнении задачи o_j имеет следующий вид:

$$z_j = \left(\frac{D(b_c,a_n)+D(a_n,b_n)}{v} - t_j\right) p_j, \quad (6)$$

где v – скорость перемещения агентов (представляет собой константу, и это значение одинаково для всех агентов РРТС). В том случае если задача o_j уже выполнена или выполняется в текущий момент времени другим агентом, то значение потенциального штрафа z_j будет равно 0.

Таким образом, на основе предложенного подхода на выходе ИНС будет получен вектор y, содержащий вероятности выбора задачи агентом согласно метрики, включающей не только расстояние между задачами, но и срочность их выполнения. Чем выше значение элемента вектора y, тем выше приоритет выполнения той задачи из множества O, индекс которой соответствует индексу элемента y. То есть агенту РРТС необходимо найти индекс элемента с наибольшим значением и оповестить других агентов о выборе этой задачи.

В качестве ИНС предлагается использовать многослойный персептрон с двумя скрытыми слоями. Входной и выходной слои будут состоять из $m+1$ и m нейронов соответственно. Количество нейронов в скрытых слоях выбирается произвольно (с учетом возможностей вычислительных платформ робототехнических устройств, которые используются в качестве агентов РРТС). Однако, по мнению авторов данной работы, размерности скрытых слоев должны быть не меньше размерности входного слоя, т.е. $m+1$. Схематически структура предлагаемой ИНС представлена на рисунке 9.

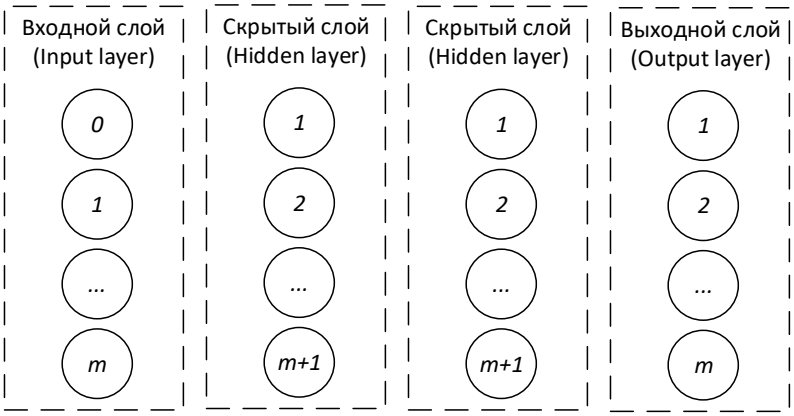


Рисунок 9 – Структура ИНС

Обучение ИНС предлагается выполнить на основе данных, полученных с использованием аналитического метода. Особенность обучающей выборки для ИНС будет заключаться в том, что необходимо использовать не решения отдельных агентов в рамках выполнения множества задач (каждый агент берет на себя только часть задач), а результаты построения плана выполнения всего множества задач каждым из агентов РРТС (каждый агент берет на себя все множество задач). Пусть $A = (A_1, A_2, \dots, A_n)$ – множество решений, полученных при использовании аналитического метода от n агентов. Каждый элемент $A_i, i = \overline{1,n}$ представляет собой множество, состоящее из множества результатов выбора агентом r_i задачи для выполнения, т.е. $A_i = (a_1, a_2, \dots, a_m)$. В свою очередь каждый результат выбора задачи агентом r_i будет содержать позицию агента p_i на момент выбора задачи, значение потенциального штрафа z_j за нарушение дедлайна при выполнении каждой из задач $o_j, j = \overline{1,m}$, рассчитанное с помощью формулы (6), и индекс задачи, которая была выбрана для выполнения $u \in [1,m]$, то есть $a_j = (p_i, z_1, z_2, \dots, z_m, u), j = \overline{1,m}$. Каждый из результатов выбора задачи будет непосредственно использован для обучения ИНС согласно ранее описанному подходу.

Аналогично оригинальной реализации алгоритма skip-gram [32] функция потерь при обучении ИНС определяется следующим образом:

$$\sum_{1 \le i \le n,\ A_i \in A} \sum_{1 \le j \le m,\ a_j \in A_i} \sum_{-c \le k \le c} \log P(o_{j+k}|o_j), \quad (7)$$

где c – размер контекстного окна (в данной работе $c = 1$), а встречаемость задач o_{j+k} и o_j рассматривается независимо от отдельно взятого плана выполнения задач a_j. Вероятность встречаемости задач $P(o_{j+k}|o_j)$ определяется с помощью функции перекрестной энтропии:

$$\log P(o_{j+k}|o_j) = \frac{\exp(v_{o_j}^T v'_{o_{j+k}})}{\sum_{p=1}^{M} \exp(v_{o_j}^T v'_o)}, \quad (8)$$

где v_o и v'_o – входное и выходное векторные представления задач; M – количество возможных позиций задач.

Из уравнений (7) и (8) видно, что предложенная модель ИНС моделирует последовательность задач, где задачи с похожим контекстом будут иметь сходные векторные представления.

Таким образом, можно выделить следующие особенности предложенного метода:

- для выбора следующей задачи необходим единовременный запуск алгоритма (например, триггером может быть завершение выполнения текущей задачи), что уменьшает нагрузку на вычислительное устройство агента (вместо перебора всех задач в каждый дискретный момент срабатывания вычислительного устройства агента при поиске транзитной задачи);
- аналитический метод позволяет явно выбрать в качестве следующей задачи ближайшую, однако ИНС позволяет учесть и скрытые зависимости при расчете подобия векторного представления задач, которые не могут быть учтены при аналитическом варианте метода;
- итеративный запуск метода позволит запланировать выполнение любого необходимого количества задач. Соответственно, такой подход может быть использован как при децентрализованном управлении, так и при централизованном, что обуслjвливает универсальность предложенного метода.

4. Эксперимент. Для проведения эксперимента была выполнена программная реализация метода-аналога и предложенных решений на языке программирования Python. Визуализация взаимодействий агентов РРТС, а также формирование графиков для оценки эффективности рассматриваемых методов выполнены с помощью библиотеки Matplotlib. При проведении моделирования был использован компьютер со следующими характеристиками: процессор Intel Core i7-8550U с тактовой частотой 1,8 ГГц, 8 ГБ оперативной памяти. Использованы параметры моделирования, указанные в таблице 1. Среда моделирования аналогична представленной на рисунке 3.

На рисунках 10–12 представлены показатели времени выполнения задач, количества просроченных задач и суммарное значение штрафа для всех агентов РРТС, полученные в результате моделирования. Полупрозрачные линии определяют результаты каждого из 100 экспериментов, а непрозрачные линии – среднее полученное значение по всем проведенным экспериментам. Аббревиатуры МА, РАМ и РНМ, представленные на рисунках 10–12, обозначают метод-аналог, разработанный аналитический метод и разработанный нейросетевой метод соответственно. Эти обозначения будут использованы и далее.

Таблица 1 – Параметры моделирования

Наименование параметра	**Значение**
Количество агентов РРТС, n, ед.	50
Количество задач, m, ед.	100
Количество экспериментов, ед.	100
Скорость перемещения агентов, м/с	0,5
Размер карты, м×м	10×10

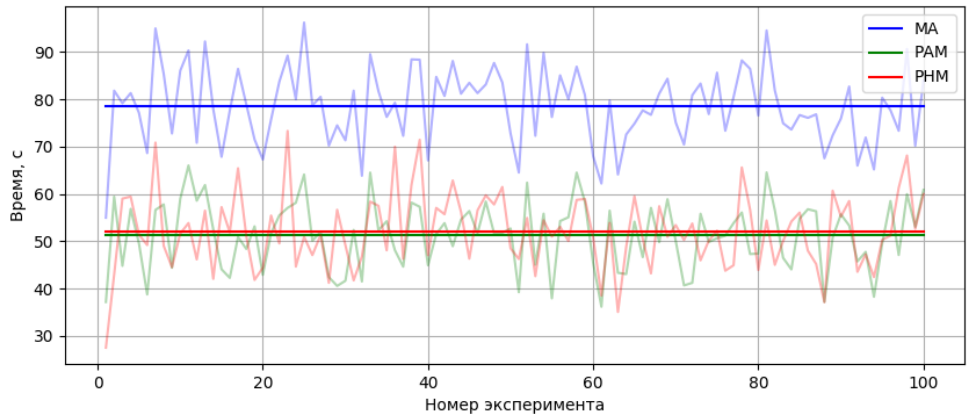


Рисунок 10 – Показатели времени, необходимого агентам РРТС для выполнения задач

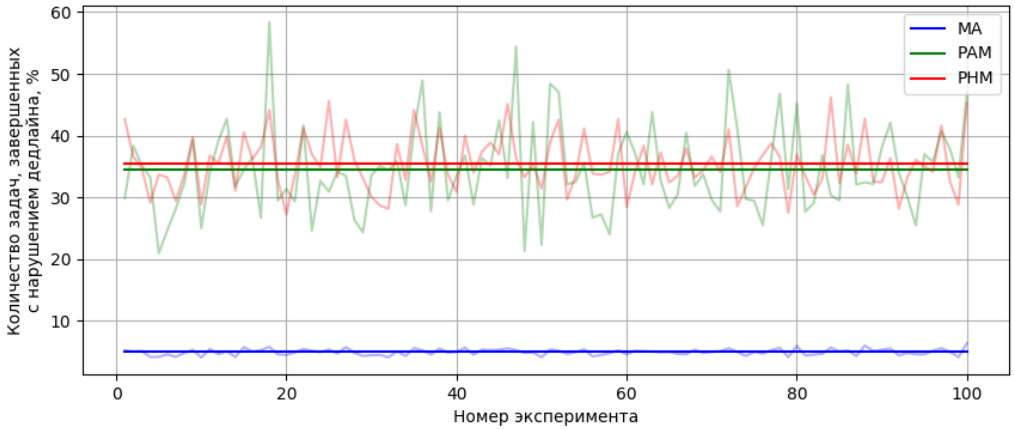


Рисунок 11 – Показатели количества задач, завершенных агентами PPTC с нарушением дедлайна

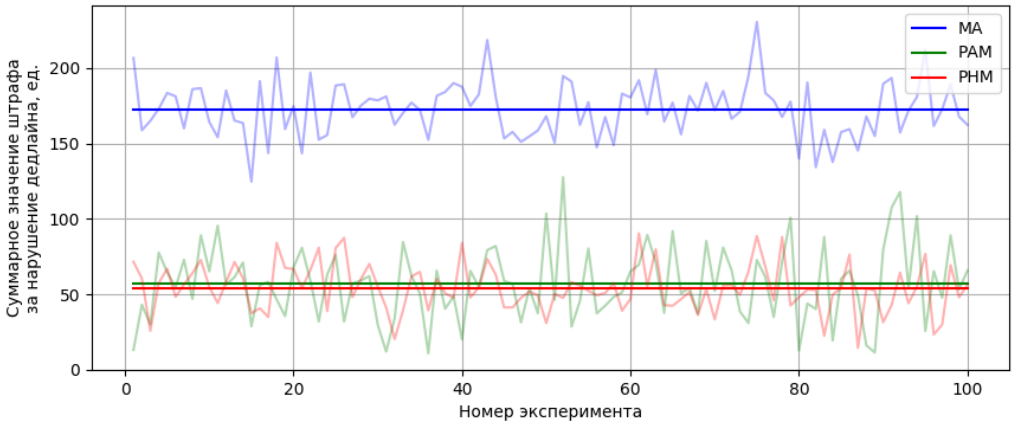


Рисунок 12 – Показатели суммарного штрафа, полученного всеми агентами PPTC в результате нарушения дедлайна при выполнении задач

На рисунках 13–15 показаны результаты обработки данных, представленных на рисунках 10–12, с использованием диаграмм размаха для более наглядного представления полученных результатов.

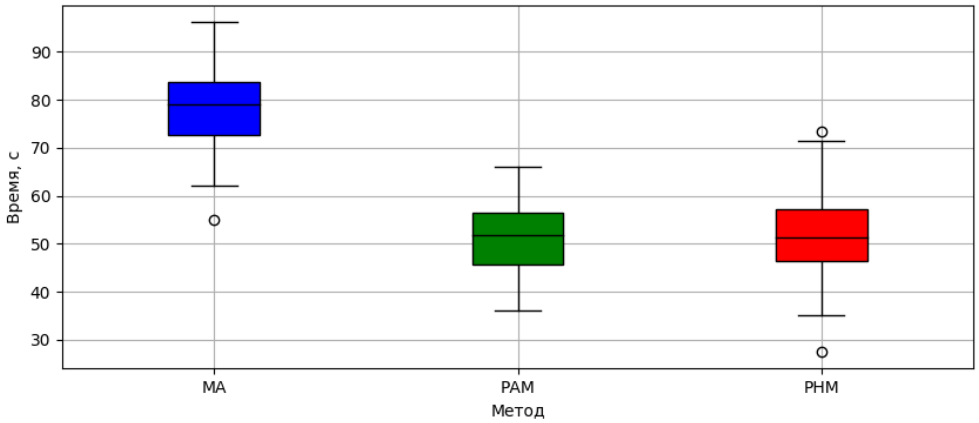


Рисунок 13 – Показатели времени, необходимого агентам PPTC для выполнения задач

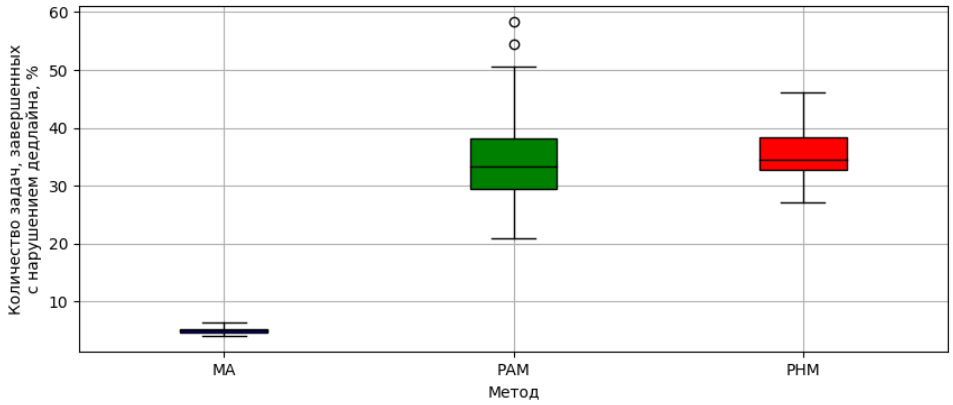


Рисунок 14 – Показатели количества задач, завершенных агентами PPTC с нарушением дедлайна

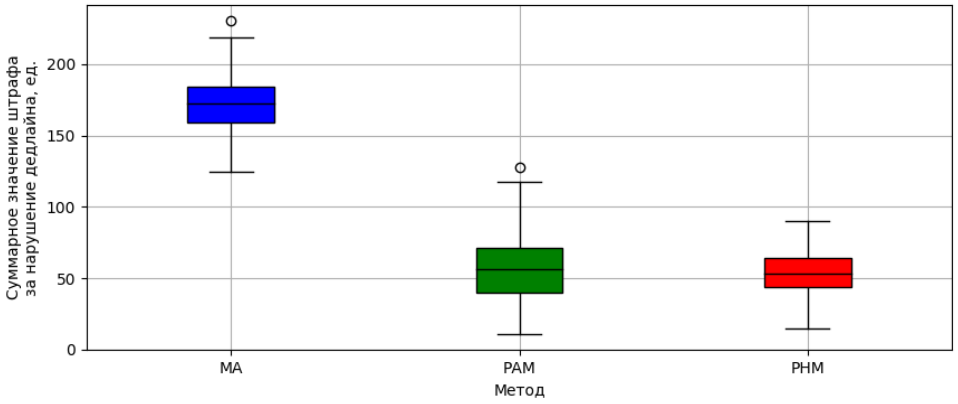


Рисунок 15 – Показатели суммарного штрафа, полученного всеми агентами PPTC в результате нарушения дедлайна при выполнении задач

Для оценки эффективности функционирования PPTC интерес также представляют максимальные, средние и минимальные значения рассматриваемых показателей эффективности выполнения задач, представленные в таблице 2.

Основной идеей MA является недопущение возникновения новых просроченных задач, поэтому показатель количества таких задач составил в среднем 4,98 % (против 34,5 % у PAM) от общего количества задач согласно результатам, представленным в таблице 2. Однако значение суммарного штрафа для PAM меньше на 66,8 % (57,33 ед. против 172,61 ед.). Это объясняется тем, что выполнение уже просроченных задач в MA откладывается на более поздний срок, что не всегда допустимо в реальных сценариях автоматизированного склада. Например, некоторый товар может иметь лимитированный срок годности, а с учетом времени, необходимого для доставки товара конечному потребителю, этот товар придет в негодность, либо же товар должен быть утилизирован, что принесет убыток автоматизированному складу. В то же время в PAM основной идеей является определение очередности горящих задач и очередности их выполнения. Также необходимо отметить, что реализованная концепция транзитных задач в PAM позволила уменьшить среднее время выполнения задач агентами PPTC на 34,7 % (51,32 с против 78,55 с).

Таблица 2 – Показатели качества выполнения задач агентами PPTC

Критерий	**MA**	**PAM**	**PHM**
Время, с			
Максимальное значение	96,2	66,01	73,3
Среднее значение	78,55	51,32	52,06
Минимальное значение	54,97	36,16	27,52

Продолжение таблицы 2

Количество задач, завершенных с нарушением дедлайна, %			
Максимальное значение	6,39	58,34	46,22
Среднее значение	4,98	34,5	35,52
Минимальное значение	4,08	20,96	27,22
Суммарное значение штрафа за нарушение дедлайна, ед.			
Максимальное значение	230,52	127,7	90,45
Среднее значение	172,61	57,33	54,26
Минимальное значение	124,77	10,96	14,68

Результаты моделирования РНМ и РАМ сопоставимы, однако необходимо отметить, что РНМ является более универсальным решением, которое может быть использовано не только для РРТС, но и для любых других типов робототехнических систем. При моделировании РНМ наблюдается несущественное увеличение средних значений времени выполнения задач и процента задач, завершенных с нарушением дедлайна. Однако суммарное значение штрафа за нарушение дедлайна меньше, чем у РАМ (54,26 ед. против 57,33 ед.), что также подтверждают максимальные значения этого показателя (90,45 ед. против 127,7 ед.). Исходя из этого, можно заключить, что использование РНМ позволяет уменьшить значение штрафа при выполнении каждой отдельно взятой задачи при сопоставимых значениях остальных показателей.

Таким образом, результаты проведенного моделирования свидетельствуют о повышении эффективности функционирования РРТС за счет разработанных решений.

Заключение. Для повышения эффективности распределения и планирования задач в РРТС в условиях недетерминированной среды с учетом ограниченных возможностей агентов РРТС и специфики децентрализованного управления в данной работе были предложены новые решения в виде аналитического и нейросетевого методов распределения и планирования выполнения задач агентами РРТС в сценарии автоматизированного склада. Наиболее близким аналогом к представленным решениям является работа [29], основная идея которой заключается в том, чтобы минимизировать количество задач, выполненных с нарушением дедлайна. Отличие методов, представленных в данной работе, заключается в том, что уже «просроченные» задачи выполняются в первую очередь, причем если появляется возможность выполнить дополнительную задачу без нарушения дедлайна задачи, следующей согласно очередности, то агенты выполняют такие задачи. Элементом научной новизны являются предложенные алгоритмы сортировки задач и поиска транзитных задач, позволяющие не только уменьшить время нарушения дедлайна при выполнении задач, но и уменьшить общее время выполнения всего множества задач. Также стоит отметить, что множество задач может быть изменено (например, дополнено новыми задачами) в любой момент функционирования РРТС. После завершения текущей задачи каждый агент продолжает перебирать связный список и выбирать наиболее подходящую задачу. Элементом научной новизны нейросетевого метода распределения и планирования последовательности выполнения задач агентами РРТС является его реализация на основе векторного представления задач и определения меры их подобия аналогично методу Word2Vec. Полученное решение является полностью децентрализованным, что делает разработанный метод универсальным и позволяет использовать его не только для РРТС, но и для любых других типов робототехнических систем. Достоверность полученных результатов подтверждена в ходе программного моделирования. Однако для анализа применимости разработанного метода на практике требуется проведение натурных экспериментов в среде, близкой к условиям функционирования РРТС в автоматизированном складе. Эта задача требует дальнейшей проработки, на что и будут направлены дальнейшие исследования.

Список литературы

1. Каляев, И. А. Модели и алгоритмы коллективного управления в группах роботов / И. А. Каляев, А. Р. Гайдук, С. Г. Капустян. – Москва : ФИЗМАТЛИТ, 2009. – 280 с.

2. Alibaba Group. – Режим доступа: https://www.alibabagroup.com/en/global/home, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.05.2022).

3. Seenu, N. Review on state-of-the-art dynamic task allocation strategies for multiple-robot systems / N. Seenu, R. M. Kuppan Chetty, M. M. Ramya, N. J. Mukund // Industrial Robot. – 2020. – Vol. 47, № 6. – P. 929–942.

4. Dai, W. Multi-robot dynamic task allocation for exploration and destruction / W. Dai, H. Lu, J. Xiao, Z. Zeng, Z. Zheng // Journal of Intelligent and Robotic Systems: Theory and Applications. – 2020. – Vol. 98, № 2. – P. 455–479.

5. Khamis, A. Multi-robot Task Allocation: A Review of the State-of-the-Art / A. Khamis, A. Hussein, A. Elmogy // Cooperative Robots and Sensor Networks. – 2015. – P. 31–51.

6. Петренко, В. И. Анализ рисков нарушения информационной безопасности в роевых робототехнических системах при масштабировании численности агентов / В. И. Петренко, Ф. Б. Тебуева, А. С. Павлов, И. В. Стручков // Прикаспийский журнал: управление и высокие технологии. – 2022. – № 2. – С. 92–109.

7. Kowalczyk, W. Target Assignment Strategy for Scattered Robots Building Formation / W. Kowalczyk // Proceedings of the Third International Workshop on Robot Motion and Control (RoMoCo '02). – 2002. – P. 181–185.

8. Ni, M. A Lagrange relaxation method for solving weapon-target assignment problem / M. Ni, Z. Yu, F. Ma, X. Wu // Mathematical Problems in Engineering. – 2011. – Vol. 1. – P. 1–10.

9. Zavlanos, M. A distributed auction algorithm for the assignment problem / M. Zavlanos, L. Spesivtsev, G. Pappas // 47th IEEE Conference on Decision and Control. – 2008. – P. 1212–1217.

10. Bertsekas, D. Parallel synchronous and asynchronous implementations of the auction algorithm / D. Bertsekas, D. Castanon // Parallel Computing. – 1991. – Vol. 17. – P. 707–732.

11. Zavlanos, M. Dynamic assignment in distributed motion planning with local coordination / M. Zavlanos, G. Pappas // IEEE Transactions on Robotics. – 2008. – Vol. 24, № 1. – P. 232–242.

12. Zavlanos, M. Sensor-based dynamic assignment in distributed motion planning / M. Zavlanos, G. Pappas // Proceedings 2007 IEEE International Conference on Robotics and Automation. – 2007. – P. 3333–3338.

13. Azad, M .M. Efficient Heuristic Approaches to the Weapon Target Assignment Problem / M. M. Azad, A. Mircea // Journal of Aerospace Computing, Information and Communication. – 2009. – Vol. 6. – P. 405–415.

14. Berman, S. Optimized Stochastic Policies for Task Allocation in Swarms of Robots / S. Berman, A. Halasz, M. A. Hsieh, V. Kumar // IEEE Transactions on Robotics. – 2009. – Vol. 25, № 4. – P. 927–937.

15. Mouton, H. Applying Reinforcement Learning to the Weapon Assignment Problem in Air Defense / H. Mouton, J. Roodt, H. Roux // Scientia Militaria South African Journal of Military Studies. – 2011. – Vol. 39, № 2. – P. 1–15.

16. Zhao, H. General Dynamic Neural Networks for the Adaptive Tuning of an Omni-Directional Drive System for Reactive Swarm Robotics / H. Zhao, M. Dorigo, M. Allwright // 25th International Conference on Methods and Models in Automation and Robotics (MMAR). – 2021. – P. 79–84.

17. Mukhedkar, R. Weapon Target Allocation Problem Using Fuzzy Model / R. Mukhedkar, S. Naik // International Journal of Application or Innovation in Engineering & Management (IJAIEM). – 2013. – Vol. 2, № 6. – P. 279–289.

18. Oliveira, S. Analysis of the population-based ant colony optimization algorithm for the TSP and the QAP / S. Oliveira, M. S. Hussin, A. Roli, M. Dorigo, T. Stützle // IEEE Congress on Evolutionary Computation (CEC). – 2017. – P. 1734–1741.

19. Liao, T. Ant Colony Optimization for Mixed-Variable Optimization Problems / T. Liao, K. Socha, M. A.Montes de Oca, T. Stützle, M. Dorigo // IEEE Transactions on Evolutionary Computation. – 2014. – Vol. 18, № 4. – P. 503–518.

20. Murphy, R. Target-Based Weapon Target Assignment Problems / R. Murphy // Nonlinear Assignment Problems. Combinatorial Optimization. – 1999. – Vol. 7. – P. 39–53.

21. Sikanen, T. Solving Weapon Target Assignment Problem with Dynamic Programming / T. Sikanen // Independent Research Projects in Applied Mathematics. – 2008. – P. 32.

22. Shimaa, T. Multiple task assignments for cooperating uninhabited aerial vehicles using genetic algorithms / T. Shima, S. Rasmussen, A. Sparks, K. Passino // Computers & Operations Research. – 2006. – Vol. 33. – P. 3252–3269.

23. Zhang, J. ACGA Algorithm of Solving Weapon Target Assignment Problem / J. Zhang, X. Wang, C. Xu // Open Journal of Applied Sciences. – 2012. – Vol. 2. – P. 74–77.

24. Sarkar, C. A Scalable Multi-Robot Task Allocation Algorithm / C. Sarkar, H. S. Paul, A. Pal // IEEE International Conference on Robotics and Automation (ICRA). – 2018. – P. 5022–5027.

25. Lu, Q. Multiple-place swarm foraging with dynamic depots / Q. Lu, J. Hecker, M. Moses // Autonomous Robots. – 2018. – Vol. 42, № 4. – P. 909–926.

26. Zhou, L. A Balanced Heuristic Mechanism for Multirobot Task Allocation of Intelligent Warehouses / L. Zhou, Y. Shi, J. Wang, P. Yang // Mathematical Problems in Engineering. – 2014. – Vol. 2014. – P. 1–10.

27. Tkach, I. A Modified Distributed Bees Algorithm for Multi-Sensor Task Allocation / I. Tkach, A. Jevtić, S. Y. Nof, Y. Edan // Sensors. – 2018. – Vol. 18. – P. 759.

28. Karaboga, D. An Idea Based on Honey Bee Swarm for Numerical Optimization / D. Karaboga // Technical Report-TR06, Department of Computer Engineering, Engineering Faculty, Erciyes University. – 2005. – P. 1–10.

29. Sarkar, C. Cannot avoid penalty? Let's minimize / C. Sarkar, M. Agarwal // International Conference on Robotics and Automation (ICRA). – 2019. – P. 1052–1058. – doi: 10.1109/ICRA.2019.8794338.

30. Zakiev, A. Swarm Robotics: Remarks on Terminology and Classification / A. Zakiev, T. Tsoy, E. Magid // Interactive Collaborative Robotics (ICR 2018). – 2018. – P. 291–300.

31. Koubaa, A. Performance Analysis of the MRTA Approaches for Autonomous Mobile Robot / A. Koubaa, H. Bennaceur, I. Chaari, S. Trigui, A. Ammar, M.-F. Sriti, M. Alajlan, O. Cheikhrouhou, Y. Javed // Robot Path Planning and Cooperation. Studies in Computational Intelligence. – 2018. – Vol. 772. – P. 169–188.

32. Mikolov, T. Distributed Representations of Words and Phrases and their Compositionality / T. Mikolov, I. Sutskever, K. Chen, G. Corrado, J. Dean // Proceedings of the 26th International Conference on Neural Information Processing Systems (NIPS'13). – 2013. – Vol. 2. – P. 3111–3119.

33. Павлов, А. С. Методика планирования траектории движения группы мобильных роботов в неизвестной замкнутой среде с препятствиями / А. С. Павлов // Системы управления, связи и безопасности. – 2021. – № 3. – С. 38–59.

34. Петренко, В. И. Метод планирования траектории движения точки в пространстве с препятствием на основе итеративной кусочно-линейной аппроксимации / В. И. Петренко, Ф. Б. Тебуева, В. О. Антонов, М. М. Гурчинский // Системы управления, связи и безопасности. – 2018. – № 1. – С. 168–182.

35. Юдинцев, Б. С. Синтез нейросетевой системы планирования траекторий для группы мобильных роботов / Б. С. Юдинцев // Системы управления, связи и безопасности. – 2019. – № 4. – С. 163–186.

References

1. Kalyaev, I. A., Gayduk, A. R., Kapustyan, S. G. *Modeli i algoritmy kollektivnogo upravleniya v gruppakh robotov* [Models and Algorithms for Collective Control in Groups of Robots]. Moscow, Fizmatlit Publ., 2009.

2. Alibaba Group. Available at: https://www.alibabagroup.com/en/global/home (accessed 18.05.2022).

3. Seenu, N., Kuppan Chetty, R. M., Ramya, M. M., Mukund, N. J. Review on state-of-the-art dynamic task allocation strategies for multiple-robot systems. *Industrial Robot,* 2020, vol. 47, no. 6, pp. 929–942.

4. Dai, W., Lu, H., Xiao, J., Zeng, Z., Zheng, Z. Multi-robot dynamic task allocation for exploration and destruction. *Journal of Intelligent and Robotic Systems: Theory and Applications*, 2020, vol. 98, no. 2, pp. 455–479.

5. Khamis, A., Hussein, A., Elmogy, A. Multi-robot Task Allocation: A Review of the State-of-the-Art. *Cooperative Robots and Sensor Networks*, 2015, pp. 31–51.

6. Petrenko, V. I., Tebueva, F. B., Pavlov, A. S., Struchkov, I. V. Analiz riskov narusheniya informatsionnoy bezopasnosti v roevykh robototekhnicheskikh sistemakh pri masshtabirovanii chislennosti agentov [Analysis of information security breach risks in swarm robotic systems when scaling the number of agents]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2022, no. 2, pp. 92–109.

7. Kowalczyk, W. Target Assignment Strategy for Scattered Robots Building Formation. *Proceedings of the Third International Workshop on Robot Motion and Control (RoMoCo '02)*, 2002, pp. 181–185.

8. Ni, M., Yu, Z., Ma, F., Wu, X. A Lagrange relaxation method for solving weapon-target assignment problem. *Mathematical Problems in Engineering*, 2011, vol. 1, pp. 1–10.

9. Zavlanos, M., Spesivtsev, L., Pappas, G. A distributed auction algorithm for the assignment problem. *47th IEEE Conference on Decision and Control,* 2008, pp. 1212–1217.

10. Bertsekas, D., Castanon, D. Parallel synchronous and asynchronous implementations of the auction algorithm. *Parallel Computing*, 1991, vol. 17, pp. 707–732.

11. Zavlanos, M., Pappas, G. Dynamic assignment in distributed motion planning with local coordination. *IEEE Transactions on Robotics*, 2008, vol. 24, no. 1, pp. 232–242.

12. Zavlanos, M., Pappas, G. Sensor-based dynamic assignment in distributed motion planning. *Proceedings 2007 IEEE International Conference on Robotics and Automation*, 2007, pp. 3333–3338.

13. Azad, M. M., Mircea, A. Efficient Heuristic Approaches to the Weapon Target Assignment Problem. *Journal of Aerospace Computing, Information and Communication*, 2009, vol. 6, pp. 405–415.

14. Berman, S., Halasz, A., Hsieh, M. A., Kumar, V. Optimized Stochastic Policies for Task Allocation in Swarms of Robots. *IEEE Transactions on Robotics*, 2009, vol. 25, no. 4, pp. 927–937.

15. Mouton, H., Roodt, J., Roux, H. Applying Reinforcement Learning to the Weapon Assignment Problem in Air Defense. *Scientia Militaria South African Journal of Military Studies,* 2011, vol. 39, № 2, pp. 1–15.

16. Zhao, H., Dorigo, M., Allwright, M. General Dynamic Neural Networks for the Adaptive Tuning of an Omni-Directional Drive System for Reactive Swarm Robotics. *25th International Conference on Methods and Models in Automation and Robotics (MMAR)*, 2021, pp. 79–84.

17. Mukhedkar, R., Naik, S. Weapon Target Allocation Problem Using Fuzzy Model. *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* 2013, vol. 2, no. 6, pp. 279–289.

18. Oliveira, S., Hussin, M. S., Roli, A., Dorigo, M., Stützle, T. Analysis of the population-based ant colony optimization algorithm for the TSP and the QAP. *IEEE Congress on Evolutionary Computation (CEC),* 2017, pp. 1734–1741.

19. Liao, T., Socha, K., Montes de Oca, M. A., Stützle, T., Dorigo, M. Ant Colony Optimization for Mixed-Variable Optimization Problems. *IEEE Transactions on Evolutionary Computation*, 2014, vol. 18, no. 4, pp. 503–518.

20. Murphy, R. Target-Based Weapon Target Assignment Problems. *Nonlinear Assignment Problems. Combinatorial Optimization*, 1999, vol. 7, pp. 39–53.

21. Sikanen, T. Solving Weapon Target Assignment Problem with Dynamic Programming. *Independent Research Projects in Applied Mathematics*, 2008, p. 32.

22. Shima, T., Rasmussen, S., Sparks, A., Passino, K. Multiple task assignments for cooperating uninhabited aerial vehicles using genetic algorithms. *Computers & Operations Research*, 2006, vol. 33, pp. 3252–3269.

23. Zhang, J., Wang, X., Xu, C. ACGA Algorithm of Solving Weapon Target Assignment Problem. *Open Journal of Applied Sciences*, 2012, vol. 2, pp. 74–77.

24. Sarkar, C., Paul, H. S., Pal, A. A Scalable Multi-Robot Task Allocation Algorithm. *IEEE International Conference on Robotics and Automation (ICRA)*, 2018, pp. 5022–5027.

25. Lu, Q., Hecker, J., Moses, M. Multiple-place swarm foraging with dynamic depots. *Autonomous Robots*, 2018, vol. 42, no. 4, pp. 909–926.

26. Zhou, L., Shi, Y., Wang, J., Yang, P. A Balanced Heuristic Mechanism for Multirobot Task Allocation of Intelligent Warehouses. *Mathematical Problems in Engineering*, 2014, vol. 2014, pp. 1–10.

27. Tkach, I., Jevtić, A., Nof, S. Y., Edan, Y. A Modified Distributed Bees Algorithm for Multi-Sensor Task Allocation. *Sensors,* 2018, vol. 18, pp. 759.

28. Karaboga, D. An Idea Based on Honey Bee Swarm for Numerical Optimization. *Technical Report-TR06, Department of Computer Engineering, Engineering Faculty, Erciyes University,* 2005, pp. 1–10.

29. Sarkar, C., Agarwal, M. Cannot avoid penalty? Let's minimize. *International Conference on Robotics and Automation (ICRA)*, 2019, pp. 1052–1058. doi: 10.1109/ICRA.2019.8794338.

30. Zakiev, A., Tsoy, T., Magid, E. Swarm Robotics: Remarks on Terminology and Classification. *Interactive Collaborative Robotics (ICR 2018)*, 2018, pp. 291–300.

31. Koubaa, A., Bennaceur, H., Chaari, I., Trigui, S., Ammar, A., Sriti, M.-F., Alajlan, M., Cheikhrouhou, O., Javed, Y. Performance Analysis of the MRTA Approaches for Autonomous Mobile Robot. *Robot Path Planning and Cooperation. Studies in Computational Intelligence*, 2018, vol. 772, pp. 169–188.

32. Mikolov, T., Sutskever, I., Chen, K., Corrado, G., Dean, J. Distributed Representations of Words and Phrases and their Compositionality. *Proceedings of the 26th International Conference on Neural Information Processing Systems (NIPS'13)*, 2013, vol. 2, pp. 3111–3119.

33. Pavlov, A. S. Metodika planirovaniya traektorii dvizheniya gruppy mobilnykh robotov v neizvestnoy zamknutoy srede s prepyatstviyami [Methodology for Planning the Trajectory of a Group of Mobile Robots in Unknown Closed Environment with Obstacles]. *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2021, no. 3, pp. 38–59.

34. Petrenko, V. I., Tebueva, F. B., Antonov, V. O., Gurchinskiy, V. V. Metod planirovaniya traektorii dvizheniya tochki v prostranstve s prepyatstviem na osnove iterativnoy kusochno-lineynoy approksimatsii [A method for planning the trajectory of a point in space with an obstacle based on iterative piecewise linear approximation]. *Sistemy upravleniya, svjazi i bezopasnosti* [Systems of Control, Communication and Security], 2018, no. 1, pp. 162–182.

1. Yudintsev, B .S. Sintez neyrosetevoy sistemy planirovaniya traektoriy dlya gruppy mobilnykh robotov [Synthesis of a neural network path planning system for a group of mobile robots]. *Sistemy upravleniya, svyazi i bezopasnosti* [Systems of Control, Communication and Security], 2019, no. 4, pp. 163–186.

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ МАШИН, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

DOI 10.54398/20741707_2022_3_44
УДК 519.178/.245:004.94

СРАВНЕНИЕ АЛГОРИТМОВ ГРАССБЕРГЕРА И АХУНЖАНОВА ДЛЯ НАХОЖДЕНИЯ ОСТОВА ПЕРКОЛЯЦИОННОГО КЛАСТЕРА В ЗАДАЧАХ ПЕРКОЛЯЦИИ УЗЛОВ НА КВАДРАТНОЙ РЕШЕТКЕ

Статья поступила в редакцию 19.08.2022, в окончательном варианте – 30.08.2022.

Гордеев Иван Иванович, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат физико-математических наук, ORCID: 0000-0001-5036-4791, e-mail: g2i@mail.ru
Саенко Наталья Сергеевна, Астраханский государственный университет им. В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
преподаватель, ORCID: 0000-0002-3595-6892, e-mail: saenko.natasha@mail.ru

В данной статье сравнивается алгоритм Грассбергера и алгоритм Ахунжанова для нахождения проводящего остова перколяционного кластера. Поскольку алгоритм Грассбергера был предложен для задач перколяции узлов на квадратной решетке, то сравнение алгоритмов производится именно в этих задачах. Для алгоритма Грассбергера подробно обсуждаются случаи, когда алгоритм некорректно присоединяет к остову висячие части. Также обсуждаются модификации алгоритма Грассбергера, позволяющие сократить количество присоединяемых к остову висячих частей. Затем обсуждается алгоритм Ахунжанова, позволяющий отделить все висячие части от остова. Дается оценка доли узлов, некорректно присоединяемых к остову разными версиями алгоритма Грассбергера. Также дается теоретическая оценка сложности по времени алгоритма Ахунжанова и экспериментальное сравнение времени работы различных версий алгоритма Грассбергера и алгоритма Ахунжанова.

Ключевые слова: идентификация остова, перколяция узлов, двумерная решетка, открытые граничные условия, алгоритмы на графах, алгоритм Грассбергера, алгоритм Ахунжанова

COMPARISON OF GRASSBERGER AND AKHUNZHANOV ALGORITHMS FOR FINDING THE BACKBONE OF PERCOLATION CLUSTER IN PROBLEMS OF SITE PERCOLATION ON SQUARE LATTICE

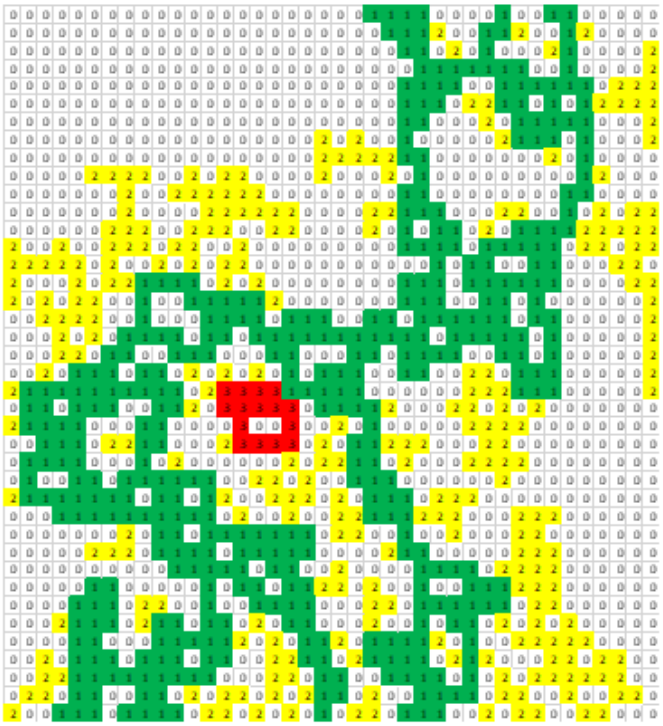
The article was received by the editorial board on 19.08.2022, in the final version – 30.08.2022.

Gordeev Ivan I., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Physics and Mathematics), ORCID: 0000-0001-5036-4791, e-mail: g2i@mail.ru
Saenko Natalya S., Astrakhan State University named after V. N. Tatishchev, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
teacher, ORCID: 0000-0002-3595-6892, e-mail: saenko.natasha@mail.ru

This article compares the Grassberger algorithm and the Akhunzhanov algorithm for finding the conducting backbone of percolation cluster. Since the Grassberger algorithm was proposed for the problems of site percolation on square lattice, the comparison of algorithms is made in these problems. For the Grassberger algorithm, we discuss in detail the cases when the algorithm incorrectly attaches dangling parts to the backbone. We discuss also modifications of the Grassberger algorithm, which allow to reduce the number of dangling parts attached to the backbone. Then Akhunzhanov`s algorithm, which allows separating all dangling parts from the backbone, is discussed. An estimate is given of the proportion of sites incorrectly attached to the backbone by different versions of the Grassberger algorithm. A theoretical estimate of the time complexity of the Akhunzhanov algorithm and an experimental comparison of the runtime of different versions of the Grassberger algorithm and the Akhunzhanov algorithm are also given.

Keywords: backbone identification, site percolation, two-dimensional lattice, open boundary conditions, graph algorithms, Grassberger algorithm, Akhunzhanov algorithm

Graphical annotation (Графическая аннотация)



Пример определения остова перколяционного кластера на квадратной решетке 40x40 (зеленый). Желтым – висячие части. Красным – висячая часть, ошибочно присоединяемая алгоритмом Грассбергера к остову.

An example of determining the core of a percolation cluster on a 40x40 square lattice (in green). In yellow – dangling parts. In red – dangling part, erroneously attached by the Grassberger algorithm to the backbone.

Введение. Задача нахождения проводящего остова относится к одной из задач теории перколяции и является актуальной для различных физических приложений [1, 2].

В теории перколяции обычно рассматриваются случайные графы, для которых ищется путь между двумя вершинами или двумя группами вершин. Обычно предполагается, что вершины из одной группы расположены «с одной стороны графа» при конкретном изображении графа на плоскости или конкретном вложении графа в трехмерное пространство. Если две вершины из разных групп входят в одну компоненту связности, то эту компоненту связности называют перколяционным кластером.

Случайные графы при моделировании перколяции могут генерироваться различными способами. Одним из наиболее популярных способов генерирования случайных графов является рассмотрение периодических решеток, узлы которых соответствуют вершинам графа, а связи между узлами – ребрам графа. Для генерации случайного графа на периодической решетке могут выбираться случайным образом либо связи, тогда говорят о *перколяции связей (bond percolation)*, либо узлы, тогда говорят о *перколяции узлов (site percolation)*. Выбранные для помещения в случайный граф элементы периодической решетки называют *занятыми (occupied)*. В перколяции связей в случайный граф считаются помещенными все вершины, инцидентные занятым ребрам, а в перколяции узлов в случайный граф считаются помещенными все ребра, инцидентные двум занятым вершинам.

С физической точки зрения, наличие перколяционного кластера означает возможность протекания между двумя группами вершин, например, электрического тока, газа или жидкости, если между вершинами из разных групп приложена разность потенциалов (разность давлений). При этом предполагается, что ко всем вершинам одной группы приложен одинаковый потенциал (одинаковое давление). При моделировании протекания электрического тока обычно предполагается, что одинаковый потенциал в одной группе вершин создается за счет подключения всех вершин одной группы к дополнительному проводнику с нулевым (или пренебрежимо малым) сопротивлением. Такой дополнительный проводник физики обычно называют *шиной (bus)*, а способ моделирования перколяции с двумя группами вершин называют *геометрией шины (bus-bar geometry)* [3–9]. Способ моделирования, когда рассматривается протекание между всего двумя вершинами, в физике называют *двухточечной геометрией (two-point geometry)* [4, 5, 10, 11, 12]. Объединение всех простых цепей, соединяющих вершину из одной группы с вершиной из другой группы, принято называть *остовом (backbone)*. В качестве синонима термина *простая цепь* (*simple chain*) [13] иногда употребляется *несамопересекающийся путь* (*non-self-intersecting path*) [14] или *самоизбегающее блуждание* (*self-avoiding walk, SAW*) [15–18].

В некоторых публикациях отмечается, что следует различать *эффективный остов* (*effective backbone*) и *геометрический остов* (*geometric backbone*) [4, 19]. Под геометрическим остовом предлагается понимать данное выше определение остова как подграфа перколяционного кластера с двумя непересекающимися путями до противоположных краев решетки или эквивалентное ему. Однако не через все элементы геометрического остова будет протекать ток из-за наличия идеально сбалансированных связей, которые соответствуют мостам Уитстона. Соответственно, эффективным остовом называют только те элементы геометрического остова, через которые протекает ненулевой ток. Далее в этой статье рассматривается именно геометрический остов, называемый для краткости просто остовом.

Части перколяционного кластера, не входящие в остов, принято называть *висячими частями* (*dangling parts*) [20], хотя некоторые авторы употребляют другие названия, например, *запутывающие части* (*tangling parts*) [14]. В ряде публикаций, посвященных нахождению остова, приводится достаточно подробная классификация висячих частей: *висячие концы* (*dangling ends*), *висячие циклы* (*dangling loops*) и *висячие дуги* (*dangling arcs*) [3, 20].

При анализе графов, допускающих укладку на плоскости, могут быть использованы специальные алгоритмы, учитывающие планарность графа. К алгоритмам, специфическим для нахождения остова в плоском графе, относятся алгоритмы, предложенные Петером Грассбергером и Ренатом Ахунжановым.

Алгоритм Грассбергера. В 1992 году Грассбергером [14] был предложен алгоритм для нахождения остовов на квадратных решетках в перколяции узлов с открытыми граничными условиями. Такие решетки можно рассматривать как частный случай плоских графов. Грассбергер определяет остов как множество несамопересекающихся путей, соединяющих противоположные края решетки.

В алгоритме Грассбергера предлагается выполнять генерирование случайного кластера одновременно с его анализом. Однако тот факт, что случайный кластер генерируется прямо во время анализа, не является принципиальным, и предложенный Грассбергером алгоритм может быть применен и к заранее сгенерированному случайному графу на квадратной решетке. Генерирование случайного кластера выполняется в алгоритме Грассбергера подобно тому, как это делается в алгоритме Лиса [21–23], хотя в алгоритме Лиса генерирование кластера выполняется от одного начального узла, а в алгоритме Грассбергера генерирование занятого кластера выполняется от одного края решетки, что напоминает один из вариантов алгоритма, предложенных Джоном Хаммерсли. Хаммерсли в одном из вариантов изучения перколяции связей предлагал рассматривать смачивание от поверхности образца [24, с. 134–135].

П. Грассбергер рассматривает перколяцию узлов на квадратной решетке и использует термин *смоченные* (*wetted*) узлы в качестве синонима термина «занятые» узлы. Хотя термин «шина» не используется в статье Грассбергера, фактически для моделирования двух шин Грассбергер предлагает считать смоченными узлы, относящиеся к двум группам на противоположных краях решетки (нижнем крае на оси x и верхнем крае $y = L$), между которыми ищется перколяционный кластер и его остов. В статье приводится три версии программного кода: упрощенная, промежуточная и продвинутая. Хотя Грассбергер пишет в статье, что края $y = 0$ и $y = L$ содержат только занятые узлы [14, с. 5478], это верно только для упрощенной версии программного кода. Если анализировать программный код продвинутой версии, то фактически в коде предполагается, что узлы при $y = 0$ заняты случайным образом, а смоченными следует формально считать узлы, соответствующие $y = -1$. Информацию об узлах двумерной решетки Грассбергер предлагает хранить в виде двумерного целочисленного массива размером $L \times L$.

В упрощенной версии Грассбергер описывает более простой рекурсивный алгоритм, который просто проверяет, существует ли перколяционный кластер, давая наиболее левый соединяющий путь и висячие части кластера слева от него. Грассбергер выделяет четыре подпрограммы east, west, south, north, каждая соответствует одному шагу в одном из четырех соответствующих направлений. Каждая функция содержит внутри еще три вызова функций, соответствующих трем возможным направлениям дальнейшего движения (кроме обратного направления). Направления движения перебираются по часовой стрелке, например, функция north вызывает по порядку west, north, east. При помощи рекурсивных вызовов алгоритм генерирует разветвленный путь, который начинается при $x = y = 0$ и, по существу, следует левой части оболочки кластера, содержащего ось x. В упрощенной версии алгоритма программа помечает те узлы, для которых предпринималась попытка случайного заполнения. Хотя программа должна предполагать независимое заполнение узлов с некоторой вероятностью p, что соответствующий узел был занят, в упрощенной версии программы имеется неаккуратность, из-за которой с вероятностью p генерируется заполнение сразу трех соседей занятого узла. Упрощенная версия программы завершается при помощи

функции exit, вызываемой функцией north, когда достигнуто значение $y = L$, сообщая перед вызовом exit, что существует перколяционный кластер. Если $y = L$ никогда не достигается, то программа сообщает об отсутствии перколяционного кластера.

Грассбергер приводит фрагменты кода на языке Си, однако, по-видимому, оригинальная реализация программы Грассбергером была на языке Фортран, поскольку из фрагмента программы видно, что предполагается возвращение функцией rand() вещественного значения в диапазоне от 0 до 1, что соответствует реализации функции rand() в языке Фортран [25], в то время как в языке Си функция rand() возвращает целые значения в диапазоне от 0 до RAND_MAX [26].

Затем Грассбергер вносит две модификации в упрощенную версию алгоритма. Первая модификация заключается в том, чтобы пометку узлов при помощи двух значений $s[x][y] = 1$ или $s[x][y] = 0$ для проверенного/непроверенного узлов заменить пометкой при помощи трех значений: $s = 0$ (непроверенный), $s = q$ (занятый) и $s = INT\_MAX$ (пустой). Здесь q является любым положительным целым, меньшим, чем INT_MAX. Вторая модификация предусматривает наращивание глобального счетчика m каждый раз при входе в подпрограмму и уменьшение этого счетчика при выходе из подпрограммы. В результате, при помощи m считается количество узлов в остове (каждый рекурсивный вызов подпрограммы соответствует обработке одного узла). Грассбергер отмечает, что если эта программа останавливается, поскольку она достигла дальней стороны $y = L$, тогда все шаги в остове соответствуют вызовам подпрограмм, из которых еще не вышли, и значение m является как раз размером остова. Более точно, эта версия программы соответствует получению в m размера самого левого простого пути, принадлежащего остову. При модификации алгоритма Грассбергер также исправил отмеченную выше неаккуратность первоначальной версии, и здесь уже занятие узлов происходит независимо с вероятностью p. В результате описанных модификаций получается промежуточная версия алгоритма.

Далее Грассбергер предлагает еще одну модификацию алгоритма, чтобы считать также все остальные соединяющие пути. Для этого удаляется вызов exit в функции north и взамен наращивается q каждый раз, когда либо достигнут верхний край, либо если q больше, чем проверенное ненулевое $s[x][y]$. Также заменяется безусловное уменьшение m уменьшением по условию, что q не изменилось со времени входа в подпрограмму. Грассбергер пишет, что изменение q показывает, что после входа в подпрограмму либо был достигнут верхний край (в таком случае данный узел принадлежит остову), либо был достигнут какой-то узел, принадлежащий остову (в таком случае данный узел также принадлежит остову).

Грассбергер отмечает, что при отсутствии смены порядка перебора направлений движения будут некорректно определяться внутренние части остова. По этой причине Грассбергер предлагает запоминать направление движения: «вверх» или «вниз». При движении вверх Грассбергер предлагает брать сперва самые левые ветви (т.е. использовать перебор направлений по часовой стрелке), а при движении вниз брать сперва самые правые ветви (т.е. использовать перебор направлений против часовой стрелки).

Чтобы запоминать направление, Грассбергер предлагает кодировать его в четности/нечетности q, начиная с четного q (например, $q = 2$), наращивать q до следующего большего нечетного числа, когда достигается верхний край $y = L$, наращивать q до следующего большего четного числа, когда достигается нижний край $y = 0$ (в статье Грассбергера опечатка: $x = 0$), и наращивать q на две единицы, когда достигается любой другой узел остова [14, с. 5482]. Таким образом, Грассбергер предлагает кодировать движение вверх и перебор направлений по часовой стрелке четными q, а движение вниз и перебор направлений против часовой стрелки – нечетными q. Отметим, что термины «вверх» или «вниз» являются достаточно условными, поскольку при движении по цепочке занятых узлов направление может изменяться сложным образом, и после достижения верхнего края решетки возможен возврат опять к верхнему краю, а после достижения нижнего края решетки возможен возврат опять к нижнему краю.

Недостатки алгоритма Грассбергера и их частичное устранение. О некоторых недостатках алгоритма Грассбергера ранее кратко докладывалось на конференции [27], где отмечалось, что при поиске остова алгоритм корректно обнаруживает все висячие концы, но присоединяет некоторые висячие циклы и висячие дуги, однако конкретных примеров, когда алгоритм Грассбергера работает некорректно, в той публикации не было приведено. В [27] предлагался способ преодоления недостатков алгоритма Грассбергера за счет рассмотрения четырех ориентаций решетки с конкретным случайным заполнением: помимо исходной ориентации рассматривался поворот решетки на 180°, а также отражения относительно вертикальной и относительно горизонтальной осей. В [27] и для различных случайных заполнений решетки, и для различных ориентаций одного случайного заполнения использовался термин «конфигурация», что не совсем удачно. В данной статье различные ориентации одного случайного заполнения решетки называются ориентациями, а термин «конфигурация»

используется для различных случайных заполнений. После публикации [27] при сравнении результатов алгоритма Грассбергера с результатами алгоритма Ахунжанова было обнаружено, что даже при рассмотрении четырех ориентаций алгоритм Грассбергера обнаруживает не все висячие циклы. В данной публикации подробно рассмотрены примеры заполнения решеток, в которых алгоритм Грассбергера работает некорректно, в том числе и для четырех ориентаций.

Для исследования алгоритма Грассбергера нами была сделана реализация этого алгоритма на C++, максимально приближенная к фрагментам кода в тексте статьи Грассбергера, с исправлением небольших неточностей в коде, приводимом в статье [14], программа PureGrasberger.cpp [28]. Для удобства регулирования размеров решетки двумерный массив был реализован в программе PureGrasberger.cpp как вектор векторов. Для удобства анализа в программу была добавлена возможность сохранения сгенерированного случайного заполнения узлов в файле.

Затем была реализована возможность анализа тем же алгоритмом конкретного заполнения, читаемого из файла, с выводом обнаруженного остова в файл для детального анализа, программа GrassbergerFileBB.cpp [28].

В результате анализа был выявлен ряд конфигураций, в которых к остову присоединяются висячие циклы и висячие дуги. Характерной особенностью этих висячих частей является то, что алгоритм Грассбергера не обнаруживает висячие части «с одной стороны». А именно алгоритм Грассбергера определяет висячие циклы с левой стороны, но не определяет висячие циклы с правой стороны (при движении «вверх» и, наоборот, при движении «вниз»). На рисунке 1 показаны соответствующие конфигурации. Цветные ячейки с ненулевыми числами соответствуют заполненным узлам. Зеленые ячейки, заполненные единицами, помечают правильный остов; желтые ячейки, заполненные двойками, являются висячими циклами, которые определяет алгоритм Грассбергера; красные ячейки, заполненные тройками, являются висячими циклами, которые алгоритм Грассбергера ошибочно присоединяет к остову.

0	0	0	0	1	0	0	0	0
0	0	2	2	1	1	1	0	0
0	0	2	0	2	0	1	0	0
0	0	2	2	2	0	1	0	0
0	0	0	0	0	0	1	0	0
0	0	2	2	2	0	1	0	0
0	0	2	0	2	0	1	0	0
0	0	2	2	1	1	1	0	0
0	0	0	0	1	0	0	0	0

а

0	0	0	0	1	0	0	0	0
0	0	1	1	1	3	3	0	0
0	0	1	0	3	0	3	0	0
0	0	1	0	3	3	3	0	0
0	0	1	0	0	0	0	0	0
0	0	1	0	3	3	3	0	0
0	0	1	0	3	0	3	0	0
0	0	1	1	1	3	3	0	0
0	0	0	0	1	0	0	0	0

б

Рисунок 1 – Алгоритм Грассбергера: а) определяет висячие циклы слева; б) не определяет висячие циклы справа

Кроме этого, алгоритм Грассбергера обнаруживает висячие дуги с верхней стороны, но не обнаруживает висячие дуги с нижней стороны решетки. На рисунке 2 показана соответствующая конфигурация. Пометка цветами и числами аналогична рисунку 1.

0	2	0	2	0	0	1	0	2	0	2	0	0
0	2	0	2	0	1	1	0	2	0	2	0	0
0	2	0	2	0	1	0	0	2	0	2	0	0
0	2	0	2	0	1	0	0	2	2	2	0	0
0	2	0	2	0	1	0	0	0	0	0	0	0
0	2	0	2	0	1	0	0	0	3	3	3	0
0	2	0	2	0	1	1	1	0	3	0	3	0
0	2	2	2	0	0	0	1	0	3	0	3	0
0	0	0	0	0	0	0	1	0	3	0	3	0
0	0	3	3	3	0	0	1	0	3	0	3	0
0	0	3	0	3	0	0	1	0	3	0	3	0
0	0	3	0	3	0	1	1	0	3	0	3	0
0	0	3	0	3	0	1	0	0	3	0	3	0

Рисунок 2 – Алгоритм Грассбергера определяет висячие дуги сверху, но не определяет снизу

Для устранения проблемы висячих частей «с одной стороны» была реализована программа, которая помимо исходной решетки рассматривает еще три ориентации той же самой решетки: поворот решетки на 180 градусов, а также отражение относительно вертикальной и горизонтальной осей, программа GrassbergerFileBB4copy.cpp [28].

На рисунке 3 показаны конфигурации с четырьмя висячими циклами, которые алгоритму Грассбергера удается обнаружить лишь в одной из четырех ориентаций решетки (для каждого из четырех циклов своя ориентация).

0	1	0	0	0	0	0	0	0	0	0	0	0	1	0
0	1	0	3	3	3	0	0	0	3	3	3	0	1	0
0	1	0	3	0	3	0	0	0	3	0	3	0	1	0
0	1	1	1	3	3	0	0	0	3	3	1	1	1	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	1	1	1	1	1	1	1	1	1	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	0	0	1	1	1	1	1	1	1	1	1	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	1	1	1	3	3	0	0	0	2	2	1	1	1	0
0	1	0	3	0	3	0	0	0	2	0	2	0	1	0
0	1	0	3	3	3	0	0	0	2	2	2	0	1	0
0	1	0	0	0	0	0	0	0	0	0	0	0	1	0

Рисунок 3 – Алгоритм Грассбергера определяет каждый из висячих циклов лишь в одной из четырех ориентаций

Кроме этого, была сделана попытка распараллелить реализованный алгоритм с использованием технологии MPI. Рекурсивные алгоритмы, к которым относится алгоритм Грассбергера, плохо поддаются распараллеливанию, но было реализовано распределение четырех вышеупомянутых ориентаций одной и той же решетки между четырьмя MPI-процессами, программа GrassbergerFileBB4copyMPI.cpp [29]. Главный процесс занимается вводом решетки из файла, рассылкой введенной решетки на остальные процессы, обработкой основной ориентации решетки, сбором окончательного остова и выводом остова в файл. Остальные процессы получают от главного процесса массив с конфигурацией решетки, затем обрабатывают свою ориентацию решетки (поворот и отражения) и отправляют результат главному процессу.

Однако следует отметить, что существуют более сложные конфигурации висячих циклов, приведенные на рисунках 4 и 5, которые алгоритм Грассбергера не обнаруживает ни в одной из четырех ориентаций. Если узел остова, к которому присоединён висячий цикл, добавляется в остов до того, как произошёл заход в цикл, то висячий цикл тоже присоединяется к остову. Общей особенностью приведенных на рисунках 4 и 5 конфигураций является то, что в этих конфигурациях висячие циклы присоединены к циклам, принадлежащим остову. Хотя алгоритм Грассбергера делает периодическую смену направления поворота, но соответствующие принадлежащие остову циклы по алгоритму Грассбергера всегда проходятся так, что прикрепленный к ним висячий цикл всегда оказывается «с необнаруживаемой стороны». На рисунке 4 приведена конфигурация со вложенными висячими циклами, а на рисунке 5 приведена конфигурация с висячими циклами с краю. Также можно отметить, что конфигурации типа рисунка 5 могут реализовываться на меньших решетках, чем конфигурации типа рисунка 4.

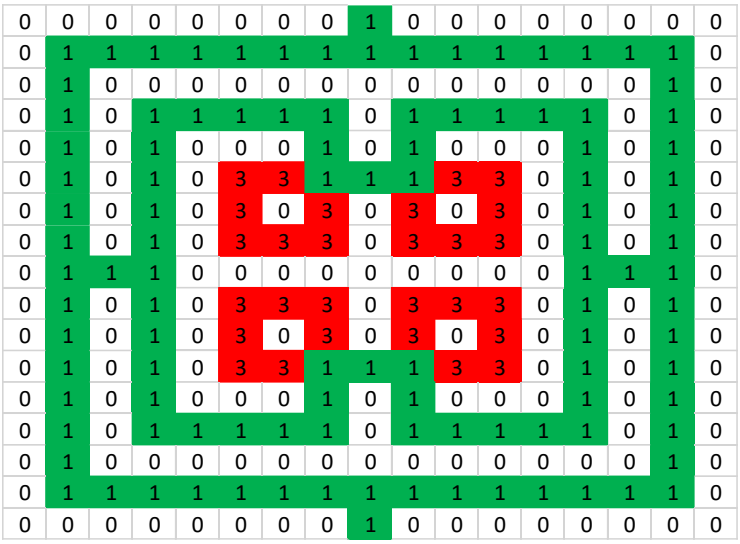


Рисунок 4 – Алгоритм Грассбергера не определяет вложенные висячие циклы ни в одной из четырех ориентаций

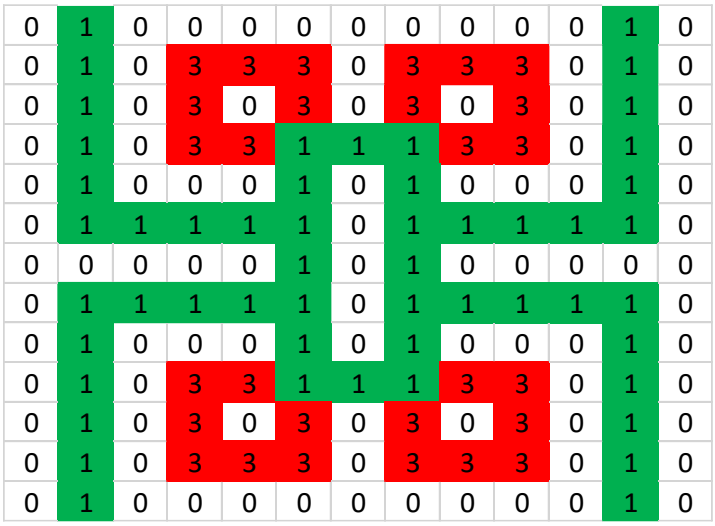


Рисунок 5 – Алгоритм Грассбергера не определяет висячие циклы по краям ни в одной из четырех ориентаций

Алгоритм Ахунжанова. Для устранения проблем алгоритма Грассбергера, связанных с присоединением висячих циклов, Ренатом Камилевичем Ахунжановым был предложен рекурсивный алгоритм, корректно находящий остовы в плоских графах [15]. Отметим, что, хотя в теории перколяции обычно рассматриваются графы без петель, а в статье [15] говорится о применении алгоритма к простым плоским графам, предложенный Ахунжановым алгоритм может быть обобщен для применения и на плоских графах с петлями.

Что касается опубликованного в статье [15] описания алгоритма, то прежде всего следует отметить досадную опечатку в псевдокоде функции NG: в строке 5 должно браться не ребро E, а ребро E', т.е. вместо оператора

$$5{:}V_1' \leftarrow AdjacentVertex\,(E, V_1, G)$$

должен быть оператор

$$5{:}V_1' \leftarrow AdjacentVertex\,(E', V_1, G)$$

К сожалению, в статье [15] не были ясно обозначены многие идеи, касающиеся общей организации алгоритма Ахунжанова, в частности практически не пояснялся псевдокод функции WF, а большая часть пояснений псевдокода функции NG сводилась к описанию чисто технических вспомогательных функций для нахождения смежной вершины ($AdjacentVertex$) и следующего ребра, прикрепленного к вершине ($NextEdge$). В статье [18] была предпринята попытка дать более подробное описание именно идей, реализованных в алгоритме, но, к сожалению, некоторые фразы в статье [18] только запутывают описание алгоритма Ахунжанова.

В качестве одного из достоинств алгоритма авторы отмечают, что алгоритм посещает не все ребра графа. Однако по неясным причинам авторы меняют терминологию: если в [15] авторы говорят о «непосещенных ребрах» (unvisited edges), то в [18] авторы говорят о «непройденных ребрах» (untraversed edges), хотя термин «посещение» (visiting) продолжают использовать. По-видимому, авторы рассматривают термины «непосещенные» и «непройденные» как синонимы, поэтому неясно, в чем преимущество использования термина «непройденные».

Еще одним существенным моментом, затрудняющим восприятие объяснений в [18], является то, что, хотя авторы ссылаются на предыдущую работу [15], к сожалению, никак не упоминают выделяемые в [15] две подпрограммы: функцию WF и процедуру NG. Более того, в [18] авторы не только не упоминают названий подпрограмм из [15], но даже вообще не говорят о выделении двух подпрограмм, из-за чего очень сложно сопоставить объяснения в [18] с описанием алгоритма, приводимым в [15]. По-видимому, первый абзац из параграфа «A. Модифицированный алгоритм следования вдоль стен» (A. Modified wall follower algorithm) приблизительно соответствует описанию функции WF, а новый словесный вариант псевдокода, состоящий из шага 1 (Step 1) и шага 2 (Step 2), в этом параграфе приблизительно соответствует описанию процедуры NG.

При описании алгоритма в [15] и [18] авторы предпочитают называть простые цепи аббревиатурой SAW. К сожалению, в словесных формулировках, описывающих алгоритм, и в [15], и в [18] встречается ряд неточностей. В частности, в [15] авторы говорят, что ищут все простые пути между входной вершиной V_{in} и выходной вершиной V_{out}. На самом деле, алгоритм не выделяет все простые пути между V_{in} и V_{out}, а выделяет *множество ребер, принадлежащих всем простым путям* между V_{in} и V_{out}. В [18] встречается еще более странная фраза о поиске множества всех SAWs между двумя заданными вершинами (входом V_{in} и выходом V_{out}), принадлежащих внешнему периметру G. Выделение всех SAWs, принадлежащих внешнему периметру, алгоритмом не реализуется, возможно, авторы имели в виду просто *множество всех ребер, принадлежащих внешнему периметру* G. Самый первый вызов функции WF, в действительности, выделяет самую левую простую цепь, принадлежащую внешнему периметру G. Далее в [18], по-видимому, для пояснения функции WF говорится, что каждый дважды пройденный перекресток (вершина $\deg V > 1$) указывает на простой цикл. На самом деле, в реализации функции WF дважды пройденные перекрестки могут соответствовать не только простым циклам, но и любым *циклическим путям* (в простом цикле повторяются только начальная и конечная вершина, а в циклических путях могут повторяться любые вершины и ребра), которые являются висячими частями.

Перечисление всех неточностей в [15] и [18] заняло бы много места, поэтому мы отметим только еще один наиболее существенный, на наш взгляд, недостаток – запутанное объяснение, сколько раз проходятся какие из ребер. В [15] авторы говорят только о посещенных и непосещенных ребрах, не уточняя, что некоторые ребра посещаются более одного раза. В [18] авторы в оценке худшего случая говорят, что ребра остова проходятся дважды, хотя на самом деле ребра остова проходятся алгоритмом трижды.

Поэтому далее мы попытаемся дать наше описание алгоритма и прояснить вопрос, сколько раз проходятся какие из ребер.

Процедура NG организует многократные вызовы функции WF для выделения простых цепей, принадлежащих остову. Процедура NG при помощи рекурсии проходит все ребра, присоединенные к остову («зеленые» ребра в терминах [15]), и при наличии инцидентных очередной вершине ребер, которые могут принадлежать остову, вызывает для обработки этих ребер функцию WF. Основной идеей, обеспечивающей применение рекурсии, является то, что процедура NG проходит присоединенные ранее к остову простые цепи, проверяя возможность присоединения новых простых цепей. С данной идеей тесно связано упоминаемое, но не объясняемое в [15] добавление удаляемых впоследствии фантомных зеленых ребер. Добавление фантомных ребер используется для первоначального запуска процедуры NG, которая предполагает, что уже была определена некоторая часть остова, и присоединение новых простых цепей осуществляется при проходе ранее определенных частей остова.

Каждый вызов функции WF определяет «гроздь» висячих частей и/или новую простую цепь, принадлежащую остову. Возможно определение «грозди» висячих частей, присоединённых к вершине V, для которой вызывается функция WF, а если будет определена простая цепь, принадлежащая остову, то будут также определены и все имеющие место висячие части, присоединенные к этой простой цепи слева, если рассматривать проход по этой простой цепи от вершины V до другого конца простой цепи. Функция WF красит внешний периметр висячих частей в желтый цвет, а принадлежащую остову простую цепь – в зеленый цвет.

В целом, алгоритм Ахунжанова может проходить ребра обрабатываемого графа от 0 до 3 раз (рисунок 6 иллюстрирует количество проходов):

- 0 раз проходятся ребра, которые являются внутренними ребрами висячих частей, т.е. не принадлежат к внешнему периметру висячих частей (черные ребра на рисунке 6). Внешний периметр висячих частей – это внешний периметр графа, получаемого объединением всех висячих частей;
- 1 раз проходятся ребра, которые принадлежат внешнему периметру висячих частей, но не являются мостами. Проход по этим ребрам делается функцией WF и, согласно [15], красит их в желтый цвет (желтые ребра на рисунке 6);
- 2 раза проходятся ребра, которые принадлежат внешнему периметру висячих частей и являются мостами (коричневые ребра на рисунке 6). Оба прохода делаются функцией WF, один проход по мосту делается для захода в висячую часть, другой – для выхода. Эти проходы, согласно [15], дважды красят ребро в желтый цвет;
- 3 раза проходятся ребра, принадлежащие остову (зеленые ребра на рисунке 6). В том числе сначала два прохода делаются функцией WF; согласно [15], первый проход делается, когда еще не найден второй конец принадлежащей остову простой цепи, и красит ребро в желтый цвет, второй проход делается для пометки ребра как принадлежащего остову и красит ребро в зеленый цвет. Третий проход делается процедурой NG для проверки, существуют ли еще простые цепи, которые следует присоединить к остову.

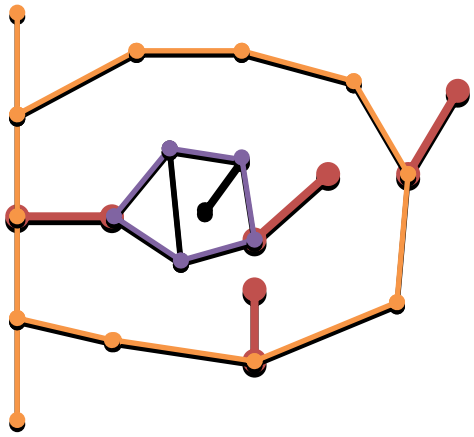


Рисунок 6 – Иллюстрация пояснения о количестве проходов по ребрам

Теоретическая оценка вычислительной сложности алгоритма Ахунжанова. В статье Ю.Ю. Тарасевича и др. [18] была проделана оценка вычислительной сложности алгоритма Ахунжанова для лучшего и для худшего случая. Авторы приводят оценку наилучшего случая сверху $O(\sqrt{N_v})$, рассматривая в качестве примера для наилучшего случая граф, показанный на рисунке 7.

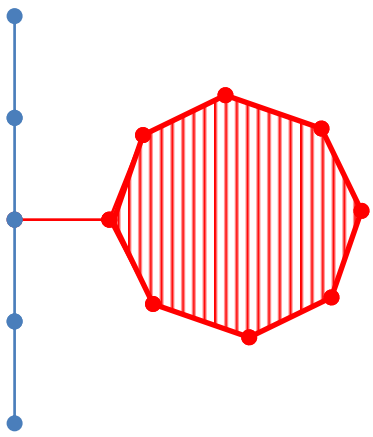


Рисунок 7 – Иллюстрация наилучшего случая в [18]

Однако не совсем ясно обоснование такой оценки. Авторы справедливо отмечают, что доля вершин и ребер, принадлежащих внешнему периметру графа, существенно зависит от структуры графа. Однако затем авторы делают вызывающее вопросы утверждение, что число вершин едва ли превышает $\sqrt{N_V}$, за исключением некоторых специально сконструированных графов. Следует отметить, что приводимый авторами граф является как раз специально сконструированным, а отнюдь не типичным для перколяционных задач. Если учесть, что авторы в своей статье рассматривают случайное осаждение стержней, концы и пересечения которых авторы считают вершинами графа, то при неравномерном осаждении стержней в некоторых областях моделирования может быть получена сколь угодно более высокая концентрация вершин. Рассматривая, например, случаи, когда огромное количество стержней попало внутрь красной заштрихованной области, можно получить графы с гораздо меньшей долей вершин, принадлежащих периметру, чем $\sqrt{N_V}$, например, $\sqrt[3]{N_V}$. Если считать такие графы лучшим случаем, то для них получается, соответственно, оценка сложности $O(\sqrt[3]{N_V})$, что существенно лучше предлагаемой авторами [18] оценки $O(\sqrt{N_V})$.

Можно предположить, что авторы имели в виду оценку лучшего случая «в среднем», хотя явно о том, что рассматривается усредненная оценка, авторы не пишут. Косвенным указанием на оценку лучшего случая в среднем является фраза о «специально сконструированных графах», поскольку эта фраза имеет обычно смысл лишь в контексте усреднения и означает в таком контексте, что случаи, называемые «специально сконструированными», имеют очень малую вероятность и не вносят заметного вклада в среднее значение. Авторы статьи справедливо отмечают, что наименьшая доля стержней и, соответственно, узлов принадлежит остову на пороге перколяции. Таким образом, если говорить о лучшем случае «в среднем», то можно предполагать, что авторы делали оценку лучшего случая «в среднем» на пороге перколяции. Однако при такой трактовке получается, что авторы [18] совсем забыли о том, что и кратчайший путь, который на рисунке 7 будет остовом, и внешний периметр (перколяционного кластера), который необходимо обойти на рисунке 7, на пороге перколяции имеют «в среднем» фрактальный характер.

В литературе можно найти соответствующие фрактальные размерности. Например, определенные с высокой точностью значения фрактальной размерности кратчайшего (минимального) пути можно найти в [32], где приводится значение $d_{min} = 1.13077(2)$, и в [33], где приводится значение $d_{SP} = 1.130 \pm 0.005$. Менее точное значение фрактальной размерности минимального пути $D_{min} = 1.13$ приводится в известной монографии Штауффера и Аарони [1, с. 52]. Точное значение фрактальной размерности внешнего периметра перколяционного кластера $D_e = \frac{4}{3}$ было получено для двумерной перколяции на основе модели кулоновского газа Салье и Дюплантье в 1987 году [34]. Недавние численные эксперименты показывают прекрасное согласие с точным значением данной размерности [35, 36].

Среднее количество вершин в графе N_V пропорционально квадрату размера моделируемой области L:

$$N_V \sim L^2, \tag{1}$$

откуда

$$L \sim N_V^{\frac{1}{2}}. \tag{2}$$

В то же время среднее количество вершин графа N_{min} во фрактальной структуре, имеющей размерность D_{min}, пропорционально соответствующей степени размера моделируемой области:

$$N_{min} \sim L^{D_{min}}. \tag{3}$$

Подставляя (2) в (3), получаем

$$N_{min} \sim \left(N_V^{\frac{1}{2}}\right)^{D_{min}} = N_V^{\frac{D_{min}}{2}}. \tag{4}$$

Используя значение $D_{min} = 1.13$ в формуле (4), получаем $N_{min} \sim N_V^{0,565}$, т.е. если сложность алгоритма пропорциональна числу вершин в кратчайшем пути N_{min}, то можно дать оценку сложности $O\left(N_V^{0,565}\right)$. Таким образом, при рассмотрении лучшего случая в среднем, даже если рассматривать обработку только кратчайшего пути с учетом его фрактальности, оценка сложности $O\left(N_V^{0,565}\right)$ оказывается заметно выше предлагаемой авторами [18] оценки $O(\sqrt{N_V})$.

Для среднего количества вершин графа во внешнем периметре N_e можно получить аналогично формуле (4) оценку

$$N_e \sim N_V^{\frac{D_e}{2}}. \tag{5}$$

Подставляя значение $D_e = \frac{4}{3}$ в формуле (5), получаем $N_e \sim N_V^{\frac{2}{3}}$, т.е. если сложность алгоритма пропорциональна числу вершин во внешнем периметре N_e, то можно дать оценку сложности

$O\left(N_V^{\frac{4}{3}}\right)$. Таким образом, если при рассмотрении лучшего случая в среднем рассматривать обработку вершин во внешнем периметре, то с учетом его фрактальности, оценка сложности $O\left(N_V^{\frac{4}{3}}\right)$ оказывается еще выше, чем предлагаемая авторами [18] оценка $O(\sqrt{N_V})$.

Особенности реализации алгоритма Ахунжанова. В приложении к статье Р.К. Ахунжанова и др. [15] на странице одного из соавторов статьи Ю.Ю. Тарасевича приводится реализация алгоритма на языке Python для плоских двумерных графов, образованных случайным осаждением стержней (файл BBSearcher.py) [29]. Разработчиком данной реализации является А.В. Есеркепов. Следует отметить некоторые существенные моменты, отличающие реализацию Есеркепова от описания алгоритма в статье [15].

Прежде всего, отметим, что в статье [15] процедура NG и функция WF имеют по четыре аргумента: $NG(E, V_1, V_2, G)$ и $WF(E_1, V, E_2, G)$, в то время как у Есеркепова [29] четвертый аргумент, соответствующий графу G, отсутствует. Вместо этого Есеркепов использует глобальные переменные, хранящие информацию о графе. Такой подход вполне разумен, чтобы уменьшить количество накапливаемых в стеке аргументов при рекурсивных вызовах процедуры NG, когда предполагается обработка всего лишь одного графа.

Еще одно существенное отличие программы Есеркепова заключается в том, что в ней была использована другая конфигурация добавочных ребер, отличающаяся от описанной в статье [15]. Согласно статье, добавляется два зеленых ребра, соединяющих вершины V_{in} и V_{out}. Одно из этих ребер используется в качестве начального ребра E_0, с которого начинается выполнение процедуры NG. Однако в программе Есеркепова добавляется только одно зеленое ребро между вершинами V_{in} и V_{out}, а еще одно зеленое ребро добавляется между вершиной V_{in} и еще одной, не описанной в статье добавочной вершиной V_0. Именно это ребро (V_0, V_{in}) используется в качестве начального ребра E_0 в программе Есеркепова при первом вызове процедуры $NG(E_0, V_{in}, V_{out})$. На рисунке 8 показано фактическое положение дополнительных ребер, соответствующее программе Есеркепова.

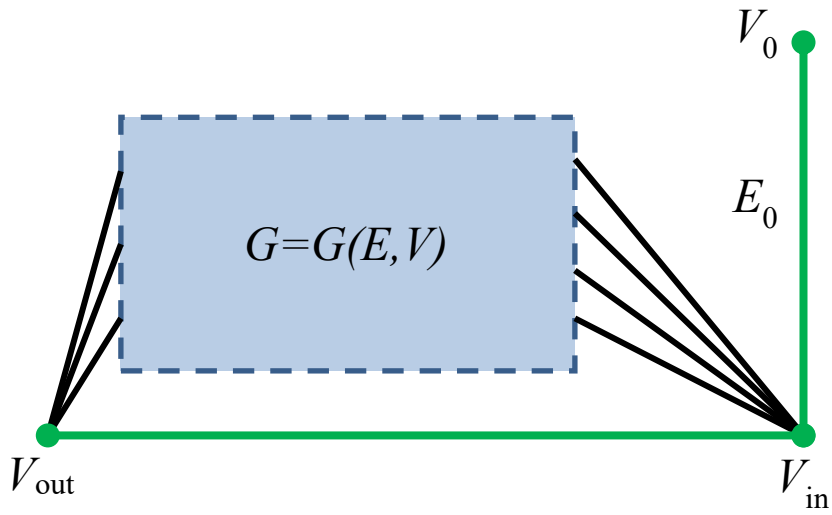


Рисунок 8 – Иллюстрация фактического расположения дополнительных ребер в программе Есеркепова

Такой вариант конфигурации дополнительных ребер для начального запуска процедуры NG тоже работает, поскольку для алгоритма Ахунжанова существенно только, чтобы существовал путь из зеленых ребер через вершину V_{in} до вершины V_{out}, а в конечном счете дополнительные ребра все равно удаляются. Однако следует более подробно остановиться на том, почему в реализации Есеркепова изменено расположение одного из дополнительных зеленых ребер. Дело в том, что соединение вершин V_{in} и V_{out} двумя различными ребрами превращает граф G в мультиграф, в котором есть кратные ребра между некоторыми парами вершин. Алгоритм Ахунжанова может с успехом обрабатывать плоские мультиграфы, но в реализации Есеркепова имеется еще одна не описанная в статье особенность, из-за которой была изменена конфигурация дополнительных ребер. Дело в том, что в реализации Есеркепова при каждом обращении к вершине выполняется сортировка прикрепленных к ней ребер против часовой стрелки, так чтобы рассматриваемое ребро оказалось первым в списке. С целью сортировки у Есеркепова рёбра рассматриваются как отрезки,

соединяющие вершины с определенными координатами на плоскости, но при таком подходе кратные ребра невозможно различить.

На самом деле, нет необходимости выполнять сортировку ребер при каждом обращении к вершине, гораздо эффективнее формировать список ребер, инцидентных вершине, сразу в порядке против часовой стрелки и рассматривать сформированный список ребер как циклический, что и было сделано нами при реализации алгоритма Ахунжанова в виде программы на C++ [30]. При этом нет необходимости рассматривать ребра как отрезки, соединяющие две точки на плоскости, а можно рассматривать соединение вершин и произвольными непрерывными линиями, что является необходимым для плоских мультиграфов. Отметим, что наша реализация алгоритма допускает обработку плоских мультиграфов и два зеленых добавочных ребра добавляются именно так, как описывается в статье Ахунжанова.

Экспериментальное сравнение алгоритмов. Было проделано экспериментальное сравнение алгоритмов по времени выполнения и доле отличий в остове на случайных решетках. Аналогично статье Грассбергера брались решетки с размерами $L = 5, 7, 10, 14, 20, 28, \ldots, 1280, 1792, 2560, 3584, 5120$. По сравнению со статьей Грассбергера максимальная сторона решетки была увеличена в 4 раза – с $L = 1280$ до $L = 5120$, соответственно, число узлов на решетке было увеличено в 16 раз. Для решетки каждого размера рассматривалось по 200 случайных реализаций. Поскольку в статье Грассбергера оценивались остовы на решетках, сгенерированные случайным смачиванием от низа решетки, то для объективности оценки неточностей в определении остова алгоритмом Грассбергера нами при тестировании всех алгоритмов рассматривались только случайные смачивания снизу решетки, сгенерированные с помощью программы PureGrasberger.cpp [28].

На рисунке 9 показана средняя доля отличий остова, получаемого алгоритмом Грассбергера, от остова, получаемого алгоритмом Ахунжанова, на решетках с размерами от $L = 80$ до $L = 5120$. Погрешность средней доли отличий показана на графике вертикальными штрихами. На всех случайных решетках такого размера обнаруживались отличия в остовах. На случайных решетках от $L = 5$ до $L = 56$ встречались экземпляры решеток без отличий. При $80 \leq L \leq 160$ было замечено некоторое возрастание среднего значения, затем определенной тенденции не было обнаружено.

Следует отметить, что, хотя средняя доля отличий не превышает 20 %, на некоторых случайных решетках остовы отличались более чем в 2 раза; максимально обнаруженное отличие на случайных решетках составляло 2,78 раза, т.е. 178 %. В файле InputGraph56_00167.txt [31] приводится пример случайной решетки с $L = 56$, на которой обнаружено отличие более чем в два раза. Остов, выделенный для этой решетки алгоритмом Грассбергера, приводится в файле BackboneGrasFile BB56_00167.txt, а остов, выделенный для этой решетки алгоритмом Ахунжанова, приводится в файле BackboneAkhunNoSortTailNoBus56_00167.txt [31]. Обнаруженный остов в обоих выходных файлах показан единицами.

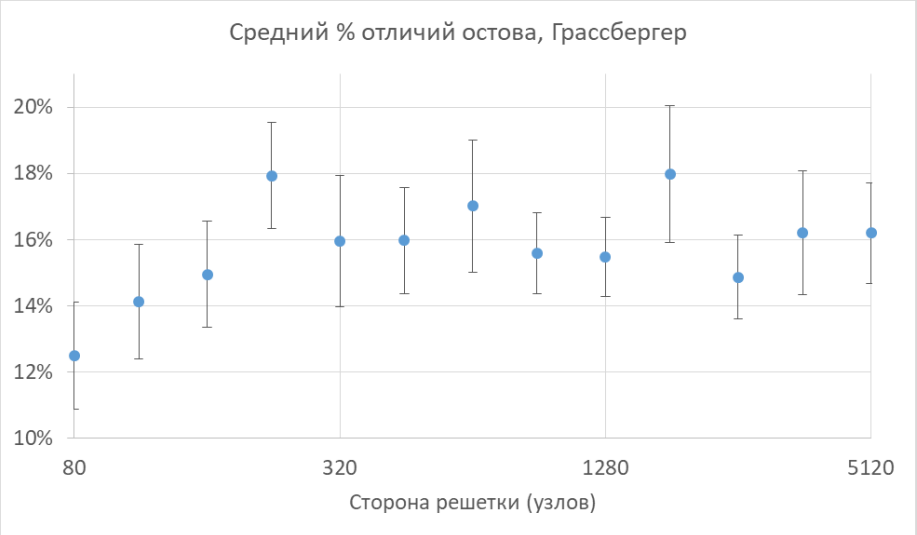


Рисунок 9 – Средний процент отличий остова, полученного алгоритмом Грассбергера, от остова, полученного алгоритмом Ахунжанова для разных размеров решеток

На рисунке 10 показана средняя доля отличий остова, получаемого применением алгоритма Грассбергера к четырем ориентациям решетки (отражения и повороты), от остова, получаемого алгоритмом Ахунжанова, на решетках с размерами от $L = 1792$ до $L = 5120$. Погрешность средней доли отличий показана на графике вертикальными штрихами. На всех случайных решетках такого размера обнаруживались отличия в остовах. На случайных решетках от $L = 40$ до $L = 1280$ встречались экземпляры решеток как с отличиями, так и без отличий. На случайных решетках от $L = 5$ до $L = 28$ отличий не встречалось. Заметна тенденция к увеличению отличия с увеличением размера решетки.

Следует отметить, что, хотя среднее отличие остова не превышало 0,05 %, на некоторых случайных решетках небольшого размера отличие составляло более 1%; максимальное обнаруженное отличие составляло 3,7 %. В файле InputGraph40_00178.txt [31] приводится пример случайной решетки с $L = 40$, на которой обнаружено отличие в 3,7 %. Остов, выделенный для этой решетки применением алгоритма Грассбергера с четырьмя ориентациями, приводится в файле Backbone Gras4copy40_00178.txt, а остов, выделенный для этой решетки алгоритмом Ахунжанова, приводится в файле BackboneAkhunNoSortTailNoBus40_00178.txt [31]. Обнаруженный остов в обоих выходных файлах показан единицами. Можно заметить, что отличие в 3,7 % было обнаружено в случае конфигурации типа, показанной на рисунке 5 (циклы по краям).

Для четырех версий программы был произведен замер времени, затрачиваемого в среднем на обработку одной решетки со стороной L узлов. Усреднение времени работы проводилось по 200 различным случайным заполнениям решетки. На рисунке 11 показаны графики зависимости среднего времени обработки решетки для четырех версий программы: алгоритм Грассбергера; алгоритм Грассбергера с четырьмя ориентациями; алгоритм Грассбергера с распараллеливанием на основе MPI по четырем ориентациям; алгоритм Ахунжанова. Стандартная погрешность для среднего времени обработки решетки не превышает размеров маркеров. На графиках показаны размеры решеток начиная с $L = 20$, поскольку на меньших размерах решеток от $L = 5$ до $L = 14$ погрешность в замерах времени оказывалась слишком большой.

Следует отметить, что с точки зрения точности определения остова алгоритм Грассбергера с четырьмя ориентациями и алгоритм Грассбергера с распараллеливанием на основе MPI по четырем ориентациям давали одинаковый результат, но на больш*и*х решетках распараллеленный алгоритм оказывался быстрее в 1,4 раза. Самым быстрым из четырех алгоритмов является алгоритм Грассбергера, который дает самую большую неточность в определении остова. На малых решетках от $L = 5$ до $L = 80$ самым медленным оказывался алгоритм Грассбергера с распараллеливанием на основе MPI по четырем ориентациям, а на больших решетках от $L = 112$ до $L = 5120$ самым медленным оказывался алгоритм Ахунжанова. Для алгоритма Грассбергера с четырьмя ориентациями на решетках от $L = 5$ до $L = 640$ распараллеленный на основе MPI алгоритм оказывался медленнее, чем нераспараллеленный, а на решетках от $L = 896$ до $L = 5120$ распараллеленный алгоритм оказывался быстрее. Более медленная работа на малых решетках объясняется тем, что доля времени затрачиваемого на взаимодействие программы со средой выполнения MPI превышает время, затрачиваемое на вычисления, а на больших решетках это время относительно невелико.

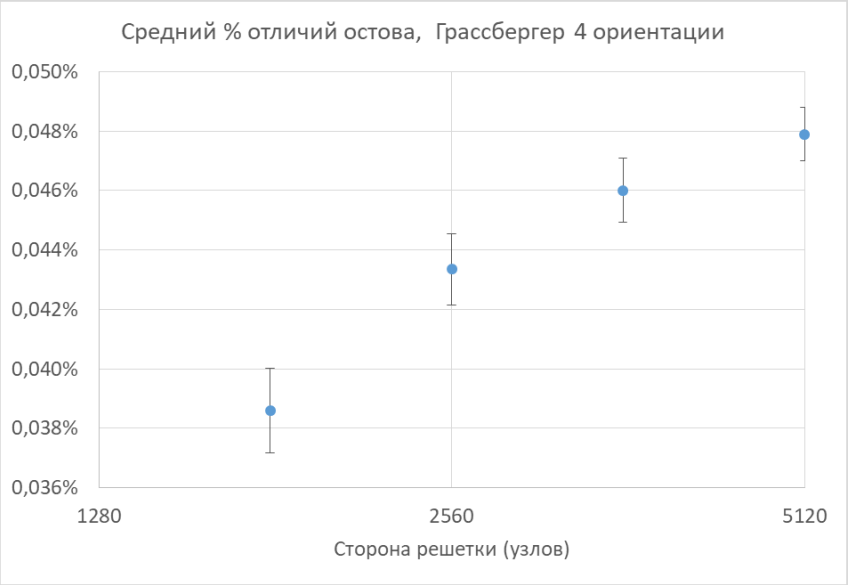


Рисунок 10 – Средний процент отличий остова, полученного алгоритмом Грассбергера с использованием четырех ориентаций, от остова, полученного алгоритмом Ахунжанова для разных размеров решеток

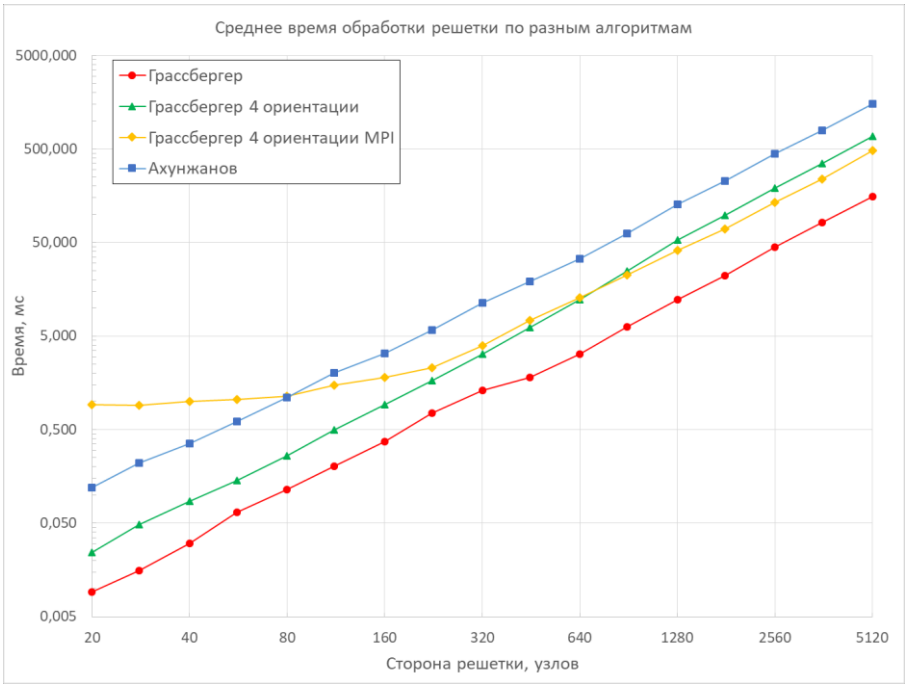


Рисунок 11 – График среднего времени обработки решетки для разных алгоритмов в зависимости от стороны решетки

Для тестирования всех программ использовался компьютер со следующими характеристиками:

- модель процессора – Intel (R) Core (TM) i3-10110U CPU;
- частота – 2,10 GHz;
- количество ядер – 2;
- количество логических процессоров – 4;
- количество оперативной памяти – 8 Гб;
- операционная система Windows 10.

Заключение. Был проделан сравнительный анализ алгоритма Грассбергера и алгоритма Ахунжанова для нахождения остова на квадратных решетках. Были выявлены недостатки алгоритма Грассбергера, связанные с неточным определением остова, и рассмотрен способ частичного устранения недостатков за счет анализа четырех ориентаций решетки.

Для алгоритма Ахунжанова был сделан более подробный теоретический анализ трудоемкости алгоритма, а также уточнены детали, связанные с количеством проходов по ребрам. Также было проделано численное сравнение результатов работы алгоритмов Ахунжанова и Грассбергера и сравнение времени их работы на решетках размером до 5120 х 5120 узлов.

Авторы благодарят А.В. Есеркепова за предоставленные исходные коды на языке Python. Также авторы благодарят Р.К. Ахунжанова и Ю.Ю. Тарасевича за стимулирующие обсуждения.

Библиографический список

1. Stauffer D. Introduction to Percolation Theory / D. Stauffer, A. Aharony. – London : Taylor and Francis, 1992.
2. Complex Media and Percolation Theory / eds: M. Sahimi, A. G. Hunt. – New York : Springer, 2021. 439 p.
3. Гордеев, И. И. Нахождение проводящего остова в двумерной решетке методом заливки / И. И. Гордеев, С. С. Овчаренко, А. А. Сизова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1 (49). – С. 94–111. – DOI: 10.21672/2074-1707.2020.49.4.094-111.
4. Tarasevich, Yu. Yu. Identification of current-carrying part of a random resistor network: electrical approaches vs. graph theory algorithms / Yu. Yu. Tarasevich, A. S. Burmistrov, V. A. Goltseva, I. I. Gordeev, V. I. Serbin, A. A. Sizova, I. V. Vodolazskaya, D. A. Zholobov // Journal of Physics: Conference Series. – 2018. – Vol. 955. – P. 012021. – DOI: 10.1088/1742-6596/955/1/012021.
5. Redner, S. Fractal and Multifractal Scaling of Electrical, Conduction in Random Resistor Networks / S. Redner // Mathematics of Complexity and Dynamical Systems. – 2011. – P. 446–462.
6. Ioselevich, A. S. Percolation with excluded small clusters and Coulomb blockade in a granular system / A. S. Ioselevich, D. S Lyubshin // Письма в Журнал экспериментальной и теоретической физики. – 2009. – Т. 90, № 10. – С. 746–752.

7. Deng, Y. Magnetic and backbone exponents of the percolation and Ising models in three dimensions / Y. Deng, H. W. J. Blöte // Physical Review E. – 2004. – Vol. 70. – P. 046106.

8. Jesper, L. J. A transfer matrix for the backbone exponent of two-dimensional percolation / L. J. Jesper, Z.-J. Paul // Journal of Physics A: Mathematical and General. – 2002. – Vol. 35 (9). – P. 2131–2144.

9. Grassberger, P. Conductivity exponent and backbone dimension in 2-d percolation / P. Grassberger // Physica A: Statistical Mechanics and its Applications. – 1999. – Vol. 262. – P. 251–263.

10. Large, M. J. Finite-size scaling in silver nanowire films: design considerations for practical devices / M. J. Large, M. Cann, S. P. Ogilvie, A. A. K. King, I. Jurewicz, A. B. Dalton // Nanoscale. – 2016. – Vol. 8. – P. 13701–13707.

11. Large, M. J. Selective mechanical transfer deposition of Langmuir grapheme films for high-performance silver nanowire hybrid electrodes / M. J. Large, S. P. Ogilvie, S. Alomairy, T. Vöckerodt, D. Myles, M. Cann, H. Chan, I. Jurewicz, A. King, A. B. Dalton // Langmuir. – 2017. – Vol. 33, № 43. – P. 12038–12045.

12. Kovacs, G. J. Effect of the substrate on the insulator–metal transition of vanadium dioxide films / G. J. Kovacs, D. Bürger, I. Skorupa, H. Reuther, R. Heller, H. Schmidt // Journal of Applied Physics. – 2011. – Vol. 109. – P. 063708.

13. Fleischner, H. Algorithms in Graph Theory. TU Wien, Algorithms and Complexity Group / H. Fleischner. – March 11, 2016. – Режим доступа: https://www.dbai.tuwien.ac.at/staff/kronegger/misc/AlgorithmsInGraph Theory_Script.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.08.2022).

14. Grassberger, P. Spreading and backbone dimensions of 2D percolation / P. Grassberger // Journal of Physics A: Mathematical and General. – 1992. – Vol. 25, № 21. – P. 5475–5484.

15. Akhunzhanov, R. K. Identification of a current-carrying subset of a percolation cluster using a modified wall follower algorithm / R. K. Akhunzhanov, A. V. Eserkepov, Y. Y. Tarasevich // Journal of Physics: Conference Series. – 2021. – Vol. 1740. – P. 012008.

16. Hong, D. C., Stanley H. E. Exact enumeration approach to fractal properties of the percolation backbone and 1/σ expansion / D. C. Hong, H. E. Stanley // Journal of Physics A: Mathematical and General. – 1983. – Vol. 16. – P. L475–L481.

17. Hong, D. C. Cumulant renormalisation group and its application to the incipient infinite cluster in percolation / D. C. Hong, H. E. Stanley // Journal of Physics A: Mathematical and General. – 1983. – Vol. 16. – P. L525–L529.

18. Tarasevich, Yu. Yu. Random nanowire networks: Identification of a current-carrying subset of wires using a modified wall follower algorithm / Yu. Yu. Tarasevich, R. K. Akhunzhanov, A. V. Eserkepov, M. V. Ulyanov // Physical Review E. – 2021. – Vol. 103. – P. 062145.

19. Roux, S. A new algorithm to extract the backbone in a random resistor network / S. Roux, A. Hansen // Journal of Physics A: Mathematical and General. – 1987. – Vol. 20. – P. L1281–L1285.

20. Yin, W.-G. Rapid algorithm for identifying backbones in the two-dimensional percolation model / W.-G Yin, R. Tao // International Journal of Modern Physics C. – 2003. – Vol. 14, № 10. – P. 1427–1437.

21. Leath, P. L. Cluster size and boundary distribution near percolation threshold / P. L. Leath // Physical review B. – 1976. – Vol. 14. – P. 5046.

22. Stauffer, D. Percolation Simulation: Large Lattices, Varying Dimensions / D. Stauffer, N. Jan // Annual Reviews of Computational Physics VIII. – Singapore, New Jersey, London, Hong Kong : World Scientific, 2001. – P. 287–300.

23. Гордеев, И. И. Сравнение различных описаний и реализаций алгоритма Лиса для перколяционных задач / И. И. Гордеев, А. А. Письменская // Научный форум: Технические и физико-математические науки : сб. ст. по материалам LIII Междунар. науч.-практ. конф. – Москва : МЦНО, 2022. – № 3 (53). – С. 49–55.

24. Hammersley, J. M. Monte Carlo Methods / J. M. Hammersley, D. C. Handscomb. – London : Me-thuen & Co Ltd., 1975.

25. RAND – Real pseudo-random number // The GNU Fortran Compiler. – Режим доступа: https://gcc.gnu.org/onlinedocs/gfortran/RAND.html, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 30.08.2021).

26. Kernighan, B. W. The C programming language / B. W. Kernighan, D. M. Ritchie. – London : Prentice-Hall International (UK) Limited, 1988.

27. Гордеев, И. И. Анализ недостатков алгоритма Грассбергера для поиска перколяционного остова на квадратной решетке и возможности его распараллеливания / И. И. Гордеев, Н. С. Саенко // Актуальные проблемы информационно-телекоммуникационных технологий и математического моделирования в современной науке и промышленности : материалы I Междунар. науч.-практ. конф. молодых учёных, Комсомольск-на-Амуре, 20–25 марта 2021 г. / редкол.: А. Л. Григорьева (отв. ред.), Я. Ю. Григорьев, И. А. Трещев. – Комсомольск-на-Амуре : ФГБОУ ВО «КнАГУ», 2021. С. 12–14. – DOI: 10.17084/978-5-7765-1488-3-2021-12.

28. G2ii2g. Grassberger-backbone2 // GitHub. – Режим доступа: https://github.com/G2ii2g/Grassberger-backbone2, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.07.2022).

29. Eserkepov, A. V. BBSearcher.py / A. V. Eserkepov // ResearchGate. – Режим доступа: https://www.researchgate.net/publication/349366739_BBSearcherpy/link/602cc40a4585158939ad6dd5/download, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 07.05.2021).

30. G2ii2g. Akhunzhanov-backbone // GitHub. – Режим доступа: https://github.com/G2ii2g/Akhunzhanov-backbone, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 08.08.2022).

31. G2ii2g. Grassberger-backbone2/tests // GitHub. – Режим доступа: https://github.com/G2ii2g/Grassberger-backbone2/tree/main/tests, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 08.08.2022).

32. Zhou, Z. Shortest-path fractal dimension for percolation in two and three dimensions / Z. Zhou, J. Yang, Y. Deng, R. Ziff // Physical Review E. – 2012. – Vol. 86. – P. 061101.

33. Schrenk, K. J. Percolation with long-range correlated disorder / K. J. Schrenk, N. Posé, J. J. Kranz, L. V. M. van Kessenich, N. A. M. Araújo, H. J. Herrmann // Physical Review E. – 2013– . Vol. 88. – P. 052102.

34. Saleur, H. Exact Determination of the Percolation Hull Exponent in Two Dimensions / H. Saleur, B. Duplantier // Physical Review Letters. – 1987. – Vol. 58. – P. 2325–2328.

35. Xu, X. Geometric structure of percolation clusters / X. Xu, J. Wang, Z. Zhou, T. M. Garoni, Y. Deng // Physical Review E. – 2014. – Vol. 89. – P. 012120.

36. d'Auriac, J.-C. A. Statistics of percolating clusters in a model of photosynthetic bacteria / J.-C. A. d'Auriac, F. Iglói // Physical Review E. – 2021. – Vol. 103. – P. 052103.

References

1. Stauffer, D., Aharony, A. *Introduction to Percolation Theory*. London, Taylor and Francis, 1992.

2. Sahimi, M., Hunt, A. G. (eds). *Complex Media and Percolation Theory*. New York : Springer, 2021. 439 p.

3. Gordeev, I. I., Ovcharenro, S. S., Sizova, A. A. Nakhozhdenie provodyashchego ostova v dvumernoy reshetke metodom zalivki [The determination of the conducting backbone in a two-dimensional lattice by the flooding method]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 1 (49), pp. 94–111. DOI: 10.21672/2074-1707.2020.49.4.094-111.

4. Tarasevich, Yu. Yu., Burmistrov A. S., Goltseva V. A., Gordeev I. I., Serbin V. I., Sizova A. A., Vodolazskaya I. V., Zholobov D. A. Identification of current-carrying part of a random resistor network: electrical approaches vs. graph theory algorithms. *Journal of Physics: Conference Series*, 2018, Vol. 955, p. 012021. DOI: 10.1088/1742-6596/955/1/012021.

5. Redner, S. Fractal and Multifractal Scaling of Electrical, Conduction in Random Resistor Networks. *Mathematics of Complexity and Dynamical Systems*, 2011, pp. 446–462.

6. Ioselevich, A. S., Lyubshin, D. S. Percolation with excluded small clusters and Coulomb blockade in a granular system. *Pisma v Zhurnal eksperimentalnoy b teoreticheskoy fiziki* [Journal of Experimental and Theoretical Physics Letters], 2009, vol. 90, no. 10, pp. 746–752.

7. Deng, Y., Blöte, H. W. J. Magnetic and backbone exponents of the percolation and Ising models in three dimensions. *Physical Review E*. 2004. Vol. 70. 046106.

8. Jesper, L. J., Paul, Z.-J. A transfer matrix for the backbone exponent of two-dimensional percolation. *Journal of Physics A: Mathematical and General*, 2002, vol. 35 (9), pp. 2131–2144.

9. Grassberger, P. Conductivity exponent and backbone dimension in 2-d percolation. *Physica A: Statistical Mechanics and its Applications*, 1999, vol. 262, pp. 251–263.

10. Large, M. J., Cann, M., Ogilvie, S. P., King, A. A. K., Jurewicz, I., Dalton, A. B. Finite-size scaling in silver nanowire films: design considerations for practical devices. *Nanoscale*, 2016, vol. 8, pp. 13701–13707.

11. Large, M. J., Ogilvie, S. P., Alomairy, S., Vöckerodt, T., Myles, D., Cann, M., Chan, H., Jurewicz, I., King, A., Dalton, A. B. Selective mechanical transfer deposition of Langmuir grapheme films for high-performance silver nanowire hybrid electrodes. *Langmuir*, 2017, vol. 33, no. 43, pp. 12038–12045.

12. Kovacs, G. J., Bürger, D., Skorupa, I., Reuther, H., Heller, R., Schmidt, H. Effect of the substrate on the insulator–metal transition of vanadium dioxide films. *Journal of Applied Physics*, 2011, vol. 109, p. 063708.

13. Fleischner, H. *Algorithms in Graph Theory*. TU Wien, Algorithms and Complexity Group, March 11, 2016. Available at: https://www.dbai.tuwien.ac.at/staff/kronegger/misc/AlgorithmsInGraphTheory_Script.pdf (accessed 11.08.2022).

14. Grassberger, P. Spreading and backbone dimensions of 2D percolation. *Journal of Physics A: Mathematical and General*, 1992, vol. 25. no. 21. pp. 5475–5484.

15. Akhunzhanov, R. K., Eserkepov, A. V., Tarasevich, Y. Y. Identification of a current-carrying subset of a percolation cluster using a modified wall follower algorithm. *Journal of Physics: Conference Series*, 2021, vol. 1740, p. 012008.

16. Hong, D. C., Stanley, H. E. Exact enumeration approach to fractal properties of the percolation backbone and 1/σ expansion. *Journal of Physics A: Mathematical and General*, 1983, vol. 16, pp. L475–L481.

17. Hong, D. C., Stanley, H. E. Cumulant renormalisation group and its application to the incipient infinite cluster in percolation. *Journal of Physics A: Mathematical and General*, 1983, vol. 16, pp. L525–L529.

18. Tarasevich, Yu. Yu., Akhunzhanov, R. K., Eserkepov, A. V., Ulyanov, M. V. Random nanowire networks: Identification of a current-carrying subset of wires using a modified wall follower algorithm. *Physical Review E*., 2021, vol. 103. 062145.

19. Roux, S., Hansen, A. A new algorithm to extract the backbone in a random resistor network. *Journal of Physics A: Mathematical and General*, 1987, vol. 20, pp. L1281–L1285.

20. Yin, W.-G., Tao, R. Rapid algorithm for identifying backbones in the two-dimensional percolation model. *International Journal of Modern Physics C*., 2003, vol. 14, no. 10, pp. 1427–1437.

21. Leath, P. L. Cluster size and boundary distribution near percolation threshold. *Physical review B*., 1976, vol. 14, p. 5046.

22. Stauffer, D., Jan, N. Percolation Simulation: Large Lattices, Varying Dimensions. *Annual Reviews of Computational Physics VIII*. Singapore, New Jersey, London, Hong Kong : World Scientific, 2001, pp. 287–300.

23. Gordeev, I. I., Pismenskaya, A. A. Sravnenie razlichnykh opisaniy i realizatsiy algoritma Lisa dlya perkolyatsionnykh zadach [Comparision of different descriptions and implementations of the Leath algorithm for percolation problems]. *Nauchnyy forum: Tekhnicheskie i fiziko-matematicheskie nauki : sbornik statey po materialam LIII*

mezhdunarodnoy nauchno-prakticheskoy konferentsii [Scientific forum: Technical and physical and mathematical sciences : a collection of articles based on the materials of the LIII International scientific-practical conference]. Moscow, ICSE LLC, 2022, no. 3 (53), pp. 49–55.

24. Hammersley, J. M., Handscomb, D. C. *Monte Carlo Methods*. London, Me-thuen & Co Ltd., 1975.

25. *RAND – Real pseudo-random number*. The GNU Fortran Compiler. Available at: https://gcc.gnu.org/onlinedocs/gfortran/RAND.html (accessed 30.08.2021).

26. Kernighan, B. W., Ritchie, D. M. *The C programming language*. London, Prentice-Hall International (UK) Limited, 1988.

27. Gordeev, I. I., Saenko, N. S. Analiz nedostatkov algoritma Grassbergera dlya poiska perkolyacionnogo ostova na kvadratnoj reshetke i vozmozhnosti ego rasparallelivaniya [Analysis of disadvantages of Grassberger's algorithm finding percolating backbone on square lattice and the possibility of its parallelization]. *Aktualnye problemy informatsionno-telekommunikatsionnykh tekhnologiy i matematicheskogo modelirovaniya v sovremennoy nauke i promyshlennosti: materialy I Mezhdunarodnoy nauchno-prakticheskoy konferentsii molodykh uchenykh, Komsomolsk-na-Amure, 20–25 marta 2021* [Actual problems of information and telecommunication technologies and mathematical modeling in modern science and industry: materials of the I International scientific-practical conference of young scientists, Komsomolsk-on-Amur, March 20–25, 2021]. Komsomolsk-on-Amur, FGBOU VO « KnAGU », 2021, pp. 12−14. DOI: 10.17084/978-5-7765-1488-3-2021-12.

28. G2ii2g. *Grassberger-backbone2*. GitHub. Available at: https://github.com/G2ii2g/Grassberger-backbone2 (accessed 28.07.2022).

29. Eserkepov, A. V. *BBSearcher.py*. ResearchGate. Available at: https://www.researchgate.net/publication /349366739_BBSearcherpy/link/602cc40a4585158939ad6dd5/download (accessed 07.05.2021).

30. G2ii2g. *Akhunzhanov-backbone*. GitHub. Available at: https://github.com/G2ii2g/Akhunzhanov-backbone (accessed 08.08.2022).

31. G2ii2g. *Grassberger-backbone2/tests*. GitHub. Available at: https://github.com/G2ii2g/Grassberger-backbone2/tree/main/tests (accessed 08.08.2022).

32. Zhou, Z., Yang, J., Deng, Y., Ziff, R. Shortest-path fractal dimension for percolation in two and three dimensions. *Physical Review E*., 2012, vol. 86, p. 061101.

33. Schrenk, K. J., Posé, N., Kranz, J. J., van Kessenich, L. V. M., Araújo, N. A. M., Herrmann, H. J. Percolation with long-range correlated disorder. *Physical review E*., 2013, vol. 88, p. 052102.

34. Saleur, H., Duplantier, B. Exact Determination of the Percolation Hull Exponent in Two Dimensions. *Physical Review Letters*, 1987, vol. 58, pp. 2325–2328.

35. Xu, X., Wang, J., Zhou, Z., Garoni, T. M., Deng, Y. Geometric structure of percolation clusters. *Physical Review E*., 2014, vol. 89, p. 012120.

36. d'Auriac, J.-C. A., Iglói, F. Statistics of percolating clusters in a model of photosynthetic bacteria. *Physical Review E*. 2021. vol. 103, p. 052103.

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DOI 10.54398/20741707_2022_3_61
УДК 004.032.26

МЕТОДИКА ОБНАРУЖЕНИЯ АТАК СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НА ОСНОВЕ АЛГОРИТМОВ АНАЛИЗА ЕСТЕСТВЕННОГО ЯЗЫКА

Статья поступила в редакцию 22.06.2022, в окончательном варианте – 31.08.2022.

Частикова Вера Аркадьевна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-2372-8275, e-mail: chastikova_va@mail.ru
Гуляй Виктория Геннадьевна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
студентка, ORCID: 0000-0002-3131-5705, e-mail: ms.gulyay@bk.ru

В последнее время наравне с техническими атаками на пользователей различных электронных коммуникационных систем возросло количество атак социальной инженерии. Так, за последний год был зафиксирован прирост атак социальной инженерии более чем на 90 %. Существующие на данный момент готовые продукты различных производителей не способны в полной мере бороться с атаками подобного типа. В данной работе рассматривается новый подход к решению задач по обнаружению атак социальной инженерии – применение алгоритмов анализа естественного языка. С целью экспериментальной проверки возможности использования данных методов в рамках поставленной задачи были реализованы следующие алгоритмы: языковая модель bag-of-words, алгоритм вложения слов Word2Vec и метод BERT, базирующийся на архитектуре Трансформер. По результатам проведенных исследований выявлено, что лучшие результаты показала модель BERT, у которой точность обработки данных контрольной выборки составила 97,35 %. Также стоит отметить алгоритм bag-of-words, имеющий значительное преимущество относительно других моделей в скорости обработки данных – примерно 1–2 м/с на одну эпоху обработки данных. Алгоритм Word2Vec показал средние результаты относительно моделей bag-of-words и BERT.

Ключевые слова: атака социальной инженерии, алгоритм анализа естественного языка, bag-of-words, Word2Vec, BERT

METHODOLOGY OF SOCIAL ENGINEERING ATTACK DETECTION BASED ON NATURAL LANGUAGE ANALYSIS ALGORITHMS

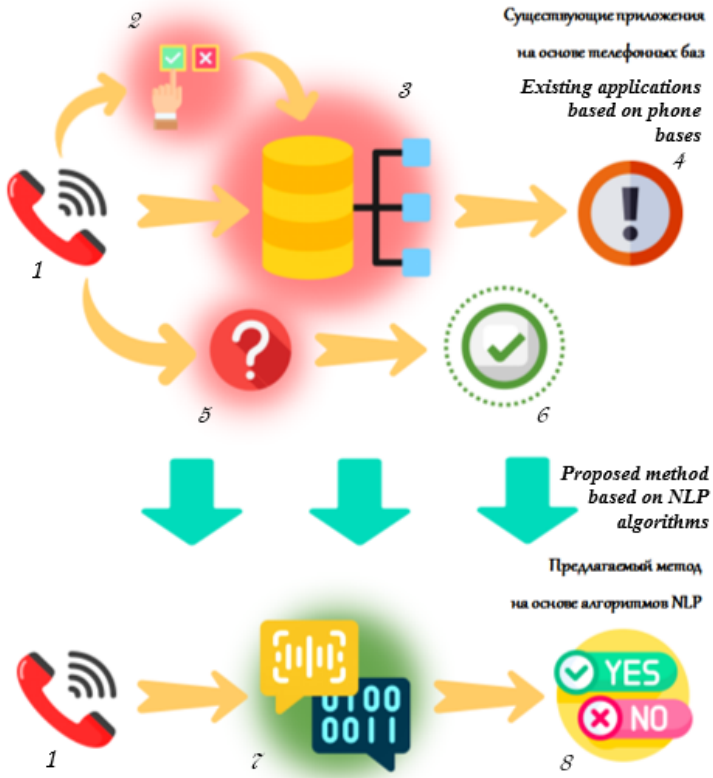
The article was received by the editorial board on 22.06.2022, in the final version – 31.08.2022.

Chastikova Vera A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-2372-8275, e-mail: chastikova_va@mail.ru
Gulyai Victoria G., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
student, ORCID: 0000-0002-3131-5705, e-mail: ms.gulyay@bk.ru

Recently, along with technical attacks on users of various electronic communication systems, the number of social engineering attacks has increased. So, over the past year, an increase in social engineering attacks has been recorded by more than 90 %. Currently existing ready-made products from various manufacturers are not able to fully combat attacks of this type. In this paper, we consider a new approach to solving problems of detecting social engineering attacks - the use of natural language analysis algorithms. In order to experimentally test the possibility of using these methods within the framework of the task, the following algorithms were implemented: the bag-of-words language model, the Word2Vec word embedding algorithm and the BERT method based on the Transformer architecture. According to the results of the study, it was found that the best results were shown by the BERT model, in which the accuracy of processing data from the control sample was 97.35 %. It is also worth noting the bag-of-words algorithm, which has a significant advantage over other models in data processing speed - approximately 1-2 ms per data processing epoch. The Word2Vec algorithm showed average results relative to the bag-of-words and BERT models. This word embedding algorithm has a processing accuracy advantage over the bag-of-words language model, and a processing speed advantage over the BERT algorithm.

Keywords: social engineering, natural language processing algorithms, bag-of-words, Word2Vec, BERT

Graphical annotation (Графическая аннотация)



1 – входящий звонок; 2 – пользователь делает отметку в специальном приложении о возможной угрозе атаки социальной инженерии, содержащейся во входящем звонке (субъективная оценка); 3 – телефонная база данных, содержащая в себе номера телефонов и пометки, сделанные пользователями; 4 – оповещение пользователя об угрозе; 5 – атака социальной инженерии с номера телефона, не зарегистрированного в телефонной базе; 6 – программа считает звонок безопасным и не предупреждает пользователя о реальной угрозе; 7 – программный комплекс на основе алгоритмов обработки естественного языка анализирует разговор (объективная оценка); 8 - программа выдает пользователю отчет о проделанном анализе и предупреждает его в случае атаки социальной инженерии.

Введение. На фоне событий последних двух лет наравне с техническими атаками на пользователей сети участились атаки с использованием методов социальной инженерии. Так, по данным Центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком» в 2021 году атаки с применением методов социальной инженерии составили около 30 % от всех осуществленных кибератак. Также согласно опросу, проведенному российской исследовательской компанией «Антифишинг» [7], доля пользователей, подвергшихся атакам мошенников, применяющих методы социальной инженерии, составила 86,4 % от всех пользователей сети, из которых порядка 18,7 % понесли серьезный ущерб. Таким образом, примерно каждый пятый человек, в адрес которого была осуществлена атака социальной инженерии, понес ощутимые материальные или финансовые потери, а также неизбежно подвергся утечке персональных данных (рис. 1).

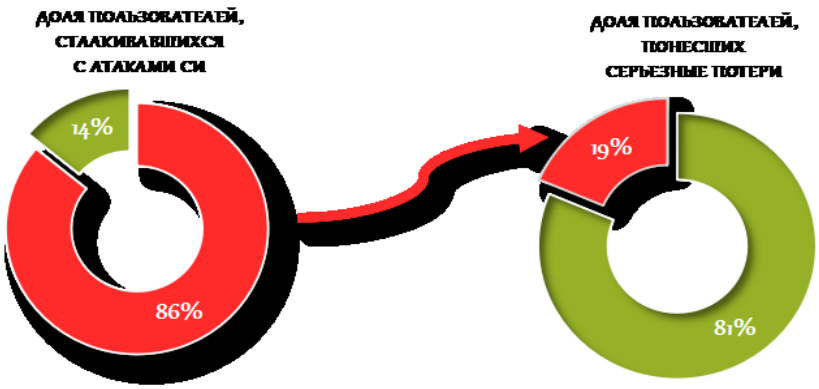


Рисунок 1 – Доля пользователей сети, подвергшихся атакам социальной инженерии и понесщих убытки соответственно

Также по данным, предоставленным российской исследовательской компанией «Антифишинг», было выявлено, что в последнее время мошенники все чаще стали использовать в своих целях вишинг *(англ. vishing, от Voice phishing)* – «выманивание» интересующей информации путем совершения телефонных звонков. Так, в рамках опроса [7] с вишингом сталкивались порядка 59 % опрошенных (рис. 2).

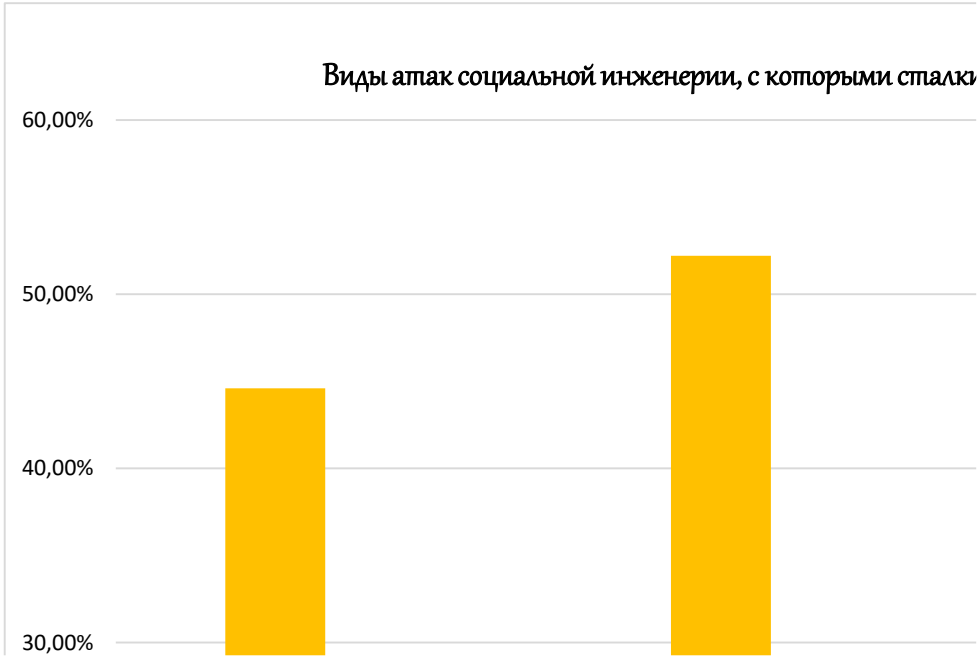


Рисунок 2 – Виды атак социальной инженерии, с которыми сталкивались пользователи за 2021 год

Обзор проблемной области. Неутихающий рост атак социальной инженерии объясняется тем, что такие атаки являются своего рода «взломом» человека, так как зачастую жертва самостоятельно выдает мошеннику всю необходимую ему конфиденциальную информацию [3]. В большинстве случаев такой способ требует от злоумышленника гораздо меньших затрат по сравнению с другими типами атак. Уже не приходится приобретать или создавать специализированное оборудование, позволяющее достигать мошеннику поставленных целей. Так, например, в случае вишинговых атак злоумышленнику достаточно лишь совершить телефонный звонок и представиться сотрудником банка/полиции/налоговой службы или придумать более изощренный способ выманивания персональных данных [3]. Главным остается одно: злоумышленнику не требуется иметь специальные навыки или особое оборудование, а соответственно, такой способ даже если не принесет выгоды, то и серьезных расходов не потребует. Благодаря этому мошенники для реализации своих целей все чаще обращаются именно к такому способу атаки.

Также стоит отметить, что некоторые способы атак социальной инженерии, такие как вишинг и фишинг, могут объединятся и с другими методами [4], представленными в таблице 1.

Таблица 1 – Методы социальной инженерии, совмещающиеся с фишинговыми и вишинговыми атаками

Название метода	Описание	Пример
Претекстинг	Использование некого предлога для выманивания у жертвы конфиденциальной информации; в большинстве случаев является неотъемлемой частью вишинга.	Мошенник совершает телефонный звонок, в котором представляется сотрудником банка и сообщает, что карта человека, которому он звонит заблокирована, для ее разблокировки необходимо сообщить номер карты и ее пин-код.
Троянский конь	Отправка пользователю сети сообщения, содержащего вредоносную ссылку, – один из самых распространенных вариантов фишинга.	На электронную почту человеку приходит письмо с описанием какого-либо очень выгодного предложения, например, скидки на нужный пользователю товар. Заинтересовавшейся жертве для более подробного ознакомления предлагается перейти по ссылке на сайт компании, продающей товар по сниженной цене. Однако ссылка оказывается ложной, и вместо перехода на сайт человек скачивает на свой компьютер или телефон вирус.

Продолжение таблицы 1

Кви про кво (услуга за услугу)	Способ, непосредственно связанный с такими видами атак, как фишинг и вишинг, так как зачастую является их основной составляющей.	Мошенник совершает звонок в крупную компанию, представившись техническим менеджером, узнает у сотрудников о наличии каких-либо неполадок в системе, после чего под предлогом «устранения» неполадок получает доступ к системе.
Обратная социальная инженерия	Способ, предполагающий ситуацию, когда жертва сама будет вынуждена обратиться к мошеннику за помощью. Такой способ часто является продолжением атаки вида «Троянский конь».	После предварительного запуска вируса на компьютере жертвы мошенник делает рассылку писем от лица фирмы, занимающейся устранением компьютерных вирусов, по электронным адресам жертв.
Лечевой серфинг	Самый простой способ получения персональных данных – подглядывание, подслушивание и т.д. Мошенник получает персональные данные жертвы путем плечевого серфинга, а затем использует их в ходе вишинговой атаки для достижения доверия со стороны жертвы.	Так, услышав, как человек в общественном месте диктует номер своего телефона и называет имя, мошенник получает возможность втереться в доверие при совершении звонка от имени сотрудника каких-либо служб. Также мошенник может пойти дальше и проследить за будущей жертвой с целью получить большее количество данных: подсмотреть номер карты на кассе в магазине, отследить, где человек работает и т.д.

Другие виды социальной инженерии, такие как «дорожное яблоко», – способ, аналогичный «троянскому коню», только имеющий не электронный, а физический вид, и реклама зачастую носит самостоятельный характер.

Возможные пути решения рассматриваемой проблемы. На данный момент существуют приложения, позволяющие вычислять мошенников, использующих в своих целях телефонную связь. Однако все они работают по одинаковому механизму, представленному на рисунке 3.

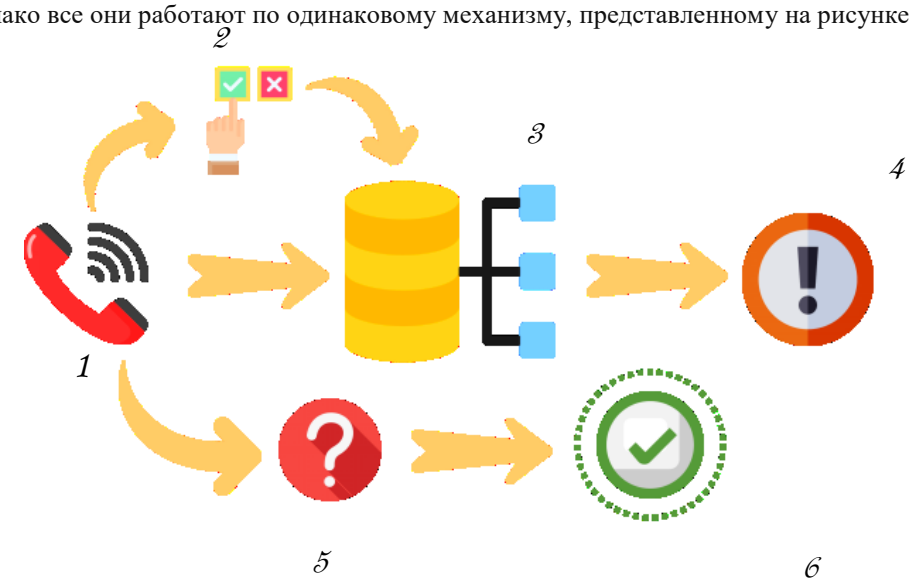


Рисунок 3 – Обобщенная схема функционирования существующих приложений для выявления телефонных мошенников: 1 – входящий звонок; 2 – пользователь делает отметку в специальном приложении о возможной угрозе атаки социальной инженерии, содержащейся во входящем звонке (субъективная оценка); 3 – телефонная база данных, содержащая в себе номера телефонов и пометки, сделанные пользователями; 4 – оповещение пользователя об угрозе; 5 – атака социальной инженерии с номера телефона, не зарегистрированного в телефонной базе; 6 – программа считает звонок безопасным и не предупреждает пользователя о реальной угрозе

Ядром каждого такого приложения является телефонная база данных, состоящая, главным образом, из номеров телефонов, содержащих различные пометки: «Спам», «Мошенник», «Робот» и т.д. Каждое конкретное приложение имеет свой набор меток. Данные приложения в зависимости от состава базы данных можно разделить на два типа:

- приложения, хранящие в базе данных только номера телефонов, имеющие метки;
- приложения, хранящие в базе данныхвсе контакты устройства, на котором данное приложение установлено.

Первый тип приложений является более безопасным, так как вероятность утечки персональных данных ниже по сравнению со вторым типом, где вопрос о сохранности личных сведений остается открытым. Это связано с тем, что подобные базы не раз из-за утечек различного рода попадали непосредственно в руки мошенников [6].

Также важно учесть, что маркируют номера телефонов сами пользователи, опираясь на свои личные ощущения, которые могут меняться и становиться обманчивыми под влиянием различных факторов, как внутренних, так и внешних. Человек может поддаться умелым убеждением мошенника и не заподозрить обмана или, наоборот, решив перестраховаться, поставить метку на номер телефона, звонок с которого не нес в себе никакой угрозы. Также в спешке человек может просто забыть пометить подозрительный номер телефона. Таким образом, такие данные являются весьма субъективными.

Ключевым моментом в механизме работы данного рода приложений является поиск в базе данных номера телефона, с которого осуществляется входящий звонок на телефон пользователя приложения. При наличии какой-либо метки у данного номера пользователю выводится оповещение с информацией о наличии возможной угрозы.

Однако такие приложения имеют еще один серьезный недостаток: если мошенник производит звонок с номера телефона, незарегистрированного в базе данных, то система не сможет заподозрить опасность, даже если этот разговор будет носит реальную угрозу для сохранности персональных данных или финансовых средств пользователя. Это связано с тем, что все приложения такого рода сфокусированы на фиксации и дальнейшем поиске номера телефона звонившего в базе данных, а не на анализе семантической значимости телефонного разговора.

Предлагаемый вариант решения. В рамках данной работы было проведено исследование, в ходе которого было выявлено, что в борьбе с мошенничеством путем применения методов социальной инженерии наиболее эффективными будут алгоритмы анализа естественного языка, так как обработка естественного языка на данный момент является одной из наиболее современных и стремительно развивающихся областей искусственного интеллекта, а также с ее помощью становится возможным анализировать семантическую нагрузку текстов, воспроизводимых на естественном языке [4, 5].

Так, одним из вариантов решения задач, связанных с обнаружением и нейтрализацией атак социальной инженерии, является создание программного комплекса, базирующегося на алгоритмах обработки естественного языка. Обобщенный принцип работы такого программного комплекса представлен на рисунке 4.

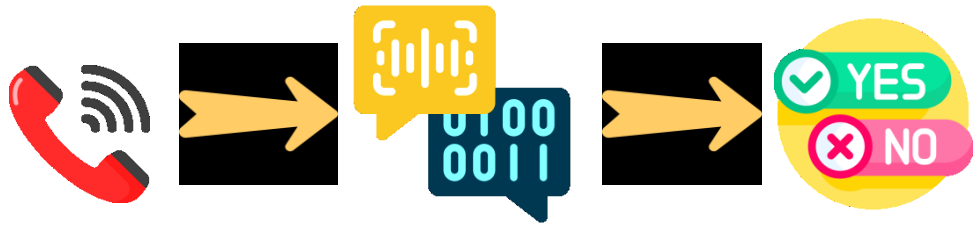


Рисунок 4 – Обобщенная схема работы предлагаемой методики: 1 – входящий звонок; 2 – программный комплекс на основе алгоритмов обработки естественного языка анализирует разговор (объективная оценка); 3 – программа выдает пользователю отчет о проделанном анализе и предупреждает его в случае атаки социальной инженерии

Для функционирования данного программного комплекса не требуется наличие телефонной базы данных, так как механизм его работы главным образом сосредоточен на анализе семантической составляющей входящего звонка. То есть программный комплекс в режиме реального времени обрабатывает телефонный разговор и при необходимости оповещает пользователя о возможной опасности.

Таким образом, приложение, базирующееся на данном программном комплексе, будет иметь ряд преимуществ относительно уже существующих продуктов:

- обработка непосредственно смысловой нагрузки разговора, позволяющая обнаруживать атаки независимо от того, производились звонки с этого номера телефона ранее или нет;
- результат анализа в режиме реального времени, то есть приложение позволяет моментально пресекать возможную атаку со стороны мошенников, не дожидаясь того, когда данный номер телефона будет помечен одним из пользователей;
- объективная оценка, не зависящая от личностных качеств и предубеждений пользователей приложения;

- безопасность приложения, обусловленная тем, что для функционирования данного программного комплекса не требуется предоставлять доступ к персональной информации, например, к номерам контактных телефонов, записанных на устройстве.

Выбор алгоритмов обработки естественного языка на основе проведенного анализа. С целью дальнейшей реализации программного комплекса был проведен сравнительный анализ существующих методов обработки естественного языка [1], в результате которого были выбраны следующие алгоритмы:

- языковая модель bag-of-words;
- алгоритм вложения слов Word2Vec;
- метод BERT, базирующийся на архитектуре Трансформ.

Языковая модель bag-of-words. Данная модель была выбрана, несмотря на ряд ее недостатков в связи с тем, что она обладает наиболее высокой скоростью обработки данных. Скорость обработки данных является важным аспектом при выборе алгоритма обработки, так как приложение, базирующееся на рассматриваемом программном комплексе, должно обрабатывать данные в режиме реального времени. Соответственно, следует отдать предпочтение модели, требующей меньшее время на обработку поступающей информации относительно других методов.

Обработка информации с помощью модели bag-of-words происходит следующим образом [1]: данные из датасета разбиваются на предложения, непосредственно составляющие датасет, и слова, входящие в него, из которых создается словарь данной модели. На основе полученных данных строится матрица, позволяющая определить наличие того или иного слова в каждом предложении [9]. Столбцами в полученной матрице являются слова из составленного словаря, а строками – исходные предложения. Общий вид механизма обработки данных с помощью bag-of-words представлен на рисунке 5.

Значительным недостатком модели bag-of-words является отсутствие связей контекстных связей между словами в предложении и, соответственно, в тексте [1]. Это связано с тем, что модель хранит лишь данные о наличии или отсутствии слова в том или ином предложении. Такой метод обработки информации может быть эффективен, но только при работе с однотипными данными.

Рисунок 5 – Механизм работы языковой модели bag-of-words

Алгоритм вложения слов Word2Vec. Данный алгоритм компенсирует недостаток модели bag-of-words за счет процесса «встраивания» слов, т.е. создания вещественного вектора, соответствующего каждому слову в тексте, в многомерном пространстве таким образом, что слова, близкие по семантическому значению, находятся на более близком расстоянии [8]. Работа непосредственно с семантической нагрузкой слов позволяет данной модели устанавливать контекстные связи с ближайшими словами, что заметно улучшает эффективность обработки данных по сравнению с моделью bag-of-words. При этом благодаря применению в базе модели сразу двух алгоритмов обработки данных (CBOW и Skip-gram) становится возможным как определение контекста заданного слова, так и обратная операция – нахождение слова по известному контексту. Благодаря этому модель Word2Vec работает эффективнее аналогичных алгоритмов вложения слов fastText и GloVe. Однако метод Word2Vec не всегда справляется с обработкой неизвестных или редких слов [1].

Обобщенная схема обработки данных с помощью алгоритма Word2Vec представлена на рисунке 6. Можно заметить, что в данном случае модель работает непосредственно со словами и их контекстом, а не с предложениями, в которых они находятся. Такой метод обработки данных как раз и способствует определению семантической нагрузки каждого слова с целью дальнейшего построения многомерного векторного пространства.

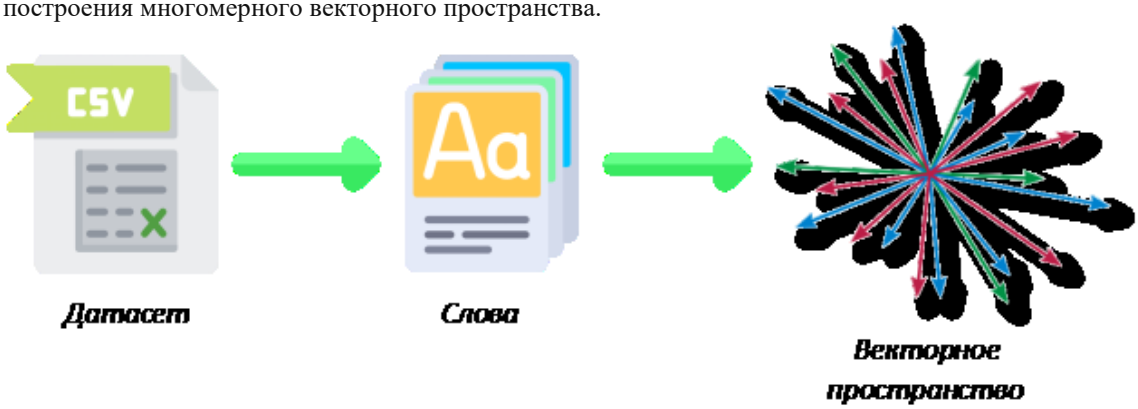


Рисунок 6 – Механизм работы алгоритма вложения слов Word2Vec

Метод BERT. Наиболее современным из рассматриваемых методов является метод BERT, базирующийся на современнейшей архитектуре Трансформер. Такая архитектура позволяет производить обучение модели даже на небольшой выборке данных за счет обработки данных по принципу «каждый с каждым» (рис. 7).

Основным отличием новой архитектуры является применение в качестве энкодера и декода алгоритма, включающего в себя механизм Multi-head Attention (рис. 8), вместо рекуррентных или сверточных нейронных сетей [2]. Данный механизм позволяет каждому входному вектору взаимодействовать с другими векторами благодаря наличию нескольких взаимосвязанных алгоритмов Self-Attention, выполняющих параллельную обработку данных. В свою очередь, каждый механизм Self-Attention имеет свой набор весовых коэффициентов, что позволяет воссоздавать полный контекстный разбор ситуации. Результаты работы всех таких механизмов объединяются в общий тензор, который в ходе последующей обработки становится итоговым результатом. Такой подход значительно увеличивает эффективность работы модели по сравнению с рекуррентными и сверточными нейронными сетями, где используется hidden state (скрытое состояние модели, необходимое для прогнозирования последовательности на выходе). В связи с этим языковые модели, базирующиеся на архитектуре Трансформер, имеют ряд преимуществ:

1. Алгоритмы обработки естественного языка, основывающиеся на архитектуре-трансформере, могут обрабатывать бесконечно длинные последовательности данных, не теряя семантическую зависимость между словами при обработке, в отличие от рекуррентных нейронных сетей, где даже применение механизмов LSTM и GPU с высокой степенью рекурсии не позволяет решить данную проблему [1].
2. Модели, базирующиеся на архитектуре Трансформер, не имеют присущей рекуррентным нейронным сетям проблемы взрывающихся и затухающих градиентов [2]. Это обусловлено тем, что благодаря архитектуре-трансформеру модель обрабатывает все имеющиеся данные за один проход, в отличие от рекуррентных и сверточных нейронных сетей, где обработка данных происходит последовательно.
3. Из второго пункта также следует, что модель, базирующаяся на данной архитектуре, требует меньшее количество шагов обучения относительно рекуррентных и сверточных нейронных сетей.

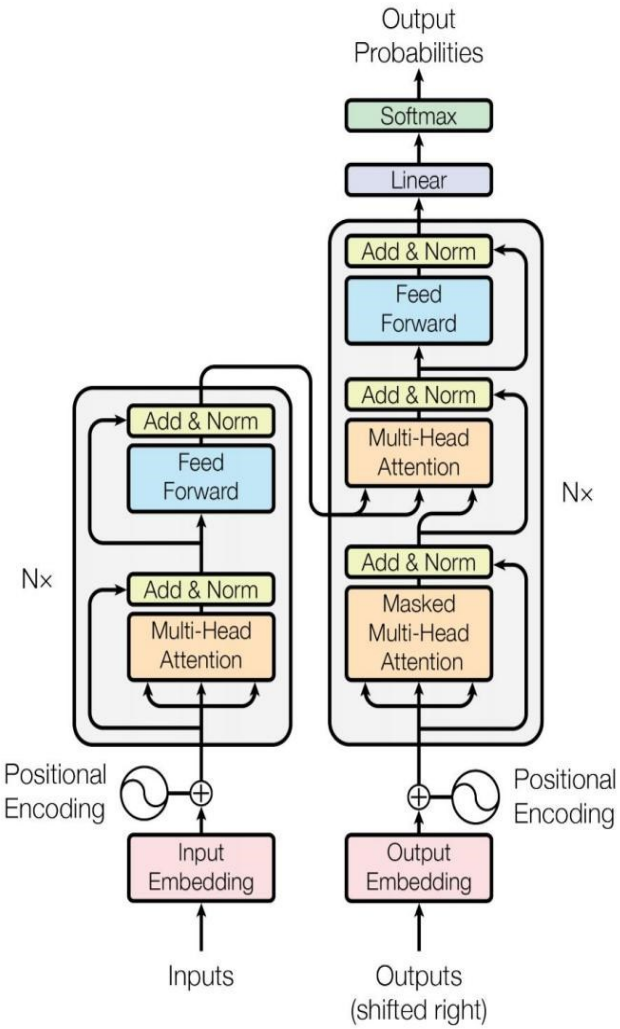


Рисунок 7 – Структура алгоритма BERT, функционирующего на базе архитектуры Трансформер [2]

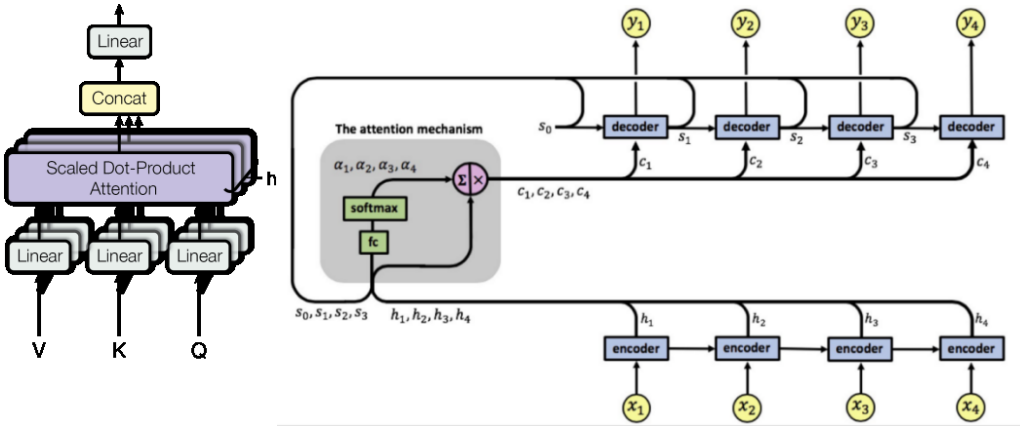


Рисунок 8 – Схема работы механизма Multi-head Attention, где Q (query) – тензор Запросов, K (key) – тензор Ключей, V (value) – тензор Значений [2]

Таким образом, метод BERT (рис. 9) аналогично алгоритму вложения слов работает непосредственно со словами, их значением и контекстом. Однако рассмотренный выше механизм Multi-head attention позволяет строить контекстные связи не только между рядом стоящими словами, но и между словами во всем предложении или тексте. Обработка данных таким образом позволяет определять семантическую нагрузку всего предложения или логически связного текста. Важно учесть, что метод затрачивает гораздо большее время на обработку информации относительно рассматриваемых ранее методов.

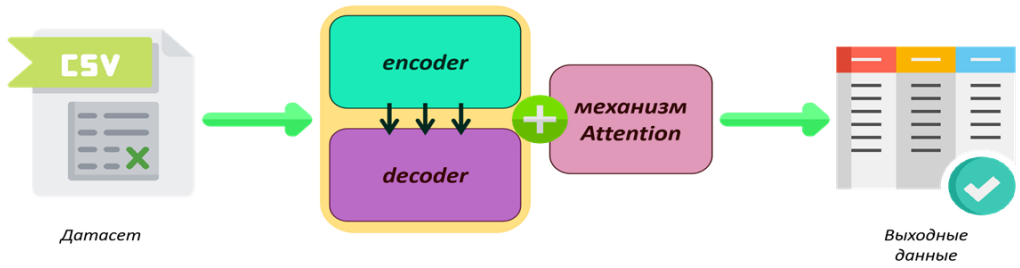


Рисунок 9 – Механизм работы метода BERT, базирующегося на архитектуре Трансформер

Разработка датасета. Для обучения любой модели NLP (natural language processing) необходим набор соответствующих данных – датасет. От корректности подобранного материала зависит точность обучения и эффективность работы алгоритма. Социальная инженерия является динамическим типом кибератак, так как регулярно появляются новые методы атак, меняются их формы и содержание. Соответственно, набор данных, разработанный для обучения программного комплекса (ПК) с целью борьбы с атаками социальной инженерии, должен содержать наиболее актуальные примеры атак на момент реализации ПК.

Поэтому в рамках данной исследовательской работы был создан набор, состоящий из 1000 примеров атак, наиболее актуальных и часто встречаемых на начало 2022 года. Для создания датасета были использованы материалы исследований компаний «Антифишинг» и «Positive Technologies». Часть полученного обучающего набора данных приведена на рисунке 10.

```
import zipfile
import os
import time
from google.colab import drive
from PIL import Image
drive.mount('/content/drive')
df = pd.read_csv('Dataset_SI.csv')
df['dialog']
```

```
1. Добрый день! Я менеджер банка, вы знакомы с инвестициями? Если нет, скажите номер вашего счета, чтобы я мог оценить ваши...
2. Здравствуйте! Это ваша управляющая компания, Произошел перерасчет оплаты за коммунальные услуги, , с вас были сняты изли...
3. Добрый день! Я сотрудник банка. На данный момент в банке снижена ставка по кредиту, не желаете ознакомиться с условиями?
4. Я Ваш новый коллега из вашего отдела, я забыл пароль от входа в систему, не подскажите его?
5. Здравствуйте! В период с 14 по 18 марта вам были предоставлены услуги ржд. Как вы оцениваете работу проводников, обслужи...
6. Я работник пенсионного фонда России, вас зовут? Вам назначена дополнительная выплата к пенсии. Укажите номер карты, на к...
7. Здравствуйте! Вы подключились к услуге «Погода онлайн». Если вы желаете отписаться позвоните по номеру *7543*004#
8. Не желаете вы принять участие в переписи населения по телефону? Для этого продиктуйте ваше полное имя и имена членов ваш...
9. Добрый день! Это работник отдела коммуникации банка, оцените работу нашего отдела от 1 до 10 баллов
10. Здравствуйте! Вас беспокоит управляющая компания, вам необходимо принять мастера для проверки счетчиков воды, иначе ваш...
...
996. С вашей карты списано рублей 5000. Продиктуйте номер вашей карты и ее CVC-код, чтобы предотвратить возможную атаку мош...
997. Вас беспокоит менеджер федеральной компании мегафон, поступил запрос от вашего имени на смену номера телефона. Вы дейс...
998. Здравствуйте! Это администрация социальной сети Вконтакте ваш аккаунт пытались взломать, сообщите ваши логин и пароль ...
999. Я сотрудник службы безопасности банка, поступила информация, что кто-то пытался поменять номер вашего мобильного банка...
1000. Я являюсь работником следственного комитета, Киров Ярослав работает у вас? Он проходит свидетелем по расследуемому дел...
```

Рисунок 10 – Вывод 15 предложений полученного датасета на экран

Полученные результаты. На основе полученного датасета было произведено обучение языковой модели, алгоритма вложения слов и метода таким образом, что 80 % предложений из датасета подавались на вход алгоритмов обработки естественного языка в качестве тренировочной выборки, а оставшиеся 20 % – в качестве проверочной. В результате обучения моделей NLP были получены результаты, приведенные в таблице 2.

Таблица 2 – Результаты исследования

	Модель bag-of-words	**Модель Word2Vec**	**Модель BERT**
Работа с предложениями целиком, без учета значения и связи отдельных слов	✓	✗	✗
Обработка текста с учетом синонимичности слов	✗	✓	✓

Продолжение таблицы 2

Возможность обучаться на датасете малого объема			
Примерное время обучения одной эпохи модели	1–2 мс	25–27 мс	122–126 мс
Результаты обработки обучающей выборки	95,37 %	98,42 %	99,16 %
Результаты обработки контрольной выборки	91,84 %	96,60 %	97,35 %

Выводы. Таким образом, исходя из результатов проведенного исследования, можно сделать вывод, что наилучшие результаты показала модель BERT, у которой точность обработки данных контрольной выборки составила 97,35 %. При этом стоит отметить, что алгоритм bag-of-words, несмотря на то, что точность обработки данных с его помощью была ниже относительно других методов, имеет значительное преимущество в скорости обработки данных. Так, время обучения одной эпохи модели bag-of-words в среднем составляло 1–2 мс. Алгоритм Word2Vec показал средние результаты относительно моделей bag-of-words и BERT.

Однако стоит заметить, что разница в точности обработки данных у рассматриваемых моделей в рамках проведенного исследования не столь значительна – 5,51 % между максимальным и минимальным показателями. Это обусловлено тем, что для обучения и дальнейшей проверки работы моделей использовался датасет большого объема – 1000 предложений различного рода. Но так как социальная инженерия является динамическим типом атак, то для эффективной работы алгоритмов обучающий датасет должен регулярно пополняться актуальными примерами атак. То есть дальнейшее обучение будет производиться на малой выборке, что, соответственно, приведет к значительному снижению точности обработки данных такими моделями, как bag-of-words и Word2Vec. Это связано с тем, что данные алгоритмы гарантируют хорошие результаты анализа данных только при наличии большой обучающей выборки. При этом модель BERT способна показывать высокую точность обработки данных и при обучении на небольшом датасете, это обусловлено архитектурой-трансформером, на которой базируется данный метод.

Библиографический список

1. Частикова, В. А. Методы обработки естественного языка в решении задач обнаружения атак социальной инженерии / В. А. Частикова, К. В. Козачек, В. Г. Гуляй // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2021. – № 4 (291). – С. 95–108. – DOI 10.53598/2410-3225-2021-4-291-95-108.

2. Ashish, Vaswani. Attention Is All You Need / Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, Illia Polosukhin // ArXiv:1706.03762. – 2017.

3. Сахно, В. В. Социальная инженерия, ее техники и способы защиты / В. В. Сахно, А. С. Пищаева // Modern Science. – 2020. – № 2–2. – С. 349–351.

4. Свищев, А. В. Искусственный интеллект как средство защиты от атак методами социальной инженерии / А. В. Свищев, Я. А. Акатьев // Colloquium-journal. – 2020. – № 7–1 (59). – С. 52–55. – DOI 10.24411/2520-6990-2020-11490.

5. Частиков, А. П., Алешин, А. В., Частикова, В. А. Выявление аномалий в базах знаний интеллектуальных систем // Пятьдесят лет развития кибернетики : труды Международной научно-технической конференции. – 1999. – С. 123–124.

6. Российская компания, специализирующаяся на разработке решений в сфере информационной безопасности Positive Technologies. Актуальные киберугрозы: итоги 2021 года // Cybersecurity Threatscape – 2022. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.05.2022).

7. Российская исследовательская компания и разработчик программного обеспечения ООО «Антифишинг». 86,4 % россиян стали жертвами цифровых мошенников // Антифишинг. – 2021. – Режим доступа: https://www.itweek.ru/security/news-company/detail.php?ID=215424&, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.05.2022).

8. Yilmaz, S. A deep learning analysis on question classification task using Word2vec representations / S. Yilmaz, S. Toklu // Neural Computing & Applications. – 2020. – Vol. 32, № 7. – P. 2909–2928. – DOI 10.1007/s00521-020-04725-w.

9. Катенко, Ю. В. Применение методов машинного обучения для анализа текстовой информации / Ю. В. Катенко // Охрана, безопасность, связь. – 2019. – Т. 3, № 4 (4). – С. 90–94.

References

1. Chastikova, V. A., Kozachek, K. V., Gulyai, V. G. Metody obrabotki estestvennogo yazyka v reshenii zadach obnaruzheniya atak socialnoy inzhenerii [Methods of natural language processing in solving problems of detecting social engineering attacks]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki* [Bulletin of the Adyghe State University. Series 4: Natural-mathematical and technical sciences], 2021, no. 4 (291), pp. 95–108.

2. Ashish, Vaswani, Noam, Shazeer, Niki, Parmar, Jakob, Uszkoreit, Llion, Jones, Aidan, N. Gomez, Lukasz, Kaiser, Illia, Polosukhin. Attention Is All You Need. *ArXiv:1706.03762*, 2017.

3. Sakhno, V. V., Pishchaeva, A. S. Sotsialnaya inzheneriya, ee tekhniki i sposoby zashchity [Social engineering, its techniques and methods of protection]. *Modern Science*, 2020, no. 2–2, pp. 349–351.

4. Svishchev A. V., Akatiev, Ya. A. Iskusstvennyy intellekt kak sredstvo zashchity ot atak metodami sotsialnoy inzhenerii [Artificial intelligence as a means of protection against attacks by social engineering]. *Colloquium-journal*, 2020, no. 7–1 (59), pp. 52–55. – DOI 10.24411/2520-6990-2020-11490.

5. Chastikov, A. P., Aleshin, A. V., Chastikova, V. A. Vyyavleniye anomaliy v bazakh znaniy intellektualnykh sistem [Identification of anomalies in the knowledge bases of intelligent systems]. *Pyatdesyat let razvitiya kibernetiki : trudy Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii* [Fifty Years of the Development of Cybernetics : Proceedings of the International Scientific and Technical Conference], 1999, pp. 123–124.

6. Rossiyskaya kompaniya, specializiruyushchayasya na razrabotke resheniy v sfere informatsionnoy bezopasnosti Positive Technologies. Aktualnye kiberugrozy: itogi 2021 goda [Russian company specializing in the development of information security solutions Positive Technologies. Actual cyber threats: results of 2021]. *Cybersecurity Threatscape – 2022*. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (accessed 05.17.2022).

7. Rossiyskaya issledovatelskaya kompaniya i razrabotchik programmnogo obespecheniya OOO «Antifishing». 86,4 % rossiyan stali zhertvami tsifrovykh moshennikov [Russian research company and software developer Antiphishing LLC 86.4 % of Russians became victims of digital scammers]. *Antifishing* [Antiphishing], 2021. Available at: https://www.itweek.ru/security/news-company/detail. php?ID=215424& (accessed 05.17.2022).

8. Yilmaz, S., Toklu, S. A deep learning analysis on question classification task using Word2vec representations. *Neural Computing & Applications*, 2020, vol. 32, no 7, pp. 2909–2928. – DOI 10.1007/s00521-020-04725-w.

9. Katenko, Yu. V. Primenenie metodov mashinnogo obucheniya dlya analiza tekstovoy informatsii [Application of machine learning methods for the analysis of textual information]. *Okhrana, bezopasnost, svyaz* [Security, safety, communication, 2019, vol. 3, no. 4 (4), pp. 90–94.

DOI 10.54398/20741707_2022_3_72
УДК 004.054

МНОГОКРИТЕРИАЛЬНАЯ ОЦЕНКА ЦЕЛОСТНОСТИ СУБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья поступила в редакцию 22.06.2022, в окончательном варианте – 22.08.2022.

Курчавов Павел Максимович, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,
аспирант, ORCID: 0000-0003-2589-6600, e-mail: aakvs@yandex.ru
Максимова Елена Александровна, МИРЭА – Российский технологический университет, 119454, Российская Федерация, г. Москва, пр. Вернадского, 78,
кандидат технических наук, доцент, ORCID: 0000-0001-8788-4256, e-mail: maksimova@ mirea.ru

Сегодня качество и уровень информационных технологий быстро растет, что приводит к эволюции угроз, заставляя разработчиков программно-аппаратных средств защиты информации работать на опережение. Один из новых классов угроз представлен угрозами, определяющими эффект инфраструктурного деструктивизма критической информационной инфраструктуры, т.е. саморазрушения информационной инфраструктуры. Данное явление может возникнуть на любом этапе жизненного цикла субъектов критической информационной инфраструктуры, в том числе в ходе эксплуатации системы, ввиду её качественных и количественных изменений. Для частичного решения данной проблемы предложена модель многокритериальной оценки инфраструктурной целостности субъекта критической информационной инфраструктуры, учитывающая его системные особенности, суть которой состоит в том, чтобы проанализировать по составленным с помощью экспертного мнения критериям возможных состояний объектов критической информационной инфраструктуры. С помощью этих результатов – возможно нахождение средней оценки целостности общего состояния инфраструктуры субъекта критической информационной инфраструктуры.

Ключевые слова: целостность, информационная безопасность, субъект, критическая информационная инфраструктура, многокритериальный анализ, инфраструктурный деструктивизм

USING MULTI-CRITERIA ANALYSIS TO ASSESS THE INTEGRITY OF THE SUBJECT OF CRITICAL INFORMATION INFRASTRUCTURE

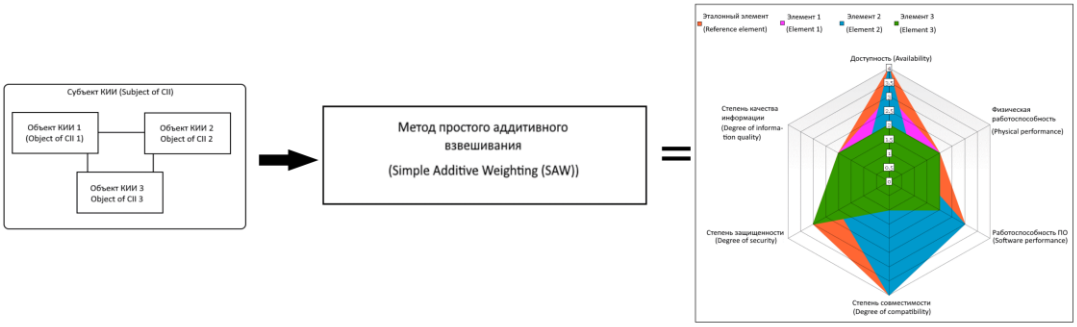
The article was received by the editorial board on 22.06.2022, in the final version – 22.08.2022.

Kurchavov Pavel M., MIREA – Russian Technological University, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
postgraduate student, ORCID: 0000-0003-2589-6600, e-mail: aakvs@yandex.ru
Maximova Elena A., MIREA – Russian Technological University, 78 Vernadsky Avenue, Moscow, 119454, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-8788-4256, e-mail: maksimova@mirea.ru

Today, the quality and level of information technology is growing rapidly, which leads to a rapid evolution of threats, forcing developers to constantly improve their information security products, look for new approaches, and be one step ahead of intruders. One of the new classes of threats is represented by threats that determine the effect of infrastructural destruction of critical information infrastructure (CII), i.e. self-destruction of information infrastructure. This phenomenon can appear at any stage of the life cycle of critical information infrastructure subjects, due to its qualitative and quantitative changes, including the operation of the system. To partially solve this problem proposed a model of multi-criteria assessment of the infrastructural integrity of the critical information infrastructure subject, taking into account of the system features of the critical information infrastructure, the essence of which is to analyze according to the criteria of possible states of CII objects compiled with the help of expert opinion. With these results, it is possible to find an average assessment of the integrity of the overall state of the critical information infrastructure subject's infrastructure.

Keywords: infrastructure analysis, security of the CII subject, critical information infrastructure, information security, multi-criteria analysis

Graphical annotation (Графическая аннотация)



Введение. Критическая информационная инфраструктура (КИИ) РФ представлена объектами КИИ, количественный и качественный состав которых в процессе эксплуатации субъектов КИИ может изменяться. Объектами КИИ являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. Субъекты КИИ – совокупность объектов КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Субъект КИИ представляет собой государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которые на каком-либо законном основании владеют объектами КИИ или же обеспечивают их взаимодействие. На рисунке 1 представлена схема, отображающая контекстное представление субъектов КИИ, а также объектов КИИ с точки зрения рассмотренного определения, а на рисунке 2 представлена типовая архитектура субъекта КИИ.

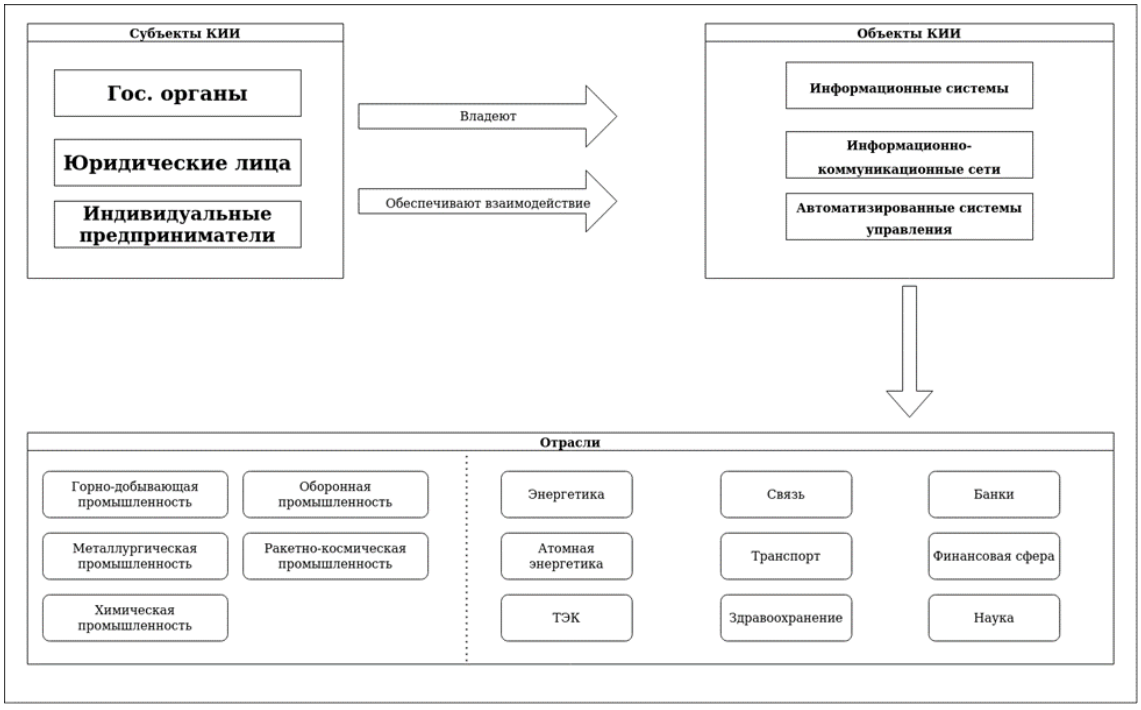


Рисунок 1 – Схема контекстного представления субъектов КИИ

Согласно [1], субъект КИИ обладает определенными правами и обязанностями, большинство из которых сводится к регулированию ситуации на объектах КИИ, обеспечению безопасности на объектах КИИ и своевременному информированию органов власти в случае нарушений функционирования объектов КИИ. Из этого следует, что субъект КИИ, в первую очередь, является юридическим лицом, которое обязано обеспечивать безопасное функционирование объектов, которыми оно владеет на законном основании. Т.е. субъекты КИИ являются элементами системы управления информационной безопасности (ИБ) КИИ. По данным ФСТЭК РФ, на сегодняшний день их более 50 000 [2].

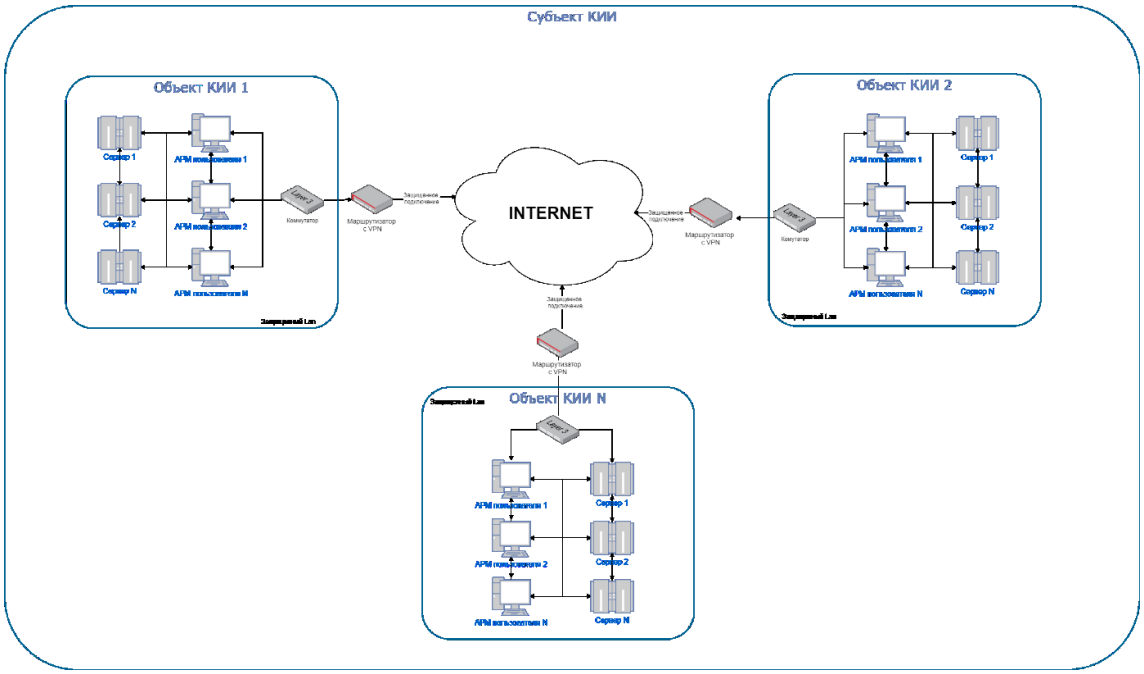


Рисунок 2 – Типовая архитектура субъекта КИИ

[1] регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. В [ст. 10, 1] детально описаны основные задачи и схема построения системы безопасности значимого объекта КИИ. В качестве ключевых задач определены:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Особенностью КИИ в контексте ИБ является феномен инфраструктурного деструктивизма, проявляющийся в саморазрушении инфраструктуры при пролонгированном влиянии деструктивных воздействий инфраструктурного генеза (происхождения) [3]. Пролонгация в данном случае возникает за счет накопительного эффекта, которым обладает данный класс имманентных угроз.

Условием для возникновения данного феномена может стать качественное и (или) количественное изменение состава субъекта КИИ, так как при этом возникают импульсные явления на уровне систем взаимодействующих объектов КИИ [4]. В конечном итоге, это может привести к нарушению целостности инфраструктуры и разрушить ее.

Методы и подходы. Для оценки целостности системы сегодня, как правило, используются различные комплексы, связанные непосредственно с отслеживанием разных аспектов безопасности в системе. Как правило, в основе таких комплексов лежит метод мониторинга, суть которого заключается в контроле процессов и приложений, качества выполнения бизнес-процессов организации и т.д. Также, как правило, благодаря таким системам возможно предупредить инциденты ИБ. Например, это:

• ПО Zabbix, предназначенное для мониторинга параметров сети, таких как жизнеспособность и целостность серверов, виртуальных машин, приложений, сервисов и т.д. Оно предлагает механизм оповещений, который дает возможность пользователям настраивать уведомления практически на любое событие. Также Zabbix предлагает функции для отчетности и визуализации данных, которые основаны на данных истории [5];

• Форпост – это ПО, предназначенное для автоматического детектирования негативного влияния на анализируемую систему, которое может быть классифицировано как компьютерная атака [6]. Существует два вида исполнения этого ПО:

1) базовое – в нем все необходимые программные компоненты установлены в рамках одного устройства, и оно сразу готово к использованию;

2) модульное, состоящее из сетевых датчиков, центра управления и автоматизированного рабочего места администратора.

Однако рассмотренные системы представляют собой комплексы для сбора данных, которые могут быть проанализированы и предоставлены экспертам для конечного вердикта. Причем экспертные оценки могут разниться, так как может существовать множество показателей, по которым можно оценить информационную систему, в соответствии с параметрами внешней среды и поставленной задачей.

На основании вышеизложенного было решено ввести понятие инфраструктурной целостности (или целостности инфраструктуры) для четкого понимания предмета исследования.

Источником определения и исследования категории «целостность инфраструктуры» является интенсионал самого понятия «целостность». Существует несколько определений целостности. Например, целостность – это обобщённая характеристика объектов, обладающих сложной внутренней структурой [7]. Данное определение выражает интегрированность, самодостаточность, автономность этих объектов, их противопоставленность окружению, связанную с их внутренней активностью. Также «целостность» определяют как качество системы, которым она обладает, если корректно выполняет все свои функции, свободна от намеренных или случайных несанкционированных манипуляций [8].

Согласно [9], существует такое понятие, как «целостность ресурсов информационной системы». Оно описывается как некое состояние ресурсов информационной системы, в котором какие-либо изменения этих ресурсов намеренно производятся исключительно субъектами, имеющими на это право. Также сохраняются их состав, содержание и организация взаимодействия. Данное определение взято за основу в рамках исследования категории «инфраструктурная целостность».

Неоднозначным является подход и к определению понятия «инфраструктура». Но, как правило, «инфраструктура» определяется как совокупность связанных между собой структур, отраслей или объектов, служащих для нормального функционирования системы [10, 11]. При этом выделяют несколько видов инфраструктур: производственная, социальная, транспортная, инженерная, информационная инфраструктура, инфраструктура экономики и др.

Для данного исследования наибольший интерес представляет информационная инфраструктура, являющаяся системой организационных структур, подсистем, обеспечивающих работу и развитие информационного пространства [12]. Инфраструктурную целостность при этом определим как состояние системы, в котором компоненты её инфраструктуры (подсистемы, физические устройства, структуры и т.п.) функционируют в полном объеме и не оказывают деструктивного воздействия на взаимодействующие элементы.

Для оценки целостности системы сегодня используются следующие методы:

- дискретная модель – в рамках этого метода в качестве меры надежности оценивается среднее время между двумя ошибочным срабатываниями [13];
- метод соотношений – заключается в определении вероятности безотказной работы сложной вычислительной системы [13];
- экспоненциальная модель – основана на модели, подразумевающей установление связи между интенсивностью обнаружения ошибок при отладке с интенсивностью проявления ошибок при нормальном функционировании комплекса программ и определенном количестве первичных ошибок [13].

В данном исследовании решено использовать методы многокритериального анализа. Это обусловлено тем, что данный вид анализа представляет собой более гибкую и настраиваемую методику, которая может быть изменена, например, переосмыслением изучаемых критериев. Также, благодаря такому подходу, можно не ориентироваться на какую-то конкретную область качества функционирования системы, т.е. целостности, а производить комплексный анализ, который как раз и будет соответствовать введенному выше определению целостности.

В качестве наиболее распространенных методов многокритериального анализа используются:

- SAW – метод, необходимый для количественного измерения значимости критериев по каждому альтернативному варианту. При этом будет построена и нормализована матрица решений, определяющая вес каждого критерия. В конечном итоге выводится обобщённая оценка для представленных альтернатив [14];

- TOPSIS – метод, основанный на концепции того, что идеальный вариант должен иметь самое малое геометрическое расстояние от положительного идеального решения и наибольшее геометрическое расстояние от отрицательного идеального решения. В ходе этого метода создается матрица оценки, состоящая из m альтернатив и n критериев. Затем эта матрица нормализуется и вычисляется ее взвешенная. После этого определяются худшая и лучшая альтернативы и вычисляется расстояние между целевой альтернативой и лучшим и худшим состояниями. В итоге определяется соответствие с наихудшим состоянием и альтернативы ранжируются [15];
- ELECTRE – семейство методов многокритериального анализа, где каждый метод обладает индивидуальными особенностями, что делает их эффективными для разных типов задач принятия решений [16];
- метод анализа иерархий. В отличие от многих других методов многокритериального анализа, не заставляет лицо, принимающее решение (ЛПР), использовать конкретное «правильное» решение, однако дает возможность в интерактивном режиме выбрать именно то решение, которое наиболее подходит под ситуацию, понимание ЛПР сути проблемы и согласуется с требованиями к решению проблемы [17].

Важно отметить, что большинство общеизвестных методов многокритериального анализа используются для сравнения множества альтернатив по критериям, что, в свою очередь, сводится к поиску наилучшего варианта.

В многокритериальном анализе широко распространены системы поддержки принятия решений (СППР). Например:

- СППР «Выбор» [18]. Данная система поддержки принятия решений основана на методе анализа иерархий. Используется для оценки качества организационных и другого типа задач. Программа разработана компанией ДТК Софтр, работает на системах семейства Windows;
- ПО Super Decisions [19]. Обеспечивает поддержку принятия решений с помощью методов анализа иерархий и аналитического сетевого процесса. Является одними из самых мощных для объединения суждений и данных с целью более эффективного ранжирования вариантов и прогнозирования результатов;
- система Expert Choice – система, также использующая метод анализа иерархий [20]. Данная система является достаточно сложной и комплексной, направленной на решения разного спектра задач бизнеса [21].

В работе [22] выполнено сравнение популярных методов многокритериального анализа посредством реализации простых программ. Интерес в этой работе представляет тот факт, что у разработанного программного обеспечения выходными данными являются, помимо наилучшего варианта, в зависимости от заданных критериев, результативные значения всех анализируемых объектов.

Дискуссия. Нарушение инфраструктурной целостности может снизить уровень ИБ как отдельного элемента системы, так и системы в целом [23]. Таким образом можно определить следующий набор направлений мониторинговых процедур, реализация которых позволит этого не допустить:

1) оценка локальной целостности элементов инфраструктуры, т.е. оценка инфраструктурной целостности на уровне каждого объекта субъекта КИИ;
2) оценка целостности систем взаимодействующих объектов;
3) непосредственная оценка целостности субъекта КИИ.

Рассмотрим реализацию первого направления в качестве базового.

Для разработки модели анализа целостности инфраструктуры субъекта КИИ использовался метод многокритериального анализа, представляющий собой практическую реализацию структуры системного исследования в решении сложных, комплексных проблем. Согласно [24], многокритериальный анализ обеспечивает рациональный, систематизированный и прозрачный процесс принятия решений при анализе влияний и взаимосвязей в сложных системах. Для использования таких методов в первую очередь необходимо проработать перечень критериев, который сможет отвечать требованиям безопасности субъекта КИИ.

В данном исследовании предлагается использовать метод многокритериального анализа не для поиска лучшего варианта, а для вычислений, по заданным критериям, множества общих состояний объектов КИИ, на основании которых станет возможным нахождение средней оценки целостности общего состояния инфраструктуры субъекта КИИ.

Обозначенное возможно при формировании перечня критериев оценки целостности объектов КИИ, благодаря которым можно будет рассчитать показатель целостности каждого из объектов, функционирующих в системе данного субъекта КИИ. В дальнейшем эти показатели можно будет использовать для оценки инфраструктурной целостности непосредственно субъекта КИИ, а также производить более гибкую диагностику. Предложенные критерии для оценки целостности объектов КИИ представлены в таблице 1.

Таблица 1 – Критерии оценки инфраструктурной целостности элемента объекта КИИ

Наименование критерия	**Что характеризует критерий**	**Показатели для многокритериального анализа**	**Вес критерия**
Доступность	Доступность объектов КИИ, входящих в состав субъекта КИИ	1) недоступен ни одному из других объектов КИИ в составе субъекта КИИ (0 %); 2) доступен малой части объектов КИИ в составе субъекта КИИ (< 50 %); 3) доступен большей части объектов КИИ в составе субъекта КИИ (> 50 %); 4) доступен всем объектам КИИ в составе субъекта КИИ (100 %).	0,1
Физическая работоспособность	Общая оценка работоспособности физических составляющих всех объектов КИИ, входящих в состав субъекта КИИ	1) не работает одно или более физическое устройство, входящее в состав объекта КИИ; 2) работают все физические устройства, входящие в состав объекта КИИ.	0,19
Работоспособность ПО	Общая оценка работоспособности программного обеспечения в составе всех объектов КИИ, входящих в состав субъекта КИИ	1) нарушена работоспособность некоторых программных компонентов объекта КИИ, что полностью нарушает выполнение задач объекта КИИ; 2) нарушена работоспособность некоторых программных компонентов объекта КИИ, что не нарушает выполнение задач объекта КИИ; 3) работают все программные компонентов объекта КИИ.	0,19
Степень совместимости	Общий уровень совместимости между объекта КИИ с другими объектами КИИ, входящими в состав субъекта КИИ	1) отсутствие совместимости со всеми объектами КИИ в составе субъекта КИИ (0 %); 2) наличие совместимости с малой частью объектов КИИ в составе субъекта КИИ (< 50 %); 3) наличие совместимости с большей частью объектов КИИ в составе субъекта КИИ (> 50 %); 4) наличие совместимости со всеми объектами КИИ в составе субъекта КИИ (100 %).	0,17
Степень защищенности	Уровень обеспечения защиты каналов конкретного объекта КИИ, входящими в состав субъекта КИИ	1) уровень обеспечения защиты каналов связи не соответствует регламентам предприятия; 2) уровень обеспечения защиты каналов связи частично соответствует регламентам предприятия; 3) уровень обеспечения защиты каналов связи полностью соответствует регламентам предприятия.	0,2
Степень качества информации	Соответствие информации, передаваемой объектом КИИ, входящим в состав субъекта КИИ, общим стандартам качества.	1) информация не соответствует общим стандартам качества; 2) информация соответствует общим стандартам качества	0,15

В соответствии с представленными критериями предлагается производить общую оценку целостности объекта КИИ с использованием метода SAW по причине его простоты и прозрачности, что может быть полезным при работе с большим количеством данных.

Как видно из схемы, представленной на рисунке 3, многокритериальный анализ объектов КИИ рассматривается на уровне их элементов. В ходе работы выстраивается матрица элементов объектов КИИ, каждый элемент которой является значением того или иного критерия из представленных в таблице 1, для каждого элемента объекта КИИ.

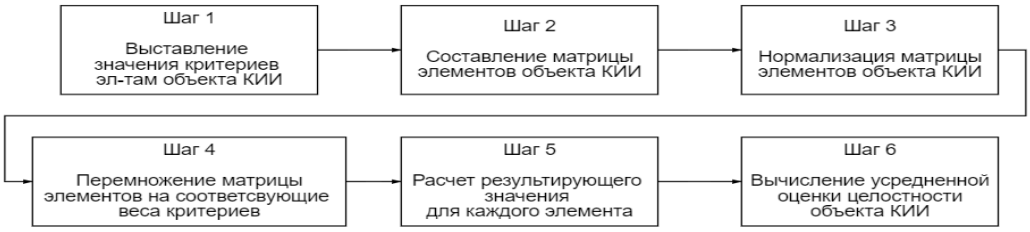


Рисунок 3 – Схема реализации метода SAWдля оценки инфраструктурной целостности объекта КИИ

После анализа и получения данных о состоянии элементов объекта КИИ становится возможным вычисление усредненного значения целостности объекта КИИ. Стоит отметить, что в рамках метода критерии являются максимизируемыми, т.е. мы заинтересованы в контексте работы системы, чтобы значения критериев были максимальными, а не минимальными. Данный факт обосновывает выбор формулы расчета нормированных значений матрицы. Формализация данного имеет вид:

$$P_{ij} = \frac{x_{ij} - x_j^{min}}{x_j^{max} - x_j^{min}}, \quad (1)$$

где xX_{ij} – значение из матрицы, соответствующее конкретному критерию; X_j^{min} – минимальное значение критерия; X_j^{max} – максимальное значение критерия.

$$\frac{\sum_{j=1}^{n} a_j \times 100\%}{X \times n}, \quad (2)$$

где n – это количество объектов КИИ; a_j – это показатель целостности j-го элемента объекта КИИ, а X – это показатель инфраструктурной целостности эталонного объекта КИИ. Для того чтобы вычислить значение X, необходимо с помощью метода SAW, просчитать результирующее значение инфраструктурной целостности для эталонного элемента объекта КИИ.

В ряде работ [8, 24–27] полагается расчет по критериям, для дальнейшего сравнения результатов между собой, для поиска самого удовлетворяющего значения. В данном исследовании для составления вывода об оценке инфраструктурной целостности изучаемого объекта необходимо оценить максимально возможные значения по данным критериям с обозначенными весами. Остро встает вопрос о необходимости эталонного значения, которое будет представлять собой некоторую абстракцию, с наивысшими значениями критериев, необходимую для проведения сравнения остальных результатов для выполнения шестого шага. В таблице 5 описаны значения критериев такого «эталонного» объекта, в соответствии со значениями критериев, представленными в таблице 2.

Таблица 2 – Значения критериев эталонного элемента объекта КИИ

Наименование критерия	Значение критерия эталонного элемента объекта КИИ	Вес критерия
Доступность	4	0,1
Физическая работоспособность	2	0,19
Работоспособность ПО	3	0,19
Степень совместимости	4	0,17
Степень защищенности	3	0,2
Степень качества информации	2	0,15

Для дальнейших расчетов нам необходим только один эталонный элемент объекта КИИ, в соответствии с чем для него будет существовать только один набор критериев. Поэтому далее получим:

$$\begin{pmatrix} 4 * 0{,}1 \\ 2 * 0{,}19 \\ 3 * 0{,}19 \\ 4 * 0{,}17 \\ 3 * 0{,}2 \\ 2 * 0{,}15 \end{pmatrix} = \begin{pmatrix} 0{,}4 \\ 0{,}38 \\ 0{,}57 \\ 0{,}68 \\ 0{,}6 \\ 0{,}3 \end{pmatrix}.$$

Результирующее значение инфраструктурной целостности для эталонного элемента объекта КИИ:

$$0{,}4 + 0{,}38 + 0{,}57 + 0{,}68 + 0{,}6 + 0{,}3 = 2{,}93.$$

Полученное значение является константой. Таким образом формула (2) примет вид:

$$\frac{\sum_{j=1}^{n} (a_j) \times 100\%}{2{,}93 * n}. \quad (3)$$

На основании предложенного метода выполнена программная реализация, на языке программирования Python, ввиду того, что данный язык достаточно часто используется для анализа данных,

а также в рамках этого языка реализовано большое количество библиотек для решения математических задач разного рода.

Экспериментальное исследование. Рассмотрим реализацию предложенного метода на примере субъекта КИИ, имеющего заданную структуру (рис. 4). Алгоритм реализации выполним в виде комплекса шагов. Более подробно остановимся на исследовании объекта КИИ № 1. Для остальных объектов в структуре субъекта КИИ пошаговое выполнение расчетов выполняется аналогично.

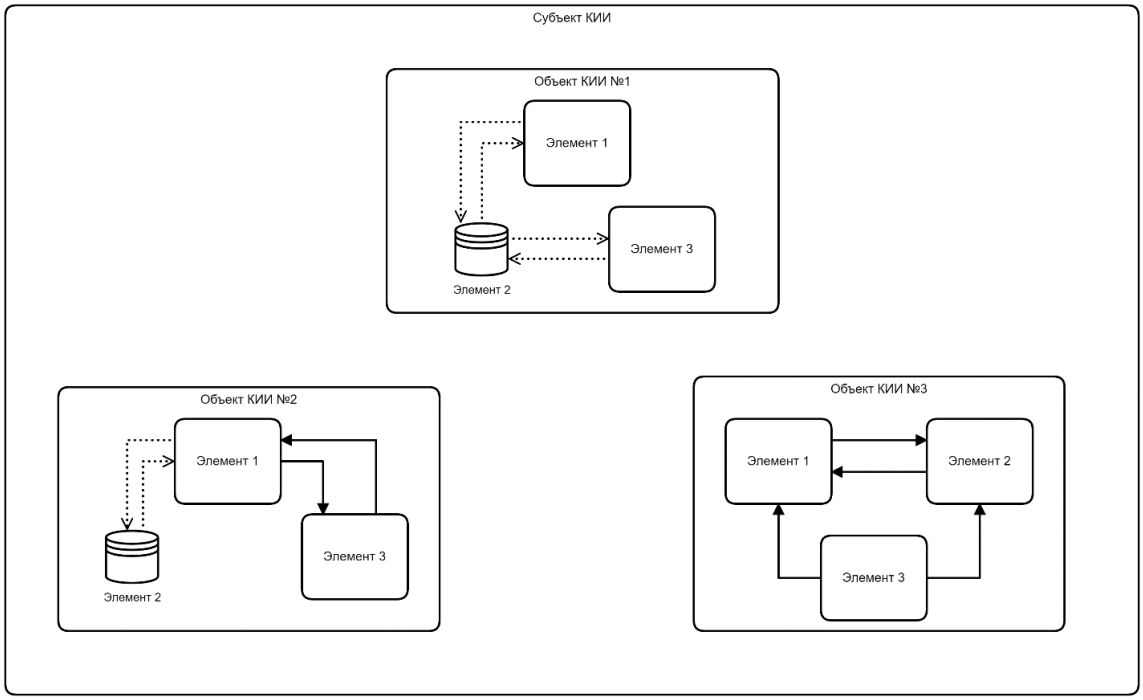


Рисунок 4 – Пример субъекта КИИ для тестового расчёта

Шаг 1: выставим значения критериев элементам тестового объекта КИИ № 1.
Шаг 2: составим матрицу элементов объекта КИИ № 1 (табл. 3).

Таблица 3 – Значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	**Значение критериев элемента 1**	**Значение критериев элемента 2**	**Значение критериев элемента 3**
Доступность	3	4	2
Физическая работоспособность	2	1	2
Работоспособность ПО	2	3	2
Степень совместимости	4	4	1
Степень защищенности	1	2	3
Степень качества информации	2	1	2

Шаг 3: выполним поиск нормированных оценок по данным таблицы 2. Для этого выполним поиск максимальных и минимальных оценок критериев путем отбора максимальных значений в строке (для каждого из критериев):

$$X_{max} = (4; 2; 3; 4; 3; 2),$$
$$X_{min} = (2; 1; 2; 1; 1; 1).$$

Далее следует расчет нормированных значений матрицы по формуле (1). Результат нормирования представлен в таблице 4.

Таблица 4 – Нормированные значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	Нормализованный результат критериев элемента 1	Нормализованный результат критериев элемента 2	Нормализованный результат критериев элемента 3
Доступность	0,5	1	0
Физическая работоспособность	1	0	1
Работоспособность ПО	0	1	0
Степень совместимости	1	1	0
Степень защищенности	0	0,5	1
Степень качества информации	1	0	1

Шаг 4: выполним произведение полученных нормированных значений на веса критериев.

Шаг 5: выполним расчет результирующих значений инфраструктурной целостности элементов объекта КИИ № 1 для тестового расчёта (табл. 5).

Таблица 5 – Итоговые значения критериев элементов объекта КИИ № 1 для тестового расчёта

Наименование критерия	Нормализованный результат критериев элемента 1	Нормализованный результат критериев элемента 2	Нормализованный результат критериев элемента 3
Доступность	0,05	0,1	0
Физическая работоспособность	0,19	0	0,19
Работоспособность ПО	0	0,19	0
Степень совместимости	0,17	0,17	0
Степень защищенности	0	0,1	0,2
Степень качества информации	0,15	0	0,15
Результирующее значение инфраструктурной целостности элементов объекта КИИ № 1	0,56	0,56	0,54

Таким образом, в ходе исследования получен условный рейтинг показателей инфраструктурной целостности элементов объекта КИИ.

На рисунке 5 представлена лепестковая диаграмма, построенная на основе значений критериев (табл. 1) элементов, взятых в рамках тестового расчета. В реальной ситуации такими элементами могут выступать: базы данных, сервера, сервисы, используемые внутри объекта КИИ и т.д.

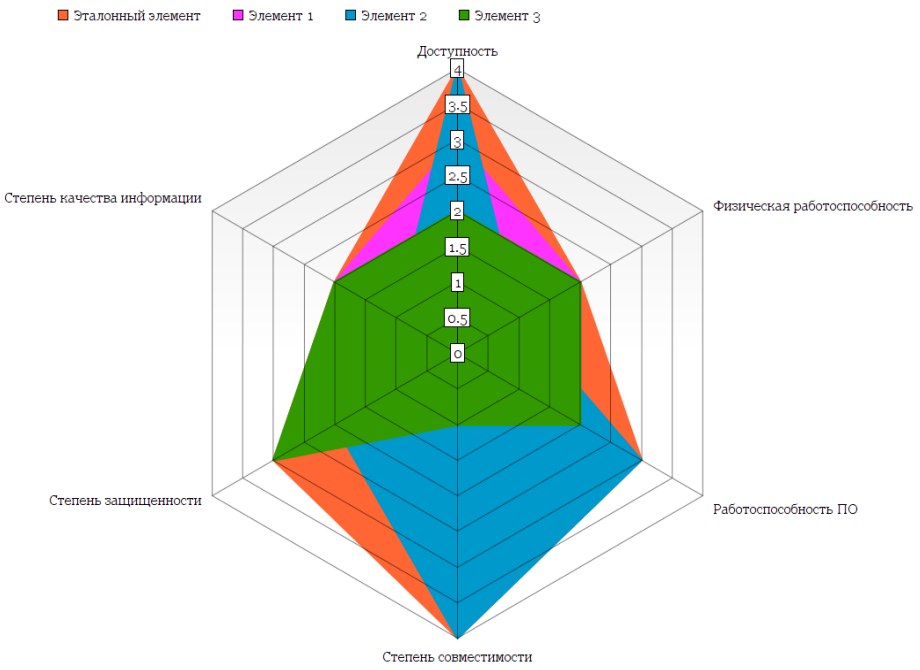


Рисунок 5 – Лепестковая диаграмма сравнения значений критериев элементов объекта КИИ № 1 для тестового расчёта

Шаг 6: в соответствии с формулой (3), завершим тестовый расчет для объекта КИИ № 1:

$$\frac{(0{,}56+0{,}56+0{,}54)\cdot 100\%}{2{,}93\cdot 3}=\frac{165}{8{,}79}=18{,}8\%.$$

Следовательно, значение результирующей оценки инфраструктурной целостности объекта КИИ № 1 для тестового расчета, в сравнении с эталонными значениями, составляет 18,8 %, что на самом деле будем считать весьма низким уровнем инфраструктурной целостности на объекте. Полученное говорит о серьезных нарушениях, функциональной нестабильности и росте инфраструктурного деструктивизма как на объекте КИИ № 1, так и на исследуемом субъекте КИИ в целом.

Заключение. Вышеописанный метод является первым шагом для оценки уровня инфраструктурной целостности субъекта КИИ. Важно отметить, что на основе методик многокритериального анализа возможно добиться получения множества состояний анализируемых объектов для дальнейшего расчета общего состояния субъекта КИИ на более высоких уровнях в соответствии с описанными ранее мониторинговыми процедурами.

Библиографический список

1. О безопасности критической информационной инфраструктуры Российской Федерации // Федеральный закон от 26.07.2017. – № 187-ФЗ.

2. Рекомендации по оценке показателей критериев экономической значимости объектов КИИ от ФСТЭК // SecurityLab.ru. – Режим доступа: https://www.securitylab.ru/blog/personal/valerykomarov /350276.php, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.04.2022).

3. Максимова, Е. А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры : монография / Е. А. Максимова. – Москва ; Волгоград : Издательство Волгоградского государственного университета, 2021.

4. Максимова, Е. А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры / Е. А. Максимова // Информатизация и связь. – 2022. – № 1 (68–74). – Режим доступа: https://www.elibrary.ru/item.asp?id=48316441, свободный. – Заглавие с экрана. – Яз. рус.

5. Что такое Zabbix // Zabbix Documentation. – Режим доступа: https://www.zabbix.com /documentation/5.0/ru/manual/introduction/about, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 28.05.2022).

6. Программно-аппаратный комплекс «Форпост» // Российские наукоемкие технологии. – Режим доступа: http://www.rnt.ru/ru/production/detail.php?ID=20, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 05.06.2022);

7. Ильичёв, Л. Ф. Философский энциклопедический словарь / Л. Ф. Ильичёв, П. Н. Федосеев, С. М. Ковалёв, В. Г. Панов. – Москва : Советская энциклопедия, 1983.

8. Домарев, В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – 2004.

9. ГОСТ Р 50.1.053-2005. Основные термины и определения в области технической защиты информации. – 2005.

10. Инфраструктура // Академик. – Режим доступа: https://investments.academic.ru/1013/Инфраструктура, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.06.2022);

11. Инфраструктура // Глоссарий.ru. – Режим доступа: http://www.glossary.ru/cgi-bin/gl_sch2. cgi?RIt(wgxywzqyzwg, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.08.2022).

12. Информационная инфраструктура // Глоссарий.ru. – Режим доступа: http://www.glossary.ru/cgi-bin /gl_sch2.cgi?RIt(uwsg.outtg9!ot(wgxywzqyzwg, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.08.2022).

13. Оценка надежности информационных систем // StudRef. – Режим доступа: https://studref.com /521413 /menedzhment/otsenka_nadezhnosti_informatsionnyh_sistem, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.06.2022).

14. Кочкина, М. В. Анализ многокритериальных методов принятия управленческих решений. (на примере задачи выбора поставщиков материально-технических ресурсов) : учеб. пособие / М. В. Кочкина, А. Н. Карамышева, И. И. Махмутова, А. Г. Исавнина, А. К. Розенцвайга. – 2017. – С. 4–8.

15. Hwang, C. L. Multiple Attribute Decision Making: Methods and Applications / C. L. Hwang, K. Yoon. – New York : Springer-Verlag, 1981.

16. Методы семейства ELECTRE // Studme.org. – Режим доступа: https://studme.org/212185/informatika /metody_semeystva_electre, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.05.2022).

17. Saaty, Thomas L. On the measurement of intengibles: a principal Eigenvector approach to relative measurement derived from paired comparisons / Thomas L. Saaty // Notices of the American Mathematical Society 60. – 2013. – P. 192–208.

18. СППР Выбор // Monobit. – Режим доступа: https://monobit.ru/sppr-vybor.html#:~:text=Система %20поддержки%20принятия%20решений%20“Выбор”,альтернативы%20по%20каждому%20из%20факторов, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.05.2022).

19. About SuperDecisions // Super Decisions. – Режим доступа: https://www.superdecisions.com/about/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.05.2022).

20. Система поддержки принятия решений Expert Choice // Studme.org. – Режим доступа: https://studme.org/212182/informatika/sistema_podderzhki_prinyatiya_resheniy_expert_choice, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.06.2022).

21. Expert Choice. – Режим доступа: https://www.expertchoice.com, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.06.2022).

22. Клоков, С. А. Сравнение и разработка методов многокритериального анализа принятия решений / С. А. Клоков // Молодой ученый. – 2021. – № 18 (360). – С. 30–33. – Режим доступа: https://moluch.ru /archive/360/80477/, свободный. – Заглавие с экрана. – Яз. рус.

23. Основы информационной безопасности. Часть 1: Виды угроз // Хабр. – Режим доступа: https://habr.com/ru/company/vps_house/blog/343110/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 14.06.2022).

24. Методы форсайт-исследования. Методы форсайта // Bstudy.net. – Режим доступа: https://bstudy.net /880551/ekonomika/metody_forsayt_issledovaniya, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 16.06.2022).

25. Ярошевич, Н. Ю. Методологические подходы к формированию аэропортов-хабов на территории страны / Н. Ю. Ярошевич, Т. С. Орлова // Journal of new economy. – 2014. – № 3. – С. 53. – Режим доступа: https://cyberleninka.ru/article/n/metodologicheskie-podhody-k-formirovaniyu-aeroportov-habov-na-territorii-strany, свободный. – Заглавие с экрана. – Яз. рус.

26. Родригес, В. С. Многокритериальная оценка альтернатив территориального планирования при строительстве плотин с использованием технологий географических информационных систем / В. С. Родригес, Н. В. Мокрова // Отходы и ресурсы : интернетжурнал. – 2020. – № 1. – DOI: 10.15862/11INOR120. – Режим доступа: https://resources.today/PDF/11INOR120.pdf, свободный. – Заглавие с экрана. – Яз. рус.

27. Подиновский, В. В. Идеи и методы теории важности критериев в многокритериальных задачах принятия решений / В. В. Подиновский. – 2019.

References

1. On the security of the critical information infrastructure of the Russian Federation. Federal Law No. 187-FZ of July 26, 2017.

2. Recommendations on the evaluation of indicators of criteria for the economic significance of CII objects from the FSTEC. *SecurityLab.ru*. Available at: https://www.securitylab.ru/blog/personal/valerykomarov/350276.php (accessed 25.04.2022).

3. Maksimova, E. A. *Infrastrukturnyy destruktivizm subektov kriticheskoy informatsionnoy infrastruktury : monografiya* [Infrastructural destructivism of subjects of critical information infrastructure : monograph]. Volgograd : Volgograd State University Publishing House, 2021.

4. Maksimova, E. A. Aksiomatika infrastrukturnogo destruktivisma subekta kriticheskoy informatsionnoy infrastruktury [Axiomatics of infrastructural destructivism of the subject of critical information infrastructure]. *Informatizatsiya i svyaz* [Informatization and communication], 2022, no. 1, pp. 68–74 (accessed 25.04.2022).

5. What is Zabbix. *Zabbix Documentation*. Available at: https://www.zabbix.com/documentation /current/ru/manual/introduction/about (accessed 28.05.2022).

6. Hardware-software complex "Forpost". *Russian high-tech technologies*. Available at: http://www.rnt.ru/ru /production/detail.php?ID=20 (accessed 05.06.2022).

7. Ilichev, L. F., Fedoseev, P. N. Kovalev, S. M., Panov, V. G. *Filosofskiy entsiklopedicheskiy slovar* [Philosophical Encyclopedic Dictionary]. Moscow, Sovetskaya entsiklopediya, 1983.

8. Domarev, V. V. *Bezopasnost informatsionnykh tekhnologiy. Sistemnyy podkhod* [Information technology security. A systematic approach], 2004.

9. *GOST R 50.1.053-2005. Osnovnyye terminy i opredeleniya v oblasti tekhnicheskoy zashchity informatsii* [State Standard 50.1.053-2005. Basic terms and definitions in scope of technical protection of information], 2006.

10. Infrastructure. *Academician*. Available at: https://investments.academic.ru/1013/Infrastruktura (accessed 07.06.2022).

11. Infrastructure. *Glossary.ru*. Available at: http://www.glossary.ru/cgi-bin/gl_sch2.cgi?RIt(wgxywzqyzwg.

12. Information infrastructure. *Glossary.ru.* Available at: http://www.glossary.ru/cgi-bin/gl_sch2. cgi?RIt(uwsg.outtg9!ot(wgxywzqyzwg (accessed 20.08.2022).

13. Assessment of the reliability of information systems. *StudRef.* Available at: https://studref.com/521413/menedzhment/otsenka_nadezhnosti_informatsionnyh_sistem.

14. Kochkina, M. V., Karamysheva, A. N., Makhmutova, I. I., Isavnina, A. G., Rozentsvayga, A. K. Analiz mnogokriterialnykh metodov prinyatiya upravlencheskikh resheniy (na primere zadachi vybora postavshhikov materialno-tekhnicheskikh resursov) [Analysis of multi-criteria methods of managerial decision-making. (using the example of the task of selecting suppliers of material and technical resources)], 2017. – P. 4–8.

15. Hwang, C. L., Yoon, K. *Multiple Attribute Decision Making: Methods and Applications*. New York : Springer-Verlag, 1981.

16. Methods of the ELECTRE family. *Studme.org*. Available at: https://studme.org/212185 /informatika/metody_semeystva_electre (accessed 11.05.2022).

17. Saaty, Thomas L. On the measurement of intengibles: a principal Eigenvector approach to relative measurement derived from paired comparisons. *Notices of the American Mathematical Society 60*, 2013, pp. 192–208.

18. DSS choice. *Monobit.* Available at: https://monobit.ru/sppr-vybor.html#:~:text=Система%20поддержки%20принятия%20решений%20“Выбор”,альтернативы%20по%20каждому%20из%20факторов (accessed 15.05.2022).

19. About SuperDecisions. *Super Decisions.* Available at: https://www.superdecisions.com/ (accessed 15.05.2022).

20. Decision Support System – Expert Choice. *Studme.org*. Available at: https://studme.org/212182/informatika/sistema_podderzhki_prinyatiya_resheniy_expert_choice (accessed 10.06.2022).

21. *Expertchoice*. Available at: https://www.expertchoice.com (accessed 15.05.2022).

22. Klokov, S. A. Sravnenie i razrabotka metodov mnogokriterial'nogo analiza prinjatija reshenij [Comparison and development of methods of multi-criteria analysis of decision-making]. *Molodoy uchenyy*. [Young Scientist], 2021, no. 18, pp. 30–33. Available at: https://moluch.ru/archive/360/80477/.

23. Fundamentals of information security. Part 1: Types of Threats. *Habr.* Available at: https://habr.com/ru/company/vps_house/blog/343110/ (accessed 14.06.2022).

24. Methods of foresight research. Foresight methods. Bstudy.net. Available at: https://bstudy.net/880551/ekonomika/metody_forsayt_issledovaniya (accessed 16.06.2022).

25. Yaroshevich N. Yu., Orlova, T. S. Metodologicheskie podkhody k formirovaniyu aeroportov-khabov na territorii strany [Methodological approaches to the formation of hub airports in the country]. *Journal of new economy*, 2014, no. 3, p. 53. Available at: https://cyberleninka.ru/article/n/metodologicheskie-podhody-k-formirovaniyu-aeroportov-habov-na-territorii-strany.

26. Rodriges, V. S., Mokrova, N. V. Mnogokriterialnaya otsenka alternativ territorialnogo planirovaniya pri stroitelstve plotin s ispolzovaniem tekhnologiy geograficheskikh informatsionnykh sistem [Multi-criteria assessment of alternatives to territorial planning in the construction of dams using geographic information system technologies]. *Otkhody i resursy* [Waste and resources], 2020, no. 1. DOI: 10.15862/11INOR120. Available at: https://resources.today/PDF/11INOR120.pdf.

27. Podinovskiy, V. V. *Idei i metody teorii vazhnosti kriteriev v mnogokriterialnykh zadachah prinyatiya resheniy* [Ideas and methods of the theory of the importance of criteria in multi-criteria decision-making tasks.], 2019.

УДК 004.001

МЕТОДЫ ЗАЩИТЫ В СОВРЕМЕННЫХ СИСТЕМАХ ГОЛОСОВОЙ АУТЕНТИФИКАЦИИ

Статья поступила в редакцию 15.04.2022, в окончательном варианте – 29.08.2022.

Евсюков Михаил Витальевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0001-7101-6251, e-mail: michael.evsyukov@gmail.com
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Немчинова Валерия Олеговна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
ассистент, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

Вместе со стремительным развитием и широким распространением голосовых интерфейсов всё более актуальной становится проблема повышения безопасности систем голосовой аутентификации. В то время как алгоритмы распознавания личности по голосу хорошо изучены и демонстрируют высокую надёжность при проверке их эффективности живыми людьми, современные системы голосовой аутентификации подвержены ряду уязвимостей. В первую очередь, это связано с повсеместной распространённостью недорогой и высококачественной техники, предназначенной для записи и воспроизведения звука. Данный факт предоставляет злоумышленникам мощные инструменты для реализации атак на системы голосовой аутентификации. Как правило, цель злоумышленника состоит в прохождении аутентификации в системе под видом другого лица. Действия, направленные на достижение этой цели, называются спуфингом. В данной статье описаны основные голосовые характеристики, применяемые при реализации систем голосовой аутентификации, приведена актуальная классификация алгоритмов распознавания личности по голосу, описаны существующие метрики оценки эффективности систем голосовой аутентификации и изложены существующие подходы к классификации методов спуфинга. Кроме того, усовершенствована классификация контрмер против спуфинга и выделены перспективные направления будущих исследований в области аутентификации по голосу.

Ключевые слова: биометрия, искусственный интеллект, машинное обучение, информационная безопасность, защита информации, аутентификация, спуфинг

PROTECTION METHODS IN MODERN VOICE AUTHENTICATION SYSTEMS

The article was received by the editorial board on 15.04.2022, in the final version – 29.08.2022.

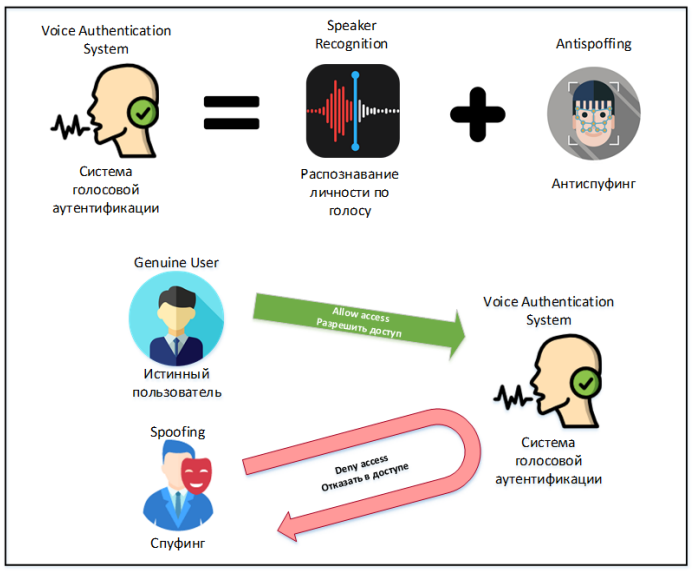
Evsyukov Michael V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0001-7101-6251, e-mail: michael.evsyukov@gmail.com
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Nemchinova Valeriya O., Kuban State Technological University, 350072, Russian Federation, 2 Moskovskaya St., Krasnodar,
Assistant, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

The problem of improving the security of voice authentication systems is becoming increasingly important due to the rapid development and widespread use of voice interfaces. Although voice recognition algorithms are well-studied and demonstrate high reliability when tested by live people, modern voice authentication systems are subject to a number of vulnerabilities. First of all, this is due to the access to affordable and high-quality devices for recording and playing sound. This fact provides attackers with powerful tools to implement attacks on voice authentication systems. As a rule, the attacker's purpose is to authenticate in the system under the guise of another person. Actions

aimed at achieving this goal are called spoofing. This article describes the main voice characteristics used in the implementation of voice authentication systems, provides an up-to-date classification of voice recognition algorithms, describes existing metrics for evaluating the effectiveness of voice authentication systems, and outlines existing approaches to classifying spoofing methods. In addition, the classification of countermeasures against spoofing has been improved and promising directions for future research in the field of voice authentication have been identified.

Keywords: biometrics, artificial intelligence, machine learning, information security, authentication, spoofing, liveness detection

Graphical annotation (Графическая аннотация)



Введение. Согласно данным Google, 500 миллионов пользователей ежемесячно используют Google Assistant [1]. Apple утверждает, что голосовой помощник Siri ежемесячно обрабатывает 25 миллиардов запросов [2]. Простота применения и экономия времени – основные причины, по которым голосовые помощники набирают популярность. Кроме того, появление широкого ассортимента умных устройств и стремительное развитие интернета вещей (IoT) делают голосовой интерфейс ещё более востребованным, поскольку он способен предоставить наиболее комфортный пользовательский опыт. Возможность управления голосом реализована, например, в смарт-колонке «Яндекс.Станция», автомобилях Tesla, а также в различных системах типа «умный дом».

Таким образом, голосовые помощники вошли в повседневную жизнь многих пользователей, и следующим естественным шагом является их внедрение в платёжные системы и банкинг. Основным драйвером развития голосовых решений является персонализация. Это связано с тем, что голосовое взаимодействие способно предоставить ценные сведения о потребностях и поведении клиентов, что позволяет банкам и FinTech-компаниям предложить услуги, наиболее полно соответствующие ожиданиям конкретного пользователя.

В результате опроса, проведённого Business Insider Intelligence в 2017 году в США, 8 % респондентов заявили, что использовали голосовые команды для покупки товаров, оплаты счетов и выполнения P2P-транзакций. Согласно прогнозам, к 2022 году количество пользователей голосовых интерфейсов вырастет до 31 % взрослого населения США [3].

Высокая потребительская ценность голосовых платежей стимулирует банки и таких платёжных провайдеров, как PayPal, Amazon, Apple и Google к развитию технологий искусственного интеллекта, специализированных на обработке голоса.

Однако проблемы информационной безопасности – основное препятствие, которое не позволяет голосовым платежам завоевать полное доверие со стороны банков и пользователей. Для того чтобы они стали такими же естественными, как взаимодействие с продавцом или сотрудником банка, необходимо усовершенствовать существующие методы защиты и аутентификации [3].

Алгоритмы подтверждения личности человека по голосу хорошо изучены, удобны в использовании и применимы как для непрерывной, так и для разовой аутентификации. Однако из-за широкого распространения недорогих устройств записи и воспроизведения звука они подвержены спуфингу, т.е. уязвимы к действиям злоумышленников, направленным на выдачу себя за другого человека. В связи с этим разработка и изучение способов противодействия спуфингу является основным направлением развития систем голосовой аутентификации.

Целью данной статьи является рассмотрение современного состояния исследований в области голосовой аутентификации. Далее будет описан концептуальный подход к голосовой аутентификации, перечислены основные голосовые характеристики, применяемые при реализации систем голосовой аутентификации, приведена актуальная классификация алгоритмов распознавания личности по голосу, описаны существующие метрики оценки эффективности систем голосовой аутентификации и изложены существующие подходы к классификации методов спуфинга. Кроме того, в рамках данного исследования усовершенствована классификация контрмер против спуфинга и выделены перспективные направления будущих исследований в области голосовой аутентификации.

Общая характеристика голосовой аутентификации. Голосовая аутентификация – динамический метод биометрической аутентификации, использующий уникальные характеристики человеческого голоса в качестве признака, позволяющего распознать субъекта и подтвердить его личность [4].

Концептуальная схема современного механизма голосовой аутентификации представлена на рисунке 1.

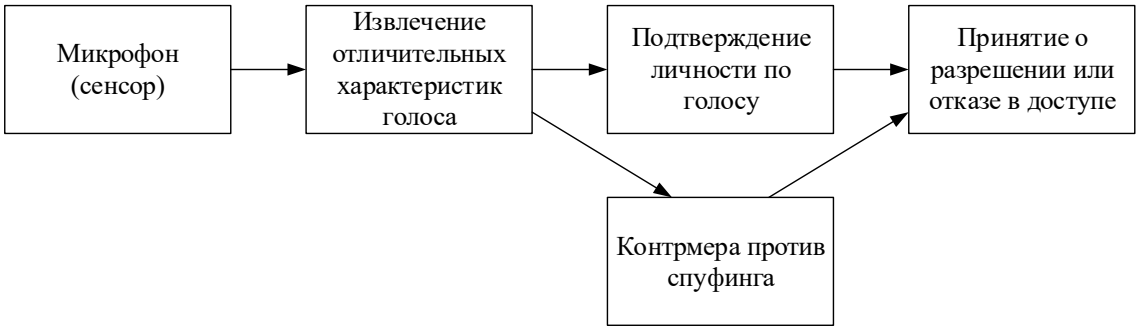


Рисунок 1 – Концептуальная схема современного механизма голосовой аутентификации

Как было упомянуто выше, голосовая аутентификация хорошо изучена и демонстрирует высокую эффективность, если при её тестировании проводить испытания только с живыми людьми. Однако её основным недостатком является уязвимость к спуфингу. В связи с этим система голосовой аутентификации должна включать в себя дополнительный механизм противодействия спуфингу, который называется контрмерой. Задача контрмеры – зафиксировать факт того, что система подвергается спуфинг-атаке.

Цикл функционирования любой системы биометрической аутентификации, в том числе голосовой, состоит из двух режимов: регистрация и верификация пользователя.

На этапе регистрации происходит сбор голосовых характеристик пользователя и формирование «голосового отпечатка», т.е. эталона биометрических характеристик, идентифицирующего пользователя.

На этапе верификации происходит предъявление пользователем его голосовых характеристик и сравнение их с хранимым в базе эталоном. Если в ходе сравнения подтверждается, что предъявляемые характеристики принадлежат заявленному пользователю, то пользователю предоставляется доступ. В противном случае ему отказывается в доступе.

В зависимости от ограничений, накладываемых на фразу, произносимую пользователем в процессе аутентификации, выделяют два вида подтверждения личности по голосу: текстонезависимое и текстозависимое.

Текстонезависимое подтверждение личности позволяет использовать произвольные фразы при регистрации и верификации пользователя. Преимуществом данного подхода является гибкость, однако для корректной работы он требует использования более длинных фраз по сравнению с текстозависимым подтверждением личности. Кроме того, как будет описано ниже, данный подход более эффективен против некоторых видов спуфинга.

Текстозависимое подтверждение личности предусматривает использование фиксированной фразы. Основное преимущество таких методов заключается в том, что они позволяют использовать фразы меньшей длины при регистрации и верификации пользователя.

Текстозависимая аутентификация тесно связана с такой задачей обработки голоса как распознавание речи, которая подразумевает выделение текста из речи. Решение данной задачи реализуется во всех системах голосового управления.

Оценка эффективности систем голосовой аутентификации. Для систем голосовой аутентификации применяются общие метрики оценки эффективности биометрических систем: вероятность ошибочного допуска, вероятность ошибочного отказа, кривая компромисса обнаружения ошибок и равная вероятность ошибки [5].

Вероятность ошибочного допуска (FAR) отражает долю спуфинговых атак, которые ошибочно верифицируются системой как истинные пользователи:

$$FAR = \frac{FA}{TA}, \quad (1)$$

где *FA* – число ошибочных допусков; *TA* – общее число попыток аутентификации.

Вероятность ошибочного отказа (FRR) отражает долю истинных пользователей, которым система ошибочно отказала в доступе:

$$FRR = \frac{FR}{TA}, \quad (2)$$

где *FR* – число ошибочных отказов в допуске; *TA* – общее число попыток аутентификации.

Обычно в процессе работы система аутентификации оценивает степень уверенности (вероятность) в том, что предъявленные биометрические характеристики принадлежат заявленному субъекту. В связи с этим имеется возможность настройки порогового значения степени уверенности. Если при попытке аутентификации степень уверенности системы больше порогового значения, то человеку разрешается доступ, а иначе – запрещается.

В зависимости от выбранного порогового значения степени уверенности, вероятность ошибочного допуска и вероятность ошибочного отказа меняют свои значения. Перечень возможных соотношений этих значений представлен кривой компромисса обнаружения ошибок.

Например, на рисунке 2 представлены кривые компромисса обнаружения ошибок для одной из систем голосовой аутентификации, участвующей в ASVSpoof 2015, при воздействии на систему каждым из 10 способов проведения спуфинг-атаки, используемом в конкурсе [6].

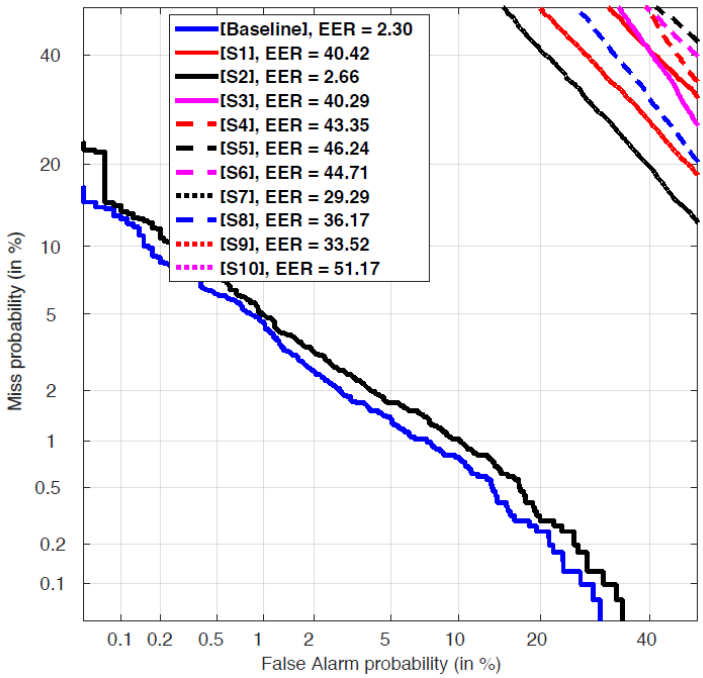


Рисунок 2 – Примеры кривых компромисса обнаружения ошибок

В качестве численного значения оценки эффективности системы аутентификации используется вероятность равной ошибки (EER) – которая соответствует точке на кривой, при котором вероятность ошибочного допуска равна вероятности ошибочного отказа.

Однако, как показано на рисунке 1, специфика работы систем голосовой аутентификации состоит в совместной работе двух классификаторов, обрабатывающих исходные данные: подсистемы подтверждения личности пользователя и контрмеры. Изначально их производительности оценивались независимо друг от друга, но в работе [7] был предложен более эффективный метод их совместной оценки – функция тандемной оценки стоимости обнаружения (t-DCF). Данная метрика хорошо зарекомендовала себя в ходе конкурса ASVSpoof, в котором она используется, начиная с 2019 года.

Наравне с выбором метрики оценки важное значение имеют условия проведения экспериментального исследования эффективности системы голосовой аутентификации.

В зависимости от возможностей доступа злоумышленника в систему выделяют два вида испытаний:

- испытания с логическим доступом (over-the-wire), при проведении которых не предусматривается использование сенсора (микрофона), и данные загружаются в цифровом виде напрямую в систему. Данный подход упрощает проведение атаки условному злоумышленнику и преимущественно используется для оценки эффективности таких видов спуфинга, как синтез и преобразование речи;
- испытания с физическим доступом (over-the-air), при проведении которых предусматривается взаимодействие с системой через сенсор (микрофон).

Также важно учитывать, что результат оценки эффективности системы голосовой аутентификации с физическим доступом подвержен влиянию следующих факторов:

- соотношение сигнал – шум;
- ревебрация;
- характеристики используемого микрофона;
- свойства помещения, в котором проводится испытание;
- качество записывающей и воспроизводящей аппаратуры, используемой при спуфинге.

Отличительные голосовые характеристики. Отличительные голосовые характеристики – это значимые особенности, извлекаемые из необработанного голосового сигнала, идентифицирующие человека.

Имеющиеся исследования свидетельствуют о том, что выбор отличительных голосовых характеристик имеет не меньшее влияние на результат работы системы голосовой аутентификации, чем выбор классификатора [6].

Для эффективного использования при реализации аутентификации и контрмер извлекаемые характеристики должны обладать следующими свойствами:

- большая вариативность у разных пользователей и малая вариативность у одного пользователя;
- устойчивость к искажениям и шуму;
- частая встречаемость в речи;
- лёгкость измерения;
- сложность подделки;
- независимость от состояния здоровья человека;
- неизменяемость у человека с течением времени.

Наибольшую распространённость получили кратковременные спектральные характеристики, при расчёте которых используются фрагменты речевого сигнала длиной 20–30 миллисекунд. Данные характеристики заключают в себе информацию о тембре и особенностях голосового тракта человека.

Кратковременные спектральные характеристики обладают следующими преимуществами:

- простота извлечения;
- потребность в небольшом объёме данных;
- независимость от текста и языка;
- возможность эффективной обработки.

По сравнению с более высокоуровневыми поведенческими характеристиками речи, кратковременные спектральные характеристики менее устойчивы к шуму и канальным искажениям, однако они гораздо лучше подходят для практической реализации системы голосовой аутентификации.

Механизм извлечения большинства таких характеристик основывается на дискретном (DFT), а точнее, на быстром преобразовании Фурье (FFT) [8]. Однако информация, которую содержит амплитудный спектр голосового сигнала, полученный при помощи FFT, избыточна. Поэтому при голосовой аутентификации используют другие характеристики, которые содержат наиболее существенную для задачи обработки голоса информацию, но имеют меньшую размерность и тем самым обеспечивают более простую обработку.

Наибольшее распространение получили мел-кепстральные частотные коэффициенты (MFCC) [9], использующие фильтр, учитывающий особенности восприятия звуков человеком (психоакустику), логарифмическое сжатие и дискретное косинусное преобразование.

Также используются методы оценки спектра, альтернативные DFT, например, линейные предсказательные частотные коэффициенты (LPCC) [10], основанные на вычислительной процедуре линейного предсказания.

Существует большое количество исследований, направленных на оценку эффективности применения различных характеристик. При этом установлено, что совместное использование характеристик, основанных на разном математическом аппарате, позволяет повысить эффективность работы системы.

Также существуют труды, рассматривающие возможность использования временных спектральных характеристик и просоидальные характеристики, однако они не получили такого широкого распространения, как кратковременные спектральные характеристики.

Алгоритмы подтверждения личности по голосу. При регистрации пользователя полученные голосовые характеристики используются для тренировки распознавателя голоса. Распознаватель голоса – это математическая модель, используемая для сравнения голоса диктора, проходящего верификацию, с эталонными характеристиками заявленного субъекта [11].

В зависимости от подхода к тренировке моделей их можно разделить на генеративные (классические) и дискриминативные. В то время как генеративные модели моделируют распределение характеристик речи конкретного пользователя, дискриминативные модели аппроксимируют границу между голосами разных людей в гиперпространстве характеристик.

В свою очередь, генеративные модели можно разделить на шаблонные (непараметрические) и вероятностные (параметрические) модели.

Шаблонные модели рассматривают предъявляемый вектор голосовых характеристик как неточную копию эталонного вектора пользователя. Исходя из этого рассчитывается степень отличия между этими векторами, на основании которой и определяется успешность аутентификации.

Вероятностные модели рассматривают человеческий голос как некоторое распределение характеристик, имеющее определённую функцию плотности вероятности. На этапе обучения производится аппроксимация параметров данной функции. На этапе верификации выполняется оценка вероятности того, что параметры речи верифицируемого пользователя соответствуют эталонной модели [11].

В таблице 1 представлены наиболее распространённые генеративные модели.

Среди перечисленных алгоритмов модель гауссовой смеси стала де факто стандартом, и эффективность других алгоритмов распознавания личности по голосу сравнивается именно с ней.

Таблица 1 – Классификация наиболее широко распространённых генеративных моделей, используемых для голосовой аутентификации

	Текстозависимая аутентификация	**Текстонезависимая аутентификация**
Шаблонные модели	Динамическая трансформация временной шкалы	Векторное квантование
Вероятностные модели	Скрытая марковская модель	Модель гауссовой смеси

К дискриминативным моделям относятся нейронные сети и машины опорных векторов. Преимущество нейронных сетей заключается в том, что они способны объединить процесс извлечения характеристик и распознавания личности. Машины опорных векторов – также широко применяемый инструмент подтверждения личности по голосу, обладающий хорошей обобщающей способностью [12]. Некоторые системы аутентификации объединяют в себе сразу несколько алгоритмов подтверждения личности по голосу, что позволяет повысить общую эффективность [13].

Разновидности спуфинга. Под спуфингом понимаются действия злоумышленника, направленные на успешную аутентификацию в системе под видом другого лица. Благодаря широкому распространению качественного записывающего и воспроизводящего звукового оборудования, системы голосовой аутентификации в существенной мере подвержены спуфингу.

Существуют следующие основные виды спуфинга [12]:

1. Выдача себя за другое лицо. Данный вид спуфинга реализуется посредством подражания одним человеком голосовым характеристикам другого человека. Выдача себя за другое лицо отличается от других видов спуфинга тем, что для его реализации злоумышленник не использует вспомогательных технических средств и методов. В связи с этим противодействие этому виду спуфинга не требует дополнительных контрмер и реализуется за счёт качественной работы системы голосовой верификации.

2. Запись речи (атака повторным воспроизведением). Запись речи – простой и эффективный вид спуфинга, который, по мнению многих исследователей, представляет наиболее серьёзную угрозу системам голосовой аутентификации. Его реализация заключается в записи фрагмента речи человека с целью его последующего предъявления системе аутентификации.

3. Преобразование речи. Преобразование речи подразумевает использование специализированных программных средств, изменяющих речь человека таким образом, чтобы она стала похожей на речь другого человека.

Оценка сопротивляемости различных контрмер данному виду спуфинга была предметом конкурса ASVSpoof 2015, в ходе которого использовались следующие алгоритмы преобразования речи [13]:

- выбор фрагментов речи на основе образца для преобразования голоса с использованием временной информации;
- подстраивание первого мел-кепстрального коэффициента под значение человека-цели (один из простейших алгоритмов);

- алгоритмы, использующие модель гауссовой смеси (самые распространённые);
- алгоритм, основанный на тензорном представлении пространства признаков пользователя;
- алгоритм, использующий регрессию частичным методом наименьших квадратов, основанный на ядре пространства.

4. Синтез речи. Данный метод подразумевает генерацию искусственного голоса на основе произвольного текста, обладающего характеристиками голоса определённого человека.

Оценка сопротивляемости различных контрмер данному виду спуфинга была предметом конкурса ASVSpoof 2015, в ходе которого использовались следующие алгоритмы синтеза речи [13]:

- синтез речи, основанный на выборе и конкатенации отдельных речевых элементов (данный вид спуфинга оказался наиболее эффективным);
- статистический синтез речи, основанный на скрытой марковской модели.

Перспективным методом синтеза и преобразования речи является технология дипфейк, подразумевающая использование генеративно-состязательных нейронных сетей. Оценка способности контрмер противостоять дипфейк-атакам является одной из задач конкурса ASVSpoof 2021.

5. Замаскированные атаки на системы обработки человеческого голоса, использующие особенности восприятия звуков человеком.

В исследовании [14] рассматриваются 4 способа преобразования записи голоса таким образом, чтобы она стала непонятной для человека, но чтобы её существенные акустические голосовые признаки остались неизменными и запись могла пройти систему голосовой аутентификации или быть обработанной системой распознавания речи.

Контрмеры против спуфинга. Общая классификация контрмер против спуфинга представлена в работе [12]. Мы предлагаем её дополненную версию.

1. Интерактивные контрмеры. Интерактивные контрмеры подразумевают явное взаимодействие пользователя с системой в ходе аутентификации. Как правило, при их использовании, система генерирует случайный текст, который нужно прочитать пользователю. Для аутентификации пользователя используется алгоритм текстонезависимого подтверждения личности, а правильность прочтения текста проверяется алгоритмом распознавания речи.

Данный тип контрмер показывает высокую эффективность противодействия наиболее опасному виду спуфинга – атакам повтором. Это связано с тем, что у злоумышленника, как правило, отсутствует возможность заранее записать речь пользователя таким образом, чтобы из её фрагментов можно было оперативно составить случайную фразу.

2. Контрмеры, использующие акустические особенности сгенерированного или синтезированного голоса.

Данное семейство контрмер концентрируется на извлечении из записи голоса несовершенств, свидетельствующих о том, что отрывок речи был получен при помощи методов синтеза или преобразования речи. Именно такие контрмеры являлись объектом исследования ASVSpoof 2015 [13].

Методы, относящиеся к этому типу, так же как и методы верификации по голосу, преимущественно опираются на использование кратковременных спектральных характеристик. Наибольшее распространение получили такие классификаторы, как модель гауссовой смеси, машины опорных векторов и искусственные нейронные сети.

Одной из особенностей данных контрмер является то, что оценку их эффективности можно проводить в формате исследования с логическим доступом.

3. Методы обнаружения живого голоса, основанные на особенностях речевого тракта человека. Поскольку спуфинг подразумевает использование звуковоспроизводящей аппаратуры, задачу голосовой аутентификации можно представить, как совокупность двух следующих задач:

- подтвердить личность человека по голосовым характеристикам (верификация);
- подтвердить, что источником голоса является живой человек (контрмера).

Данное семейство контрмер опирается на особенности речевого тракта человека, приводящие к возникновению акустических эффектов, которые затруднительно записать и воспроизвести при помощи искусственных средств.

Примеры методов обнаружения живого голоса, основанных на особенностях речевого тракта человека:

- обнаружение живого голоса, основанное на хлопающем шуме, вызванном дыханием человека [14];
- обнаружение живого голоса для аутентификации на смартфонах, основанное на локализации фонем;
- обнаружение живого голоса, основанное на артикулярных жестах.

4. Методы обнаружения живого голоса, основанные на особенностях воспроизведения звука громкоговорителем. На данный момент широкому кругу пользователей доступны устройства записи и

воспроизведения звука, способные копировать голос человека с очень высоким качеством, которые продолжают развиваться. При использовании приведённых ранее голосовых характеристик (например, мел-кепстральных частотных коэффициентов) искусственный голос крайне затруднительно отличить от живого, о чём свидетельствуют результаты конкурса ASVSpoof 2017 [15].

В связи с этим высказываются предложения по применению других демаскирующих признаков, позволяющих понять, что при попытке аутентификации звук воспроизводится искусственным громкоговорителем. Например, в работе [16] предлагается использовать магнитное поле для того, чтобы отличить громкоговоритель от живого человека.

5. Совместное использование разных биометрических методов. Данный подход подразумевает повышение эффективности системы аутентификации и устойчивости к спуфингу за счёт использования двух или более несвязанных биометрических характеристик. Например, в работе [17] предлагается бимодальная система подтверждения личности, использующая модель гауссовой смеси с универсальной фоновой моделью для голосовой аутентификации и систему верификации лица, при помощи признаков Гэбора и линейного дискриминантного анализа.

Кроме того, в качестве дополнительной категории контрмер можно выделить методы, повышающие качество распознавания личности по голосу за счёт использования множества микрофонов.

Заключение. В данной статье были перечислены основные отличительные голосовые характеристики, используемые при реализации систем голосовой аутентификации, и описаны ключевые особенности их применения. Приведена актуальная классификация алгоритмов распознавания личности по голосу в зависимости от фиксации конкретной фразы при аутентификации и вида применяемого математического аппарата. Описаны существующие метрики оценки эффективности систем голосовой аутентификации: показаны как общие метрики оценки эффективности систем аутентификации, так и уникальная метрика, используемая для систем голосовой аутентификации. Изложены существующие подходы к классификации методов спуфинга.

Кроме того, усовершенствована классификация контрмер против спуфинга и выделены перспективные направления будущих исследований в области голосовой аутентификации.

Библиографический список

1. Eadicco, L. Google just revealed that half a billion people around the world are using the Google Assistant as it battles with Amazon to conquer the smart home / L. Eadicco // Insider. – Режим доступа: https://www.businessinsider.com/google-assistant-500-million-users-challenges-amazon-alexa-2020-1, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2022).

2. Kinsella, B. Apple Still in Holding Pattern on Voice, Siri Used 25 Billion Times Per Month But New Features Limited / B. Kinsella // Voicebot.ai. – Режим доступа: https://voicebot.ai/2020/06/22/apple-still-in-holding-pattern-on-voice-siri-used-25-billion-times-per-month-but-new-features-limited/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2022).

3. Dyke, D. V. Soon nearly a third of US consumers will regularly make payments with their voice / D.V. Dyke // Insider. – Режим доступа: https://www.businessinsider.com/the-voice-payments-report-2017-6#:~:text=Voice%20payments%20are%20catching%20on,of%20US%20adults%20by%202022, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2022).

4. Ravika, N. An Overview of Automatic Speaker Verification System / N. Ravika // Intelligent Computing and Information and Communication : Proceedings of 2nd International Conference, ICICC 2017, 2–4 August 2017. – Pune, India, 2017. – P. 603–610.

5. El-Abed, M. Evaluation of Biometric Systems / M. El-Abed, C. Charrier // New Trends and Developments in Biometrics. – 2012. – P. 149–169.

6. Wu, Z. ASVspoof 2015: the First Automatic Speaker Verification Spoofing and Countermeasures Challenge / Z. Wu, T. Kinnunen, N. Evans, J. Yamagishi, C. Hanilçi, M. Sahidullah, A. Sizov // 16th Annual Conference of the International Speech Communication Association (Interspeech 2015). – Dresden, Germany, 2015.

7. Kinnunen, T. t-DCF: a Detection Cost Function for the Tandem Assessment of Spoofing Countermeasures / T. Kinnunen, K. Lee, H. Delgado, N. Evans, M. Todisco, et al. // Speaker Odyssey 2018. The Speaker and Language Recognition Workshop, 17th August 2018. – Les Sables-d'Olonne, France, 2018. – Режим доступа: https://hal.inria.fr/hal-01880306/document, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2022).

8. Oppenheim, A. Discrete-Time Signal Processing. Second edition / A. Oppenheim, R. Schafer, J. Buck. – New Jersey : Prentice Hall, 1999. – 893 p.

9. Deller, J. Discrete-Time Processing of Speech Signals. Second edition / J. Deller, J. Hansen, J. Proakis. – New York : IEEE Press, 2000. – 936 p.

10. Huang, X. Spoken Language Processing: a Guide to Theory, Algorithm, and System Development / X. Huang, A. Acero, H.-W. Hon. – New Jersey : Prentice-Hall, 2001. – 935 p.

11. Kinnunen, T. An Overview of Text-Independent Speaker Recognition: from Features to Supervectors / T. Kinnunen, H. Li // Speech Communication. – 2010. – № 52. – P. 12–40.

12. Hao, B. Voice Liveness Detection for Medical Devices / B. Hao, X. Hei // Design and Implementation of Healthcare Biometric Systems. – 2019. – P. 109–136.

13. Wu, Z. ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge / Z. Wu, J. Yamagishi, T. Kinnunen, C. Hanilc, M. Sahidullah, A. Sizov, N. Evans, M. Todisco // IEEE Journal of Selected Topics in Signal Processing. – 2017. – Vol. 11, № 4. – P. 588–604.

14. Abdullah, H. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems / H. Abdullah, W. Garcia, C. Peeters, P. Traynor, K. Butler, J. Wilson // The Network and Distributed System Security Symposium, NDSS 2019, 24–27 February 2019. – San Diego, USA, 2019. – Режим доступа: https://hal.inria.fr/hal-01880306/document, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 20.01.2022).

15. Kinnunen, T. // The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection / T. Kinnunen, M. Sahidullah, H. Delgado, M. Todisco, N. Evans, J. Yamagishi, K. A. Lee // 19th Annual Conference of the International Speech Communication Association (Interspeech 2018). – Stockholm, Sweden, 2018.

16. Li, L. A study on replay attack and anti-spoofing for automatic speaker verification / L. Li, Y. Chen, D. Wang // 18th Annual Conference of the International Speech Communication Association (Interspeech 2017). – Stockholm, Sweden, 2018. – P. 92–96.

17. Usoltsev, A. Full Video Processing for Mobile Audio-Visual Identity Verification / A. Usoltsev, D. Petrovska-Delacrétaz, K. Houssemeddine // Proceedings of the 5th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2016). – Rome, Italy, 2016. – P. 552–557.

References

1. Eadicco, L. Google just revealed that half a billion people around the world are using the Google Assistant as it battles with Amazon to conquer the smart home. *Insider.* Available at: https://www.businessinsider.com/google-assistant-500-million-users-challenges-amazon-alexa-2020-1 (accessed 20.01.2022).

2. Kinsella, B. Apple Still in Holding Pattern on Voice, Siri Used 25 Billion Times Per Month But New Features Limited. *Voicebot.ai.* Available at: https://voicebot.ai/2020/06/22/apple-still-in-holding-pattern-on-voice-siri-used-25-billion-times-per-month-but-new-features-limited (accessed 20.01.2022).

3. Dyke, D. V. Soon nearly a third of US consumers will regularly make payments with their voice. *Insider.* Available at: https://www.businessinsider.com/the-voice-payments-report-2017-6#:~:text=Voice%20payments%20are%20catching%20on,of%20US%20adults%20by%202022 (accessed 20.01.2022).

4. Ravika, N. An Overview of Automatic Speaker Verification System. *Intelligent Computing and Information and Communication. Proceedings of 2nd International Conference. ICICC.* Pune, India, 2017, pp. 603–610.

5. El-Abed, M., Charrier, C. *Evaluation of Biometric Systems. New Trends and Developments in Biometrics*, 2012, pp. 149–169.

6. Wu, Z., Kinnunen, T., Evans, N., Yamagishi, J., Hanilçi, C., Sahidullah, M., Sizov, A. ASVspoof 2015: the First Automatic Speaker Verification Spoofing and Countermeasures Challenge. *16th Annual Conference of the International Speech Communication Association (Interspeech 2015).* Dresden, Germany, 2015.

7. Kinnunen, T., Lee, K., Delgado, H., Evans, N., Todisco, M., et al. t-DCF: a Detection Cost Function for the Tandem Assessment of Spoofing Countermeasures *Speaker Odyssey 2018. The Speaker and Language Recognition Workshop, 17th August 2018.* – Les Sables-d'Olonne, France, 2018. Available at: https://hal.inria.fr/hal-01880306/document (accessed 20.01.2022).

8. Oppenheim, A., Schafer, R., Buck, J. *Discrete-Time Signal Processing.* Second edition. New Jersey, Prentice Hall, 1999. 893 p.

9. Deller, J., Hansen, J., Proakis, J. *Discrete-Time Processing of Speech Signals.* Second edition. New York, IEEE Press, 2000. 936 p.

10. Huang, X., Acero, A., Hon, H.-W. *Spoken Language Processing: a Guide to Theory, Algorithm, and System Development.* New Jersey, Prentice Hall, 2001. 935 p.

11. Kinnunen, T., Li, H. An Overview of Text-Independent Speaker Recognition: from Features to Supervectors. *Speech Communication*, 2010, no. 52, pp. 12–40.

12. Hao, B., Hei, X. Voice Liveness Detection for Medical Devices. *Design and Implementation of Healthcare Biometric Systems,* 2019, pp. 109–136.

13. Wu, Z., Yamagishi, J., Kinnunen, T., Hanilc, C., Sahidullah, M., Sizov, A., Evans, N., Todisc,o M. ASVspoof: the Automatic Speaker Verification Spoofing and Countermeasures Challenge. *IEEE Journal of Selected Topics in Signal Processing,* 2017, vol. 11, no. 4, pp. 588–604.

14. Abdullah, H., Garcia, W., Peeters, C., Traynor, P., Butler, K., Wilson, J. Practical Hidden Voice Attacks against Speech and Speaker Recognition Systems. *The Network and Distributed System Security Symposium. NDSS.* San Diego, USA, 2019. Available at: https://hal.inria.fr/hal-01880306/document (accessed 20.01.2022).

15. Kinnunen, T., Sahidullah, M., Delgado, H., Todisco, M., Evans, N., Yamagishi, J., Lee, K. A. The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection. *19th Annual Conference of the International Speech Communication Association (Interspeech 2018).* Stockholm, Sweden, 2018.

16. Li, L., Chen, Y., Wang, D. A study on replay attack and anti-spoofing for automatic speaker verification. *18th Annual Conference of the International Speech Communication Association (Interspeech 2017).* Stockholm, Sweden, 2018, pp. 92–96.

17. Usoltsev, A., Petrovska-Delacrétaz, D., Houssemeddine, K. Full Video Processing for Mobile Audio-Visual Identity Verification. *Proceedings of the 5th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2016).* Rome, Italy, 2016, pp. 552–557.

УДК 004.896

РАЗРАБОТКА МЕТОДА АУТЕНТИФИКАЦИИ СПУТНИКА, РЕАЛИЗОВАННОГО В МОДУЛЯРНОМ КОДЕ С ПСЕВДОСЛУЧАЙНОЙ ЗАМЕНОЙ ПОРОЖДАЮЩИХ ЭЛЕМЕНТОВ[1]

Статья поступила в редакцию 26.08.2022, в окончательном варианте – 26.08.2022.

Чистоусов Никита Константинович, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
аспирант, ORCID: 0000-0002-0286-7391, e-mail: chistousov.nik@yandex.ru
Калмыков Игорь Анатольевич, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
доктор технических наук, профессор, ORCID: 0000-0002-9854-5310, e-mail: ikalmykov@ncfu.ru
Копытов Владимир Вячеславович, Северо-Кавказский федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,
профессор, ORCID: 0000-0002-3053-1641, e-mail:vkopytov@ncfu.ru
Тищенко Евгений Николаевич, Ростовский государственный экономический университет (РИНХ), 344002, Российская Федерация, Ростов-на-Дону, ул. Большая Садовая, 1,
доктор экономических наук, декан факультета, ORCID: 0000-0003-1527-4904, e-mail: celt@inbox.ru
Чернышев Александр Борисович, Пятигорский институт (филиал) Северо-Кавказского федерального университета, 357500, Российская Федерация, г. Пятигорск, пр. 40 лет Октября, 56,
доктор технических наук, профессор, ORCID: 0000-0002-0237-2911, e-mail: achernyshev@ncfu.ru

Низкоорбитальные системы спутниковой связи являются неотъемлемой частью перспективных проектов, которые реализует Российская Федерация по освоению побережья Северного Ледовитого океана. Стратегическое развитие Северного морского пути, формирование и размещение сил быстрого реагирования, обеспечивающих защиту и охрану территориальной целостности страны в Арктике, освоение месторождений запаса газа и нефти, расположенных на шельфе Северного Ледовитого океана, возможно только на основе использования низкоорбитальных систем спутниковой связи. Это обусловлено способностью низкоорбитальных спутников обеспечить бесперебойную и устойчивую связь с объектами, расположенными за полярным кругом. В настоящее время по мере освоения Крайнего Севера наблюдается тенденция увеличения числа группировок низкоорбитальных космических аппаратов. В результате может возникнуть ситуация, когда чужой спутник-нарушитель, оказавшись в зоне видимости приемника, попытается навязать ретрансляционную помеху. Одним из эффективных способов противодействия навязыванию спуфинг-помехи является использование системы «свой-чужой» для опознавания спутника. Чтобы повысить имитостойкость системы опознавания космических аппаратов, предлагается использовать метод аутентификации с нулевым разглашением знаний, реализованный в модулярном коде. В этом случае за счет параллельной обработки данных обеспечивается снижение времени, необходимого для проверки сигнала ответчика, расположенного на борту космических аппаратов. Это приводит к снижению вероятности подбора правильного сигнала ответчика спутником-нарушителем. Дальнейшее повышение имитостойкости низкоорбитальных систем спутниковой связи возможно за счет псевдослучайной замены порождающих элементов мультипликативной группы при вычислениях. Поэтому разработка метода аутентификации спутника, реализованного в модулярном коде с псевдослучайной заменой порождающих элементов, является актуальной задачей. Цель работы – повышение имитостойкости низкоорбитальных систем спутниковой к спуфинг-помехам за счет применения системы «свой-чужой», использующей разработанный метод аутентификации.

Ключевые слова: низкоорбитальная система спутниковой связи, имитостойкость, метод аутентификации с нулевым разглашением знаний, модулярный код, элемент, порождающий мультипликативную группу

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90009.

DEVELOPMENT OF A SATELLITE AUTHENTICATION METHOD IMPLEMENTED IN A MODULAR CODE WITH PSEUDORANDOM REPLACEMENT OF GENERATIVE ELEMENTS

The article was received by the editors 26.08.2022, in the final version – 26.08.2022.

Chistousov Nikita K., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,
postgraduate student, ORCID: 0000-0002-0286-7391, e-mail: chistousov.nik@yandex.ru
Kalmykov Igor A., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,
Doct. Sci. (Engineering), Professor, ORCID: 0000-0002-9854-5310, e-mail: ikalmykov@ncfu.ru
Kopytov Vladimir V., North Caucasian Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,
professor, ORCID: 0000-0002-3053-1641, e-mail: vkopytov@ncfu.ru
Tishchenko Evgeny N., Rostov State University of Economics (RINH), 1, Bolshaya Sadovaya St., Rostov-on-Don, 344002, Russian Federation,
Doct. Sci. (Economics), Dean of the Faculty, ORCID: 0000-0003-1527-4904, e-mail: celt@inbox.ru
Chernyshev Alexander B., Pyatigorsk Institute (branch) of the North Caucasian Federal University, 56 prospect 40 let Oktyabrya, Pyatigorsk, 357500, Russian Federation,
Doct. Sci. (Engineering), Professor, ORCID: 0000-0002-0237-2911, e-mail: achernyshev@ncfu.ru

Low orbit satellite communication systems are an integral part of the promising projects that the Russian Federation is implementing to develop the coast of the Arctic Ocean. The strategic development of the Northern Sea Route, the formation and deployment of rapid reaction forces that ensure the protection and protection of the country's territorial integrity in the Arctic, the development of gas and oil reserves located on the shelf of the Arctic Ocean is possible only through the use of low orbit satellite communication systems. This is due to the ability of low-orbit satellites to provide uninterrupted and stable communication with objects located beyond the Arctic Circle. Currently, as the development of the Far North, there is a tendency to increase the number of groups of low-orbit spacecraft. As a result, a situation may arise when an alien intruder satellite, once in the receiver's visibility zone, will try to impose relay interference. One of the effective ways to counter the imposition of spoofing interference is to use the "friend or foe" system to identify the satellite. To increase the imitation resistance of the spacecraft identification system, it is proposed to use the zero-knowledge authentication method implemented in a modular code. In this case, due to parallel data processing, the time required to check the transponder signal located on board the spacecraft is reduced. This leads to a decrease in the probability of selecting the correct transponder signal by the intruder satellite. A further increase in the imitation resistance of the low orbit satellite communication systems is possible due to the pseudo-random replacement of the generating elements of the multiplicative group in the course of calculations. Therefore, the development of a satellite authentication method implemented in a modular code with pseudo-random replacement of generating elements is an urgent task. The purpose of the work is to increase the resistance of the low orbit satellite communication systems to spoofing interference by using the "friend or foe" system using the developed authentication method.

Keywords: low-orbit satellite communication system, imitation resistance, zero-knowledge authentication method, modular code, element that generates a multiplicative group

Введение. Повышенный интерес к освоению территорий страны, расположенных за полярным кругом связан с объемами запасов полезных ископаемых. Так, по прогнозам ученых, на шельфе Северного Ледовитого океана хранится до 20 % запасов углеводородов. Поэтому одним из стратегических проектов, реализуемых Российской Федерацией, является освоение месторождений запаса нефти, расположенных на шельфе Северного Ледовитого океана. С целью снижения затрат на добычу и транспортировку углеводородов современные корпорации будут использовать автоматизированные системы дистанционного управления нефтяными месторождениями [1]. Так как большинство объектов управления будут размещаться за полярным кругом, то единственной системой связи, обеспечивающей круглосуточный обмен данными, является низкоорбитальная система спутниковой связи (НССС). Как правило, группировка НССС содержит от 46 до 64 космических аппарата (КА) [2–4].

По мере освоения территорий акватории Северного Ледовитого океана различными странами будет наблюдаться тенденция по увеличению числа таких группировок. А это будет способствовать возрастанию деструктивных воздействий на НССС со стороны спутников-нарушителей. Проведенные исследования показали, что, учитывая ограничения энергии, поступающей от солнечных батарей, наиболее эффективным деструктивным воздействием на НССС является постановка спуфинг-помехи. Для ее генерации спутник-нарушитель перехватывает правильный сигнал, задерживает его, а затем навязывает его приемнику. Так как параметры спуфинг-помехи совпадают с параметрами используемых сигналов, то приемник обработает данный сигнал и передаст его

объект управления. В результате этого может быть нарушена работа системы дистанционного управления нефтяными месторождениями. А это, при определенных условиях, может спровоцировать экологическую катастрофу.

Предотвратить такое деструктивное воздействие на НССС можно за счет повышения ее имитостойкости. Для достижения данной цели предлагается использовать систему «свой-чужой» для опознавания спутника. Перед началом сеанса система опознавания проверяет спутник, появившийся в зоне видимости. Если спутник является «свой», то ему предоставляется сеанс связи. Если спутник является чужим, то ему отказывают в сеансе связи. В результате этого спутник-нарушитель не сможет навязать спуфинг-помехи. Очевидно, что чем больше времени отводится на проверку КА, тем больше вероятность подбора правильного ответа на вопрос запросчика у спутника-нарушителя. Тем выше вероятность пропуска чужого спутника системой «свой-чужой». Поэтому разработка метода аутентификации, обладающего минимальными временными затратами на определение статуса спутника и использующего псевдослучайную замену порождающих элементов, является актуальной задачей.

Материал и методы исследования. Для того чтобы снизить вероятность пропуска спутника-нарушителя, было предложено использовать метод аутентификации, использующий доказательство с нулевым разглашением. Данный метод обладает высокой криптографической стойкостью без использования систем шифрования. В работах [5, 6] представлен метод аутентификации, построенный на основе доказательства с нулевым разглашением знаний и обладающий минимальным количеством этапов определения статуса претендента. Перед началом аутентификации КА необходимо найти большое простое число P, для которого существует число p, порождающее Z_P. В качестве секретных данных в методе аутентификации выступают: секретный ключ КА – число E, где параметров $E < P$; числа Q и G, где $\{Q,G\} < P-2$, с помощью которых генерируются сеансовый ключ Q(n) для n-го сеанса проверки и число G(n), которое используется в процессе проверки повторного использования сеансового ключа Q(n). Для нахождения Q(n) и числа G(n) используется генератор псевдослучайной функции.

На первом этапе метода ответчик (O), который находится на КА, определяет истинный статус аппарата

$$O: U(n) = (p^{E(n)} p^{Q(n)} p^{G(n)}) \bmod P, \tag{1}$$

где $n = 1, 2, \ldots$ – номер сеанса связи спутника.

На втором этапе ответчик выбирает числа $\Delta E(n), \Delta Q(n), \Delta G(n)$ для зашумления секретных данных

$$O: \Delta E(n), \Delta Q(n), \Delta G(n) \mid \Delta E(n), \Delta Q(n), \Delta G(n) < \varphi(P) - 1, \tag{2}$$

где $\varphi(P) = P - 1$ – функция Эйлера простого числа P.

Зашумление секретных данных выполняется согласно

$$\begin{aligned} O: E^*(n) &= (E + \Delta E(n)) \bmod \varphi(P), \\ O: Q^*(n) &= (Q(n) + \Delta Q(n)) \bmod \varphi(P), \\ O: G^*(n) &= (G(n) + \Delta G(n)) \bmod \varphi(P). \end{aligned} \tag{3}$$

На третьем этапе ответчик определяет «искаженный» статус КА

$$O: U^*(n) = (p^{E^*(n)} p^{Q^*(n)} p^{G^*(n)}) \bmod P. \tag{4}$$

Рассмотрим процесс аутентификации спутника.

На первом этапе, после того КА залетел в зону видимости системы «свой-чужой», запросчик (З) генерирует число H(n). Данное число передается ответчику

$$З \to O: H(n) \mid H(n) < \varphi(P). \tag{5}$$

На втором этапе ответчик, используя «вопрос» H(n), вычисляет ответы

$$O: W^1(n) = (E^*(n) - H(n)E\ (n)) \bmod \varphi(P), \tag{6}$$

$$O: W^2(n) = (Q^*(n) - H(n)Q(n)) \bmod \varphi(P), \tag{7}$$

$$O: W^3(n) = (G^*(n) - H(n)G(n)) \bmod \varphi(P). \tag{8}$$

На третьем этапе формируется сигнал ответчика, который передается запросчику

$$O \to З: \{U(n) \parallel U^*(n) \parallel W^1(n) \parallel W^2(n) \parallel W^3\}. \tag{9}$$

На четвертом этапе запросчик осуществляет проверку сигнала ответчика

$$3: R(n) = (U^{H(n)} p^{W^1(n)} p^{W^2(n)} p^{W^3(n)}) \bmod P. \quad (10)$$

При выполнении равенств $R(n) = U^*(n)$ спутник считается «своим». После успешной аутентификации спутнику предоставляется сеанс связи. Если равенство не выполняется, то спутнику не предоставляется сеанс связи, так как его статус – «чужой».

Основным недостатком данного метода аутентификации является использование при вычислениях большого простого числа P, что не обеспечивает минимального времени на проверку статуса КА. Чтобы снизить временные затраты на аутентификацию КА, в работах [7, 8] предложена реализация данного метода аутентификации в модулярном коде системы остаточных классов (СОК).

При построении кода СОК используется кортеж простых чисел m_i, $i = 1,2,...,k$. Данные числа являются основаниями кода СОК [9, 10]. При этом основания выбираются из условия

$$m_1 < m_2 < ... < m_{k-1} < m_k. \quad (11)$$

Набор оснований задает рабочий диапазон кода СОК

$$M_k = \prod_{i=1}^{k} m_i. \quad (12)$$

Тогда в коде СОК при выполнении условия $Y < M_k$ справедливо равенство

$$Y = (y_1, y_2, ..., y_{k-1}, y_k), \quad (13)$$

где $y_i \equiv Y \bmod m_i$; $i = 1,..., k$.

Повышение скорости выполнения модульных операций в коде СОК обусловлено параллельной природой их реализации. При этом операции сложения, вычитания и умножения выполняются с числами, значения которых не превышает основания СОК. Тогда справедливо

$$Y \circ V = ((y_1 \circ v_1) \bmod m_1, (y_2 \circ v_2) \bmod m_2, ..., (y_k \circ v_k) \bmod m_k), \quad (14)$$

где $\circ$ – операции сложения, вычитания и умножения; $v_i \equiv V \bmod m_i$; $i = 1,..., k$.

Благодаря параллельным вычислениям в коде СОК было достигнуто сокращение временных затрат на аутентификацию КА. А это приводит, в свою очередь, к уменьшению интервала времени, который имеется у спутника-нарушителя для подбора правильного сигнала-ответа на поставленный вопрос запросчиком. В результате сокращается вероятность пропуска спутника-нарушителя системой «свой-чужой».

Дальнейшее повышение стойкости метода аутентификации возможно за счет псевдослучайной замены порождающего элемента (ПЭ), которая существует для простых оснований кода СОК. Рассмотрим реализацию метода аутентификации спутника, реализованного в модулярном коде с псевдослучайной заменой порождающих элементов.

Перед началом работы системы «свой-чужой», реализующей разработанный метод аутентификации, выбираются основания кода СОК из условия

$$P < M_k = \prod_{i=1}^{k} m_i, \quad (15)$$

где $m_1, ..., m_k$ – простые числа; P – простое число, используемое в одномодульном методе аутентификации.

Затем секретные данные $\{E, Q, G\} < M_k - 2$ метода аутентификации представляются в коде СОК

$$E = (E_1, E_2, ..., E_k), \quad (Q_1(n), ..., Q_k(n)), \quad (G_1(n), G_2(n), ..., G_k(n)), \quad (16)$$

где $E_i \equiv E \bmod m_i$; $Q_i \equiv Q \bmod m_i$; $G_i \equiv G \bmod m_i$; $i = 1,..., k$; $n = 1, 2,...$ – сеанс аутентификации.

После этого для каждого основания кода СОК $m_1, ..., m_k$ вычисляются порождающие элементы $\{s_{1d}\}, \{s_{2b}\}, ..., \{s_{kv}\}$. Данные числа заносятся в блок, реализующий псевдослучайную замену ПЭ при аутентификации спутника.

На первом этапе ответчик и запросчик выбирают одинаковые порождающие элементы. Пусть это будут числа

$$s_{1D}, s_{2B}, ..., s_{kV}.$$

На втором этапе ответчик вычисляет истинный статус спутника, представленный в коде СОК:

$$\begin{aligned}
&O: U_1(n) = (s_{1D}^{E_1} s_{1D}^{Q_1(n)} s_{1D}^{G_1(n)}) \bmod m_1,\\
&O: U_2(n) = (s_{2B}^{E_2} s_{2B}^{Q_2(n)} s_{2B}^{G_2(n)}) \bmod m_2,\\
&\vdots\\
&O: U_k(n) = (s_{kV}^{E_k} s_{kV}^{Q_k(n)} s_{kV}^{G_k(n)}) \bmod m_k,
\end{aligned} \tag{17}$$

где $E_i \equiv E \bmod m_i$; $Q_i(n) \equiv Q(n) \bmod m_i$; $G_i(n) \equiv G(n) \bmod m_i$; $i = 1,...,k$.

На третьем этапе ответчик зашумляет текущие секретные параметры

$$\begin{aligned}
&O: E_i^*(n) = (E_i + \Delta E_i(n)) \bmod \varphi(m_i),\\
&O: Q_i^*(n) = (Q_i(n) + \Delta Q_i(n)) \bmod \varphi(m_i),\\
&O: G_i^*(n) = (G_i(n) + \Delta G_i(n)) \bmod \varphi(m_i),
\end{aligned} \tag{18}$$

где $\Delta E(n), \Delta Q(n), \Delta G(n)$ – случайные числа; $\Delta E(n), \Delta Q(n), \Delta G(n) < \prod_{i=1}^{k} \varphi(m_i) - 1$;

$\Delta E_i(n) \equiv \Delta E(n) \bmod m_i$; $\Delta Q_i(n) \equiv \Delta Q(n) \bmod m_i$; $\Delta G_i(n) \equiv \Delta G(n) \bmod m_i$.

На четвертом этапе ответчик получает зашумленный статус КА, представленный в коде СОК

$$\begin{aligned}
&O: U_1^*(n) = (s_{1D}^{E_1^*(n)} s_{1D}^{Q_1^*(n)} s_{1D}^{G_1^*(n)}) \bmod m_1,\\
&O: U_2^*(n) = (s_{2B}^{E_2^*(n)} s_{2B}^{Q_2^*(n)} s_{2B}^{G_2^*(n)}) \bmod m_2,\\
&\vdots\\
&O: U_k^*(n) = (s_{kV}^{E_k^*(n)} s_{kV}^{Q_k^*(n)} s_{kV}^{G_k^*(n)}) \bmod m_k.
\end{aligned} \tag{19}$$

Процесс аутентификации спутника имеет следующие этапы.

На первом этапе запросчик генерирует вопрос. Данное число передается ответчику

$$З \to O: H = (H_1(n), H_2(n),..., H_k(n)) , \tag{20}$$

где $H(n) < \prod_{i=1}^{k} \varphi(m_i) - 1$; $H_i(n) \equiv H(n) \bmod m_i$; $i = 1,...,k$.

На втором этапе ответчик приступает к вычислению трех выражений:

$$\begin{cases}
W_1^1(n) = (E_1^*(n) - H_1 E_1) \bmod \varphi(m_1),\\
W_2^1(n) = (E_2^*(n) - H_2 E_2) \bmod \varphi(m_2),\\
\vdots\\
W_k^1(n) = (E_k^*(n) - H_k E_k) \bmod \varphi(m_k).
\end{cases} \tag{21}$$

$$\begin{cases}
W_1^2(n) = (Q_1^*(n) - H_1 Q_1(n)) \bmod \varphi(m_1),\\
W_2^2(n) = (Q_2^*(n) - H_2 Q_2(n)) \bmod \varphi(m_2),\\
\vdots\\
W_k^2(n) = (Q_k^*(n) - H_k Q_k(n)) \bmod \varphi(m_k).
\end{cases} \tag{22}$$

$$\begin{cases}
W_1^3(n) = (G_1^*(n) - H_1 G_1(n)) \bmod \varphi(m_1),\\
W_2^3(n) = (G_2^*(n) - H_2 G_2(n)) \bmod \varphi(m_2),\\
\vdots\\
W_k^3(n) = (G_k^*(n) - H_k G_k(n)) \bmod \varphi(m_k).
\end{cases} \tag{23}$$

Затем ответчик формирует сигнал для запросчика. Он имеет вид

$$O \to З: \left\{U_1(n),..., U_k(n) \parallel U_1^*(n), ..., U_k^*(n) \parallel W_1^1(n),..., W_k^1(n) \parallel W_1^2(n),..., W_k^2(n) \parallel W_1^3(n),..., W_k^3(n)\right\}.$$

На третьем этапе запросчик проверяет сигнал от ответчика

$$\begin{cases}
R_1(n) = (U_{1D}^{H_1(n)} s_{1D}^{W_1^1(n)} s_{1D}^{W_1^2(n)} s_{1D}^{W_1^3(n)}) \bmod m_1,\\
R_2(n) = (U_2^{H_2(n)} s_{2B}^{W_2^1(n)} s_{2B}^{W_2^2(n)} s_{2B}^{W_2^3(n)}) \bmod m_1,\\
\vdots\\
R_k(n) = (U_k^{H_k(n)} s_{kV}^{W_k^1(n)} s_{kV}^{W_k^2(n)} s_{kV}^{W_k^3(n)}) \bmod m_k.
\end{cases} \tag{24}$$

Спутник получит сеанс связи, если его статус будет «свой». Это возможно, только если

$$(R_1(n), R_2(n),..., R_k(n)) = (U_1^*(n), U_2^*(n),..., U_k^*(n)) . \tag{25}$$

Применение псевдослучайной замены порождающих элементов оснований кода СОК приводит к снижению вероятности подбора правильного ответа спутником-нарушителем из-за необходимости определения текущего кортежа ПЭ. В этом случае вероятность определения текущего кортежа ПЭ определяется

$$P_{\text{ПКПЭ}} = \left(\prod_{i=1}^{k} L_i \right)^{-1}, \tag{26}$$

где L_i – количество порождающих элементов для основания m_i кода СОК; $i = 1, 2, ..., k$.

Результаты исследования и их обсуждение. Рассмотрим пример реализации разработанного метода аутентификации спутника, реализованного в модулярном коде с псевдослучайной заменой порождающих элементов.

Пусть выбраны основания кода СОК $m_1 = 19, m_2 = 29, m_3 = 37$. Для модуля $m_1 = 19$ порождающими элементами являются $\{2,3,10,13,14,15\}$. Для модуля $m_2 = 29$ порождающими элементами являются числа $\{2,3,8,10,11,14,15,18,19,21,26,27\}$. Для модуля $m_3 = 37$ имеем числа $\{2,5,13,15,17,18,19,20,22,24,32,35\}$. Согласно равенству (12) имеем $M_3 = \prod_{i=1}^{3} m_i = 20387$. Пусть секретный ключ равен $E = 2345 = (8, 25, 14)$, а числа $Q(1) = 1234 = (18, 16, 13)$ и $G(1) = 2003 = (8, 2, 5)$.

На первом этапе ответчик и запросчик выбирают одинаковые порождающие элементы. Пусть это будут числа $\{s_1 = 3, s_2 = 8, s_3 = 19\}$.

На втором этапе ответчик вычисляет истинный статус спутника, представленный в коде СОК

$$U_1(1) = \left| 3^8 \cdot 3^{18} \cdot 3^8 \right|_{19}^{+} = \left| 3^{16} \right|_{19}^{+} = 17,$$
$$U_2(1) = \left| 8^{25} \cdot 8^{16} \cdot 8^2 \right|_{29}^{+} = \left| 8^{15} \right|_{29}^{+} = 19,$$
$$U_3(1) = \left| 19^{14} \cdot 19^{13} \cdot 19^5 \right|_{37}^{+} = \left| 19^{32} \right|_{37}^{+} = 16.$$

Получили значение истинного статуса спутника равное $U(1) = (17,19,16)$.

На третьем этапе ответчик зашумляет текущие секретные параметры. Пусть имеем числа
$\Delta E(1) = 191 = (1, 17, 6)$, $\Delta Q(1) = 237 = (9, 5, 15)$, $\Delta G(1) = 167 = (15, 22, 19)$.

Тогда зашумленные значения в коде СОК имеют вид

$$E^*(1) = (|8+1|_{18}^{+}, |25+17|_{28}^{+}, |14+6|_{36}^{+}) = (9, 14, 20),$$
$$Q^*(1) = (|18+9|_{18}^{+}, |16+5|_{28}^{+}, |13+18|_{36}^{+}) = (9, 21, 28),$$
$$G^*(1) = (|8+15|_{18}^{+}, |2+22|_{28}^{+}, |5+19|_{36}^{+}) = (5, 24, 24).$$

На четвертом этапе ответчик получил следующие результаты:

$$U_1^*(1) = \left| 3^9 \cdot 3^9 \cdot 3^5 \right|_{19}^{+} = \left| 3^5 \right|_{19}^{+} = 15,$$
$$U_2^*(1) = \left| 8^{14} \cdot 8^{21} \cdot 8^{24} \right|_{29}^{+} = \left| 8^3 \right|_{29}^{+} = 19,$$
$$U_3^*(1) = \left| 19^{20} \cdot 19^{28} \cdot 19^{24} \right|_{37}^{+} = \left| 19^0 \right|_{37}^{+} = 1.$$

В коде СОК зашумленный статус задается комбинацией $U^*(1) = (15,19,1)$.

Процесс аутентификации спутника на первом сеансе.

На первом этапе запросчик выбрал число, которое затем представил в коде СОК $H(1) = 134 = (1, 18, 23)$. Полученный вопрос поступает на вход приемника ответчика.

На втором этапе ответчик вычисляет три ответа. Вычислим первый ответ:

$$\begin{cases} W_1^1(1) = \left|E_1^*(1) - H_1(1)E_1(1)\right|_{\varphi(m_1)}^+ = \left|9 - 1\cdot 8\right|_{18}^+ = 1, \\ W_2^1(1) = \left|E_2^*(1) - H_2(1)E_2(1)\right|_{\varphi(m_2)}^+ = \left|14 - 18\cdot 25\right|_{28}^+ = 12, \\ W_3^1(1) = \left|E_3^*(1) - H_3(1)E_3(1)\right|_{\varphi(m_3)}^+ = \left|20 - 23\cdot 14\right|_{36}^+ = \left|-14\right|_{36}^+ = 36 - 14 = 22. \end{cases}$$

В коде СОК первый ответ имеет вид $W^1(1) = (1, 12, 22)$.

Вычислим второй ответ:

$$\begin{cases} W_1^2(1) = \left|Q_1^*(1) - H_1(1)Q_1(1)\right|_{\varphi(m_1)}^+ = \left|9 - 1\cdot 18\right|_{18}^+ = 9, \\ W_2^2(1) = \left|Q_2^*(1) - H_2(1)Q_2(1)\right|_{\varphi(m_2)}^+ = \left|21 - 18\cdot 16\right|_{28}^+ = \left|-15\right|_{28}^+ = 28 - 15 = 13, \\ W_3^1(1) = \left|Q_3^*(1) - H_3(1)Q_3(1)\right|_{\varphi(m_3)}^+ = \left|28 - 23\cdot 13\right|_{36}^+ = \left|-12\right|_{36}^+ = 36 - 12 = 16. \end{cases}$$

В коде СОК второй ответ имеет вид $W^2(1) = (9, 13, 16)$.

Вычислим третий ответ:

$$\begin{cases} W_1^3(1) = \left|G_1^*(1) - H_1(1)G_1(1)\right|_{\varphi(m_1)}^+ = \left|5 - 1\cdot 8\right|_{18}^+ = 15, \\ W_2^3(1) = \left|G_2^*(1) - H_2(1)G_2(1)\right|_{\varphi(m_2)}^+ = \left|24 - 18\cdot 2\right|_{28}^+ = 16, \\ W_3^3(1) = \left|G_3^*(1) - H_3(1)G_3(1)\right|_{\varphi(m_3)}^+ = \left|24 - 23\cdot 5\right|_{36}^+ = 17. \end{cases}$$

В коде СОК третий ответ имеет вид $W^3(1) = (15, 16, 17)$.

Затем ответчик формирует сигнал для запросчика. Он имеет вид

$$\left\{U_1(1), U_2(1), U_3(1) \,\|\, U_1^*(1), U_2^*(1), U_3^*(1) \,\|\, W_1^1(1), W_2^1(1), W_3^1(1) \,\|\, W_1^2(1), W_2^2(1), W_3^2(1) \,\|\, W_1^3(1), W_2^3(1), W_3^3(1)\right\} =$$
$$= \left\{(17,19,16) \,\|\, (15,9,1) \,\|\, (1,12,22) \,\|\, (9,13,16) \,\|\, (15,16,17)\right\}.$$

Запросчик проверяет сигнал ответчика. При этом он применяет порождающие элементы

$$\left\{s_1 = 3, s_2 = 8, s_3 = 19\right\}.$$

Тогда

$$R_1(1) = \left|U_1^{H_1(1)} s_1^{W_1^1(1)} s_1^{W_1^2(1)} s_1^{W_1^3(1)}\right|_{m_1}^+ = \left|17^1 \cdot 3^1 \cdot 3^9 \cdot 3^{15}\right|_{19}^+ = 15,$$

$$R_2(1) = \left|U_2^{H_2(1)} s_2^{W_2^1(1)} s_2^{W_2^2(1)} s_2^{W_2^3(1)}\right|_{m_2}^+ = \left|19^{18} \cdot 8^{12} \cdot 8^{13} \cdot 8^{16}\right|_{29}^+ = 19,$$

$$R_3(1) = \left|U_3^{H_3(1)} s_3^{W_3^1(1)} s_3^{W_3^2(1)} s_3^{W_3^3(1)}\right|_{m_3}^+ = \left|16^{23} \cdot 19^{22} \cdot 19^{17} \cdot 19^{17}\right|_{37}^+ = 1.$$

Запросчик генерирует сигнал «свой» и спутник организует сеанс связи, так как

$$(R_1(1), R_2(1), R_3(1)) = (U_1^*(1), U_2^*(1), U_3^*(1)) = (15, 19, 1).$$

Рассмотрим второй раунд аутентификации этого же спутника. Пусть секретный ключ равен $E = 2345 = (8, 25, 14)$, а числа $Q(2) = 1001 = (13, 15, 2)$ и $G(2) = 3012 = (10, 25, 15)$.

На первом этапе ответчик и запросчик выбирают одинаковые порождающие элементы. Пусть это будут числа $\left\{s_1 = 13, s_2 = 11, s_3 = 17\right\}$.

На втором этапе ответчик вычисляет истинный статус спутника, представленный в коде СОК

$$U_1(2) = \left|13^8 \cdot 13^{13} \cdot 13^{10}\right|_{19}^+ = \left|13^{13}\right|_{19}^+ = 15,$$

$$U_2(2) = \left|11^{25} \cdot 11^{15} \cdot 11^{25}\right|_{29}^+ = \left|11^{11}\right|_{29}^+ = 2,$$

$$U_3(2) = \left|17^{14} \cdot 17^2 \cdot 17^{15}\right|_{37}^+ = \left|17^{31}\right|_{37}^+ = 2.$$

Получили значение истинного статуса спутника, равное $U(2) = (15, 2, 2)$.

На третьем этапе ответчик зашумляет текущие секретные параметры. Пусть имеем числа, представленные в коде СОК

$$\Delta E(2) = 356 = (14, 8, 23),\ \Delta Q(2) = 457 = (1, 22\ 13),\ \Delta G(2) = 289 = (4, 28, 30).$$

Тогда зашумленные значения в коде СОК имеют вид

$$E^*(2) = (|8+14|_{18}^+, |25+8|_{28}^+, |14+23|_{36}^+) = (4, 5, 1),$$

$$Q^*(2) = (|13+1|_{18}^+, |15+22|_{28}^+, |2+13|_{36}^+) = (14, 9, 15),$$

$$G^*(2) = (|10+4|_{18}^+, |25+28|_{28}^+, |15+30|_{36}^+) = (14, 25, 9).$$

На четвертом этапе ответчик получил следующие результаты

$$U_1^*(2) = \left|13^4 \cdot 13^{14} \cdot 13^{14}\right|_{19}^+ = \left|13^{14}\right|_{19}^+ = 5,$$

$$U_2^*(2) = \left|11^5 \cdot 11^9 \cdot 11^{25}\right|_{29}^+ = \left|11^{11}\right|_{29}^+ = 10,$$

$$U_3^*(2) = \left|17^1 \cdot 17^{15} \cdot 17^9\right|_{37}^+ = \left|19^{25}\right|_{37}^+ = 22.$$

В коде СОК зашумленный статус задается комбинацией $U^*(2) = (55, 10, 22)$.

Процесс аутентификации спутника на втором сеансе.

На первом этапе запросчик выбрал число, которое затем представил в коде СОК $H(2) = 1000 = (12, 14, 1)$. Полученный вопрос поступает на вход приемника ответчика.

На втором этапе ответчик вычисляет три ответа. Вычислим первый ответ:

$E = 2345 = (8, 25, 14)$, а числа $Q(2) = 1001 = (13, 15, 2)$ и $G(2) = 3012 = (10, 25, 15)$

$$\begin{cases} W_1^1(2) = \left|E_1^*(2) - H_1(2)E_1(2)\right|_{\varphi(m_1)}^+ = |4 - 12 \cdot 8|_{18}^+ = 16, \\ W_2^1(2) = \left|E_2^*(2) - H_2(2)E_2(2)\right|_{\varphi(m_2)}^+ = |5 - 14 \cdot 25|_{28}^+ = 19, \\ W_3^1(2) = \left|E_3^*(2) - H_3(2)E_3(2)\right|_{\varphi(m_3)}^+ = |1 - 1 \cdot 14|_{36}^+ = 23. \end{cases}$$

В коде СОК первый ответ имеет вид $W^1(1) = (1, 12, 22)$.

Вычислим второй ответ:

$$\begin{cases} W_1^2(2) = \left|Q_1^*(2) - H_1(2)Q_1(2)\right|_{\varphi(m_1)}^+ = |14 - 12 \cdot 13|_{18}^+ = 2, \\ W_2^2(2) = \left|Q_2^*(2) - H_2(2)Q_2(2)\right|_{\varphi(m_2)}^+ = |5 - 14 \cdot 15|_{28}^+ = 23, \\ W_3^1(2) = \left|Q_3^*(2) - H_3(2)Q_3(2)\right|_{\varphi(m_3)}^+ = |15 - 1 \cdot 2|_{36}^+ = 13. \end{cases}$$

В коде СОК второй ответ имеет вид $W^2(2) = (2, 23, 13)$.

Вычислим третий ответ:

$$\begin{cases} W_1^3(2) = \left|G_1^*(2) - H_1(2)G_1(2)\right|_{\varphi(m_1)}^+ = |14 - 12 \cdot 10|_{18}^+ = 2, \\ W_2^3(2) = \left|G_2^*(2) - H_2(2)G_2(2)\right|_{\varphi(m_2)}^+ = |25 - 14 \cdot 25|_{28}^+ = 11, \\ W_3^3(2) = \left|G_3^*(2) - H_3(2)G_3(2)\right|_{\varphi(m_3)}^+ = |9 - 1 \cdot 15|_{36}^+ = 30. \end{cases}$$

В коде СОК третий ответ имеет вид $W^3(2) = (2, 11, 30)$.

Затем ответчик формирует сигнал для запросчика. Он имеет вид

$$O \to 3 : \{(15, 2, 2) \parallel (5, 10, 22) \parallel (16, 19, 23) \parallel (2, 33, 12) \parallel (2, 11, 30)\}.$$

Запросчик проверяет сигнал ответчика. При этом он применяет порождающие элементы $\{s_1 = 13, s_2 = 11, s_3 = 17\}$. Тогда

$$R_1(2) = \left| U_1^{H_1(2)} s_1^{W_1^1(2)} s_1^{W_1^2(2)} s_1^{W_1^3(2)} \right|_{m_1}^{+} = \left| 15^{12} \cdot 13^{16} \cdot 13^{2} \cdot 13^{2} \right|_{19}^{+} = 5,$$

$$R_2(2) = \left| U_2^{H_2(2)} s_2^{W_2^1(2)} s_2^{W_2^2(2)} s_2^{W_2^3(2)} \right|_{m_2}^{+} = \left| 2^{14} \cdot 11^{19} \cdot 11^{23} \cdot 11^{11} \right|_{29}^{+} = 10,$$

$$R_3(2) = \left| U_3^{H_3(2)} s_3^{W_3^1(2)} s_3^{W_3^2(2)} s_3^{W_3^3(2)} \right|_{m_3}^{+} = \left| 2^{1} \cdot 17^{23} \cdot 17^{13} \cdot 17^{30} \right|_{37}^{+} = 22.$$

Запросчик генерирует сигнал «свой» и спутник организует сеанс связи, так как

$$(R_1(2), R_2(2), R_3(2)) = (U_1^*(2), U_2^*(2), U_3^*(2)) = (15\ 10, 22)\ .$$

Рассмотрим вопросы повышения имитостойкости НССС за счет использования разработанного метода аутентификации спутника, реализованного в модулярном коде с псевдослучайной заменой порождающих элементов. Для рассмотренного примера найдем вероятность определения кортежа ПЭ, используя выражение (26). Получаем, что

$$P_{\text{ПКПЭ}} = (864)^{-1} = 1{,}16 \cdot 10^{-3}\ .$$

Таким образом, разработанный метод аутентификации спутника, реализованный в модулярном коде с псевдослучайной заменой порождающих элементов снижает вероятность подбора сигнала ответчика спутником-нарушителем в 864 раза по сравнению с протоколом аутентификации, использующим код СОК с одним ПЭ для всех оснований. Следовательно, имитостойкость НССС повысилась в 864 раза.

Заключение. В статье рассмотрены вопросы повышения имитостойкости НССС от спуфинг-помеха за счет использования системы «свой-чужой» для опознавания КА. Рассмотрен одномодульный метод аутентификации с нулевым разглашением знаний, обеспечивающий высокую имитостойкость НССС без использования шифрования. Показано, что сократить время аутентификации КА возможно за счет использования кода СОК. Так как операции сложения, вычитания и умножения выполняются параллельно основаниям СОК, то это обеспечивает минимальные временные затраты на определение статуса КА, что приводит к снижению вероятности подбора правильного сигнала ответчика спутником-нарушителем. Для дальнейшего повышения имитостойкости НССС предложено в методе аутентификации, реализованном в СОК, использовать псевдослучайную замену порождающих элементов оснований кода. Представлен пример выполнения разработанного метода аутентификации спутника, реализованного в модулярном коде с псевдослучайной заменой порождающих элементов. Проведенные исследования показали, что при использовании трех оснований $m_1 = 19, m_2 = 29, m_3 = 37$ имитостойкость НССС повысилась в 864 раза по сравнению с протоколом аутентификации, использующим код СОК с одним ПЭ для всех оснований. Цель работы достигнута.

Библиографический список

1. Воробьев, А. В. Цифровизация нефтяной промышленности: «интеллектуальный» нефтепромысел / А. В. Воробьев, Х. Тчаро, К. А. Воробьев // Вестник Евразийской науки. – 2018. – Т. 10, № 3. – Режим доступа: https://esj.today/PDF/77NZVN318.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.07.2022).

2. Кукк, К. И. Спутниковая связь: прошлое, настоящее, будущее / К. И. Кукк. – Москва : Горячая линия – Телеком, 2019. – 286 с.

3. Анпилогов, В. А. Эффективность низкоорбитальных систем спутниковой связи на основе малых космических аппаратов / В. А. Анпилогов // Технологии и средства связи. – 2015. – № 4. – С. 62–67.

4. Анпилогов, В. А. Проблемы реализации LEO-HTS / В. А. Анпилогов // Технологии и средства связи. Специальный выпуск «Спутниковая связь и вещание-2017». – 2016. – № 6–2. – С. 30–38.

5. Kalmykov, I. A. Application of Information Security Technologies for Improving the Imitation Resistance of Low-Orbital Satellite Communication Systems / I. A. Kalmykov, M. A. Lapina, M. I. Kalmykov // Informatics and Cybernetics in Intelligent Systems : Proceedings of 10th Computer Science On-line Conference 2021. – 2021. – Vol. 3. – P. 54–63.

6. Pashintsev, V. P. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication / V. P. Pashintsev, R. N. Rezenkov, P. A. Zhuk // International Journal of Mechanical Engineering and Technology (IJMET). – 2018. – Vol. 9, issue 5, May. – P. 958–965.

7. Pashintsev, V. P. Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System / V. P. Pashintsev, A. P. Zhuk, A. A. Olenev // International Journal of Engineering and Advanced Technology. – 2019. – № 8 (5). – P. 2557–2562.

8. Chistousov, N. K. Development of Algorithms for Increasing the Information Secrecy of the Satellite Communication System Based on the Use of Authentication Technology / N. K. Chistousov, A. A. Olenev, N. A. Kalmykova // Advanced in Information Security Management and Applications 2021. – 2021. – Vol. 3094. – P. 59–64.

9. Omondi, A. Residue Number Systems: Theory and Implementation / A. Omondi. – Imperial College Press, UK, 2007. – 293 p.

10. Ananda, Mohan. Residue Number Systems. Theory and Applications / Ananda Mohan. – Springer International Publishing, Switzerland, 2016. – 351 p.

References

1. Vorobyov, A. V., Tcharo, Kh., Vorobyov, K. A. Tsifrovizatsiya neftyanoy promyshlennosti: «intellektualnyy» neftepromysel [Digitalization of the oil industry: "intellectual" oil field]. *Vestnik Evraziyskoy nauki* [Bulletin of Eurasian Science], 2018, vol. 10, no. 3. Available at: https://esj.today/PDF/77NZVN318 (accessed 20.07.2022).

2. Kukk, K. I. *Sputnikovaya svyaz: proshloye, nastoyashcheye, budushcheye* [Satellite communications: past, present, future]. Moscow, Goryachaya liniya – Telekom Publ., 2019. 286 p.

3. Anpilogov, V. A. Effektivnost nizkoorbitalnykh sistem sputnikovoy svyazi na osnove malykh kosmicheskikh apparatov [Efficiency of low-orbit satellite communication systems based on small spacecraft]. *Tekhnologii i sredstva svyazi* [Technologies and means of communication], 2015, no. 4, pp. 62–67.

4. Anpilogov, V. A. Problemy realizatsii LEO-HTS [Problems of implementation of LEO-HTS]. *Tekhnologii i sredstva svyazi. Spetsialnyy vypusk "Sputnikovaya svyaz i veshchaniye-2017* [Technologies and means of communication. Special issue "Satellite communications and broadcasting-2017"], 2016, no. 6–2, pp. 30–38.

5. Kalmykov, I. A., Lapina, M. A., Kalmykov, M. I. Application of Information Security Technologies for Improving the Imitation Resistance of Low-Orbital Satellite Communication Systems. *Informatics and Cybernetics in Intelligent Systems. Proceedings of 10th Computer Science On-line Conference*, 2021, vol. 3, pp. 54–63.

6. Pashintsev, V. P., Rezenkov, R. N., Zhuk, P. A. Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication. *International Journal of Mechanical Engineering and Technology (IJMET)*, 2018, vol. 9, issue 5, May, pp. 958–965.

7. Pashintsev, V. P., Zhuk A. P., Olenev A. A. Development of Satellite Authentication System for Low Earth Orbit Satellite Communication System on the Basis of Polynomial Residue Number System. *International Journal of Engineering and Advanced Technology*, 2019, no. 8 (5), pp. 2557–2562.

8. Chistousov, N. K., Olenev A. A., Kalmykova N. A. Development of Algorithms for Increasing the Information Secrecy of the Satellite Communication System Based on the Use of Authentication Technology. *Advanced in Information Security Management and Applications*, 2021, vol. 3094, pp. 59–64.

9. Omondi, A. *Residue Number Systems: Theory and Implementation.* Imperial College Press, UK, 2007. 293 p.

10. Ananda, Mohan. *Residue Number Systems. Theory and Applications.* Springer International Publishing Switzerland, 2016. 351 p.

УДК 004.001

РАЗРАБОТКА МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА ОСНОВЕ КОРРЕЛЯЦИОННОГО АНАЛИЗА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ

Статья поступила в редакцию 15.04.2022, в окончательном варианте – 29.08.2022.

Шишков Сергей Анатольевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
магистрант, ORCID: 0000-0001-5681-3850, e-mail: serge_gk4@mail.ru
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0003-0414-6034, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Немчинова Валерия Олеговна, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
ассистент, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

По мере развития информационных технологий обработка информации стала основной проблемой обеспечения защиты, так как число источников, из которых поступают актуальные данные по текущему состоянию защищенности, непрерывно увеличивается. Решением проблемы является использование систем SIEM. SIEM объединяет в себе классы управления информацией по безопасности и управления событиями безопасности. Решения управления информацией по безопасности обеспечивают долгосрочное хранение и анализ данных различных объектов инфраструктуры организации. Системы управления событиями безопасности реализуют мониторинг событий безопасности в реальном времени. Совмещая эти решения в SIEM-системах, специалисты по информационной безопасности могут выявить кибератаки и нарушения политик безопасности на ранних стадиях и минимизировать ущерб от них. Также решения SIEM помогают оценить защищенность информационных систем и актуальные для предприятия риски. В статье представлен анализ существующих решений информационной безопасности в области SIEM-систем. Описаны источники события для систем корреляции, указаны решаемые задачи SIEM, разобрана логика и структура SIEM. Произведен обзор популярных методов корреляции, описано применение данной системы как инструмента в области информационной безопасности. В статье представлена процедура разработки правила корреляции на примере системы MaxPatrol SIEM.

Ключевые слова: SIEM-система, событие ИБ, инцидент ИБ, информационная безопасность, угроза ИБ, уязвимость

DEVELOPMENT OF METHODS FOR DETECTING MALICIOUS IMPACT BASED ON CORRELATION ANALYSIS OF INFORMATION SECURITY EVENTS IN SIEM SYSTEMS

The article was received by the editorial board on 15.04.2022, in the final version – 29.08.2022.

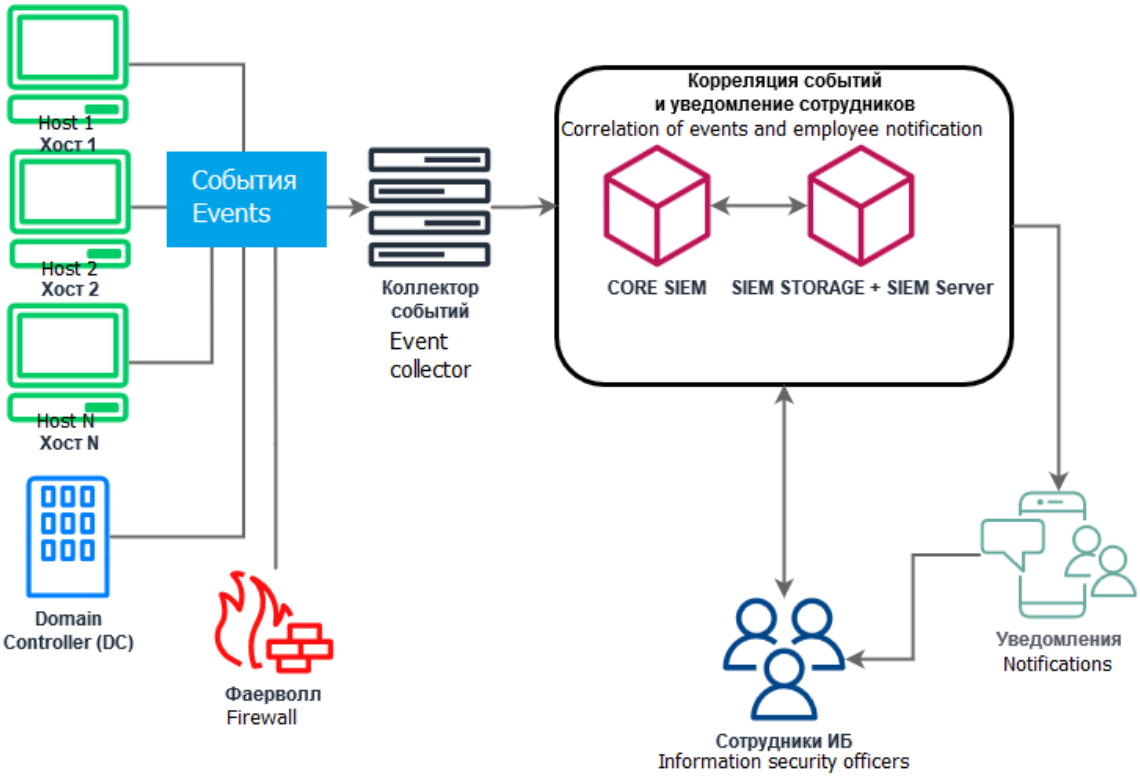
Shishkov Sergey A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0001-7101-6251, e-mail: michael.evsyukov@gmail.com
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru
Nemchinova Valeriya O., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Assistant, ORCID: 0000-0002-4428-7128, e-mail: nemchinova.valeriya@yandex.ru

During the development of information technologies information processing has become the main problem of ensuring protection, since the number of sources from which up-to-date data on the current state of security is continuously increasing. Using SIEM systems can solve the problem. SIEM combines the SEM (Security Event

Management, "Security event management") and SIM (Security Information Management, "security information management") classes. SEM solutions implement real-time monitoring of security events. SIM systems provide long-term data storage and analysis of various infrastructure objects of the organization. SIEM solutions perform both of these tasks. With the help of SIEM, information security specialists can identify cyber attacks and violations of security policies at an early stage and minimize damage from them. SIEM solutions also help to assess the security of information systems and risks relevant to the enterprise. The article presents an analysis of existing information security solutions in the field of SIEM systems. Event sources for correlation systems are described, the SIEM tasks to be solved are indicated, the logic and structure of SIEM are analyzed. The review of popular correlation methods is made, the application of this system as a tool on information security is described. The article presents the procedure for developing a correlation rule using for example the MaxPatrol SIEM system.

Keywords: SIEM system, IS event, IS incident, information security, IS vulnerability, IS threat

Graphical annotation (Графическая аннотация)



Введение. На сегодняшний день существование отделов информационной безопасности в условиях крупных предприятий, а также организаций с высокими требованиями к безопасности хранения, доступности и использования информации является необходимостью. Каждая система защиты информации неумолимо развивается и адаптируется к новым методам и стратегиям кибератак. Количество средств обнаружения атак постоянно увеличивается, соответственно, при использовании нескольких СОВ увеличивается количество инцидентов, а также время для своевременного реагирования на них. Решением подобной проблемы является использование систем управления инцидентами информационной безопасности (SIEM-систем).

Утрата данных может рассматриваться как одна из основных угроз ИТ-безопасности. Преднамеренные действия персонала или злоумышленников, неисправность аппаратных средств могут послужить причиной нарушения целостности информации [15].

Во избежание реализации таких угроз создаются центры информационной безопасности, контролирующие работу средств защиты информации и проверяющие защищаемые автоматизированные системы [13, 14]. Степень защищенности информации и автоматизированных систем можно повысить использованием центров информационной безопасности [12].

Известно, что цифровая трансформация оказывает значительное влияние на технологии: от принятия решений на основе данных до внедрения облачных технологий, мобильности и взрывного развития Интернета вещей (IoT), при этом сам процесс ЦТ выходит за рамки простого развертывания новых решений в области ИКТ-технологий. В ходе ЦТ организации должны пересмотреть сложившиеся бизнес-модели и процессы для стимулирования инноваций и улучшения результатов

своей деятельности. Именно совместное применение цифровых технологий и информационных процессов дает поводы для переосмысления моделей бизнеса, а это – нелегкая задача [9].

Теория SIEM. Для решения задач оперативного мониторинга и реагирования на инциденты безопасности существует определённый класс программного обеспечения – SIEM-системы (Security Information and Event Management) [6]. Система управления инцидентами ИБ не способна к самостоятельному реагированию и предотвращению атак, её задача состоит в удобном и своевременном представлении информации из множества источников данных. Вследствие того, что в некоторых случаях промежуток времени между обнаружением и реакцией на инцидент ИБ должен быть как можно меньше, необходимо как можно больше автоматизировать процесс реагирования на инциденты [8]. Источниками данных могут служить другие информационные системы, такие как: операционные системы, бухгалтерские системы, справочные, сетевые системы, системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS), файерволлы веб-приложений (WAF), средства защиты информации от несанкционированного доступа, антивирусные средства, почтовые службы, базы данных, системы мониторинга. Кроме представления уже обработанных инцидентов из систем ИБ, SIEM-система позволяет производить множество операций с необработанными (сырыми) данными (например, Windows Event Log). Такими операциями являются нормализация, корреляция, агрегация, обогащение событий. Такая система поддерживает тонкую настройку генерирования инцидентов по предопределенным критериям, а также отправку уведомлений пользователям (например, при превышении определенного значения загрузки ЦП на определенном узле). SIEM-системы позволяют самостоятельно писать правила обработки данных из источников (нормализации), правила обогащения и корреляции.

Источники данных схематично изображены на рисунке 1.

Рисунок 1 – Источники данных SIEM

Структура SIEM состоит из следующих звеньев:

- сервер базы данных для хранения событий и работы с ними;
- агент, осуществляющий сбор данных с настроенных коллекторов;
- сервер-коллектор событий, осуществляющий сбор событий из источников (например, доменный сервер, забирающий логи с доменном АРМ);
- коррелятор, принимающий данные для последующей их обработки по правилам нормализации, корреляции и обогащения.

Задача SIEM-системы – получить данные от источников. Источник данных может быть «активным», который самостоятельно может передавать данные по указанному пути приемника, а также и «пассивным», к которому SIEM-система обращается сама [10].

Реализация механизмов корреляции и прогнозирования в SIEM-системах. Выделяется 2 вида методов корреляции:

- сигнатурные;
- бессигнатурные.

Сигнатурные методы позволяют администратору определять правила идентификации инцидентов, настраивать их конфигурации, определять исключения, вносить правки. Бессигнатурные методы менее гибкие в настройке, а все параметры в них заложены в этапе разработки системы. Управление настройками идентификации угроз при использовании бессигнатурных методов практически невозможно.

Методы корреляций событий в SIEM-системах:

- Statistical – бессигнатурный метод корреляции событий. Основан на измерении двух или более переменных и вычислении степени статистической связи между ними;
- RBR – метод, в котором взаимосвязи между событиями определяются правилами в заранее заданных специфических правилах;
- CBR – корреляция производится по подходящим векторам из предварительно заданной матрицы событий;
- MBR – метод, основанный на абстракции объектов и наблюдения за ними в рамках модели;
- Graph based. Корреляция заключается в поиске зависимостей между системными компонентами в графическом представлении (network devices, hosts, services) и построении графа на их основе. Если зависимость обнаруживается, граф используется для поиска основной причины возникновения проблемы;
- Neural network based – нейронная сеть, обучаемая для обнаружения аномалий в потоке событий [16].

В простейшем варианте в SIEM-системе корреляция работает в режиме RBR (Rule Based Reasoning). Они содержат в себе предопределенные условия, триггеры, счетчики и другие механизмы. Примером может служить механизм правила о создании и быстром удалении задания в ОС Windows – в таком случае при наступлении событии А (создание задания) запускается таймер, и если в момент работы таймера происходит событие Б (удаление задания), то срабатывает правило корреляции и генерируется инцидент ИБ. SIEM-система способна выявлять факты сетевых атак, эпидемиологических заражений вредоносным ПО, попытки несанкционированного доступа к конфиденциальной информации. Кроме этого, используя дополнительные инструменты, представляется возможным определять ошибки в работе информационных систем, определять уровень уязвимости того или иного ресурса [17].

Разработчики SIEM-систем в основном применяют сигнатурные методы, поскольку они гораздо более гибкие, имеют большую эффективность при обнаружении угроз [11].

SIEM как инструмент работы в ИБ. SIEM является мощным инструментом информационной безопасности, но может работать только вкупе с другими инструментами ИБ. Система позволяет добиться автоматического выявления угроз, позволяет обрабатывать события и работать с инцидентами, дает возможность своевременно обнаруживать аномалии и риски, может обеспечивать непрерывность работы информационных систем путем правильной настройки механизма корреляций. В совокупности позволяет существенно сократить риски ИБ, а значит, финансовые, репутационные и иные потери [17].

Внедрение SIEM-системы представляется сложным и дорогим механизмом, требующим должного внимания в длительной настройке, а для использования такой системы требуется высоко квалифицированный персонал, который позволит контролировать бесперебойный сбор событий, управлять правилами корреляций, своевременно их обновлять как с изменениями структуры организации, так и с выходом обновлений. Установка SIEM в формате «как есть» со встроенными разработчиками правил из коробки не даст должного результата, что приведет к нерациональной трате финансовых средств. В то же время успешное внедрение и правильная настройка решает множество задач, такие как:

- осуществление корреляций и оценка событий ИБ;
- проведение анализа структуры организации;
- реализация автоматизации процессов обнаружения угроз и аномалий;
- проведение аудита политик и стандартов соответствия [17], возможность выпуска отчетов;
- проведение правильного реагирования благодаря наличию инструментов и доказательной базы;
- возможность расследования давно произошедших инцидентов.

В России представлены большинство представителей рынка SIEM-систем, многие из которых имеют сертификаты ФСТЭК России. Потенциальным потребителям представляется обширная возможность определения нужной системы с необходимым ему набором функций.

Maxpatrol SIEM позволяет гибко фильтровать, группировать и настраивать выборки событий. А также позволяет строить диаграммы и чарты на основе поступающих событий.

Выборка может использоваться для изменения представления большого количества данных, а фильтр может использоваться для просмотра на основе критериев выбора[7]. На рисунке 2 показана столбчатая диаграмма, отражающая рейтинг хостов, с которых происходил брутфорс.

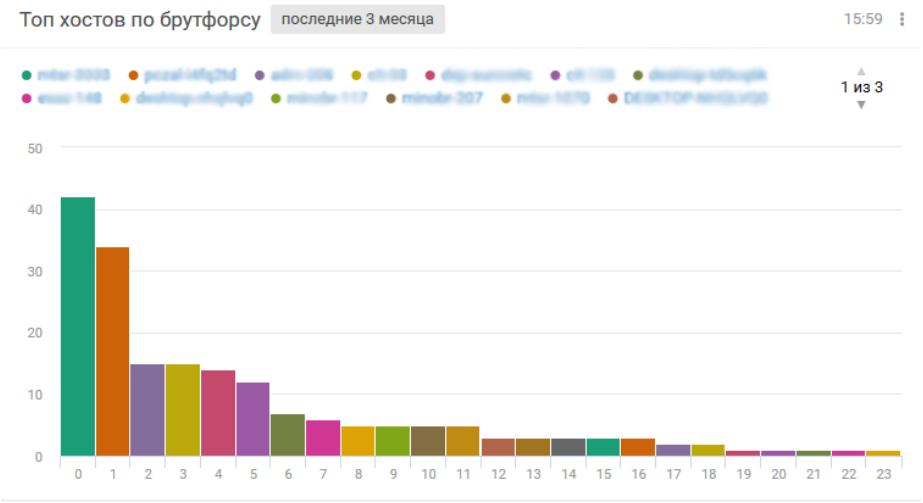


Рисунок 2 – Диаграмма рейтинга хостов по критерию выбора брутфорс

Разработка правила корреляции MaxPatrol SIEM. Для написания правил корреляции можно воспользоваться PTSIEM SDK GUI – набором средств разработки для PT SIEM.

Задача, решаемая правилом корреляции, состоит в следующем:

Существует организация, обслуживающая несколько других организаций в области ИБ. Все обслуживаемые организации имеют собственный домен Active Directory в лесу главного домена, управляемого системой Windows Server. В каждом домене есть свой доменный контроллер. При создании нового доменного пользователя внутри поддомена пользователь создается на хосте доменного контроллера. SIEM получает логи с доменных АРМ и обрабатывает их события. В доменах существуют группы пользователей с административными правами. Необходимо написать правило корреляции, которое будет анализировать следующие события и генерировать инциденты:

- создание нового пользователя и добавление в группу с администраторскими привилегиями;
- добавление любого пользователя в группу с администраторскими привилегиями;
- изменение паролей пользователя, состоящего в группе с администраторскими привилегиями.

Для решения такой задачи необходимо:

- иметь список узлов контроллеров домена;
- иметь список администраторских групп внутри доменов;
- реализовать решение задачи в контексте SIEM-системы.

В написании правил корреляции в выбранной системе используется язык PDQL (Positive Data Query Language). Для начала необходимо создать табличные списки для доменных контроллеров и списков пользователей и заполнить их. Список доменных контроллеров будет динамическим (будет автоматически формироваться при запросе из правила корреляции к нему). Создание динамического списка состоит из 2 шагов:

1. Выборка активов с ролью доменного контроллера. Запрос на языке PDQL – «Host.HostRoles.Role = 'Domain Controller'».

2. Создание табличного списка с запросом – «select(@Host as host_name)».

Теперь приступаем к написанию правила корреляции. При создании пользователя в журнале EventLog Windows генерируется событие с идентификатором 4720, при изменении пароля 4723 или 4724, а при добавлении в группу – 4728. Для удобства будет создано 2 правила – в первом правиле будем отслеживать 2 события:

- создание пользователя и добавление его в группу администраторов в течение 20 минут;
- добавление любого пользователя в группу администраторов.

Таким образом, нам надо фильтровать события с идентификаторами 4720 и 4728.

Во втором правиле отслеживается одно событие – изменение пароля пользователя, состоящего в группе администраторов, то есть событие с идентификатором 4724.

Для проверки написанных правил будем использовать специально созданные тестовые учетные записи. В начале заполняем табличный список в MaxPatrol SIEM, содержащий группы с правами администратора домена – добавляем запись в колонку group «testadmins». Далее создаем группу «testadmins» и доменного пользователя с именем «testsiem» и добавляем его в группу.

Правило корреляции добавления пользователя в группу с правами администратора изображено на рисунке 3.

Правило корреляции CIT_incident_create_user_important

```
query Check_Important_host($host_name) from Domain_Controllers {(host_name == $host_name)}
query Check_Admin_Groups($group) from CIT_Admin_Groups {(group==$group)}

    event Create_User_4720:
    key:
        event_src.host
    filter{
        msgid == "4720"
        and exec_query ("Check_Important_host", [lower(event_src.host)])
    }
    event Add_User_To_Admins:
    key:
        event_src.host
    filter{

        msgid =="4728"
        and exec_query("Check_Admin_Groups",[lower(object.name)])
        }
    rule CIT_incident_create_user_important: ((Create_User_4720 -> Add_User_To_Admins) within 20m) or Add_User_To_Admins
        on Create User 4720 {
```

Рисунок 3 – Правило корреляции при добавлении пользователя в группу с правами администратора

Результат корреляции представлен на рисунке 4. Из карточки инцидента мы видим, что инцидент состоит из 3 событий – создание пользователя «testsiem», добавление в группу «testadmins» и события корреляции (Пользователь … с узла … добавил пользователя в группу «testadmins»).

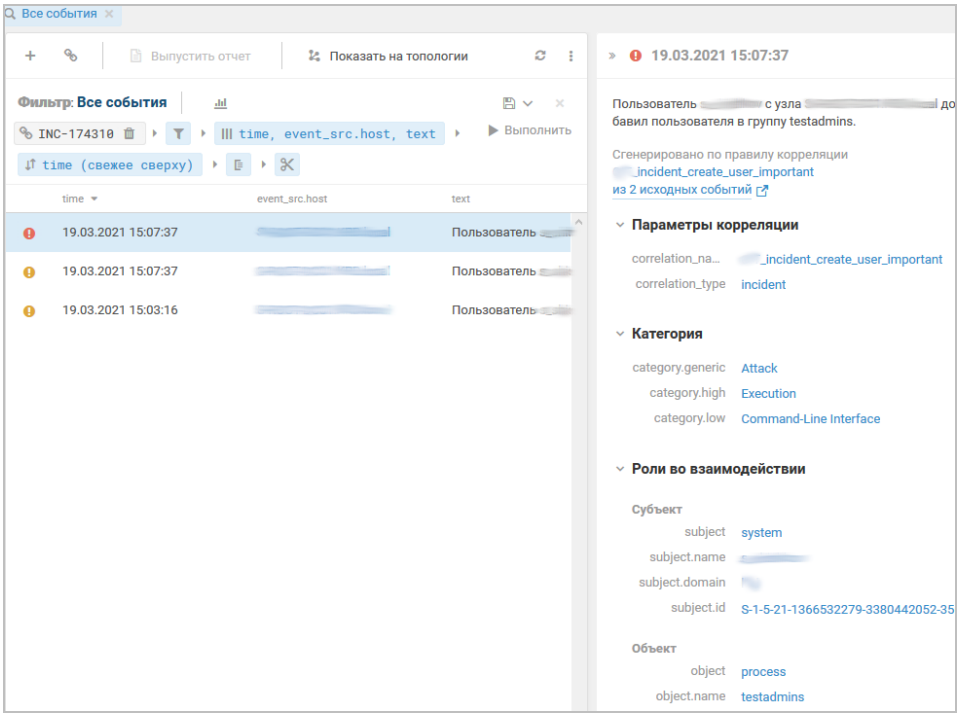


Рисунок 4 – Карточка инцидента 1

Корреляционное правило для отслеживания изменения паролей пользователей представлена на рисунке 5. В нем система будет отслеживать события с идентификатором 4724, при котором имя субъекта будет входить в табличный список «CIT_Admin_Users».

Для проверки правила создадим АРМ «test_server». В нем создадим пользователя «тест_администратор». Далее добавим в табличный список запись с именем этого пользователя. Теперь после смены пароля данному пользователю возникает корреляционное событие. Карточка инцидента представлена на рисунке 6.

Правило корреляции CIT_Incident_Change_User_Important

```
query Check_Admin_Users($username) from CIT_Admin_Users{(username==$username)}

    event Change_User_Pass:
    key:
        event_src.host
    filter{
        msgid =="4724"
        and string(regex(lower(object.name), "healthmailbox", 0)) == null
        and exec_query("Check_Admin_Users",[lower(object.name)])
        }

    rule CIT_Incident_Change_User_Important: Change_User_Pass


    on Change_User_Pass {

        $subject.id = subject.id
        $subject.name = subject.name
        $subject.domain = subject.domain
        $subject.privileges = subject.privileges
```

Рисунок 5 – Правила корреляции изменения паролей пользователей

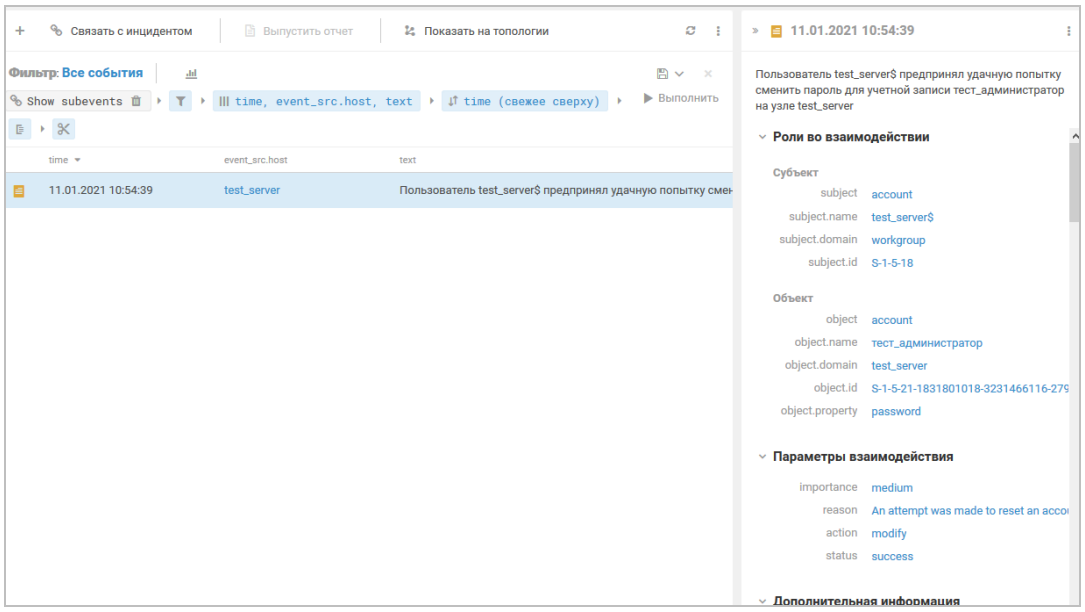


Рисунок 6 – Карточка инцидента 2

В результате внедрения данных корреляций отдел ИБ может отслеживать создание и редактирование учетных записей с критическими высокими и важными в области безопасности правами. При проникновении злоумышленника в корпоративную сеть злоумышленник будет пытаться получить доступ к целевой системе посредством использования скомпрометированных учетных записей или путем эксплуатации уязвимостей в системе. Если ему удастся получить доступ к учетной записи администатора путем сброса пароля, либо создать такую учетную запись, то сотрудники отдела ИБ будут об этом осведомлены.

Для своевременного реагирования следует настроить уведомления по электронной почте на срабатывание данных коррелляций и подключить уведомления в мессенджеры, чтобы иметь возможность оперативно реагировать.

Заключение. SIEM-системы предлагают богатый инструментарий для обеспечения состояния информационной безопасности на предприятии. Для эффективного использования требуется тонкая настройка под каждую конкретную информационную систему, иначе SIEM не будет эффективным инструментом в руках сотрудников отдела ИБ. Главным плюсом этой системы является предоставление широких возможностей для конфигурирования правил, возможность использования собственных корреляций, настройка и отправка уведомлений по множеству критериев.

В рамках данной статьи была продемонстрирована возможность реализаций собственных правил корреляций в среде Maxpatrol SIEM, тем самым повышая степень уровня контроля действий с учетными записями администраторов доменной инфраструктуры, что является крайне важным для защиты от перемещения по периметру и эскалации привилегий в уже зараженной системе и позволяет оперативно обнаружить злоумышленника в корпоративной сети.

Библиографический список

1. Золотухин, А. В. Принцип работы и типовая структура средств управления событиями безопасности информации / А. В. Золотухин, А. С. Тимохович // Academy. – 2017. – № 10 (25). – Режим доступа: https://cyberleninka.ru/article/n/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.10.2021).
2. Королев, И. Д. Анализ проблематики системы управления информацией и событиями безопасности в информационных системах / И. Д. Королев, В. И. Попов, В. А. Ларионов // Инновации в науке. – 2018. – № 12 (88). – Режим доступа: https://cyberleninka.ru/article/n/analiz-problematiki-sistemy-upravleniya-informatsiey-i-sobytiyami-bezopasnosti-v-informatsionnyh-sistemah свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 08.10.2021).
3. itsec.by: Информационная безопасность. Системы управления информацией и событиями безопасности (Security Information and Event Management). – Режим доступа: http://itsec.by/produktyi-siem-sistemyi-upravleniya-infor-2/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021)
4. www.pacifica.kz: Инновационное решение MaxPatrol SIEM для управления событиями и информацией ИБ. – Режим доступа: https://www.pacifica.kz/catalog/monitoring-sobytiy-bezopasnosti-siem-/maxpatrol-siem/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021).
5. Хлестова, Д. Р. Анализ актуальности использования SIEM-систем на предприятиях / Д. Р. Хлестова, К. Г. Попов // Символ науки. – 2016. – № 7–1. – Режим доступа: https://cyberleninka.ru/article/n/analiz-aktualnosti-ispolzovaniya-siem-sistem-na-predpriyatiyah, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 09.10.2021).
6. Макарян, А. С. Анализ практической реализации механизмов выявления кибератак в SIEM-системе Splunk / А. С. Макарян, М. М. Путято, А. Р. Очередько // Информационные системы и технологии в моделировании и управлении : сборник трудов V Международной научно-практической конференции. Ялта, 20–22 мая 2020 года / отв. редактор К. А. Маковейчук. – Ялта : Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2020. – С. 252–256.
7. Подход к построению процедур выявления и предотвращения распределенных атак типа отказ в обслуживании на основе SIEM-систем / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Научные труды КубГТУ. – 2021. – № 1. – С. 20–32.
8. Очередько, А. Р. Исследование iгр-систем на основе анализа механизмов реагирования на инциденты информационной безопасности / А. Р. Очередько, Д. А. Бачманов, М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2021. – № 1 (53).
9. Артамонов, В. А. Кибербезопасность в условиях цифровой трансформации социума / В. А. Артамонов, Е. В. Артамонова // Большая Евразия: развитие, безопасность, сотрудничество. – 2022. – № 5–1.
10. Комаров, А. Н. Анализ и мониторинг сети предприятия в реальном времени / А. Н. Комаров // Глобус: технические науки. – 2020. – № 5 (36).
11. Очередько, А. Р. Исследование SIEM-систем на основе анализа механизмов выявления кибератак / А. Р. Очередько, В. С. Герасименко, М. М. Путято, А. С. Макарян // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2020. – № 2 (261).
12. Королев, И. Д. Повышение уровня автоматизации процессов сбора данных о выявленных событиях и инцидентах информационной безопасности / И. Д. Королев, Е. С. Литвинов, Д. И. Маркин // ИВД. – 2021. – № 10 (82).
13. Махлин, Б. М. Единая система управления информационной безопасности / Б. М. Махлин // Научный формат. – 2019. – № 2 (2).
14. Madani, A. Log management comprehensive architecture in security operation center (soc) / A. Madani, S. Rezayi and H. Gharaee // Computational Aspects of Social Networks (CASoN) 2011 : International Conference. – 2011. – P. 284–289.
15. Курбанова, Н. Э. Методы предотвращения угроз кибербезопасности / Н. Э. Курбанова // Science and Education. – 2021. – № 8.
16. Борисов, В. И. О применении сигнатурных методов анализа информации в SIEM-системах / В. И. Борисов, А. С. Шабуров // Вестник УРФО. Безопасность в информационной сфере. – 2015. – № 3 (17).
17. Кириллов, В. А. Система сбора и корреляции событий (SIEM) как ядро системы информационной безопасности / В. А. Кириллов, А. Р. Касимова, А. Д. Алёхин // Вестник технологического университета. – 2016. – № 13.

References

1. Zolotukhin, A. V., Timokhovich, A. S. Princip raboty i tipovaya struktura sredstv upravleniya sobytiyami bezopasnosti informatsii [Principle of operation and typical structure of information security event management tools]. *Academy*, 2017, no. 10 (25). Available at: https://cyberleninka.ru/article/n/printsip-raboty-i-tipovaya-struktura-sredstv-upravleniya-sobytiyami-bezopasnosti-informatsii (accessed 08.10.2021).
2. Korolev, I. D., Popov, V. I., Larionov, V. A. Analiz problematiki sistemy upravleniya informatsiey i sobytiyami bezopasnosti v informatsionnykh sistemakh [Analysis of security information and event management system issues in information systems]. *Innovatsii v nauke* [Scientific Innovation], 2018, no. 12 (88). Available at: https://cyberleninka.ru/article/n/analiz-problematiki-sistemy-upravleniya-informatsiey-i-sobytiyami-bezopasnosti-v-informatsionnyh-sistemah (accessed 08.10.2021).

3. *itsec.by: Informatsionnaya bezopasnost. Sistemy upravleniya informatsiey i sobytiyami bezopasnosti (Security Information and Event Management)* [itsec.by: Information security. Security Information and Event Management systems]. Available at: http://itsec.by/produktyi-siem-sistemyi-upravleniya-infor-2/ (accessed 09.10.2021).

4. *www.pacifica.kz: Innovatsionnoe reshenie MaxPatrol SIEM dlya upravleniya sobytiyami i informatsiey IB* [www.pacifica.kz: The innovative MaxPatrol SIEM solution for managing IS events and information]. Available at: https://www.pacifica.kz/catalog/monitoring-sobytiy-bezopasnosti-siem-/maxpatrol-siem/ (accessed 09.10.2021).

5. Khlestova, D. R., Popov, K. G. Analiz aktualnosti ispolzovaniya SIEM-sistem na predpriyatiyakh [Analysis of the relevance of the use of SIEM systems in enterprises]. *Simvol nauki* [Symbol of Science], 2016, no. 7–1. Available at: https://cyberleninka.ru/article/n/analiz-aktualnosti-ispolzovaniya-siem-sistem-na-predpriyatiyah (accessed 09.10.2021).

6. Makaryan, A. S., Putyato, M. M., Ocheredko, A. R. Analiz prakticheskoy realizatsii mekhanizmov vyyavleniya kiberatak v SIEM-sisteme Splunk [Analysis of the practical implementation of cyberattack detection mechanisms in the Splunk SIEM system]. *Informatsionnye sistemy i tekhnologii v modelirovanii i upravlenii : sbornik trudov V Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Yalta, 20–22 maya 2020 goda* [Information systems and technologies in modelling and management : Proceedings of the V International Scientific-Practical Conference, Yalta, May 20–22, 2020]. Yalta : Typography «Arial» Publ., 2020, pp. 252–256.

7. Ocheredko, A. R., Bachmanov, D. A., Putyato, M. M., Makaryan, A. S. Podkhod k postroeniyu protsedur vyyavleniya i predotvrashcheniya raspredelennykh atak tipa otkaz v obsluzhivanii na osnove SIEM-sistem [An approach to building procedures for detecting and preventing distributed denial of service attacks based on SIEM systems]. *Nauchnye trudy KubGTU* [Scientific Proceedings of Kuban State Technical University], 2021, no. 1, pp. 20–32.

8. Ocheredko, A. R., Bachmanov, D. A., Putyato, M. M., Makaryan, A. S. Issledovanie IRP-sistem na osnove analiza mekhanizmov reagirovaniya na intsidenty informatsionnoy bezopasnosti [A study of IRP systems based on an analysis of information security incident response mechanisms]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: control and high technologies], 2021, no. 1 (53).

9. Artamonov, V. A., Artamonova, E. V. Kiberbezopasnost v usloviyakh tsifrovoy transformatsii sotsiuma [Cybersecurity in the Digital Transformation of Society]. *Bolshaya Evraziya: razvitie, bezopasnost, sotrudnichestvo* [Greater Eurasia: Development, Security, Cooperation], 2022, no. 5–1.

10. Komarov, A. N. Analiz i monitoring seti predpriyatiya v realnom vremeni [Real-time enterprise network analysis and monitoring]. *Globus: tekhnicheskie nauki* [Globe: Technical Sciences.], 2020, no. 5 (36).

11. Ocheredko, A. R., Gerasimenko, V. S., Putyato, M. M., Makaryan, A. S. Issledovanie SIEM-sistem na osnove analiza mekhanizmov vyyavleniya kiberatak [SIEM research based on analysis of cyber-attack computation mechanisms]. Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki [Vestnik of Adygeyan State University], 2020, no. 2 (261).

12. Korolev, I. D., Litvinov, E. S., Markin, D. I. Povyshenie urovnya avtomatizatsii protsessov sbora dannykh o vyyavlennykh sobytiyakh i intsidentakh informatsionnoy bezopasnosti [Improving automation of data collection processes for detected information security events and incidents]. *IVD* [IVD], 2021, no. 10 (82).

13. Makhlin, B. M. Edinaya sistema upravleniya informatsionnoy bezopasnosti [A unified information security management system]. *Nauchnyy format* [Scientific Format], 2019, no. 2 (2).

14. Madani, A., Rezayi, S. and Gharaee, H. Log management comprehensive architecture in security operation center (soc). *Computational Aspects of Social Networks (CASoN) 2011 : International Conference*, 2011, pp. 284–289.

15. Kurbanova, N. E. Metody predotvrashcheniya ugroz kiberbezopasnosti [Methods to prevent cybersecurity threats]. *Science and Education*, 2021, no. 8.

16. Borisov, V. I., Shaburov, A. S. O primenenii signaturnykh metodov analiza informatsii v SIEM-sistemakh [About the application of signature analysis method in the SIEM-systems]. *Vestnik URFO. Bezopasnost v informatsionnoy sfere* [Bulletin of URFO. Information-technology (IT) security], 2015, no. 3 (17).

17. Kirillov, V. A., Kasimova, A. R, Alyokhin, A. D. Sistema sbora i korrelyatsii sobytiy (SIEM) kak yadro sistemy informatsionnoy bezopasnosti [Event Collection and Correlation System (SIEM) as the core of an information security system]. *Vestnik tekhnologicheskogo universiteta* [Bulletin of the Technological University], 2016, no. 13.

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

DOI 10.54398/20741707_2022_3_112
УДК 004.42:004.3'1

ПРИМЕНЕНИЕ МИКРОКОНТРОЛЛЕРНЫХ СИСТЕМ В ИССЛЕДОВАНИЯХ (НА ПРИМЕРЕ МАШИНЫ АТВУДА)[1]

Статья поступила в редакцию 15.06.2022, в окончательном варианте – 12.08.2022.

Сухомлинов Никита Михайлович, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 28,
студент, ORCID: 0000-0001-7898-217X, e-mail: nikita-2015s@yandex.ru
Финогеев Алексей Германович, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40,
доктор технических наук, профессор, ORCID: 0000-0002-4777-3364, e-mail: alexeyfinogeev@gmail.com
Смирнова Татьяна Владимировна, Волгоградский государственный социально-педагогический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 27,
доцент, ORCID: 0000-0003-2861-3119, e-mail: smirnova.tatiana.2013@yandex.ru
Иващенко Владислав Дмитриевич, Волгоградский государственный технический университет, 400074, Российская Федерация, г. Волгоград, ул. Академическая, 1,
студент, ORCID: 0000-0001-6154-0703, e-mail: iwashenko.vlad@mail.ru
Парыгин Данила Сергеевич, Волгоградский государственный технический университет, 400074, Российская Федерация, г. Волгоград, ул. Академическая, 1,
кандидат технических наук, доцент, ORCID: 0000-0001-8834-5748, e-mail: dparygin@gmail.com

Микроконтроллеры сегодня являются неотъемлемой составной частью подавляющего числа электронного оборудования. Понимание принципов их применения важно для построения современных систем управления во всех сферах жизнедеятельности человека. Одной из таких сфер стала наука, где микроконтроллеры успешно используются для проведения опытов и экспериментов. В данной статье рассматриваются преимущества такого подхода и общие принципы разработки устройств под управлением микроконтроллеров. На примере микропроцессорного устройства с микроконтроллером STM32 продемонстрирован процесс реализации электронного блока управления установкой (машиной Атвуда) для проведения лабораторных работ и демонстрационного эксперимента по механике.

Ключевые слова: микроконтроллеры, машина Атвуда, блок управления, FreeRTOS, семисегментный индикатор, принцип динамической индикации

APPLICATION OF MICROCONTROLLER SYSTEMS IN RESEARCH (USING THE EXAMPLE OF THE ATWOOD MACHINE)

The article was received by the editorial board on 15.06.2022, in the final version – 12.08.2022.

Sukhomlinov Nikita M., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
student, ORCID: 0000-0001-7898-217X, e-mail: nikita-2015s@yandex.ru
Finogeev Alexey G., Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation,
Doct. Sci. (Engineering), Professor, ORCID 0000-0002-4777-3364, e-mail: alexeyfinogeev@gmail.com
Smirnova Tatiana V., Volgograd State Pedagogical University, 27 Lenin Ave., Volgograd, 400005, Russian Federation,
Associate Professor, ORCID 0000-0003-2861-3119, e-mail: smirnova.tatiana.2013@yandex.ru

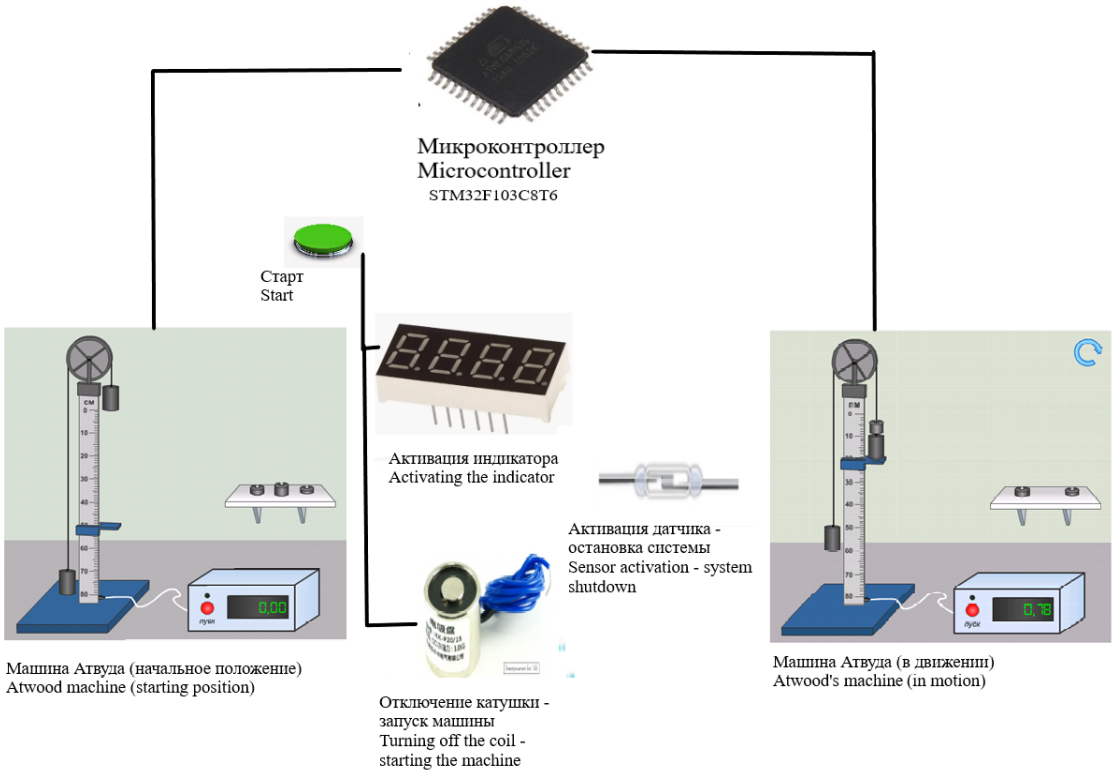
[1] Исследование выполнено за счет гранта Российского научного фонда и Волгоградской области № 22-11-20024, https://rscf.ru/project/22-11-20024/. Результаты части 2 получены в рамках гранта Российского научного фонда № 20-71-10087.

Ivashchenko Vladislav D., Volgograd State Technical University, 1 Akademicheskaya St., 400074, Russian Federation, Volgograd,
student, ORCID: 0000-0001-6154-0703, e-mail: iwashenko.vlad@mail.ru
Parygin Danila S., Volgograd State Technical University, 1 Akademicheskaya St., Volgograd, 400074, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID 0000-0001-8834-5748, e-mail: dparygin@gmail.com

Microcontrollers today are an integral part of the vast majority of electronic equipment. Understanding the principles of their application is important for building modern control systems in all spheres of human life activity. One of these areas has become science, where microcontrollers are successfully used to conduct experiments. This article discusses the advantages of this approach and the general principles for the development of devices controlled by microcontrollers. The process of implementing an electronic control unit for an apparatus (Atwood machine) for laboratory work and a demonstration experiment in mechanics is demonstrated using the example of a microprocessor device with an STM32 microcontroller.

Keywords: microcontrollers, Atwood machine, control unit, FreeRTOS, seven-segment indicator, dynamic display principle

Graphical annotation (Графическая аннотация)



Введение. Датой появления первого микроконтроллера считается 1976 год, когда компания Intel представила микросхему i8048, состоящую из центрального микропроцессора, памяти объемом 1 Кбайт, двух восьмибитных таймеров, генератора часов и 27 портов ввода/вывода [12]. Но не все ученые разделяют это мнение, указывая на то, что еще в 1971 году был выдан первый патент на однокристальную микро-ЭВМ инженерам М. Кочрену и Г. Буну из американской компании Texas Instruments. Но так или иначе изобретение микроконтроллеров справедливо признается прорывом в области вычислительной техники. Со временем с целью выигрыша в гибкости, производительности и стоимости стали появляться все новые модели этих устройств. А микроконтроллеры нашли свое применение в различных сферах науки, техники и быта [17]. Например, микроконтроллеры используются в вычислительной технике (материнские платы, дисководы, калькуляторы), бытовых устройствах (стиральные машины, микроволновые печи, телефоны, «домашние» роботы), автоматизации промышленного оборудования и др. [8, 19].

Не обошли стороной микроконтроллеры и сферу науки, где они используются, в том числе, для производства различных научных опытов и экспериментов в областях химии, физики и некоторых других [6]. Значение именно такого применения микроконтроллеров состоит в одновременном

решении двух ключевых проблем: проблемы обеспечения безопасности эксперимента и проблемы автоматизации экспериментальных исследований [2].

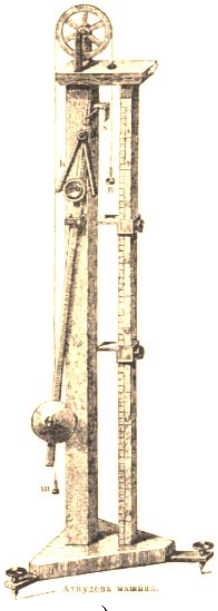
В качестве примера преодоления первой проблемы может служить применение микроконтроллеров в роли управляющих устройств на атомных и тепловых электрических станциях, позволяющих исследователям контролировать процессы, находясь на безопасной дистанции от воздействия вредных факторов (излучения) [22]. Во втором случае использование микроконтроллера не только облегчит труд экспериментатора, но и прежде всего уменьшит влияние на результаты экспериментов субъективного фактора. В итоге исследователь сможет сохранить такие характеристики эксперимента, как воспроизводимость и контролируемость, а также снизить до минимума показатели погрешности измерения [23].

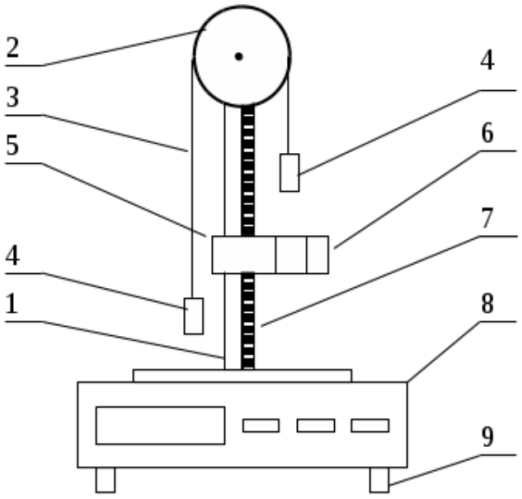
С учетом вышеизложенного, в настоящем исследовании выполнена разработка электронного блока управления на базе микроконтроллера одной из классических установок, используемых в лабораторном практикуме по механике – машиной Атвуда [20]. Эта установка используется для изучения законов кинематики равноускоренного прямолинейного движения. Актуальность работы обусловлена современными тенденциями к миниатюризации электронных приборов, стремлением минимизации человеческого фактора и показателей погрешности при проведении эксперимента, а также обеспечения высокой наглядности за счет использования современных средств отображения информации.

1. Обзор объекта исследования. Машина Атвуда представляет собой укрепленную вертикальную стойку, на которую нанесена шкала, с двумя кронштейнами. Вверху стойки закреплен блок, через который переброшена нить с двумя грузами. А принцип ее работы можно описать следующим образом. Система находится в покое пока удерживается один из грузов. Благодаря наличию «противовеса» удается контролировать вертикальное движение груза вниз. До начала опыта один из грузов закреплён, и вся система находится в состоянии покоя. При освобождении первого груза система приводится в движение [25].

Первая версия машины Атвуда обладала недостатком, заключавшимся во влиянии субъективного фактора на результаты измерений. Экспериментатор был вынужден самостоятельно приводить систему в движение, при этом запуская секундомер и останавливая его при ударе подвешенного груза о поверхность. Очевидно, что одновременное выполнение всех этих действий одним человеком или с помощником приведет к неточностям в измерении [21].

С учетом вышеназванных нюансов стали разрабатываться автоматизированные версии машины Атвуда, ключевым моментом которых является создание точного секундомера, сопряженного с устройством запуска движения (устройством включения электромагнита). Ниже на рисунках приведены классическая модель машины Атвуда (рис. 1а) и одна из усовершенствованных ее версий – модель ФМ-11 (рис. 1б) [15].





1 -стойка; 2 - блок; 3 - нить; 4 - грузы; 5 - средний кронштейн; 6 - фотодатчик; 7 - линейка; 8 - миллисекундомер; 9 - опора

а) б)

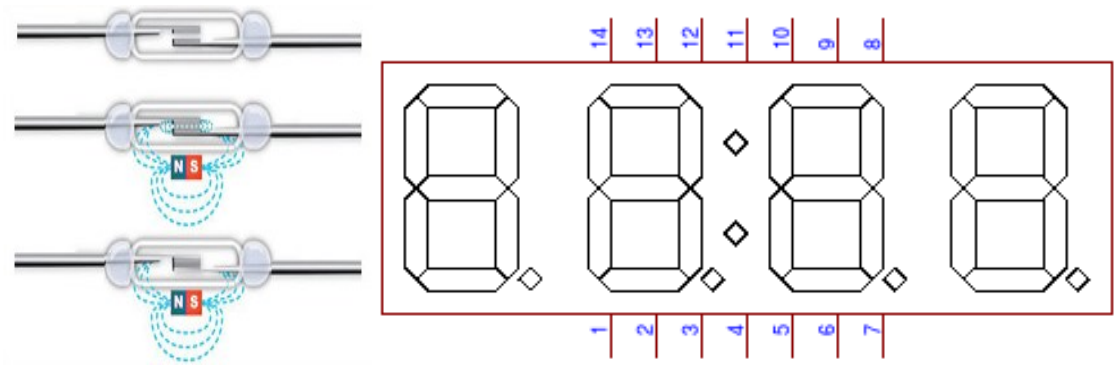
Рисунок 1 – Машина Атвуда: а) классическая модель [1]; б) усовершенствованная модель ФМ-11 [16]

В эксперименте с использованием установки ФМ-11 при нажатии кнопки отключается электромагнитная катушка, играющая роль тормоза, и система приходит в движение. В свою очередь в оба кронштейна встроены фотодатчики, и при начале движения груза вверх первый фотодатчик, подключенный к секундомеру, срабатывает, когда первый груз достигнет отметки, что инициирует начало отчета времени на секундомере. Когда же второй груз достигнет поверхности, то благодаря второму фотодатчику отсчет времени останавливается. Соответственно, время на дисплее секундомера и будет временным промежутком нахождения груза в движении.

В целом установка ФМ-11 по своим характеристикам и устройству максимально приближена к классической Атвудовой машине, которую представляли себе исследователи. С ее применением процесс проведения эксперимента практически полностью автоматизирован [13]. В то же время улучшенной альтернативой данной установки может служить устройство, разработанное на базе микроконтроллера, берущего на себя функцию не только отсчета временных промежутков, но и общего управления системой.

2. Выбор аппаратной части для разрабатываемой установки. Аппаратную часть было решено построить на основе микроконтроллера STM32F107VCT6, герконового датчика, семисегментного многоразрядного индикатора и электромагнита. Микроконтроллер STM32F107VCT6, представитель семейства 32-битных микроконтроллеров STM, включает в себя ядро (ARM Cortex-M3), статическую RAM-память, флеш-память, отладочные и различные периферийные интерфейсы [24].

Герконовый датчик, представляющий собой запаянную в стеклянной колбе пару ферромагнитных контактов (сердечников) с зазором между ними, служит для определения момента падения груза на поверхность (рис. 2а). Принцип его работы заключается в замыкании либо размыкании электрических контактов под влиянием магнитного поля [3].



а) б)

Рисунок 2 – Компоненты аппаратной части: а) герконовый датчик (внутреннее строение); б) семисегментный индикатор

Для удержания груза до момента начала эксперимента используется электромагнитная катушка, подключенная к источнику постоянного тока и создающая магнитное поле [5].

Отдельно стоит сказать о семисегментном индикаторе (рис. 2б), выполняющем функции секундомера в эксперименте. Его работа основывается на принципе динамической индикации, состоящем в поочередном включении цифр в разрядах путем циклической подачи тока через транзисторные ключи на общие катоды, что позволяет создать иллюзию одновременного свечения всех разрядов. Техническая реализация достигается за счет параллельного соединения анодов соответствующих сегментов всех разрядов и совместного соединения катодов различных сегментов одного разряда (либо, наоборот, общими для каждого разряда являются аноды, а катоды различных разрядов индикатора выводятся на шину данных) [7].

Соответственно, алгоритм работы создаваемого устройства будет состоять в следующем. По нажатию кнопки на микроконтроллере либо отправки соответствующей команды через интерфейс USART [4] отключается электромагнит и одновременно включается секундомер, реализованный на семисегментном индикаторе, начинается падение груза. Далее, при падении груза, срабатывает герконовый датчик, подключенный к микроконтроллеру, что является условием для выполнения команды приостановления отсчета на секундомере. Общая схема устройства изображена на рисунке 3.

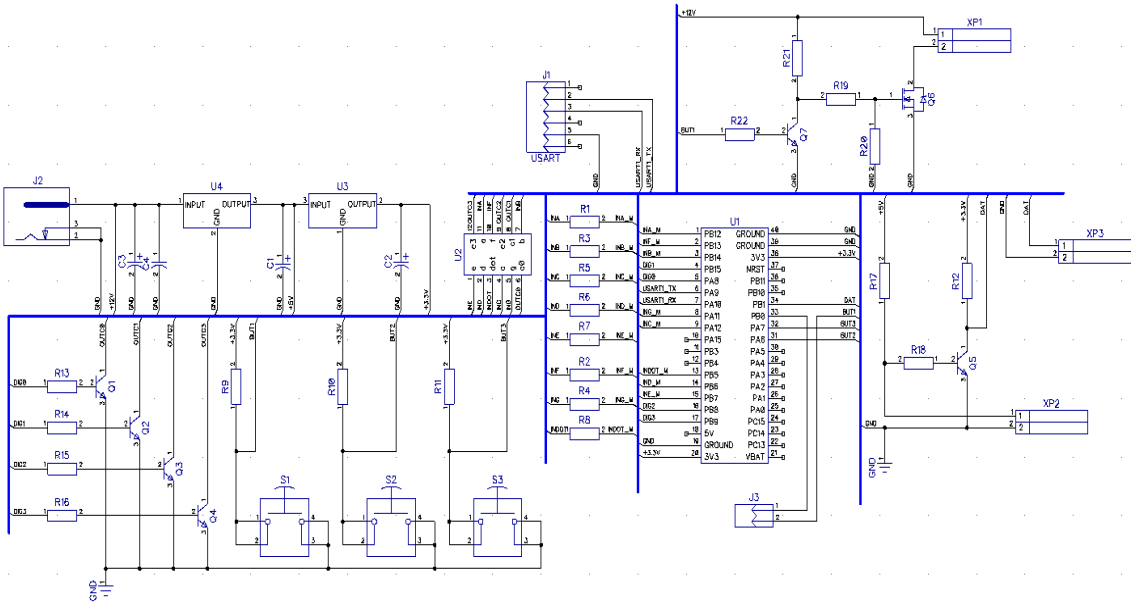


Рисунок 3 – Схема электрическая принципиальная

3. Разработка программного обеспечения для управления устройства. Разработка программы для микроконтроллера осуществлялась с помощью среды разработки Keil uVision 5 [14]. В сам проект включены файлы с настройками семисегментного индикатора, функциями запуска и остановки секундомера, вывода на дисплей заданной цифры в заданную позицию, включения/выключения магнита. Также присутствуют файлы, позволяющие скомпилировать операционную систему FreeRTOS [10]. Именно функция-задача FreeRTOS обеспечивает вывод строки из четырех символов на дисплей на основе принципа динамической индикации. Ниже приведен общий алгоритм работы программы (рис. 4а) и диаграмма последовательностей (рис. 5).

Настройка семисегментного индикатора начинается с его тактирования с помощью команды RCC_APB2PeriphClockCmd(RCC_APB2Periph_GPIOA, ENABLE), где APB2 – это одна из периферийных шин данных [18]. Далее следует объявление инициализационной структуры для настройки портов, параметрами которой являются его частота (GPIO_Speed) и режим работы (GPIO_Mode). В данном случае выбран режим GPIO_Mode_Out_PP. Вывод заданной цифры (digit) в заданную позицию (position) на дисплее осуществляется в функции onOffDigit() [11]. С помощью конструкции switch-case устанавливается для каждой цифры от 0 до 9 комбинация входных сигналов на порты A и B микроконтроллера. Алгоритм работы индикатора представлен на рисунке 4б.

Как уже отмечалось выше, основным устройством разрабатываемого электронного блока управления машиной Атвуда является секундомер, запускающийся по нажатию кнопки и останавливающийся при срабатывании герконового датчика. Причем значение на дисплее после срабатывания датчика должно оставаться неизменным. При настройках по умолчанию тактовая частота микроконтроллера, установленного на плате STM32 Blue Pill [9], составляет 72 МГц, и такая же частота подается по шине тактирования на таймеры-счетчики. Если установить предделитель таймера равным 720, тактовая частота, на которой он будет работать, будет составлять 100 кГц, то есть период этого сигнала будет равен 0,01 мс. При установке периода таймера равным 1000 таймер-счетчик будет срабатывать каждые 10 мс, то есть каждые 0,01 с. Как раз через такой промежуток времени должны меняться значения младшего разряда на семисегментном индикаторе.

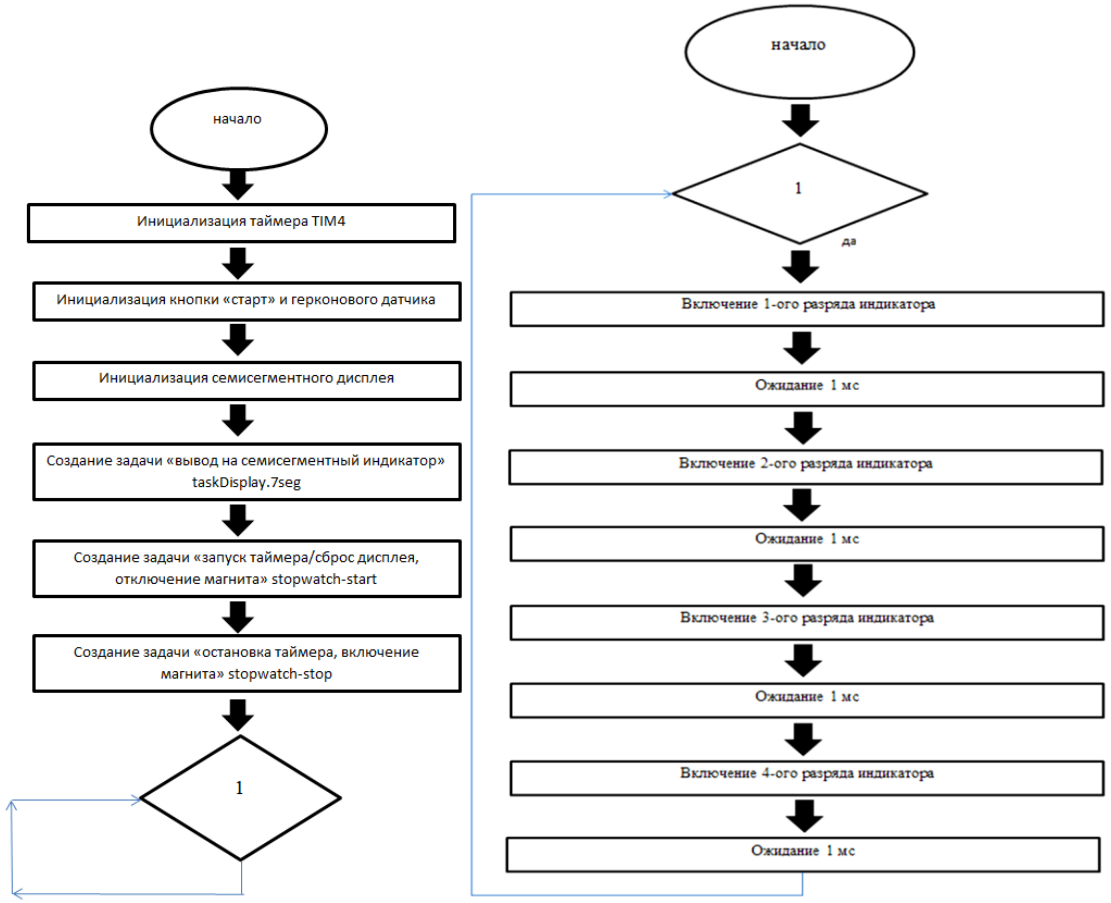


Рисунок 4 – Алгоритмы работы компонентов программы управления разрабатываемым устройством: а) начальная настройка устройства; б) переключение разрядов на четырехпозиционном семисегментном индикаторе

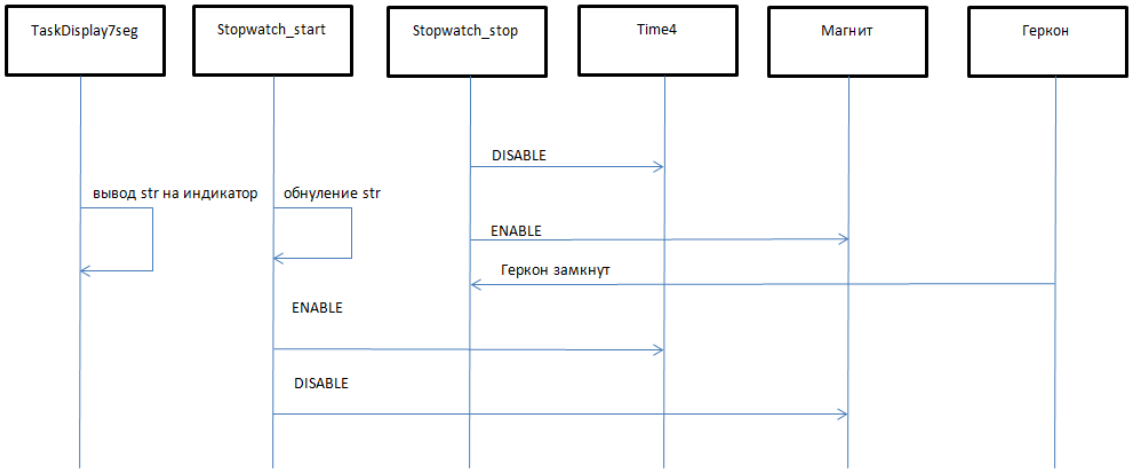


Рисунок 5 – Диаграмма последовательностей

Специальная функция-задача FreeRTOS, названная stopwatch_start(), активирует начало отсчета при поступлении соответствующего сигнала с линии 7 порта A (нажатие кнопки). При этом обнуляются значения переменных millisecond, millisecondTwo, second, secondTwo (соответсвенно, десятки секунд, секунды, десятые доли секунды, сотые доли секунды), а затем разрешается прерывание по переполнению от таймера TIM4. Схема описанного алгоритма представлена на рисунке 6а.

Здесь же второй функцией-задачей FreeRTOS является функция stopwatch_stop(), в которой выполняется остановка отсчета при срабатывании герконового датчика (ожидается сигнал логического нуля с 0-го пина порта B). Алгоритм, реализованный в функции stopwatch_stop(), представлен на рисунке 6б.

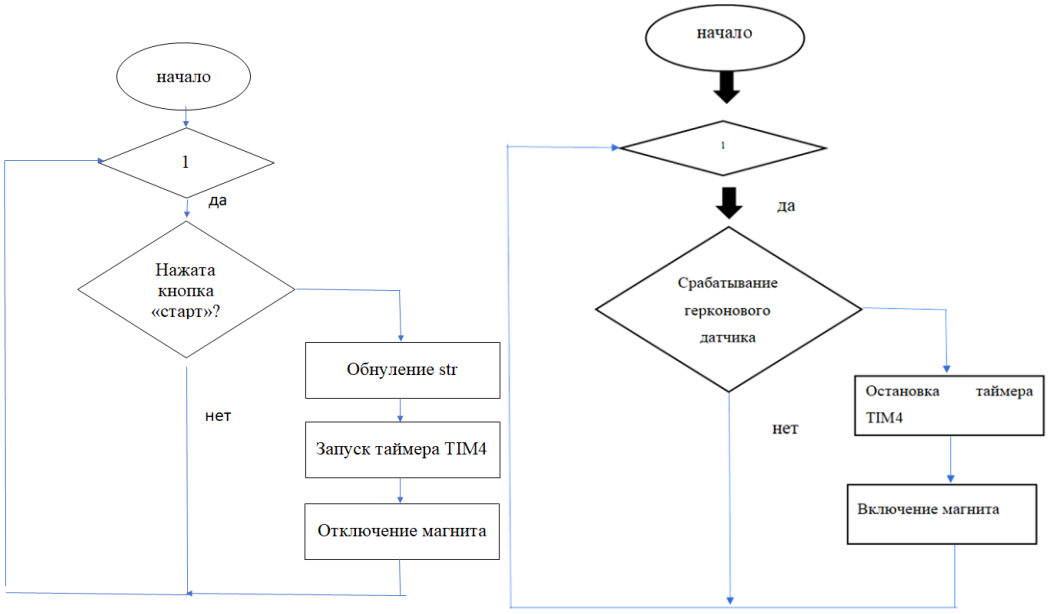


Рисунок 6 – Алгоритмы реализации функций программы управления: а) stopwatch_start(); б) FreeRTOS по остановке таймера при условии срабатывания герконового датчика

Работа программы испытывалась на имеющемся в распоряжении стенде, содержащем подключенный как дополнительный модуль плату BluePill STM32, четырехпозиционный семисегментный индикатор, светодиоды и кнопки, модуль USB-UART [26] (рис. 7).

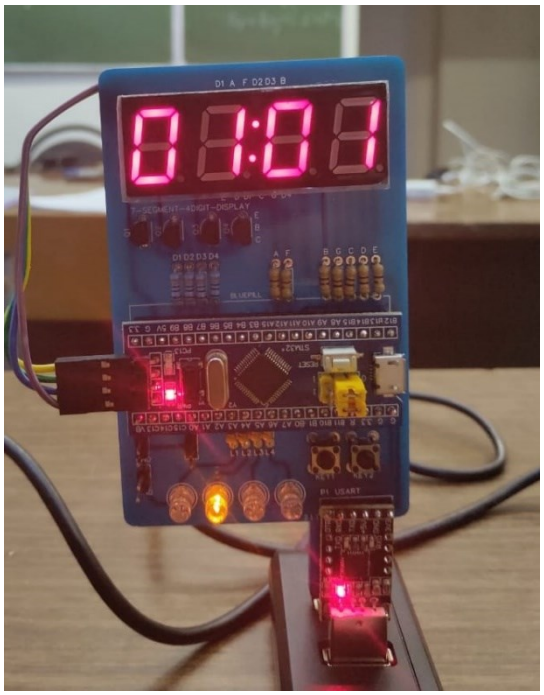


Рисунок 7 – Разработанный стенд для испытания работы программы

Для запуска секундомера использовалась правая кнопка, для имитации срабатывания герконового датчика – левая кнопка, для отображения состояния электромагнита – левый нижний светодиод. Принципиальная схема стенда и разрабатываемого устройства в части подключения семисегментного индикатора совпадают с точностью до переключения некоторые сегментов, что было сделано из соображений удобства разводки дорожек печатной платы. Программа показала свою работоспособность.

Заключение. Таким образом, подводя итог проведенному исследованию, можно сделать следующие выводы. В сконструированном устройстве в рамках данной работы, в отличие от модели ФМ-11 машины Атвуда, два фотодатчика были заменены на один герконовый, а управление машиной полностью «передано» микроконтроллеру. В качестве основных компонентов устройства использовались микроконтроллер STM32F107VCT6 для управления работой всего устройства, герконовый датчик для определения момента приземления груза на поверхность, электромагнитная катушка в качестве тормоза системы и компоненты «классической модели» Атвудовой машины (штатив, грузы, нить). Цель исследования достигнута, поскольку подобный подход в создании новой модели машины Атвуда позволил максимально автоматизировать процесс проведения эксперимента по изучению движения тел в поле силы тяготения и избежать возникновения субъективных погрешностей.

Библиографический список

1. Атвудова машина. – 2022. – Режим доступа: http://www.vehi.net/brokgauz/all/006/6245.shtml, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 02.02.2022).

2. Волосатова, Т. М. Анализ направлений применения принципа модульности при разработке и использовании учебных проектов по робототехнике в вузах / Т. М. Волосатова, Д. А. Барсуков, П. И. Тамков // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 4. – С. 133–148.

3. Герконовые датчики – особенности применения. – 2022. – Режим доступа: https://rusautomation.ru/articles/gerkonovye-datchiki-osobennosti-primeneniya/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 01.04.2022).

4. Интерфейс USART. – 2022. – Режим доступа: https://www.gaw.ru/html.cgi/txt/doc/micros/avr/arh_xmega/20.htm, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.04.2022).

5. Котенёв, С. В. Расчет и оптимизация тороидальных трансформаторов и дросселей / С. В. Котенёв, А. Н. Евсеев. – Москва : Горячая линия – Телеком, 2013. – 360 с.

6. Кравченко, А. В. 10 практических устройств на AVR-микроконтроллерах / А. В. Кравченко. – Санкт-Петербург : Корона-Век, 2014. Кн. 2. – 320 с.

7. Максимально универсальный семисегментный дисплей. Часть первая – Hardware. – 2022. – Режим доступа: https://habr.com/ru/post/485696/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.03.2022).

8. Мань, Н. С. Подсистема управления процессом формирования входных данных в системе интеллектуального управления зданием / Н. С. Мань, Г. А. Попов, И. Ю. Кучин // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 142–158.

9. Модуль разработки STM32F103C8T6 Blue pill. – 2022. – Режим доступа: https://compacttool.ru/modul-razrabotki-stm32f103c8t6-blue-pill, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 25.03.2022).

10. Операционная система FreeRTOS. – 2022. – Режим доступа: https://robotclass.ru/articles/c_book_freertos/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.03.2022).

11. Разработка таймера на STM32 и индикаторе SA56-11SRWA. – 2022. – Режим доступа: http://engio.ru/vstraivaemyie-sistemyi/podklyuchaem-k-stm32-.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.04.2022).

12. Ревич, Ю. В. Практическое программирование микроконтроллеров Atmel AVR на языке ассемблера / Ю. В. Ревич. – 2-е изд., испр. – Санкт-Петербург : БХВ-Петербург, 2011. – 352 с.

13. Снежков, В. И. Физика: методические указания к лабораторной работе № 4а «Изучение второго закона Ньютона при помощи лабораторной установки ФМ-11 «Машина Атвуда» для обучающихся по всем направлениям подготовки и специальностям / В. И. Снежков, Е. Б. Русакова. – Ростов-на-Дону : Рост. гос. строит. ун-т, 2015. – 11 с.

14. Среда разработки Keil uVision 5 MDK-ARM. – 2022. – Режим доступа : https://cxemka.com/144-sreda-razrabotki-keil-uvision-5-mdk-arm-skachat.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 24.02.2022).

15. Установка лабораторная «Машина Атвуда». ФМ-11. – 2022. – Режим доступа: https://www.учебнаятехника.рф/wps/ustanovka-laboratornaya-mashina-atvuda-fm-11/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.03.2022).

16. Установка лабораторная Машина Атвуда. – 2022. – Режим доступа: http://uchcollector-spb.ru/item/ustanovka-laboratornaya-mashina-atvuda, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.02.2022).

17. Parygin, D. S. A convergent model for distributed processing of Big Sensor Data in urban engineering networks / D. S. Parygin, A. G. Finogeev, V. A. Kamaev, A. A. Finogeev, E. P. Gnedkova, A. P. Tyukov // Journal of Physics: Conference Series : Proceedings of the International Conference on Information Technologies in Business and Industry 2016, Tomsk, Russia, 21–23 September 2016. – IOP Publishing, 2017. – Vol. 803/012112. – P. 1–6. – DOI: 10.1088/1742-6596/803/1/012112.

18. AHB/APB. – 2022. – Режим доступа: https://russianblogs.com/article/8344537335/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 01.05.22).

19. Agarwal, A. K. Analysis of Environmental Factors for Smart Farming: An Internet of Things Based Approach / D. Ather, R. Astya, D. Parygin, A. Garg, D. Raj // SMART 2021 : Proceedings of the 2021 10th International

Conference on System Modeling and Advancement in Research Trends, Moradabad, India, 10–11 December 2021. – IEEE, 2022. – P. 210–214. – DOI: 10.1109/SMART52563.2021.9676305.

20. Atwood's Machine. – 2022. – Режим доступа: http://physics.kenyon.edu/EarlyApparatus/Mechanics /Atwoods_Machine/Atwoods_Machine.html, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 12.03.2022).

21. Greenslade, T. B. Jr. Atwood's machine / T. B. Greenslade Jr. // Physics Teaching. – 1985. – № 29. – P. 24–28.

22. Parygin, D. Management of Information from Surveillance Cameras at the Infrastructure Facility / D. Parygin, A. Gurtyakov, A. Finogeev, A. Ignatyev, T. Yereshchenko // Intelligent Systems Reference Library : New Trends and Applications in Internet of Things (IoT) and Big Data Analytics. – Springer, Cham, 2022. – Vol. 221. – P. 173–186. – DOI: 10.1007/978-3-030-99329-0_12.

23. Parygin, D. Multi-agent approach to distributed processing big sensor data based on fog computing model for the monitoring of the urban infrastructure systems / D. Parygin, N. Nikitsky, V. Kamaev, A. Matokhina, A. Finogeev, A. Finogeev // SMART 2016 : Proceedings of the 5th International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, 25–27 November 2016. – IEEE, 2017. – P. 305–310. – DOI: 10.1109/SYSMART.2016.7894540.

24. STM32F107VCT6. – 2022. – Режим доступа: https://ru.farnell.com/stmicroelectronics/stm32f107vct6 /mcu-32bit-cortex-m3-72mhz-lqfp/dp/1737141, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.03.2022).

25. Tipler, P. A. Physics For Scientists and Engineers / P. A. Tipler. – New York : Worth Publishers, 1991. – 160 p.

26. USB to TTL UART – Модули преобразования порта USB в порт UART. – 2022. – Режим доступа: https://mirrobo.ru/micro/usb-to-uart/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.04.2022).

References

1. *Atvudova mashina* [Atwood machine]. Available at: http://www.vehi.net/brokgauz/all/006/6245.shtml (accessed 02.02.2022).

2. Volosatova, T. M., Barsukov, D. A., Tamkov, P. I. Analiz napravleniy primeneniya printsipa modulnosti pri razrabotke i ispolzovanii uchebnykh proyektov po robototekhnike v vuzakh [Analysis of directions for applying the principle of modularity in the development and use of educational projects on robotics in universities]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020., no. 4, pp. 133–148.

3. *Gerkonovyye datchiki – osobennosti primeneniya* [Reed sensors - application features]. Available at: https://rusautomation.ru/articles/gerkonovye-datchiki-osobennosti-primeneniya/ (accessed 01.04.22).

4. *Interfeys USART* [USART interface]. Available at: https://www.gaw.ru/html.cgi/txt/doc /micros/avr/arh_xmega/20.htm (accessed 07.04.2022).

5. Kotenev, S. V., Evseev, A. N. *Raschet i optimizatsiya toroidalnykh transformatorov i drosseley* [Calculation and optimization of toroidal transformers and chokes]. Moscow, 2013. 360 p.

6. Kravchenko, A. V. *10 prakticheskikh ustroystv na AVR-mikrokontrollerakh* [10 practical devices on AVR microcontrollers]. St. Petersburg, 2014. Book 2. 320 p.

7. *Maksimalno universalnyy semisegmentnyy displey. Chast pervaya – Hardware* [The most versatile seven-segment display. Part One – Hardware]. Available at: https://habr.com/ru/post/485696/ (accessed 10.03.2022).

8. Man, N. S., Popov, G. A., Kuchin, I. Yu. Podsistema upravleniya protsessom formirovaniya vkhodnykh dannykh v sisteme intellektualnogo upravleniya zdaniyem [Subsystem for managing the process of generating input data in the intelligent building management system]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2015, no. 3, pp. 142–158.

9. *Modul razrabotki STM32F103C8T6 Blue pill* [STM32F103C8T6 Blue pill development module]. Available at: https://compacttool.ru/modul-razrabotki-stm32f103c8t6-blue-pill (accessed 25.03.2022).

10. *Operatsionnaya sistema FreeRTOS* [FreeRTOS operating system]. Available at: https://robotclass.ru/articles/c_book_freertos/ (accessed 15.03.2022).

11. *Razrabotka taymera na STM32 i indikatore SA56-11SRWA* [Development of a timer on STM32 and the SA56-11SRWA indicator]. Available at: http://engio.ru//vstraivaemyie-sistemyi/podklyuchaem-k-stm32-.html (accessed 21.04.2022).

12. Revich, Yu. V. *Prakticheskoye programmirovaniye mikrokontrollerov Atmel AVR na yazyke assemblera* [Practical programming of Atmel AVR microcontrollers in assembly language]. St. Petersburg, 2011. 352 p.

13. Snezhkov, V. I., Rusakova, E. B. *Fizika: metodicheskiye ukazaniya k laboratornoy rabote № 4a «Izucheniye vtorogo zakona Nyutona pri pomoshchi laboratornoy ustanovki FM-11 «Mashina Atvuda» dlya obuchayushchikhsya po vsem napravleniyam podgotovki i spetsialnostyam* [Physics: guidelines for laboratory work No. 4a "Studying Newton's second law using the laboratory installation FM-11 "Atwood Machine" for students in all areas of training and specialties]. Rostov-on-Don, 2015. 11 p.

14. *Sreda razrabotki Keil uVision 5 MDK-ARM* [Keil uVision 5 MDK-ARM Development Environment]. Available at: https://cxemka.com/144-sreda-razrabotki-keil-uvision-5-mdk-arm-skachat.html (accessed 24.02.2022).

15. *Ustanovka laboratornaya «Mashina Atvuda». FM-11* [Laboratory installation "Atwood Machine". FM-11]. Available at: https://www.учебнаятехника.рф/wps/ustanovka-laboratornaya-mashina-atvuda-fm-11/ (accessed 22.03.2022).

16. *Ustanovka laboratornaya Mashina Atvuda* [Atwood Laboratory Machine]. Available at: http://uchcollector-spb.ru/item/ustanovka-laboratornaya-mashina-atvuda (accessed 12.02.2022).

17. Parygin, D. S., Finogeev, A. G., Kamaev, V. A., Finogeev, A. A., Gnedkova, E. P., Tyukov, A. P. A convergent model for distributed processing of Big Sensor Data in urban engineering networks. *Journal of Physics: Conference Series*, 2017, vol. 803/012112, pp. 1–6. DOI: 10.1088/1742-6596/803/1/012112.

18. *AHB/APB*. Available at: https://russianblogs.com/article/8344537335/ (accessed 01.05.2022).

19. Agarwal, A. K., Ather, D., Astya, R., Parygin, D., Garg, A., Raj, D. Analysis of Environmental Factors for Smart Farming: An Internet of Things Based Approach. *Proceedings of the 2021 10th International Conference on System Modeling and Advancement in Research Trends*, 2022, pp. 210–214. DOI: 10.1109/SMART 52563.2021.9676305.

20. *Atwood's Machine*. Available at: http://physics.kenyon.edu/EarlyApparatus/Mechanics /Atwoods_Machine/Atwoods_Machine.html (accessed 12.03.2022).

21. Greenslade, T. B. Jr. Atwood's machine. *Physics Teaching*, 1985, no. 29, pp. 24–28.

22. Parygin, D., Gurtyakov, A., Finogeev, A., Ignatyev, A., Yereshchenko, T. Management of Information from Surveillance Cameras at the Infrastructure Facility. *Intelligent Systems Reference Library. New Trends and Applications in Internet of Things (IoT) and Big Data Analytics*, 2022, vol. 221, pp. 173–186. DOI: 10.1007/978-3-030-99329-0_12.

23. Parygin, D., Nikitsky, N., Kamaev, V., Matokhina, A., Finogeev, A., Finogeev ,A. Multi-agent approach to distributed processing big sensor data based on fog computing model for the monitoring of the urban infrastructure systems. *SMART 2016 : Proceedings of the 5th International Conference on System Modeling & Advancement in Research Trends, Moradabad, India, 25–27 November 2016.* 2017, pp. 305–310. DOI: 10.1109/SYSMART.2016.7894540.

24. *STM32F107VCT6*. Available at: https://ru.farnell.com/stmicroelectronics/stm32f107vct6/mcu-32bit-cortex-m3-72mhz-lqfp/dp/1737141 (accessed 15.03.2022).

25. Tipler, P. A. *Physics For Scientists and Engineers*. New York, 1991, 160 p.

26. *USB to TTL UART – Moduli preobrazovaniya porta USB v port UART* [USB to TTL UART – Modules for converting a USB port to a UART port], 2022. Available at: https://mirrobo.ru/micro/usb-to-uart/ (accessed 11.04.2022).

ПРАВИЛА ДЛЯ АВТОРОВ

1. В журнале публикуются материалы на английском и русском языках по тематике, соответствующей утвержденным для журнала отраслям наук, группам специальностей.

2. В список соавторов работ включаются только те лица, которые внесли творческий вклад в подготовку представленных материалов. Лицам, оказавшим только техническую помощь, можно выразить благодарность в конце статьи. Один человек может быть автором (соавтором) не более чем двух статей в одном номере журнала, причем единственным автором он может быть только в одной статье.

3. Объем публикаций для научных статей должен быть не менее 8 страниц, а количество источников в библиографическом списке (списке литературы) – не менее 10 позиций.

4. Содержание каждой статьи должно включать следующие элементы: УДК; название статьи; сведения об авторах, включая их место работы, должность, адрес электронной почты; аннотацию объемом от 100 до 250 слов, ключевые слова (от 9 до 13); графическую аннотацию, отражающую содержание статьи; название статьи, сведения об авторах, аннотацию и ключевые слова на английском языке (для англоязычных статей – на русском языке); введение – оно должно заканчиваться формулировкой цели работы в явной форме; собственно текст статьи – очень желательна его сегментация на разделы, имеющие содержательные заголовки; выводы или за- ключение (должны соответствовать формулировке цели статьи).

5. Для русскоязычных статей приводится два библиографических списка: на языке оригинала статьи; список с транслитерацией русскоязычных источников на латиницу и (дополнительно) приведением в квадратных скобках переводов названий статей и названий источников на английский язык.

В «русскоязычном» библиографическом списке (списке литературы) порядок следования источников – по алфавиту фамилий авторов (сначала русскоязычные источники, потом иноязычные). На все источники, включенные в библиографический список, должны быть даны ссылки в тексте статьи в квадратных скобках. При необходимости авторы могут указывать номера страниц в источниках, на которые даются ссылки. Приветствуются ссылки на иноязычные источники, а также на материалы, опубликованные ранее в журнале «Прикаспийский журнал: управление и высокие технологии». Однако в последнем случае количество таких ссылок не должно превышать 20 % от общего количества источников, включенных в библиографический список. Для источников, имеющих DOI, целесообразно его указывать. При ссылках на статьи, опубликованные в журнале «Прикаспийский журнал: управление и высокие технологии», целесообразно в конце библиографического описания источника в круглых скобках указывать гиперссылку, указывающую на место размещения статьи на страничке сайта Астраханского государственного университета имени В. Н. Татищева.

Ссылки в библиографическом списке на материалы, размещенные в интернете, допускаются при соблюдении следующих условий: если у материала, на который дается ссылка, имеется автор и/или название, то они должны быть указаны для этого источника; должен быть приведен полный маршрут доступа к источнику в интернете; должна быть указана дата обращения (доступа) к источнику.

Ограничения по списку литературы: доля самоцитирований для любого из авторов статьи, а также по совокупности всех авторов статьи, не должна превышать 25 %; доля ссылок на статьи с участием одного автора, не являющегося автором (соавтором) статьи, не должна превышать 25 %.

6. Суммарная доля таблиц и иллюстраций в общем объеме представляемой статьи не должна превышать 40 %. Под иллюстрациями понимаются следующие объекты: диаграммы; графики; рисунки; эскизы; фотографии; карты и т.п.

7. Доля оригинального текста в статьях (оцениваемого через систему «Антиплагиат» на сайте www.antiplagiat.ru) должна быть не менее 80 %.

8. Указание на то, что работа финансируется по какому-либо гранту, в рамках Федеральной целевой программы, государственного заказа и пр. дается в виде постраничной сноски после заголовка (названия) работы.

9. В сведения об авторах работ помимо места работы и должности целесообразно включать ORCID автора и гиперссылку на страничку с его личными наукометрическими показателями на сайте www.elibrary.ru. По желанию можно привести также ссылки на странички с наукометрическими показателями на Scopus, в ResearchGate; на личную страничку, размещенную на сайте организации.

10. Основные технические требования к оформлению статей (материалов):

10.1. Текст должен быть расположен по ширине страницы формата А4 с учётом полей (все поля по 2,5 см), набран шрифтом Times New Roman, кегль 10, межстрочный интервал 1,0. В таблицах, подрисуночных надписях допускается уменьшенный шрифт – вплоть до 8 кегля. Альбомная ориентация страниц допускается только в порядке исключения для следующих случаев: широкоформатные таблицы с большим количеством колонок; иллюстрации большого размера, которые не умещаются на странице с книжной ориентацией.

Абзацные отступы одинаковы по всему тексту – 0,75 см. Кавычки («»), скобки ([ ], ( )), маркеры и другие знаки должны быть аналогичными на протяжении всего предоставляемого для публикации материала.

Прикаспийский журнал: управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2022
№ 3 (59)

Свидетельство о регистрации средства массовой информации
Федеральной службы по надзору в сфере массовых коммуникаций,
связи и охраны культурного наследия
ПИ № ФС77-31932 от 16 мая 2008 г.

Учредитель
Астраханский государственный университет имени В.Н. Татищева
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Адрес редакции:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20

Адрес издателя:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Издание включено в Интернет-каталог
ООО «Агентство «Книга-Сервис» 2022/1

Редактирование,
компьютерная правка, верстка *Н.Н. Сахно*

Дата выхода в свет 10.10.2022 г.

Цена свободная
Уч.-изд. 10,8. Усл. печ. л. 15,1.
Заказ № 4464. Тираж 500 экз. (первый завод – 23 экз.)

Астраханский государственный университет имени В. Н. Татищева
414056, г. Астрахань, ул. Татищева, 20а Тел. (8512) 24-64-95, тел./факс (8512) 24-68-37
E-mail: asupress@yandex.ru