

Международный журнал
информационных технологий
и энергоэффективности |



Том 9 Номер 4 (42)



2024



СОДЕРЖАНИЕ / CONTENT

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

-
- | | | |
|----|---|-----------|
| 1. | Денисов Д.В. Анализ методов машинного обучения для тематической классификации текстов | 5 |
| | Denisov D.V. Analysis of machine learning methods for thematic classification of texts | |
| 2. | Лисин И.С. Основные подходы к автоматизации систем массового обслуживания | 12 |
| | Lisin I.S. The main approaches to automation of queuing systems | |
| 3. | Смирнов А.Д., Хасанов Р.Х. Разработка распределенной системы на основе модели MAPREDUCE в кластере KUBERNETES | 21 |
| | Smirnov A.D., Khasanov R.H. Development of distributed system based on MAPREDUCE model in KUBERNETES cluster | |
| 4. | Калашников А.С. Особенности разработки WEB-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении | 27 |
| | Kalashnikov A.S. Features of the development of a WEB application for automated accounting of students' activities in an educational institution | |
| 5. | Бакай Ю.О., Карташевский И.В. Исследование систем моделирования для туманных вычислений: особенности, преимущества и недостатки | 37 |
| | Bakai Yu.O., Kartashevsky I.V. Research of modeling systems for foggy computing: features, advantages and disadvantages | |
| 6. | Кириллина Ю.В., Курнаков К.А. Реинжиниринг бизнес-процесса «Организация премирования основного персонала» на примере аптечной организации | 44 |
| | Kirillina Yu.V., Kurnakov K.A. Reengineering of the business process "Organization of bonuses for key personnel" on the example of a pharmacy organization | |
| 7. | Куликова А.В., Богословский Ф.И. Анализ цифровых следов и средств расследования в области киберпреступности | 56 |
| | Kulikova A.V., Bogoslovsky F.I. Analysis of digital traces and investigative tools in the field of cybercrime | |
-

8.	Кириллина Ю.В., Курнаков К.А. Информационное обеспечение бизнес-процесса «Организация премирования основного персонала» на примере аптечной организации	63
	Kirillina Yu.V., Kurnakov K.A. Information support of the business process "Organization of bonuses for key personnel" on the example of a pharmacy organization	
9.	Перевертун Д.Р. Ассемблер: искусство программирования у самых основ	73
	Perevertun D.R. Assembler: the art of programming at the very basics	
10.	Школьников П.Н., Белоусов А.В. Управление строительством крупных промышленных объектов с применением интегрированных информационных систем	79
	Shkolnikov P.N., Belousov A.V. Construction management of large industrial facilities using integrated information systems	
11.	Перевертун Д.Р. Вирусы программного обеспечения и меры обеспечения безопасности	84
	Perevertun D.R. Software viruses and security measures	
12.	Гельфанд А.М., Кузнецов С.А., Анучин К.Н. Совершенствование защиты от социальных атак в области информационной безопасности	89
	Gelfand A. M., Kuznetsov S. A., Anuchin K. N. Improving protection against social attacks in the field of information security	
13.	Перевертун Д.Р. Психологические аспекты кибербезопасности	95
	Perevertun D.R. Psychological aspects of cybersecurity	
14.	Смирнов А.А., Черенков А.В., Подольский Е.А. Сравнительный анализ сред исполнения JAVASCRIPT КОДА NODE.JS, DENO и BUN для разработки серверной части ВЕБ-приложения	100
	Smirnov A.A., Cherenkov A.V., Podolsky E.A. Comparative analysis of the JAVASCRIPT CODE EXECUTION ENVIRONMENTS OF NODE.JS, DEMO and BAN for developing the backend of a WEB application	
15.	Денисов Н.А. Методика разработки и внедрения защитных протоколов для IoT устройств с учетом распространенных уязвимостей	107
	Denisov N.A. Methodology for development and implementation of security protocols for IoT devices, considering common vulnerabilities	
16.	Туманова И.В. Возможности применения языковой модели GPT-3.5 для обучения русскому языку студентов системы СПО	115
	Tumanova I.V. The possibilities of using the GPT-3.5 language model for teaching russian to students of the educational system	
17.	Вахрушев А.В. Системный подход в качестве надежности информационных систем	120
	Vakhrushev A.V. A systematic approach to the reliability of information systems	
18.	Гергедава Д.А. Анализ эффективности алгоритма муравьиной колонии в задаче маршрутизации транспортных средств с ограниченной вместимостью	128

	Gergedava D.A. Analysis of the ant colony algorithm's efficiency in the capacity vehicle routing problem	
19.	Друзьяка Д.В. Цифровые технологии в управлении жилищно-коммунальным хозяйством	138
	Druzyaka D.V. Digital technologies in housing and communal services management	
20.	Балашов О.В., Букачев Д.С. Способ формализации целей и задач организационно-технических систем	143
	Balashov O.V., Bukachev D.S. A way to formalize the goals and objectives of organizational and technical systems	
21.	Удальцов К.Р. Алгоритмы и структуры данных: основы для начинающих программистов	152
	Udaltsov K.R. Algorithms and data structures: basics for beginner programmers	
22.	Урамбеков Э.Б. Разработка модели функции фазоманипулированного сигнала для улучшения разрешающей способности БРЛС (бортовая радиолокационная станция)	156
	Urambekov E.B. Development of a phase-manipulated signal function model to improve radar resolution	
23.	Гулин М.С., Куркин А.А., Кулагин А.Л., Кузмичёв В.А., Капустин А.Г. Анализ аэродинамических показателей гоночного автомобиля класса Formula Student	163
	Gulin M.S., Kurkin A.A., Kulagin A.L., Kuzmichev V.A., Kapustin A.G. Analysis of aerodynamic parameters of a Formula Student class racing car	



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.8

АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ТЕМАТИЧЕСКОЙ КЛАССИФИКАЦИИ ТЕКСТОВ

Денисов Д.В.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ "МИСИС", Москва, Россия (119049, город Москва, Ленинский пр-кт, д. 4стр1), e-mail: m2205669@edu.misis.ru

В контексте растущего объема информации в цифровом пространстве, анализ и обработка текстовых данных приобретают стратегическое значение для корпоративных структур и академических групп. Сегодня текстовые данные оказывают неоспоримое влияние на процессы принятия решений, автоматизацию и стимулирование внедрения инноваций в различных отраслях. В статье приводится использование и оценка современных методов обработки и классификации текстов в базе знаний для выявления их тематической направленности.

Ключевые слова: Классификация, машинное обучение, классификация текста, анализ естественного языка, предобработка текста.

ANALYSIS OF MACHINE LEARNING METHODS FOR THEMATIC CLASSIFICATION OF TEXTS

Denisov D.V.

NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY "MISIS", Moscow, Russia (119049, Moscow, Leninsky Ave., 4bldg1), e-mail: m2205669@edu.misis.ru

In the context of the growing volume of information in the digital space, the analysis and processing of textual data is becoming strategically important for corporate structures and academic groups. Today, text data has an undeniable impact on decision making, automation, and driving innovation across industries. The article describes the use and evaluation of modern methods for processing and classifying texts in a knowledge base to identify their thematic focus.

Keywords: Classification, machine learning, text classification, natural language analysis, text preprocessing.

Введение

Алгоритмы машинного обучения не могут работать с текстом на естественном языке и для работы с ним нужна предварительная обработка, результатом которой является получение набора признаков [1]. Признаки в текстовых данных представляют собой характеристики текста, которые могут быть использованы для его классификации. Как правило, признаки извлекаются из текста с помощью различных методов обработки естественного языка (Natural Language Processing, NLP). Эти методы могут включать в себя токенизацию, лемматизацию, удаление стоп-слов, выделение ключевых слов и фраз, выделение частей речи и т.д.

Полученные признаки могут быть как качественными (например, наличие определенного слова или фразы), так и количественными (например, частота встречаемости слова в тексте).

Классификация — это контролируемая задача в машинном обучении, цель которой — изучить сопоставление входных объектов с выходными метками на основе набора обучающих данных. Задача классификации — это задача отнесения объекта к одному из заранее определенных классов на основании его формализованных признаков. Каждый из объектов в этой задаче представляется в виде вектора в N -мерном пространстве, каждое измерение в котором представляет собой описание одного из признаков объекта.

В области машинного обучения, задача классификации относится к категории обучения с учителем, где объекты обучающей выборки разделены на заранее определенные классы.

Методы классификации позволяют получить вероятностные характеристики для системы поддержки принятия решений. Модель классификации могут сформировать такие методы как: логистическая регрессия, дерево решений, метод опорных векторов, k -ближайших соседей, наивный байесовский метод, случайный лес, нейронные сети и т. д.

Данная статья представляет собой анализ применения и результатов использования алгоритмов машинного обучения для классификации текстов.

Предварительная обработка текстовых данных

На начальном этапе анализа текстовые данные часто состоят из разнообразных элементов, которые могут препятствовать структурированному представлению информации. Этот этап предварительной обработки включает в себя удаление нежелательных компонентов, включая теги HTML, специальные символы, числовые значения, а также стандартизацию текста посредством преобразования регистра и других манипуляций, направленных на приведение текстовых данных к более чистой форме для последующего анализа.

После процесса очистки данных текст необходимо преобразовать в набор отдельных компонентов, известных как токены. Это подразумевает сегментирование текста на отдельные слова, символы или фразы, которые затем можно использовать для последующего анализа. Каждый токен служит независимой элементарной единицей текста, облегчающей дальнейший анализ.

При токенизации текст подвергается процедуре, направленной на удаление формы из слова и связанной с ним информации. Этот процесс, называемый лемматизацией, преобразует слова в их базовые формы, позволяя проводить анализ, основанный на их внутреннем значении. В качестве альтернативного решения также применяется стемминг, который предполагает сокращение слов до их корня (стема), игнорируя лингвистические нюансы и семантическое содержание.

Многие системы классификации текста используют несколько простых методов предварительной обработки, таких как преобразование прописных букв в строчные и удаление стоп-слов. Однако большинство систем не используют все доступные методы предварительной обработки, и исследователи полагают, что некоторые методы могут фактически оказать негативное влияние на результаты классификации. Например, исследование Формана по метрикам выбора функций для классификации текстов [2] предполагает, что стоп-слова из-за их неоднозначной природы и частого появления не обладают различительной способностью для какого-либо конкретного класса. И наоборот, ХаКоэн-Кернер и др. [3] показали, что включение словесных униграмм, содержащих стоп-

слова, в сферу ивритско-арамейских юридических документов приводит к улучшению результатов классификации по сравнению с результатами, полученными при исключении стоп-слов из словесных униграмм».

Использование текста в качестве данных для моделей машинного обучения как правило требует преобразования его в числовые признаки. Для этого используются различные методы, такие как "мешок слов", TF-IDF (term frequency-inverse document frequency), word embeddings.

Процесс векторизации текста "мешок слов" заключается в том, что каждое уникальное слово в тексте кодируется в виде отдельной размерности вектора, а сам текст формируется в виде вектора, где каждая размерность соответствует количеству употреблений соответствующего слова в тексте [4]. Таким образом, каждый текст представляется в виде вектора фиксированной длины, где каждая размерность соответствует отдельному слову из словаря. Одним из основных применений этого метода является построение моделей машинного обучения. Также этот метод может быть использован для анализа тональности текста, определения тематики текста и автоматического реферирования.

К преимуществам метода векторизации текста "мешок слов" относятся его простота и универсальность. Данный подход не требует сложных вычислений и может быть применен к любому тексту независимо от его содержания и структуры. Кроме того, этот метод позволяет эффективно работать с большими объемами текстовой информации.

Процесс векторизации текста с использованием метода TF-IDF начинается с подсчета частоты встречаемости каждого слова в каждом документе коллекции. Затем вычисляется обратная частота встречаемости слова во всех документах коллекции. Итоговый вектор для каждого документа представляет собой комбинацию значений TF и IDF для каждого слова, присутствующего в документе. TF (Term Frequency) отражает частоту встречаемости слова в документе и вычисляется как отношение числа вхождений слова к общему числу слов в документе. IDF (Inverse Document Frequency) отражает уникальность слова и вычисляется как логарифм отношения общего числа документов к числу документов, содержащих данное слово.

Метод TF-IDF позволяет выделить ключевые слова и фразы в тексте, учитывая их значимость и уникальность для каждого документа. Это делает его полезным инструментом для решения задач анализа текстовых данных, таких как поиск информации, категоризация документов, автоматическое извлечение ключевых слов и тематическое моделирование. Кроме того, метод TF-IDF может быть использован для оценки сходства между текстовыми документами, что позволяет проводить поиск и кластеризацию документов на основе их содержания.

Таким образом были рассмотрены методы предварительной обработки текстовых данных и методы создания признаков для моделей машинного обучения, особенности их применения, сильные и слабые стороны.

Методы классификации текстовых данных

Логистическая регрессия — это статистический метод, используемый для моделирования взаимосвязи между бинарной зависимой переменной и одной или несколькими независимыми переменными. Независимые переменные, также известные как предикторы или признаки, могут быть непрерывными, категориальными или сочетанием того и другого. Логистическая функция преобразует любое действительное число в диапазон $[0, 1]$,

что делает его пригодным для моделирования вероятностей. К положительным сторонам алгоритма можно отнести в простоте интерпретации результатов. К недостаткам – линейное влияние признаков на независимую переменную и требование, чтобы каждая точка данных была независимой [5].

Дерево решений представляет собой прозрачный механизм, который позволяет пользователям легко следить за древовидной структурой и видеть, как принимается решение. Это структура, подобная блок-схеме, в которой каждый внутренний узел представляет проверку атрибута, каждая ветвь представляет результат проверки, а каждый лиственный узел представляет метку класса или числовое значение. Обычно все алгоритмы дерева решений строятся в два этапа:

- рост дерева, в котором обучающий набор, основанный на локальных оптимальных критериях, рекурсивно разбивается до тех пор, пока большая часть записей, принадлежащих разделу, не будет иметь одну и ту же метку класса;
- обрезка дерева, в котором размер дерева уменьшен, что облегчает понимание.

Деревья решений популярны благодаря своей интерпретируемости, поскольку их можно легко визуализировать.

Метод опорных векторов — это мощный и универсальный алгоритм, который особенно эффективен в многомерных пространствах. SVM работает путем поиска гиперплоскости, которая лучше всего разделяет классы в пространстве объектов, с целью максимизировать разницу между классами. Опорные вектора — это точки данных, которые лежат ближе всего к поверхности решения [6]. Основным преимуществом SVM является его способность решать широкий спектр задач классификации, включая задачи большой размерности, которые не являются линейно разделимыми. Одним из основных недостатков SVM является то, что для достижения отличных результатов классификации требуется правильная установка ряда ключевых параметров.

В методе *K-ближайших соседей* (KNN) ближайший сосед измеряется относительно значения k , которое определяет, сколько ближайших соседей необходимо проверить, чтобы описать класс выборки точки данных. Одним из основных преимуществ метода KNN является то, что он эффективен для больших обучающих данных и устойчив к зашумленным обучающим данным.

Наивный байесовский метод - алгоритм вероятностной классификации, основанный на теореме Байеса с «наивным» предположением о независимости между признаками. Он часто используется в классификации текста, фильтрации спама и системах рекомендаций. Наивный алгоритм Байеса основан на самоопределяющихся предположениях. Эти гипотезы явно во многом реализуются в NLP с различными вариациями, обеспечивающим текстовую, семантическую, синтаксическую и рациональную схему [7]. К положительным сторонам относится простота интерпретации, возможность использовать большие выборки и проводить мультиклассовую классификацию. К недостаткам относится то, что не всегда выполняется предположение о независимости характеристик.

Сравнение и анализ алгоритмов

В данной работе использовались следующие, реализованные на языке программирования Python, алгоритмы: дополняющий наивный байесовский классификатор, метод опорных векторов, дерево решений, случайный лес, логистическая регрессия.

В качестве набора данных выступали вопросы и ответы, взятые из базы знаний и предобработанные с использованием мешка слов и TF-IDF.

В качестве зависимой переменной рассматривался идентификационный номер тематики в базе знаний. В качестве метрики оценки качества классификации рассматривались метрики матрицы ошибок: Accuracy, Precision, Recall и F1-Score.

Оценка качества классификации номера сообщества при использовании мешка слов представлена в Таблице 1.

Таблица 1 – Результаты классификации при использовании метода "Мешок слов"

Метрики/ Методы	Accuracy	Precision	Recall	F1
Logistic Regression	0.90	0.90	0.90	0.89
kNN	0.75	0.80	0.75	0.76
Random Forest	0.70	0.68	0.70	0.65
Complement naive Bayes	0.84	0.85	0.84	0.87
SVM	0.87	0.88	0.87	0.87

Как видно по результатам, было определено несколько методов, чье значение метрик качества классификации превышает 0.85. К ним относятся метод опорных векторов и дополняющий наивный байесовский классификатор. При этом наилучшие результаты были получены с использованием логистической регрессии

Оценка качества классификации номера сообщества при использовании TF-IDF представлена в Таблице 2.

Таблица 2 – Результаты классификации при использовании метода "TF-IDF"

Метрики/ Методы	Accuracy	Precision	Recall	F1
Logistic Regression	0.75	0.72	0.75	0.70
kNN	0.62	0.88	0.62	0.68
Random Forest	0.63	0.60	0.63	0.55
Complement naive Bayes	0.87	0.87	0.87	0.86

SVM	0.84	0.84	0.84	0.82
-----	------	------	------	------

В сравнении с “Мешком слов” использование TF-IDF позволило получить как менее значительные показатели как точности, так и полноты. При этом методами, показавшими лучший результат, являются метод опорных векторов и дополняющий наивный байесовский классификатор, которые получили результаты, идентичные использованию метода “Мешок слов”.

Таким образом были определены методы классификации, позволяющие получить более точный и полный результат при использовании различных методов предобработки текстовых данных.

Список литературы

1. Акжолов Р.К., Верига А.В. ПРЕДОБРАБОТКА ТЕКСТА ДЛЯ РЕШЕНИЯ ЗАДАЧ NLP// Вестник науки. 2020. №3 (24). URL: <https://cyberleninka.ru/article/n/predobrabotka-teksta-dlya-resheniya-zadach-nlp> (дата обращения: 11.11.2023)
2. HaCohen-Kerner Y., Rosenfeld A., Sabag A., & Tzidkani M. Topic-based classification through unigram unmasking. *Procedia Computer Science*, - 2018. 126, pp. 69–76.
3. Song F., Liu S., & Yang J. A comparative study on text representation schemes in text categorization. *Pattern analysis and applications*. – 2021. 8(1–2), pp. 199–209.
4. Sebastiani F. Machine learning in automated text categorization. *ACM computing surveys (CSUR)*. – 2002. 34(1), pp. 1–47.
5. Huang, K. Unconstrained Smartphone Sensing and Empirical Study for Sleep Monitoring and Self-Management. Ph.D. Thesis, University of Massachusetts Lowell. - 2015.
6. Y. Ke, M. Hagiwara, An English neural network that learns texts, finds hidden knowledge, and answers questions, *J. Artif. Intell. Soft Comput. Res.*, 7 (4) (2017), pp. 229-242
7. S. Vijayarani, M.J. Ilamathi, M. Nithya, Preprocessing techniques for text mining-an overview *Int. J. Comput. Sci. Commun. Networks*, 5 (1) (2015), pp. 7-16

References

1. Akzholov R.K., Veriga A.V. TEXT PREPROCESSING FOR SOLVING NLP PROBLEMS. 2020. №3 (24). URL: <https://cyberleninka.ru/article/n/predobrabotka-teksta-dlya-resheniya-zadach-nlp> (accessed: 11.11.2023)
2. HaCohen-Kerner Y., Rosenfeld A., Sabag A., & Tzidkani M. Topic-based classification through unigram unmasking. *Procedia Computer Science*, - 2018. 126, pp. 69–76.
3. Song F., Liu S., & Yang J. A comparative study on text representation schemes in text categorization. *Pattern analysis and applications*. – 2021. 8(1–2), pp. 199–209.
4. Sebastiani F. Machine learning in automated text categorization. *ACM computing surveys (CSUR)*. – 2002. 34(1), pp. 1–47.
5. Huang, K. Unconstrained Smartphone Sensing and Empirical Study for Sleep Monitoring and Self-Management. Ph.D. Thesis, University of Massachusetts Lowell. - 2015.
6. Y. Ke, M. Hagiwara, An English neural network that learns texts, finds hidden knowledge, and answers questions, *J. Artif. Intell. Soft Comput. Res.*, 7 (4) (2017), pp. 229-242

7. S. Vijayarani, M.J. Pamathi, M. Nithya, Preprocessing techniques for text mining-an overview
Int. J. Comput. Sci. Commun. Networks, 5 (1) (2015), pp. 7-16
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

ОСНОВНЫЕ ПОДХОДЫ К АВТОМАТИЗАЦИИ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ

Лисин И.С.

ФГБОУ ВО "КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ", Казань, Россия (420015, Республика Татарстан, город Казань, ул. Карла Маркса, д.68), e-mail: lisin-igor@mail.ru

На сегодняшний день вопросы автоматизации самых различных систем обслуживания населения стоят остро и нуждаются в рассмотрении с разных сторон. Во-первых, организационный подход к массовому обслуживанию меняется слишком медленно, в то время как программы обеспечения разрабатываются и предоставляются на различных уровнях работы с населением. Во-вторых, подход к работе с электронной очередью существует во многих системах в условной форме, что мешает полному переоснащению и автоматизации учреждений. Цель работы – рассмотреть подходы к автоматизации систем массового обслуживания. Методы: обзор литературы, рассмотрение ключевых алгоритмов. В результате представлены предложения по оптимизации существующих подходов к автоматизации.

Ключевые слова: Автоматизация, подходы, организация обслуживания, система массового обслуживания, социальная сфера.

THE MAIN APPROACHES TO AUTOMATION OF QUEUING SYSTEMS

Lisin I.S.

KAZAN NATIONAL RESEARCH TECHNOLOGICAL UNIVERSITY, Kazan, Russia (420015, Republic of Tatarstan, Kazan, Karl Marx st., 68), e-mail: lisin-igor@mail.ru

Today, the issues of automation of various public service systems are acute and need to be considered from different sides. Firstly, the organizational approach to mass service is changing too slowly, while support programs are being developed and provided at various levels of work with the population. Secondly, the approach to working with the electronic queue exists in many systems in a conditional form, which prevents the complete re-equipment and automation of institutions. The purpose of the work is to consider approaches to automation of queuing systems. Methods: literature review, consideration of key algorithms. As a result, proposals are presented to optimize existing approaches to automation.

Keywords: Automation, approaches, service organization, queuing system, social sphere.

Введение

Массовое обслуживание – это, с одной стороны, вопрос социального обеспечения и реализации автоматизации социальной сферы жизни общества. Но, с момента разработки первых алгоритмов успешного формирования электронных записей регистрации и обслуживания, данное направление перешло в область прикладной математики [10. С. 391-405].

Как результат, на сегодняшний день теория массового обслуживания успешно смоделировала пропускную способность в различных отраслях, в том числе в отделениях неотложной помощи, отелях, социальных службах и даже в ресторанах быстрого питания.

Однако, в современной России существует ряд препятствий к полноценному переходу на автоматическую систему массового обслуживания. Во-первых, разный возраст контингента определяет степень просвещенности в вопросах использования автоматических систем. Во-вторых, сам персонал не во всех учреждениях готов к работе с автоматическими системами регистрации, создания электронной очереди и т.д. В-третьих, во многих учреждениях продолжают работать в рамках живой очереди и прямого обслуживания, что обусловлено отсутствием и/или неработоспособностью оборудования. Но с другой стороны, разработка программного обеспечения, моделирование новых систем обслуживания и работы с массовым потребителем говорят о том, что данное направление актуально и востребовано.

Цель работы – рассмотреть подходы к автоматизации систем массового обслуживания.

Методы:

В рамках обзора литературы проведен анализ истории развития подходов к массовому обслуживанию и рассмотрены современные идеи в данном направлении.

Рассмотрение ключевых алгоритмов позволяет сделать вывод, что современные разработчики стремятся оптимизировать систему массового обслуживания с целью ее распространения и закрепления в массах, которые и являются непосредственными пользователями и в перспективе именно их потребности будут определять дальнейшее развитие автоматизации социальной сферы.

Анализ литературы

Начиная с второй половины XX века, когда встал вопрос оптимизации системы обслуживания населения, различные исследователи увидели в этом возможность развития автоматических процессов, которые только стали появляться в Европе, затем в США и Азии. В России система массового обслуживания в рамках похода математических процессов и алгоритмов появилась только в конце XX века, что обусловило отставание от других стран [8. С. 563-572].

В то же время, за рассмотренный период было изучено несколько подходов, главным из которых были случайные процессы, стройная очередь и мультиплексирования. Данные подходы, к 80-м годам XX века привели к использованию дифференциальных уравнений, характеризующих стационарное распределение занятости буфера [6. С. 131-136]. Но уже в 90-х годах XX века ориентация разработчиков была направлена на развитие понятия эффективной полосы пропускания и связанных с ним методов контроля доступа. Последующие годы шли активные споры и разработки в области моделирования и практического применения новых теорий, но все они сводились к вычислению возможностей по приему граждан в тех или иных учреждениях [7. С. 1889-1904].

В начале 2000-ных анализ системы массового обслуживания стали проводить с опорой на подход фиксированного (детерминированного) времени прибытия, в результате чего сам процесс обслуживания стал легче и перестал представлять затруднения с распределением пациентов/гостей отелей/ нуждающихся в социальной поддержке и т.д. [1, 9]

Как результат исследователи рассматривали модели или системы, в которых одно или оба фактора (время между поступлениями и обслуживанием) являются стохастическими. Их

анализ, как правило включал стохастическое описание системы и связанные с ней показатели производительности, следующим образом:

1. Распределение числа $N(t)$ в системе в момент времени t (число в очереди и обслуживаемое, если таковое имеется). $N(t)$ также называется длиной очереди системы в момент времени t . Под количеством в системе (очереди) разработчики стали понимать количество клиентов в системе (очереди).

2. Распределение времени ожидания в очереди (в системе), времени, которое пришедший должен ожидать в очереди (оставаться в системе). Если W_n обозначает время ожидания n -го прибытия, то интерес представляет распределение W_n .

3. Распределение виртуального времени ожидания $W(t)$ — время ожидания прибывшего, если бы он прибыл в момент t .

4. Распределение периода занятости — это продолжительность времени, в течение которого сервер остается занятым. Период занятости — это интервал от момента прихода объекта в пустую систему до момента, когда канал впервые становится свободным. Период занятости является случайной величиной.[4]

В данный период исследователи акцентировали свое внимание на показателях производительности [11. С. 322-338]. А ключевыми проблемами и подходами к автоматизации массового обслуживания стали следующие:

1. Стохастическое поведение различных случайных величин или возникающих случайных процессов и оценка соответствующих показателей эффективности;

2. Методы решения — точный, преобразованный, алгоритмический, асимптотический, численный, аппроксимационный и т. д.;

3. Характер решения — зависящий от времени, предельная форма и т. д.;

4. Управление и проектирование очередей — сравнение поведения и производительности в различных ситуациях, а также дисциплины очереди, правил обслуживания, стратегий и т. д.;

5. Оптимизация конкретных целевых функций, включающих показатели производительности, связанные с ними функции затрат и т. д. [15. С. 1945-1951].

В результате изучения вышеперечисленных проблем исследования в области управления массовым обслуживанием выявили три важные аспекта реализации разработанных проектов:

- моделирование (как процесс подбора оптимального алгоритма);
- согласование инфраструктуры (система распространения знаний и представлений об атомической системе и возможности ее применения и использования);
- логика процедурного субъекта (адресация разработки)[5. С.1-18].

Эти аспекты отражают доминирующие способы мышления в системе автоматизации массового обслуживания, отраженные в разрабатываемых предположениях, практиках применения тех или иных алгоритмов и значимости их реализации. Последнее так же определится простотой применения и доступностью самым неосведомленным группам. В данном контексте необходимо отметить, что ряд исследователей, изучая данные положения пришли к мнению, что применимость этих основополагающих допущений при теоретизировании система массового обеспечения нуждается в пересмотре в контексте цифровой трансформации [2. С. 692-695].

Основываясь на исследованиях, проведенных в отдельных компаниях и медицинских учреждениях, переживающих цифровую трансформацию, исследователи выявили

противоречия, связанные с применением перечисленных выше аспектов, которые указывают на необходимость обновления лежащих в их основе предположений. Как результат, А. Байере, Х. Салмела и Т. Тапанайнен предлагают новую концепцию автоматизации описывая ее как процессы легкого касания (минимального использования труда человека), гибкость инфраструктуры (удаленного доступа) и внимательные участники (ориентация на современных пользователей) [3. С.1-23].

Сегодня исследователи опираются на уравнения массового обслуживания и моделируют потребность в различных процессах внутри обслуживания пациентов/туристов/уязвимых категорий граждан и помогают учитывать влияние изменчивости на задержки и время обслуживания [16. С.373-390]. Изменчивость — это мера производительности процесса относительно спроса, которая обеспечивает быстрый способ сравнения спроса на определенные ресурсы [14. С.120-140].

Но, несмотря на некоторые значительные успехи в применении теории массового обслуживания к различным отраслям социального обеспечения, эта область по-прежнему недостаточно используется в операциях, осуществляемых социальными учреждениями в различных городах РФ.

Результаты

На сегодняшний день работа с большими данными – залог успешной автоматизации самых различных процессов. И безусловно, постепенно некоторые управленческие решения уже сегодня оказываются в сфере работы ИИ, поскольку выполняемые задачи включают аналитическую и рациональную обработку знаний. Как результат, на сегодняшний день перед разработчиками стоит принцип совместной оптимизации социальных и технических компонентов рабочих систем, который актуален сегодня так же, как и на заре проектирования социотехнических систем [13. С. 114-122].

Для разработки оптимальных предложений по внедрению программного обеспечения в рамках автоматизации системы социального обслуживания можно рассмотреть сравнительную таблицу влияния ИИ на реализацию социально-значимых решений (Таблица 1) [12. С. 1171-1204]

Таблица 1 – Влияние искусственного интеллекта, роботов, алгоритмов и других современных технологий на ключевые аспекты реализации социального обслуживания

Тип работы	Положительные эффекты	Отрицательные эффекты	Требования к соц.работникам
Контроль рабочих процессов	Локализация принятия решений в результате более широкого распространения информации	Замена человеческого суждения. Возможность полной потери контроля со стороны человека	Наличие навыков работы с ИТ, образование, технологическая самоэффективность, возраст
Автоназначение/поиск места в очереди	Виртуальная/удаленная и другие формы гибкой работы с поддержкой технологий.	Алгоритмическое управление, которое оказывает давление на работников относительно того, когда и сколько им работать.	Адаптация под новые условия работы, учет и распространение информации о возможной удаленной регистрации и формирования места в очереди
Модель распределения оставшихся функций	<ul style="list-style-type: none"> • Замена рутинных когнитивных задач. Смена идеологии организации работы/управления • Участие сотрудников в разработке и внедрении технологий 	Автоматизация вызвала снижение активного использования навыков при усилении мониторинга	Степень вовлеченности сотрудников в процессы происходящие в организации определяют уровень активации ключевых алгоритмов и задач
Отзывы/оценки/система вопрос-ответ	Боты разгружают нагрузку с человека и реализуют алгоритмическое управление и предоставление «объективной» обратной связи	Ухудшает ситуационную осведомленность. Может привести к падению уровня знаний работников	Повышение квалификации и получение актуальных профессиональных знаний в рамках выполняемой работы

Как видно из данных Таблицы 1, на сегодняшний день, в сфере социального обслуживания прослеживается как положительный, так и отрицательный опыт применения различных функций ИИ и алгоритмов в рамках работы с людьми. Однако, такое положение

сохраняется преимущественно в РФ, в то время, как в странах Запада и Азии автоматизация социальной сферы охватывает широкий перечень выполняемых работ. И проблемы, которые обозначены, как возможная утрата контроля со стороны человека, в более развитых странах уже решена. Деятельность человека перенаправлена на продуктивное взаимодействие с ИИ, что потребовало от сотрудников социально ориентированных организаций провести мониторинг собственной производительности, пройти курсы повышения квалификации и ряд практических курсов по наработке навыков работы с новыми алгоритмами обслуживания, приема и распределения пациентов/гостей отеля/нуждающихся категорий населения и проч.

Заключение

На протяжении второй половины XX века система обслуживания в социальной сфере трансформировалась из непосредственной работы с людьми в возможность предоставления качественных услуг на основе современных технологий. В конце XX века социальное обслуживание оказалось в сфере математического моделирования, и за 80-90-е годы XX века исследователи стремились оптимизировать подход к разработке уравнений массового обслуживания. Это привело к тому, что в XXI в. в основе разрабатываемых алгоритмов оказались вопросы приема, распределения и возможностей быстрого обслуживания. Как результат, зарубежные ученые и сегодня моделируют потребности людей, которые будут обращаться в социально ориентированную службу. В то время как в РФ стремятся полноценно внедрить автоматизацию в сферу обслуживания населения и если частные отели и различного рода компании, работающие с различными категориями граждан успешно переходят на предлагаемые им программы, то в медицинских учреждениях, социально направленных службах прослеживается отставание.

Следовательно, можно выдвинуть несколько предложений:

- заинтересованность в автоматизации должна исходить не только от государства, но и от руководства и сотрудников, следовательно, последних необходимо обучить и указать на возможности снижения трудовой нагрузки;
- внедрение технологий не означает сокращение штата сотрудников, но подразумевает качественный переход на новый уровень сотрудничества, следовательно, руководители так же должны быть готовы к переменам в системе принятия решений и их последующей реализации;
- ориентация на потребности населения должна быть понятной и доступной самому населению, что определит уровень востребованности.

Но, данные предложения носят рекомендательный характер и предполагают, что учреждение, обращенное к системе массового обслуживания населения имеет достаточное техническое оснащения для полноценного перехода к автоматизации процессов.

Список литературы

1. Akhavian R. Behzadan A. H. Evaluation of queuing systems for knowledge-based simulation of construction processes// *Automation in Construction*. 2014. №47. pp. 37-49. doi: 10.1016/j.autcon.2014.07.007
2. Alexeev V., Domashnev P. Development of an Approach to Implement an Electronic Queue System with Multi-Stage Customer Service// *IEEE transactions on automatic control* iee transactions on automatic control. 2020. №79. pp. 692-695. doi: 10.1109/SUMMA50634.2020.9280579.
3. Baiyere A., Salmela H., Tapanainen T. Digital transformation and the new logics of business process management// *European journal of information systems*. 2020. №8. pp. 1-23. doi: 10.1080/0960085X.2020.1718007
4. Boiko A., Shendryk V.V. Stages of information system development in the process approach// *Procedia Computer Science*. 2015. № 77. P.365. doi: 10.1016/j.procs.2015.12.365
5. Chen C., Tiong R. L. K. Using queuing theory and simulated annealing to design the facility layout in an AGV-based modular manufacturing system// *International Journal of Production Research*. 2018. №57(12). P.1-18. DOI:10.1080/00207543.2018.1533654
6. Clemons E. K. Information systems for sustainable competitive advantage// *Information & Management*. 1986. №11. P.131-136. doi: 10.1016/0378-7206(86)90010-8
7. Dai J.G., Meyn, S.P. Stability and convergence of moments for multiclass queueing networks via fluid limit models// *IEEE transactions on automatic control*. 1995. №40. pp.1889-1904. doi: 10.1109/9.471210
8. Joseph JW. Queuing Theory and Modeling Emergency Department Resource Utilization// *Emergency Medicine Clinics of North America*. 2020. №38(3). pp.563-572. doi: 10.1016/j.emc.2020.04.006.
9. Katsman J. J., Apachidi X. N. Algorithm simulation of resource allocation of the queueing systems, based on the priorities// *IEEE transactions on automatic control*. 2014. №14. pp. 1-6, doi: 10.1109/MEACS.2014.6986896.
10. Kegoro, H., & Ochieng, J. Automated queuing system on performance of selected state-owned commercial entities in kenya: a conceptual paper// *International Journal of Research – Granthaalayah*. 2021. №9(9). pp.391–405. <https://doi.org/10.29121/granthaalayah.v9.i9.2021.4220>
11. May M. C., Albers A., Fischer M. D., Mayerhofer F., Schäfer Louis., Lanza G. Queue Length Forecasting in Complex Manufacturing Job Shops// *Forecasting*. 2021. №2. pp.322-338. doi: 10.3390/forecast3020021
12. Parke r S.K., Grote G. Automation, Algorithms, and Beyond: Why Work Design Matters More Than Ever in a Digital World// *Applied Psychology*. 2019. Volume 71, № 4. pp. 1171-1204. <https://doi.org/10.1111/apps.12241>
13. Peter O. P., Sivasamy R. Queueing theory techniques and its real applications to health care systems – Outpatient visits, *International Journal of Healthcare Management*. 2021. №14:1. P. 114-122, DOI: 10.1080/20479700.2019.1616890
14. Sreelatha K. S., Soorya S. D. Application of queuing theory to reduce waiting period at ATM using a simulated approach// *IOP Conference Series: Materials Science and Engineering*. 2021. №1145 (1). P.120—140. DOI:10.1088/1757-899X/1145/1/012041

15. Tarasov V. N., Bakhareva N. F. Analysis and Calculation of Queuing System with Delay// Automation and Remote Control. 2015. №76(11). pp.1945-1951
16. Xu J., Gautam N. Peak Age of Information in Priority Queuing Systems// IEEE Transactions on Information Theory. 2021. vol. 67, № 1, p. 373-390. doi: 10.1109/tit.2020.3033501

References

1. Akhavian R. Behzadan A. H. Evaluation of queuing systems for knowledge-based simulation of construction processes// Automation in Construction. 2014. №47. pp. 37-49. doi: 10.1016/j.autcon.2014.07.007
2. Alexeev V., Domashnev P. Development of an Approach to Implement an Electronic Queue System with Multi-Stage Customer Service// IEEE transactions on automatic control iee transactions on automatic control. 2020. №79. pp. 692-695. doi: 10.1109/SUMMA50634.2020.9280579.
3. Baiyere A., Salmela H., Tapanainen T. Digital transformation and the new logics of business process management// European journal of information systems. 2020. №8. pp. 1-23. doi: 10.1080/0960085X.2020.1718007
4. Boiko A., Shendryk V.V. Stages of information system development in the process approach// Procedia Computer Science. 2015. № 77. P.365. doi: 10.1016/j.procs.2015.12.365
5. Chen C., Tiong R. L. K. Using queuing theory and simulated annealing to design the facility layout in an AGV-based modular manufacturing system// International Journal of Production Research. 2018. №57(12). P.1-18. DOI:10.1080/00207543.2018.1533654
6. Clemons E. K. Information systems for sustainable competitive advantage// Information & Management. 1986. №11. P.131-136. doi: 10.1016/0378-7206(86)90010-8
7. Dai J.G., Meyn, S.P. Stability and convergence of moments for multiclass queueing networks via fluid limit models// IEEE transactions on automatic control. 1995. №40. pp.1889-1904. doi: 10.1109/9.471210
8. Joseph JW. Queuing Theory and Modeling Emergency Department Resource Utilization// Emergency Medicine Clinics of North America. 2020. №38(3). pp.563-572. doi: 10.1016/j.emc.2020.04.006.
9. Katsman J. J., Apachidi X. N. Algorithm simulation of resource allocation of the queueing systems, based on the priorities// IEEE transactions on automatic control. 2014. №14. pp. 1-6, doi: 10.1109/MEACS.2014.6986896.
10. Kegoro, H., & Ochieng, J. Automated queuing system on performance of selected state-owned commercial entities in kenya: a conceptual paper// International Journal of Research – Granthaalayah. 2021. №9(9). pp.391–405. <https://doi.org/10.29121/granthaalayah.v9.i9.2021.4220>
11. May M. C., Albers A., Fischer M. D., Mayerhofer F., Schäfer Louis., Lanza G. Queue Length Forecasting in Complex Manufacturing Job Shops// Forecasting. 2021. №2. pp.322-338. doi: 10.3390/forecast3020021
12. Parke r S.K., Grote G. Automation, Algorithms, and Beyond: Why Work Design Matters More Than Ever in a Digital World//Applied Psychology. 2019. Volume 71, № 4. pp. 1171-1204. <https://doi.org/10.1111/apps.12241>

13. Peter O. P., Sivasamy R. Queueing theory techniques and its real applications to health care systems – Outpatient visits, *International Journal of Healthcare Management*. 2021. №14:1. P. 114-122, DOI: 10.1080/20479700.2019.1616890
 14. Sreelatha K. S., Soorya S. D. Application of queuing theory to reduce waiting period at ATM using a simulated approach// *IOP Conference Series: Materials Science and Engineering*. 2021. №1145 (1). P.120—140. DOI:10.1088/1757-899X/1145/1/012041
 15. Tarasov V. N., Bakhareva N. F. Analysis and Calculation of Queuing System with Delay// *Automation and Remote Control*. 2015. №76(11). pp.1945-1951
 16. Xu J., Gautam N. Peak Age of Information in Priority Queuing Systems// *IEEE Transactions on Information Theory*. 2021. vol. 67, № 1, p. 373-390. doi: 10.1109/tit.2020.3033501
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.75

РАЗРАБОТКА РАСПРЕДЕЛЕННОЙ СИСТЕМЫ НА ОСНОВЕ МОДЕЛИ MAPREDUCE В КЛАСТЕРЕ KUBERNETES

Смирнов А.Д., ¹Хасанов Р.Х.

ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: ¹hasanov_ramazan@bk.ru

В данной статье рассматривается процесс разработки распределенной системы на основе модели MapReduce в кластере Kubernetes. Приведено описание основных компонент и общей архитектуры системы оркестрации контейнерными приложениями Kubernetes. Приведено описание модели распределенных вычислений MapReduce, ее основные этапы работы и использование во фреймворке для разработки распределенных вычислительных систем Apache Hadoop. Представлен процесс интеграции системы Apache Hadoop в кластер Kubernetes, что обеспечивает высокую масштабируемость, эффективность использования ресурсов и оптимизированное управление для обработки больших объемов данных.

Ключевые слова: Распределенные системы, кластер Kubernetes, модель MapReduce, фреймворк Apache Hadoop, микросервис, оркестрация.

DEVELOPMENT OF DISTRIBUTED SYSTEM BASED ON MAPREDUCE MODEL IN KUBERNETES CLUSTER

Smirnov A.D., ¹Khasanov R.H.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia (105005, Moscow, 2nd Baumanskaya str., 5/1), e-mail: ¹hasanov_ramazan@bk.ru

This paper discusses the process of developing a distributed system based on the MapReduce model in a Kubernetes cluster. The description of the main components and general architecture of the Kubernetes container application orchestration system is given. The description of the MapReduce distributed computing model, its main stages of operation and its use in Apache Hadoop distributed computing development framework is given. The process of integrating Apache Hadoop into a Kubernetes cluster is presented, which provides high scalability, resource efficiency and optimized management for processing large amounts of data.

Keywords: Distributed systems, Kubernetes cluster, MapReduce model, Apache Hadoop framework, microservice, orchestration.

Введение

В настоящее время многие задачи машинного обучения и интеллектуального анализа данных требуют большие наборы данных. Примерами такой обработки являются задачи обработки текстов, поиска в Интернете, онлайн-рекламы и обработки сигналов [1]. Соответственно при этом возникает необходимость в высоких вычислительных ресурсах для такого объема данных. Поэтому важным и актуальным направлением является разработка

распределенных вычислительных систем, позволяющих применять существующие методы машинного обучения и анализа данных на больших выборках. Один из самых известных и распространенных способов проектирования распределенных систем основан на модели MapReduce.

Важным моментом является то, что при проектировании информационной инфраструктуры современного предприятия первоочередной задачей является выбор стека технологий для реализации основных производственных ИТ-процессов предприятия. К таким первоочередным задачам можно отнести задачи хранения данных, мониторинга и оповещения, а также процессы непрерывной доставки и развертывания приложений. В последние годы все больше и больше компаний решают данные задачи с использованием микросервисной архитектуры. Эти задачи объединяет необходимость использования большого количества аппаратных ресурсов, собранных в кластер, для обеспечения связи между микросервисами, а также динамического выделения ресурсов. Наиболее подходящим для решения подобных задач решением является Kubernetes.

Использование кластера Kubernetes при проектировании распределенной системы позволяет получить крайне эффективное вычислительное средство для обработки больших объемов данных.

MapReduce

Модель распределенных вычислений MapReduce была разработана и представлена компанией Google в статье [2]. Данная архитектура позволяет выполнять параллельные задачи на множестве вычислительных машин на разных наборах данных.

Основными компонентами данной модели являются две описываемые разработчиком функции – Map и Reduce. Решение конкретной задачи сводится к последовательному выполнению MapReduce-задач, в свою очередь состоящих из двух этапов – выполнения функций Map и Reduce [3]. Схема работы модели MapReduce представлена на Рисунке 1.

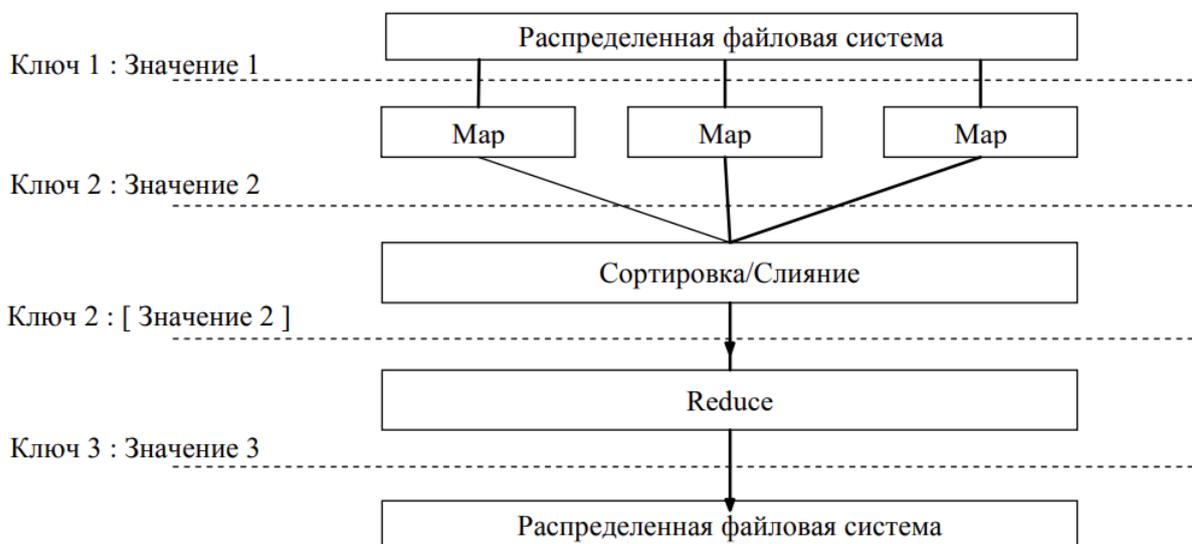


Рисунок 1 – Модель MapReduce [3]

Механизм MapReduce работает следующим образом: сначала функция Map принимает пару ключ-значение и возвращает массив промежуточных значений, также представляющих собой пары ключ-значение. Затем среда исполнения MapReduce запускает несколько экземпляров функции Map одновременно на разных вычислительных узлах, автоматически распределяя данные между ними. После этого происходит барьер, где все задачи Map ожидают выполнения, и затем промежуточные данные из всех узлов Map группируются по ключу и передаются в функцию Reduce. Функция Reduce получает пару ключ-"массив значений" и выполняет агрегацию данных, в результате чего порождаются новые пары ключ-значение. Эти пары записываются в распределенную файловую систему и могут быть как окончательным результатом, так и исходными данными для следующей задачи MapReduce.

Самым распространенным способом реализации модели MapReduce является Apache Hadoop. Hadoop - это программный фреймворк для надежных, масштабируемых, параллельных и распределенных вычислений. Вместо того, чтобы полагаться на дорогостоящее оборудование и дорогостоящие системы для обработки и хранения данных, Apache Hadoop обеспечивает параллельную обработку больших данных на стандартном оборудовании. HDFS и стандарт программирования MapReduce позволяют выполнять аналитические задачи, требующие больших объемов данных, благодаря своей масштабируемой архитектуре и способности обрабатывать данные параллельным образом в многоузловых кластерах [4].

Kubernetes

Kubernetes является системой оркестрации контейнеров с открытым исходным кодом, позволяющей автоматически масштабировать и управлять ресурсами кластера [5]. Прототип Kubernetes начал разрабатываться командой инженеров компании Google в 2014 году [6], когда Google запустил проект под названием Borg. Это была система оркестрации контейнеров, предназначенная для управления и масштабирования микросервисов в облаке. Borg был построен на базе собственного механизма управления ресурсами, который не мог быть использован другими компаниями, что ограничивало его применение. В 2015 году команда Borg начала работать над проектом под названием Omega, целью которого было создание универсального механизма оркестрации ресурсов. В результате они разработали концепцию "Kubernetes", которая стала основой для будущего проекта. Kubernetes был официально выпущен в 2016 году под руководством Cloud Native Computing Foundation (CNCF). CNCF – это некоммерческая организация, которая занимается поддержкой и продвижением проектов, связанных с облачными и контейнерными технологиями. После этого Kubernetes стал одним из самых популярных инструментов для работы с контейнерами и получил широкое распространение в индустрии.

Структура кластера Kubernetes

Кластер обычно состоит из нескольких узлов (node), которые по факту являются физическими или виртуальными вычислительными устройствами. В каждом кластере независимо от размера обязательно будет хотя бы один управляющий узел (master), а также произвольное количество рабочих узлов (worker node) [7].

Такое разделение используется для большей надежности всей системы, несмотря на возможность развертывания рабочей нагрузки на любом узле кластера крайне рекомендуется использовать только рабочие узлы. На Рисунке 2 изображен пример кластера, состоящего из одного управляющего узла и двух рабочих узлов.

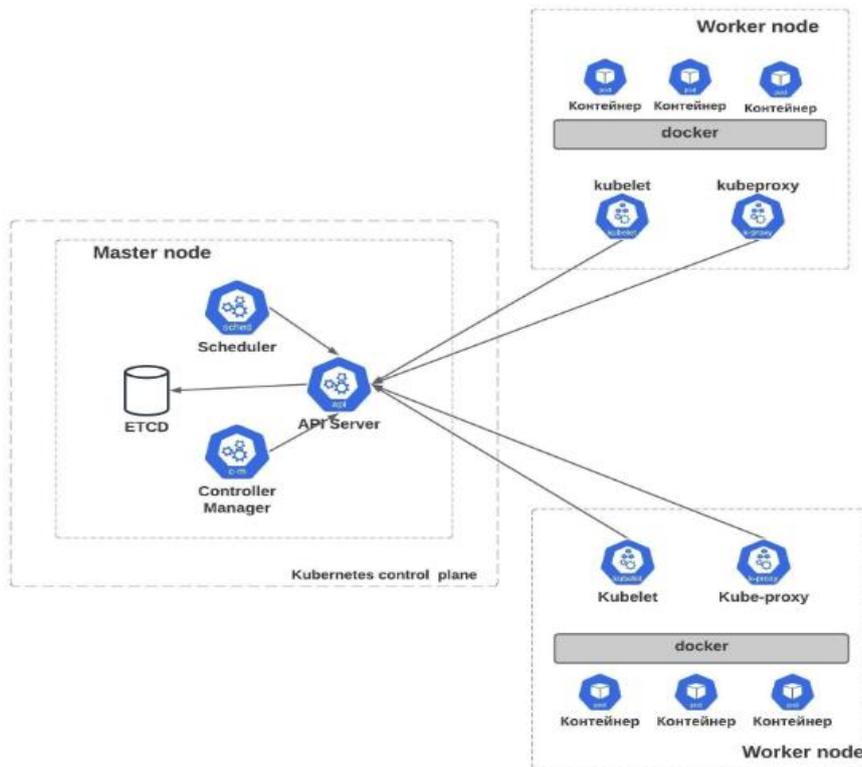


Рисунок 2 – Пример кластера Kubernetes

Как видно на Рисунке 2, на разных узлах используются разные компоненты, про каждый из них будет рассказано далее.

Управляющий узел состоит из:

- API сервер (kube-apiserver) – обрабатывает все запросы на манипуляции с ресурсами (создание, изменение, удаление);
- Контроллер менеджер – следит за состоянием ресурсов в кластере и применяют необходимые изменения. Например, если какой-то ресурс стал недоступен, контроллер может создать его заново;
- etcd – хранит состояния кластера (данные о ресурсах, их состоянии и т.д.).

Стоит отметить, что в крупных кластерах зачастую используется несколько управляющих узлов, которые распределяют административную нагрузку между собой, а также обеспечивают дополнительную отказоустойчивость.

Как было сказано выше, рабочие узлы используются для разворачивания рабочей нагрузки, такой как микросервисы, базы данных или простые контейнеры. Однако для работы в кластере необходимо иметь обязательный набор административных процессов, в основном для связи с управляющим узлом.

Рабочий узел состоит из:

- kubelet – это основной компонент рабочего узла, который отвечает за управление и запуск контейнеров. Он взаимодействует с API сервером управляющего узла и выполняет команды, которые поступают от контроллера;
- docker – это основная часть рабочего узла, которая отвечает за запуск и управление контейнерами. Он взаимодействует с демоном kubelet и выполняет его команды;
- kubernetes – это прокси-сервер, который работает на управляющем узле Kubernetes и предоставляет сервисы для коммуникации между контейнерами в кластере. Он обеспечивает маршрутизацию запросов между контейнерами, скрывает информацию о внутренних адресах узлов и балансирует нагрузку на кластер.

Создание инфраструктуры для Hadoop на Kubernetes

Для развертывания компонентов Hadoop поверх Kubernetes необходимо решить несколько важных архитектурных задач [8]. В первую очередь нужно выбрать тип кластера Kubernetes – использовать облачное решение от какой-либо компании или же использовать собственные вычислительные мощности. Также нужно убедиться, что сетевая связь между узлами подходит под необходимые для Hadoop стандарты.

Вторым важным шагом является разбиение компонентов Hadoop на отдельные микросервисы, например HDFS, YARN, MapReduce. Стоит отметить, что для работы файловой системы HDFS необходимо использовать специальные типы объектов внутри Kubernetes – Persistent Volumes и Persistent Volume Claims. Для связи микросервисов друг с другом нужно использовать объект типа Service, а также особый тип сервисов для связи со внешним миром – NodePort или LoadBalancer.

Третьим этапом является настройка мониторинга состояния кластера. Для этого лучше всего использовать связку инструментов Grafana и Prometheus, что позволит снимать необходимые метрики напрямую с кластера и предоставлять их в удобном формате.

Заключение

В данной статье описан способ разработки распределенной системы на основе модели MapReduce в кластере Kubernetes.

Дано описание использования Kubernetes в качестве инструмента при проектировании микросервисной архитектуры современного предприятия. Показаны основные ее компоненты и способы их взаимодействия между ними.

Представлено описание модели распределенных вычислений MapReduce и основные этапы работы ее в распределенной системе.

Дается подход для интеграции Apache Hadoop в кластер Kubernetes для обеспечения высокой масштабируемости и эффективности вычислений для больших наборов данных.

Изложенный выше подход для проектирования кластера Hadoop в информационной структуре предприятия на основе Kubernetes является одним из наиболее удобных для реализации, а также поддержки. Реализация Hadoop таким способом предусматривает высокую надежность и удобные инструменты для масштабирования кластера.

Список литературы

1. Дурнов Р. В. Модель распределенной вычислительной сети //Известия Тульского государственного университета. Технические науки. – 2022. – №. 9. – С. 151-153.
2. Dean, J. and Ghemawat, S. (2004). MapReduce : Simplified Data Processing on Large Clusters. In OSDI' 04, San Francisco.
3. Митяков А. В., Татаринов Ю. С. Подходы к эффективному исполнению итеративных алгоритмов на модели MapReduce //Известия ЛЭТИ. – 2014. – №. 2. – С. 30-41.
4. Ghazi M. R., Gangodkar D. Hadoop, MapReduce and HDFS: a developers perspective //Procedia Computer Science. – 2015. – Т. 48. – С. 45-50.
5. Luksa M. Kubernetes in action. – Simon and Schuster, 2017. – С. 38-45.
6. The History of Kubernetes & the Community Behind It. URL: <https://web.archive.org/web/20220227112321/https://kubernetes.io/blog/2018/07/20/the-history-of-kubernetes-the-community-behind-it/> (date of application: 03.03.2024).
7. Sayfan G. Mastering kubernetes. – Packt Publishing Ltd, 2017. – С. 5-10.
8. Zhang X. et al. Zeus: Improving resource efficiency via workload colocation for massive kubernetes clusters //IEEE Access. – 2021. – Т. 9. – С. 105192-105204.

References

1. Durnov R. V. Model of a distributed computing network //Proceedings of Tula State University. Technical sciences. - 2022. – No. 9. – pp. 151-153.
 2. Dean, J. and Ghemawat, S. (2004). MapReduce : Simplified Data Processing on Large Clusters. In OSDI' 04, San Francisco.
 3. Mityakov A.V., Tatarinov Yu. S. Approaches to the effective execution of iterative algorithms based on the MapReduce model //News of LETI. – 2014. – №. 2. – pp. 30-41.
 4. Ghazi M. R., Gangodkar D. Hadoop, MapReduce and HDFS: a developers perspective //Procedural Computer Science. – 2015. – Vol. 48. – pp. 45-50.
 5. Luksa M. Kubernetes in action. – Simon and Schuster, 2017. – pp. 38-45.
 6. The History of Kubernetes & the Community Behind It. URL: <https://web.archive.org/web/20220227112321/https://kubernetes.io/blog/2018/07/20/the-history-of-kubernetes-the-community-behind-it/> (date of application: 03.03.2024).
 7. Sayfan G. Mastering kubernetes. – Packt Publishing Ltd, 2017. – pp. 5-10.
 8. Zhang X. et al. Zeus: Improving resource efficiency via workload colocation for massive kubernetes clusters //IEEE Access. – 2021. – Vol. 9. – pp. 105192-105204.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.453.3

ОСОБЕННОСТИ РАЗРАБОТКИ WEB-ПРИЛОЖЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННОГО УЧЕТА ДЕЯТЕЛЬНОСТИ ОБУЧАЮЩИХСЯ В ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ

Калашников А.С.

ФГБОУ ВО "КАЛУЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. К.Э.

ЦИОЛКОВСКОГО", Калуга, Россия (248023, Калужская область, город Калуга, ул. Степана Разина, д.26), e-mail: 4553585@yandex.ru

Настоящее исследование посвящено анализу и характеристике разработки web-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении. Также в статье представлены проблемы и пути решения, связанные с разработкой web-приложения. Кроме того, автором обозначены примеры web-приложений для автоматизированного учета деятельности обучающихся в образовательном учреждении.

Ключевые слова: WEB-приложение, обучающиеся, образовательное учреждение, учет, деятельность.

FEATURES OF THE DEVELOPMENT OF A WEB APPLICATION FOR AUTOMATED ACCOUNTING OF STUDENTS' ACTIVITIES IN AN EDUCATIONAL INSTITUTION

Kalashnikov A.S.

KALUGA STATE UNIVERSITY. K.E. TSIOLKOVSKY", Kaluga, Russia (248023, Kaluga region, Kaluga city, Stepana Razina st., 26), e-mail: 4553585@yandex.ru

This study is devoted to the analysis and characterization of the development of a web application for automated accounting of students' activities in an educational institution. The article also presents problems and solutions related to the development of a web application. In addition, the author identifies examples of web applications for automated accounting of students' activities in an educational institution.

Keywords: WEB application, students, educational institution, accounting, activity.

Актуальность темы обусловлена несколькими ключевыми факторами. Во-первых, современный образовательный процесс требует высокой степени организации, доступности и аналитики информации о деятельности студентов и школьников. Во-вторых, в условиях растущего объема информации и увеличения числа учебных заданий и проектов необходимы эффективные инструменты для их управления. В-третьих, развитие цифровых технологий и Интернета открывает новые возможности для улучшения качества образования через автоматизацию рутинных процессов и оптимизацию взаимодействия между всеми участниками образовательного процесса.

Целью исследования является создание удобного, масштабируемого и функционального инструмента, который обеспечит автоматизацию учета успеваемости и посещаемости обучающихся, повышение эффективности образовательного процесса.

Разработка web-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении включает в себя ряд особенностей, которые определяются спецификой задач, стоящих перед системой, и требованиями пользователей к ее функционалу. Ключевые аспекты такой разработки включают:

1. Пользовательский интерфейс и удобство использования:
 - Интуитивно понятный интерфейс для всех категорий пользователей (учащихся, преподавателей, администрации).
 - Адаптивный дизайн, обеспечивающий корректную работу на различных устройствах (ПК, планшеты, смартфоны).
 - Персонализация рабочего пространства под конкретного пользователя с возможностью настройки виджетов и уведомлений.
2. Функциональность и модульность:
 - Модуль для учета успеваемости и посещаемости с возможностью ввода, хранения и анализа данных.
 - Модуль для планирования учебного процесса, включая расписание занятий, дедлайны курсовых и контрольных работ.
 - Инструменты для коммуникации между пользователями системы: форумы, чаты, системы обмена сообщениями.
 - Интеграция с электронными библиотеками и образовательными ресурсами.
3. Безопасность и конфиденциальность:
 - Защита личных данных учащихся и преподавателей в соответствии с законодательством.
 - Многоуровневая система аутентификации и авторизации пользователей.
 - Шифрование данных и транзакций для защиты от несанкционированного доступа.
4. Масштабируемость и производительность:
 - Архитектура, позволяющая легко масштабировать систему с увеличением числа пользователей и объема данных.
 - Оптимизация производительности для обеспечения быстрой обработки запросов и минимальных задержек.

Важным аспектом является также соблюдение правовых норм и этических стандартов, особенно в части обработки и хранения личных данных учащихся и преподавателей. Внедрение системы требует не только технических усилий, но и подготовки пользователей к ее эффективному использованию через обучение и поддержку. В целом, успешная реализация такого проекта способствует повышению качества образования, делая его более доступным, персонализированным и соответствующим современным требованиям к цифровой грамотности и компетенциям [1, с. 1784].

В процессе разработки необходимо учитывать специфику образовательного процесса в конкретном учреждении, включая учебные планы, методики преподавания и оценки, а также индивидуальные потребности учащихся и преподавателей. Это позволит создать максимально

эффективный и удобный инструмент, способствующий повышению качества образования и оптимизации учебного процесса.

Интеграция с существующими информационными системами и образовательными ресурсами обеспечит целостность данных и упростит доступ к необходимой информации и учебным материалам. При этом важно обеспечить высокую производительность и масштабируемость системы, чтобы она могла эффективно работать с большим числом пользователей и объемами данных.

Внедрение современных технологий, таких как искусственный интеллект и машинное обучение, может дополнительно расширить возможности приложения, включая персонализацию обучения, автоматическую оценку работ и анализ поведения пользователей для предотвращения академической нечестности и повышения вовлеченности студентов.

Таким образом, разработка web-приложения для автоматизированного учета деятельности обучающихся является сложной, но важной задачей, требующей комплексного подхода и тесного взаимодействия разработчиков с представителями образовательного учреждения. При успешной реализации такое приложение станет неотъемлемым инструментом в учебном процессе, способствуя его оптимизации и повышению качества образования.

В современном цифровом мире образовательные ресурсы в Интернете представлены широким спектром веб-сайтов, каждый из которых выполняет уникальные функции и обслуживает различные аспекты учебного и научного процесса. Их многообразие и постоянный рост затрудняют навигацию и эффективное использование, подчеркивая важность систематизации этих ресурсов [2, с. 19]. Для лучшего понимания этого многообразия можно классифицировать образовательные сайты по следующим категориям:

1. Сайты образовательных учреждений: представляют собой официальные платформы школ, колледжей и университетов, содержащие информацию о программе обучения, преподавательском составе и студенческой жизни.
2. Платформы дистанционного обучения: предлагают онлайн-курсы и программы, позволяя пользователям обучаться независимо от их географического положения.
3. Информационно-образовательные порталы: включают виртуальные библиотеки, образовательные журналы и газеты, а также виртуальные музеи, расширяющие доступ к знаниям и культурным ценностям.
4. Научно-исследовательские сайты: служат платформой для публикации научных работ, обмена знаниями и сотрудничества в области научных исследований.
5. Информационно-справочные сайты: предоставляют данные и статистику, необходимые для образовательных и исследовательских целей.
6. Сайты образовательных конкурсов и проектов: организуют и продвигают соревновательную деятельность в образовательной среде, стимулируя учебный процесс [3, с. 61].
7. Учебно-методические ресурсы: предлагают материалы и инструменты для учителей и преподавателей, включая методические рекомендации, тематические вебинары и платформы для профессионального развития.

Разработка web-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении сталкивается с рядом проблем, которые требуют комплексных решений.

Можно представить следующие проблемы:

1. Интеграция с существующими системами. Многие образовательные учреждения уже используют различные информационные системы, которые могут быть несовместимы с новым приложением.

Решение: разработка модульных и гибких архитектур, которые легко интегрируются с различными системами. Использование API для обмена данными между системами.

2. Конфиденциальность и безопасность данных. Сохранение конфиденциальности личной информации студентов и преподавателей является критически важным.

Решение: реализация строгих мер безопасности, включая шифрование данных, многоуровневую аутентификацию и регулярное тестирование на уязвимости.

3. Удобство использования. Приложение должно быть удобным для всех категорий пользователей, включая студентов, преподавателей и административный персонал.

Решение: Разработка интуитивно понятного пользовательского интерфейса и предоставление подробных руководств и обучающих материалов.

4. Масштабируемость. Система должна быть способна адаптироваться к увеличению числа пользователей и объема данных без снижения производительности [4, с. 42].

Решение: использование облачных технологий и микросервисной архитектуры для гарантии масштабируемости и гибкости системы.

5. Аналитика и отчетность. Необходимо предоставлять администрации учреждения подробные отчеты и аналитику для принятия обоснованных управленческих решений.

Решение: внедрение расширенных функций аналитики и визуализации данных, позволяющих генерировать комплексные отчеты в реальном времени.

Примеры разработки web-приложений для автоматизированного учета деятельности обучающихся в образовательных учреждениях включают в себя различные системы и платформы, которые могут охватывать широкий спектр функциональностей, от учета посещаемости до комплексного управления учебным процессом. Вот несколько примеров таких систем:

1. Google Classroom

Google Classroom – это популярная платформа, которая позволяет учителям создавать, распространять и оценивать задания в бумажном виде, а также облегчает коммуникацию между учителями и учащимися. Хотя Google Classroom не является полноценной системой учета, он позволяет учителям отслеживать выполнение заданий и участие студентов в курсе.

2. Moodle

Moodle – это широко используемая открытая платформа для электронного обучения, которая предлагает широкий спектр инструментов для создания персонализированных учебных курсов онлайн. Она включает в себя функции для учета успеваемости, посещаемости и предоставляет различные ресурсы для обучения и взаимодействия между учащимися и преподавателями.

3. Canvas

Canvas – это еще одна интегрированная система обучения, которая обеспечивает учителей и студентов инструментами для управления курсами. Она позволяет преподавателям публиковать оценки, домашние задания, и проводить тесты онлайн, а также отслеживать прогресс студентов и взаимодействовать с ними через форумы и чаты.

4. Blackboard

Blackboard – это коммерческая платформа для управления обучением, которая предлагает комплексные решения для учета деятельности студентов, включая оценки, посещаемость, а также инструменты для совместной работы и общения. Она широко используется в высших учебных заведениях для поддержки как традиционного, так и дистанционного обучения.

Актуальность темы обусловлена несколькими ключевыми факторами. Во-первых, современный образовательный процесс требует высокой степени организации, доступности и аналитики информации о деятельности студентов и школьников. Во-вторых, в условиях растущего объема информации и увеличения числа учебных заданий и проектов необходимы эффективные инструменты для их управления. В-третьих, развитие цифровых технологий и Интернета открывает новые возможности для улучшения качества образования через автоматизацию рутинных процессов и оптимизацию взаимодействия между всеми участниками образовательного процесса.

Целью исследования является создание удобного, масштабируемого и функционального инструмента, который обеспечит автоматизацию учета успеваемости и посещаемости обучающихся, повышение эффективности образовательного процесса.

Разработка web-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении включает в себя ряд особенностей, которые определяются спецификой задач, стоящих перед системой, и требованиями пользователей к ее функционалу. Ключевые аспекты такой разработки включают:

1. Пользовательский интерфейс и удобство использования:
 - Интуитивно понятный интерфейс для всех категорий пользователей (учащихся, преподавателей, администрации).
 - Адаптивный дизайн, обеспечивающий корректную работу на различных устройствах (ПК, планшеты, смартфоны).
 - Персонализация рабочего пространства под конкретного пользователя с возможностью настройки виджетов и уведомлений.
2. Функциональность и модульность:
 - Модуль для учета успеваемости и посещаемости с возможностью ввода, хранения и анализа данных.
 - Модуль для планирования учебного процесса, включая расписание занятий, дедлайны курсовых и контрольных работ.
 - Инструменты для коммуникации между пользователями системы: форумы, чаты, системы обмена сообщениями.
 - Интеграция с электронными библиотеками и образовательными ресурсами.
3. Безопасность и конфиденциальность:
 - Защита личных данных учащихся и преподавателей в соответствии с законодательством.

- Многоуровневая система аутентификации и авторизации пользователей.
 - Шифрование данных и транзакций для защиты от несанкционированного доступа.
4. Масштабируемость и производительность:
- Архитектура, позволяющая легко масштабировать систему с увеличением числа пользователей и объема данных.
 - Оптимизация производительности для обеспечения быстрой обработки запросов и минимальных задержек.

Важным аспектом является также соблюдение правовых норм и этических стандартов, особенно в части обработки и хранения личных данных учащихся и преподавателей. Внедрение системы требует не только технических усилий, но и подготовки пользователей к ее эффективному использованию через обучение и поддержку. В целом, успешная реализация такого проекта способствует повышению качества образования, делая его более доступным, персонализированным и соответствующим современным требованиям к цифровой грамотности и компетенциям [1, с. 1784].

В процессе разработки необходимо учитывать специфику образовательного процесса в конкретном учреждении, включая учебные планы, методики преподавания и оценки, а также индивидуальные потребности учащихся и преподавателей. Это позволит создать максимально эффективный и удобный инструмент, способствующий повышению качества образования и оптимизации учебного процесса.

Интеграция с существующими информационными системами и образовательными ресурсами обеспечит целостность данных и упростит доступ к необходимой информации и учебным материалам. При этом важно обеспечить высокую производительность и масштабируемость системы, чтобы она могла эффективно работать с большим числом пользователей и объемами данных.

Внедрение современных технологий, таких как искусственный интеллект и машинное обучение, может дополнительно расширить возможности приложения, включая персонализацию обучения, автоматическую оценку работ и анализ поведения пользователей для предотвращения академической нечестности и повышения вовлеченности студентов.

Таким образом, разработка web-приложения для автоматизированного учета деятельности обучающихся является сложной, но важной задачей, требующей комплексного подхода и тесного взаимодействия разработчиков с представителями образовательного учреждения. При успешной реализации такое приложение станет неотъемлемым инструментом в учебном процессе, способствуя его оптимизации и повышению качества образования.

В современном цифровом мире образовательные ресурсы в Интернете представлены широким спектром веб-сайтов, каждый из которых выполняет уникальные функции и обслуживает различные аспекты учебного и научного процесса. Их многообразие и постоянный рост затрудняют навигацию и эффективное использование, подчеркивая важность систематизации этих ресурсов [2, с. 19]. Для лучшего понимания этого многообразия можно классифицировать образовательные сайты по следующим категориям:

1. Сайты образовательных учреждений: представляют собой официальные платформы школ, колледжей и университетов, содержащие информацию о программе обучения, преподавательском составе и студенческой жизни.
2. Платформы дистанционного обучения: предлагают онлайн-курсы и программы, позволяя пользователям обучаться независимо от их географического положения.
3. Информационно-образовательные порталы: включают виртуальные библиотеки, образовательные журналы и газеты, а также виртуальные музеи, расширяющие доступ к знаниям и культурным ценностям.
4. Научно-исследовательские сайты: служат платформой для публикации научных работ, обмена знаниями и сотрудничества в области научных исследований.
5. Информационно-справочные сайты: предоставляют данные и статистику, необходимые для образовательных и исследовательских целей.
6. Сайты образовательных конкурсов и проектов: организуют и продвигают соревновательную деятельность в образовательной среде, стимулируя учебный процесс [3, с. 61].
7. Учебно-методические ресурсы: предлагают материалы и инструменты для учителей и преподавателей, включая методические рекомендации, тематические вебинары и платформы для профессионального развития.

Разработка web-приложения для автоматизированного учета деятельности обучающихся в образовательном учреждении сталкивается с рядом проблем, которые требуют комплексных решений.

Можно представить следующие проблемы:

1. Интеграция с существующими системами. Многие образовательные учреждения уже используют различные информационные системы, которые могут быть несовместимы с новым приложением.

Решение: разработка модульных и гибких архитектур, которые легко интегрируются с различными системами. Использование API для обмена данными между системами.

2. Конфиденциальность и безопасность данных. Сохранение конфиденциальности личной информации студентов и преподавателей является критически важным.

Решение: реализация строгих мер безопасности, включая шифрование данных, многоуровневую аутентификацию и регулярное тестирование на уязвимости.

3. Удобство использования. Приложение должно быть удобным для всех категорий пользователей, включая студентов, преподавателей и административный персонал.

Решение: Разработка интуитивно понятного пользовательского интерфейса и предоставление подробных руководств и обучающих материалов.

4. Масштабируемость. Система должна быть способна адаптироваться к увеличению числа пользователей и объема данных без снижения производительности [4, с. 42].

Решение: использование облачных технологий и микросервисной архитектуры для гарантии масштабируемости и гибкости системы.

5. Аналитика и отчетность. Необходимо предоставлять администрации учреждения подробные отчеты и аналитику для принятия обоснованных управленческих решений.

Решение: внедрение расширенных функций аналитики и визуализации данных, позволяющих генерировать комплексные отчеты в реальном времени.

Примеры разработки web-приложений для автоматизированного учета деятельности обучающихся в образовательных учреждениях включают в себя различные системы и платформы, которые могут охватывать широкий спектр функциональностей, от учета посещаемости до комплексного управления учебным процессом. Вот несколько примеров таких систем:

1. Google Classroom

Google Classroom – это популярная платформа, которая позволяет учителям создавать, распространять и оценивать задания в бумажном виде, а также облегчает коммуникацию между учителями и учащимися. Хотя Google Classroom не является полноценной системой учета, он позволяет учителям отслеживать выполнение заданий и участие студентов в курсе.

2. Moodle

Moodle – это широко используемая открытая платформа для электронного обучения, которая предлагает широкий спектр инструментов для создания персонализированных учебных курсов онлайн. Она включает в себя функции для учета успеваемости, посещаемости и предоставляет различные ресурсы для обучения и взаимодействия между учащимися и преподавателями.

3. Canvas

Canvas – это еще одна интегрированная система обучения, которая обеспечивает учителей и студентов инструментами для управления курсами. Она позволяет преподавателям публиковать оценки, домашние задания, и проводить тесты онлайн, а также отслеживать прогресс студентов и взаимодействовать с ними через форумы и чаты.

4. Blackboard

Blackboard – это коммерческая платформа для управления обучением, которая предлагает комплексные решения для учета деятельности студентов, включая оценки, посещаемость, а также инструменты для совместной работы и общения. Она широко используется в высших учебных заведениях для поддержки как традиционного, так и дистанционного обучения.

5. Schoology

Schoology представляет собой социальную сеть для обучения, которая сочетает в себе систему управления обучением с элементами социальных сетей. Она предоставляет инструменты для управления курсами, оценки студентов, обсуждения в классе и индивидуального общения между участниками образовательного процесса.

6. Edmodo

Edmodo похожа на Schoology в том, что объединяет элементы социальной сети и платформы для обучения. Она позволяет учителям создавать группы, назначать задания, проводить опросы и тесты, а также обеспечивает обмен файлами и сообщениями между учащимися и учителями [5, с. 107].

Таким образом, разработка web-приложений для автоматизированного учета деятельности обучающихся в образовательных учреждениях играет ключевую роль в современном образовательном процессе. Эти приложения обеспечивают учителей, студентов и административный персонал мощными инструментами для управления учебными планами,

отслеживания успеваемости и посещаемости, а также для эффективного взаимодействия и сотрудничества.

Примеры таких систем, как Google Classroom, Moodle, Canvas, Blackboard, Schoology и Edmodo, демонстрируют разнообразие доступных решений, каждое из которых предлагает уникальный набор функций и возможностей, адаптированных под различные образовательные потребности и контексты. Эти платформы способствуют не только более эффективному и организованному образовательному процессу, но и создают условия для более глубокого и индивидуализированного подхода к обучению каждого студента.

Список литературы

1. Абрамян Г.В. Сервисы обучения информатике и новая наука о сервисах, управлении и инжиниринге как основе инновационной деятельности в современной высшей школе / Г.В. Абрамян, Р.Р. Фокин, М.А. Абиссова, А.А. Емельянов//Письма в Эмиссия. Оффлайн: электронный научный журнал. 2018. – № 4. – С. 1783-1789.
2. Гречушкина Н.В. Факторы интеграции онлайн-курсов в образовательную систему вуза / Рязань: сборник трудов конференции «Электронное обучение в непрерывном образовании», 2018. – С. 16-23.
3. Колесников И.Н. Интерфейс и веб-сервис для системы средств контроля обучающихся в образовательных учреждениях/И.Н. Колесников, А.Г. Финогеев//Молодой ученый. – 2017. – № 13 (147). – С. 60-62.
4. Кубова Р.М., Шамраева В.В. Использование Web-технологий как средства автоматизации мониторинга и оценки качества педагогической деятельности на примере разработки сайта для конкурса педагогических работников//Научное обозрение. Технические науки. – 2019. – № 2. – С. 38-44.
5. Шумкова И.Г., Абрамян Г.В. Особенности, значение и принципы формирования информационно-образовательного пространства вуза на основе интернет – ресурса «СПБ ГИПИСР»/И.Г.Шумкова, Г.В.Абрамян//В сборнике: Информационно-телекоммуникационные системы и технологии Всероссийская научно-практическая конференция. – 2015. – № 4. – С. 100-112.

References

1. Abramyan G.V. Computer science teaching services and the new science of services, management and engineering as the basis of innovative activity in modern higher education / G.V. Abramyan, R.R. Fokin, M.A. Abissova,
2. A.A.Yemelyanov//Letters to the Issue. Offline: an electronic scientific journal. 2018. – No. 4. – pp. 1783-1789.
3. Grechushkina N.V. Factors of integration of online courses into the educational system of the university/Ryazan: proceedings of the conference "E-learning in continuing education", 2018. – pp. 16-23.
4. Kolesnikov I.N. Interface and web service for the system of control tools for students in educational institutions/I.N. Kolesnikov,
5. A.G. Finogeev//Young scientist. – 2017. – № 13 (147). – pp. 60-62.

6. Kubova R.M., Shamraeva V.V. The use of Web technologies as a means of automating monitoring and evaluating the quality of pedagogical activity on the example of developing a website for a competition of teaching staff // Scientific Review. Technical sciences. – 2019. – No. 2. – pp. 38-44.
 7. Shumkova I.G., Abramyan G.V. Features, significance and principles of the formation of the information and educational space of the university based on the Internet resource "SPB GIPISR" / I.G. Shumkova, G.V. Abramyan // In the collection: Information and telecommunication systems and technologies All-Russian scientific and practical conference. – 2015. – No. 4. – pp. 100-112.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004. 004.05

ИССЛЕДОВАНИЕ СИСТЕМ МОДЕЛИРОВАНИЯ ДЛЯ ТУМАННЫХ ВЫЧИСЛЕНИЙ: ОСОБЕННОСТИ, ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

¹Бакай Ю.О., Карташевский И.В.

ФГБОУ ВО "ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ», Самара, Россия (443010, Самарская область, город Самара, ул. Льва Толстого, д.23), e-mail: ¹ov.bakai@gmail.com

Туманные вычисления стали перспективной парадигмой, которая расширяет возможности облачных вычислений до границ сети, позволяя эффективно обрабатывать и анализировать данные ближе к источнику. Чтобы эффективно использовать потенциал туманных вычислений, были разработаны различные системы моделирования. В этой статье мы рассмотрим основные особенности, преимущества и недостатки существующих систем моделирования для туманных вычислений.

Ключевые слова: Туманные вычисления, системы моделирования, облако, iFogSim, CloudSim.

RESEARCH OF MODELING SYSTEMS FOR FOGGY COMPUTING: FEATURES, ADVANTAGES AND DISADVANTAGES

¹Bakai Yu.O., Kartashevsky I.V.

VOLGA REGION STATE UNIVERSITY OF TELECOMMUNICATIONS AND INFORMATICS, Samara, Russia (443010, Samara, Leo Tolstoy St., 23), e-mail: ¹ov.bakai@gmail.com

Cloud computing has become a promising paradigm that extends the capabilities of cloud computing to the boundaries of the network, allowing efficient processing and analysis of data closer to the source. In order to effectively exploit the potential of foggy computing, various modeling systems have been developed. In this article, we will look at the main features, advantages and disadvantages of existing modeling systems for fog computing.

Keywords: Fog computing, modeling systems, cloud, iFogSim, CloudSim.

Введение

Туманные вычисления – это парадигма вычислительной модели, где данные и вычисления обрабатываются не только в центральных облачных узлах, но и на локальных устройствах. Благодаря этому можно достичь более низкой задержки и улучшенной производительности при выполнении вычислений и обработке данных. Стандартным архитектурным решением воспроизведения тумана считается трехуровневая модель, состоящая из уровня облака (облачных вычислений), слоя тумана (узлов тумана) и конечных устройства (краевых устройств).

Системы моделирования туманных вычислений – инновационные инструменты, которые имитируют и воспроизводят поведение туманно-вычислительных систем. Они

разработаны для изучения, анализа и оптимизации таких систем, а также для исследования различных сценариев применения тумана.

По мере того как туманные вычисления набирают обороты в сфере граничных вычислений, появляются системы моделирования, облегчающие проектирование, оценку и оптимизацию туманных вычислительных сред. [1] Существуют различные системы моделирования туманных вычислений, которые предлагают разные подходы и возможности, со своими отличительными особенностями, преимуществами и недостатками.

Системы моделирования

Рассмотрим некоторые из этих систем моделирования:

1. iFogSim: Эта система моделирования основана на симуляторе распределенных систем CloudSim, функционал которого был расширен для учета возможностей туманных вычислительных сред. iFogSim позволяет моделировать и анализировать различные параметры туманных вычислительных систем, такие как задержка, энергопотребление и надежность соединения. iFogSim предназначена в первую очередь для работы на платформах, основанных на Java, что делает систему совместимым с операционными Windows, macOS и Linux.

iFogSim предлагает несколько ключевых функций, такие как:

- Гетерогенные узлы тумана: iFogSim поддерживает моделирование гетерогенных узлов тумана с различными вычислительными возможностями, энергопотреблением и коммуникационными характеристиками.[2]
- Планирование задач: Обеспечивает гибкие алгоритмы планирования задач для оптимизации использования ресурсов и минимизации задержек.
- Анализ энергопотребления: iFogSim позволяет пользователям оценить энергопотребление узлов тумана, что помогает в разработке энергосберегающих приложений.

К преимуществам системы относятся:

- Комплексное моделирование: iFogSim предоставляет комплексную среду моделирования, позволяющую исследователям оценивать производительность приложений для туманных вычислений в различных сценариях.
- Настраиваемость: Пользователи могут легко настраивать среду туманных вычислений, задавая собственные характеристики узлов тумана и требования к приложениям.
- Открытый исходный код: iFogSim является инструментом с открытым исходным кодом.[3]

Также рассмотрим основные недостатки системы:

- Сложность понимания: iFogSim требует глубокого понимания концепций туманных вычислений и методов моделирования, что усложняет понимание использования системы.
- Ограниченная визуализация: Возможности визуализации в iFogSim относительно ограничены, что может повлиять на возможность анализа сложных результатов моделирования.

2. FogTorch: FogTorch - это фреймворк для моделирования и оптимизации, позволяющий оценивать производительность и оптимизировать системы туманных вычислений. FogTorch - платформонезависимый инструмент, который можно использовать в операционных системах Windows, macOS и Linux.

Его основные возможности включают:

- Оценка производительности: FogTorch позволяет пользователям оценивать производительность туманных вычислительных систем с точки зрения задержки, времени отклика и использования ресурсов.
- Оптимизация: FogTorch предоставляет алгоритмы оптимизации для поиска наилучших стратегий развертывания туманных приложений с учетом таких факторов, как задержка, энергопотребление и стоимость.[4]
- Анализ масштабируемости: FogTorch поддерживает анализ масштабируемости для оценки поведения системы при различной рабочей нагрузке и доступности ресурсов.

Преимущества:

- Возможности оптимизации: Алгоритмы оптимизации FogTorch помогают находить оптимальные стратегии развертывания, обеспечивая эффективное использование ресурсов.
- Анализ масштабируемости: Функция анализа масштабируемости помогает выявить потенциальные «узкие» места и оптимизировать производительность системы при увеличении рабочей нагрузки.

Недостатки:

- Ограниченная среда моделирования: FogTorch в основном ориентирован на оптимизацию, и в нем отсутствует комплексная среда моделирования для оценки сложных сценариев туманных вычислений.
- Отсутствие визуализации: В инструменте отсутствуют расширенные возможности визуализации, что может ограничить возможность эффективного анализа и интерпретации результатов моделирования.

3. Fogbed: Это симулятор с открытым исходным кодом, который позволяет создавать виртуальные среды для моделирования туманных вычислительных систем. Fogbed позволяет исследователям создавать и настраивать различные узлы и сети в соответствии с требуемыми характеристиками, такими как процессор (CPU), память (RAM) и сетевая пропускная способность.

Ключевые особенности FogBed включают:[5]

- Моделирование узлов тумана: FogBed позволяет пользователям моделировать узлы тумана с различными вычислительными возможностями, объемом памяти и коммуникационными характеристиками, что обеспечивает реалистичное моделирование.
- Управление виртуальными машинами: Предоставляет механизмы для управления виртуальными машинами (VM) в узлах тумана, включая миграцию VM и распределение ресурсов.
- Интеграция устройств IoT: FogBed поддерживает интеграцию IoT-устройств, что позволяет моделировать взаимодействие IoT и тумана.

- Анализ энергопотребления: FogBed предлагает возможности анализа энергопотребления, что помогает в разработке энергоэффективных вычислительных систем тумана (fog).

Преимущества:

- Реалистичное моделирование: FogBed предоставляет реалистичную среду моделирования, позволяющую оценивать производительность приложений для туманных вычислений в различных сценариях.[6]
- Расширяемость: Пользователи могут расширять функциональность FogBed, подключая пользовательские модули и алгоритмы, что позволяет проводить индивидуальные моделирования.
- Открытый исходный код: открытым исходным кодом способствует совершенствованию продукта и введению новых функциональных особенностей.

Недостатки:

- Сложность: Широкие функции и возможности настройки FogBed могут оказаться сложными в эксплуатации и изучении, в особенности с новыми пользователями.
- Ограниченная визуализация: Возможности визуализации в FogBed существенно ограничены, что может стать препятствием для воспроизведения сценариев туманных вычислений.

4. FLAME: Эта система моделирования предназначена для моделирования межсетевого взаимодействия и ресурсного управления в туманных вычислительных системах. FLAME - это комплексная среда моделирования и симуляции, ориентированная на агентное моделирование систем туманных вычислений. Она представляет собой гибкую и масштабируемую платформу для моделирования крупномасштабных сценариев туманных вычислений.

FLAME - это инструмент который можно использовать на различных платформах, включая Windows, macOS и Linux. Он реализован преимущественно на C++, что обеспечивает высокую производительность моделирования.

Основные функциональные особенности:

- Агентное моделирование: FLAME позволяет пользователям моделировать и моделировать отдельных агентов, представляющих узлы тумана, IoT-устройства и другие объекты в экосистеме туманных вычислений.
- Масштабируемость: FLAME предназначен для крупномасштабного моделирования, позволяя оценивать системы туманных вычислений со значительным числом агентов.
- Моделирование коммуникаций: FLAME предоставляет механизмы для моделирования и имитации коммуникационных протоколов и взаимодействия между агентами, что позволяет реалистично моделировать туманные вычисления.
- Динамическая среда: FLAME поддерживает моделирование динамических сред, что позволяет оценивать системы туманных вычислений в изменяющихся условиях.

Преимущества:

- Агентный подход: Агентный подход к моделированию FLAME позволяет детально представить отдельные объекты и их взаимодействие, что дает представление о поведении и производительности вычислительных систем тумана.

- Масштабируемость: Способность FLAME к крупномасштабному моделированию делает его пригодным для оценки сложных сценариев туманных вычислений со значительным числом агентов.
- Гибкость: FLAME предлагает гибкую платформу, которая может быть настроена для моделирования различных архитектур и сценариев туманных вычислений.

Недостатки:

- Сложность использования: Агентный подход к моделированию в FLAME требует глубокого понимания концепций агентного моделирования.
- Ограниченная визуализация: FLAME не предоставляет широких средства для визуализации моделируемых сред, что может существенно ограничить возможности использования платформы.

5. FFCloudSim: FFCloudSim - это набор инструментов для моделирования и симуляции, специально разработанный для туманных и пограничных вычислительных сред. Он основан на популярном фреймворке CloudSim и расширяет его возможности для сценариев туманных вычислений. FFCloudSim позволяет моделировать различные алгоритмы и стратегии развития туманно-вычислительных систем. Приведём основные особенности системы:

- Моделирование мобильности: FFCloudSim поддерживает моделирование мобильных узлов тумана с различными характеристиками, что облегчает оценку приложений туманных вычислений с учетом мобильности.
- Моделирование с учетом энергопотребления: Позволяет пользователям оценивать энергопотребление узлов тумана, помогая в разработке энергоэффективных приложений.
- Планирование задач: Поддерживает алгоритмы планирования задач для оптимизации использования ресурсов и минимизации задержек в средах туманных вычислений.

Преимущества:

- Реализация CloudSim: FFCloudSim опирается на широко используемый фреймворк CloudSim, что облегчает пользователям, уже знакомым с CloudSim, переход к моделированию туманных вычислений.
- Возможности планирования задач: Алгоритмы планирования задач в FFCloudSim помогают оптимизировать распределение ресурсов и повысить общую производительность системы.

Недостатки:

- Ограниченный анализ масштабируемости: В FFCloudSim отсутствуют возможности всестороннего анализа масштабируемости, что может ограничить оценку поведения системы при различной рабочей нагрузке и доступности ресурсов.
- Относительно новый инструмент: FFCloudSim - относительно новый инструмент, и его функционал может быть не таким обширным, как у других хорошо зарекомендовавших себя систем моделирования.

Заключение

Системы моделирования играют важнейшую роль в оценке и оптимизации систем туманных вычислений. В то время как одни системы предлагают комплексную среду моделирования, другие в большей степени ориентированы на оптимизацию и анализ масштабируемости. Системы имеют свои преимущества и недостатки, и их выбор зависит от конкретных требований сценария туманных вычислений. Пользователи и исследователи могут использовать эти системы моделирования для разработки и развертывания эффективных приложений для туманных вычислений, что в конечном итоге позволит раскрыть весь потенциал сред с туманными вычислениями и эффективно воспроизводить сложные сценарии эксплуатации сред тумана.

Список литературы

1. G.A.Fortino, R.Gravina, and W.Russo, "iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in the Internet of Things, Edge and Fog Computing Environments," *Software: Practice and Experience*, vol. 47, no. 9, pp. 1275-1296, 2017.
2. M.Capra, M.Musolesi, and J.Crowcroft, "FogTorch: A Performance Evaluation Framework for Fog Computing," *ACM Transactions on Internet Technology*, vol. 18, no. 2, pp. 1-23, 2018.
3. A.Yousefpour, M.F.Zhani, and R.Langar, "FogBed: A Comprehensive Simulation and Emulation Environment for Fog Computing," *IEEE Access*, vol. 6, pp. 26418-26433, 2018.
4. M.Aazam, M.St-Hilaire, and L. Lung, "FFCloudSim: A Toolkit for Modeling and Simulation of Fog and Edge Computing Environments," *Future Generation Computer Systems*, vol. 88, pp. 239-251, 2018.
5. Turner A., Anagnostou A., & Tyler, P. (2017). FLAME GPU: A Novel Approach to Agent-Based Simulation. In *International Conference on Parallel Problem Solving from Nature* (pp. 1-14). Springer.
6. Turner A., Anagnostou A., & Tyler P. (2019). FLAME: A Framework for Large-Scale Agent-Based Modelling and Simulation. *Journal of Artificial Societies and Social Simulation*, 22(1), 10.

References

1. G. A. Fortino, R. Gravina, and W. Russo, "iFogSim: A Toolkit for Modeling and Simulation of Resource Management Techniques in the Internet of Things, Edge and Fog Computing Environments," *Software: Practice and Experience*, vol. 47, No. 9, pp. 1275-1296, 2017.
2. M. Capra, M. Musolesi, and J. Crowcroft, "FogTorch: A Performance Evaluation Framework for Fog Computing," *ACM Transactions on Internet Technology*, vol. 18, No. 2, pp. 1-23, 2018.
3. A. Yousefpour, M. F. Zhani, and R. Langar, "FogBed: A Comprehensive Simulation and Emulation Environment for Fog Computing," *IEEE Access*, vol. 6, pp. 26418-26433, 2018.
4. M. Aazam, M. St-Hilaire, and L. Lung, "FFCloudSim: A Toolkit for Modeling and Simulation of Fog and Edge Computing Environments," *Future Generation Computer Systems*, vol. 88, pp. 239-251, 2018.

5. Turner, A., Anagnostou, A., & Tyler, P. (2017). FLAME GPU: A Novel Approach to Agent-Based Simulation. In International Conference on Parallel Problem Solving from Nature (pp. 1-14). Springer.
 6. Turner, A., Anagnostou, A., & Tyler, P. (2019). FLAME: A Framework for Large-Scale Agent-Based Modelling and Simulation. *Journal of Artificial Societies and Social Simulation*, 22(1), 10.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.046

РЕИНЖИНИРИНГ БИЗНЕС-ПРОЦЕССА «ОРГАНИЗАЦИЯ ПРЕМИРОВАНИЯ ОСНОВНОГО ПЕРСОНАЛА» НА ПРИМЕРЕ АПТЕЧНОЙ ОРГАНИЗАЦИИ

¹Кириллина Ю.В., ²Курнаков К.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: ¹jvk05@mail.ru, ²kurnakov.k.a@edu.mirea.ru

В статье рассмотрен результат реинжиниринга бизнес-процесса «Организация премирования основного персонала» в аптечной организации. На основе исследования организации сформировано текстовое описание бизнес-процесса и построена графическая модель "as is" в нотации IDEF0. Последующий структурный анализ позволил сформулировать проблемы в текущем исполнении бизнес-процесса. Для совершенствования бизнес-процесса проведен реинжиниринг процесса и построена модель "to be" с возможными изменениями в его выполнении. Количественный анализ времени выполнения процесса в вариантах исполнения "as is" и "to be" позволил сделать выводы о целесообразности реинжиниринга.

Ключевые слова: Бизнес-процесс, реинжиниринг бизнес-процессов, IDEF0, структурный анализ, количественный анализ, информационная система.

REENGINEERING OF THE BUSINESS PROCESS "ORGANIZATION OF BONUSES FOR KEY PERSONNEL" ON THE EXAMPLE OF A PHARMACY ORGANIZATION

¹Kirillina Yu.V., ²Kurnakov K.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹jvk05@mail.ru, ²kurnakov.k.a@edu.mirea.ru

The article considers the result of the reengineering of the business process "Organization of bonuses for key personnel" in a pharmacy organization. Based on the study of a typical organization, a textual description of the business process was formed and a graphical model "as is" in IDEF0 notation was built. The subsequent structural analysis allowed us to formulate problems in the current execution of the business process. To improve the business process, the process was reengineered and a "to be" model was built with possible changes in its implementation. A quantitative analysis of the process execution time in the "as is" and "to be" versions allowed us to draw conclusions about the feasibility of reengineering.

Keywords: Business process, reengineering of business processes, IDEF0, structural analysis, quantitative analysis, information system.

Основоположники теории реинжиниринга бизнес-процессов М. Хаммер и Дж. Чампи определили реинжиниринг бизнес-процессов как: «... фундаментальное переосмысление и радикальное перепроектирование бизнес-процессов для достижения существенных улучшений в таких ключевых показателях результативности, как затраты, качество, уровень обслуживания и оперативность» [5, с. 59].

В настоящее время реинжинирингом называют совокупность методов и средств, предназначенных для улучшений основных показателей деятельности любого (малого, среднего, крупного) предприятия, при помощи которых переосмысливается и перепроектируется существующий бизнес-процесс предприятия. Реинжиниринг бизнес-процесса организации позволяет улучшить показатели деятельности организации, а также снизить затраты на выполнение бизнес-процесса.

Одним из направлений реализации реинжиниринга является изменение технологии сбора, обработки, передачи и хранения информации, реализуемое в бизнес-процессе. Именно данное направление было выбрано при решении вопроса реинжиниринга обеспечивающего процесса «Организация премирования основного персонала» в аптечной организации.

Премирование — это выплата работникам денежных средств сверх основного заработка в целях поощрения за достижение определенных результатов, выполнение обязательств, стимулирования их деятельности [4, с. 113].

Бизнес-процесс «Организация премирования основного персонала» в аптечной организации начинается с анализа существующей системы премирования. Специалист по оценке персонала анализирует размер начисленной премии основным сотрудникам аптечной организации, анализирует объем проданных лекарственных препаратов и формирует отчет. Затем бухгалтер определяет бюджет премиального фонда на основе информации о количестве сотрудников аптечной организации и отчета, содержащего информацию о доходах и расходах аптечной организации. Задача бухгалтера определить чистый доход организации и размер части чистого дохода для премиального фонда. Бухгалтер формирует бюджет премиального фонда, в котором указывается информация о том, сколько денежных средств будет выделено в премиальный фонд. Бухгалтер согласовывает сформированный бюджет премиального фонда с генеральным директором и передает согласованный документ для дальнейшей обработки руководителю аптечного отдела. Руководитель аптечного отдела получает отчет «Анализ эффективности системы премирования» от специалиста по оценке персонала, а от бухгалтера согласованный бюджет премиального фонда. Затем руководитель аптечного отдела определяет вид премии и размер премиальной выплаты. После этого формирует служебную записку о премировании работников и согласовывает ее с генеральным директором аптечной организации.

В завершении процесса «Организация премирования основного персонала» бухгалтер получает согласованную служебную записку о премировании работников и согласованный бюджет премиального фонда, сравнивает премиальный фонд с суммой назначенных премиальных выплат и формирует отчет о результате сравнения с последующей передачей его генеральному директору.

Графическая модель "as is" бизнес-процесса «Организация премирования основного персонала» в аптечной организации в нотации IDEF0, отображающей процесс на уровне функций [2, с. 140], представлена на Рисунках 1-6.

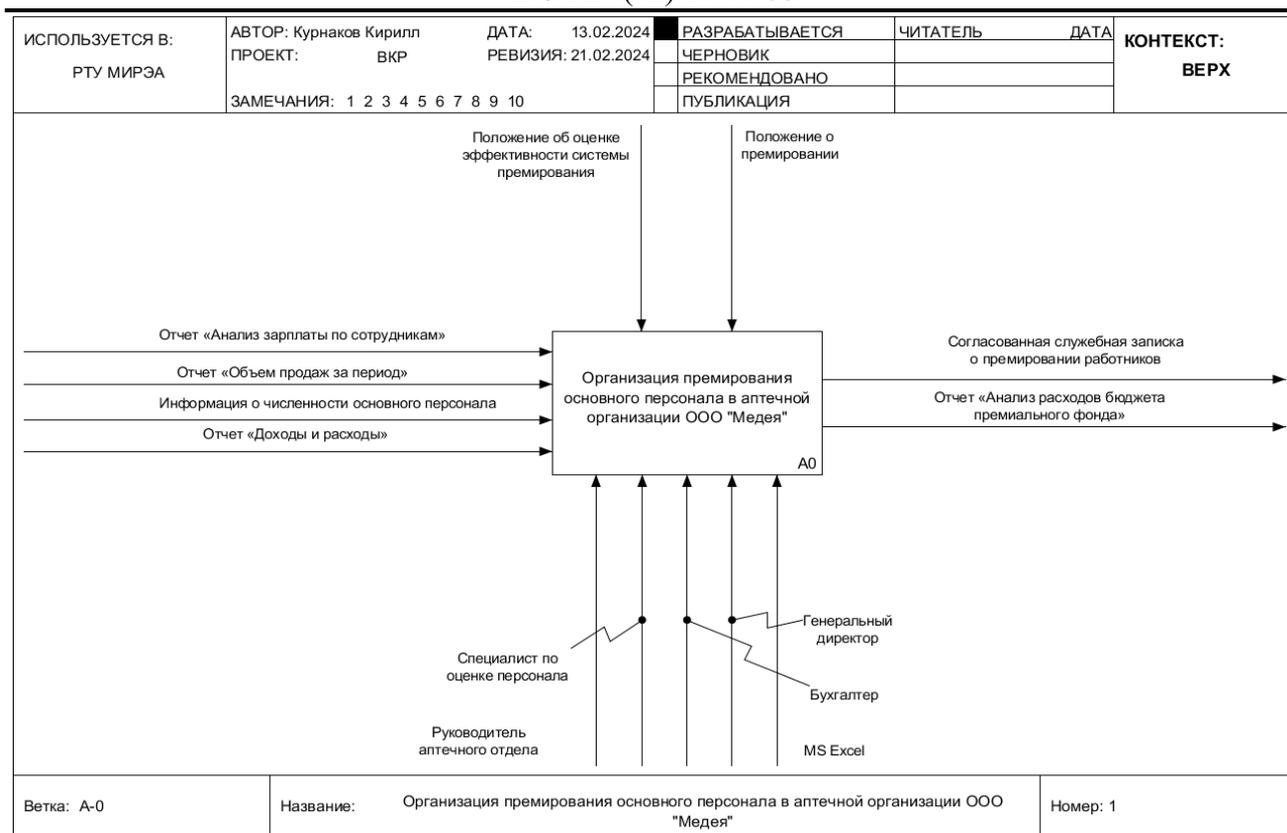


Рисунок 1 – Контекстная диаграмма бизнес-процесса «Организация премирования основного персонала»

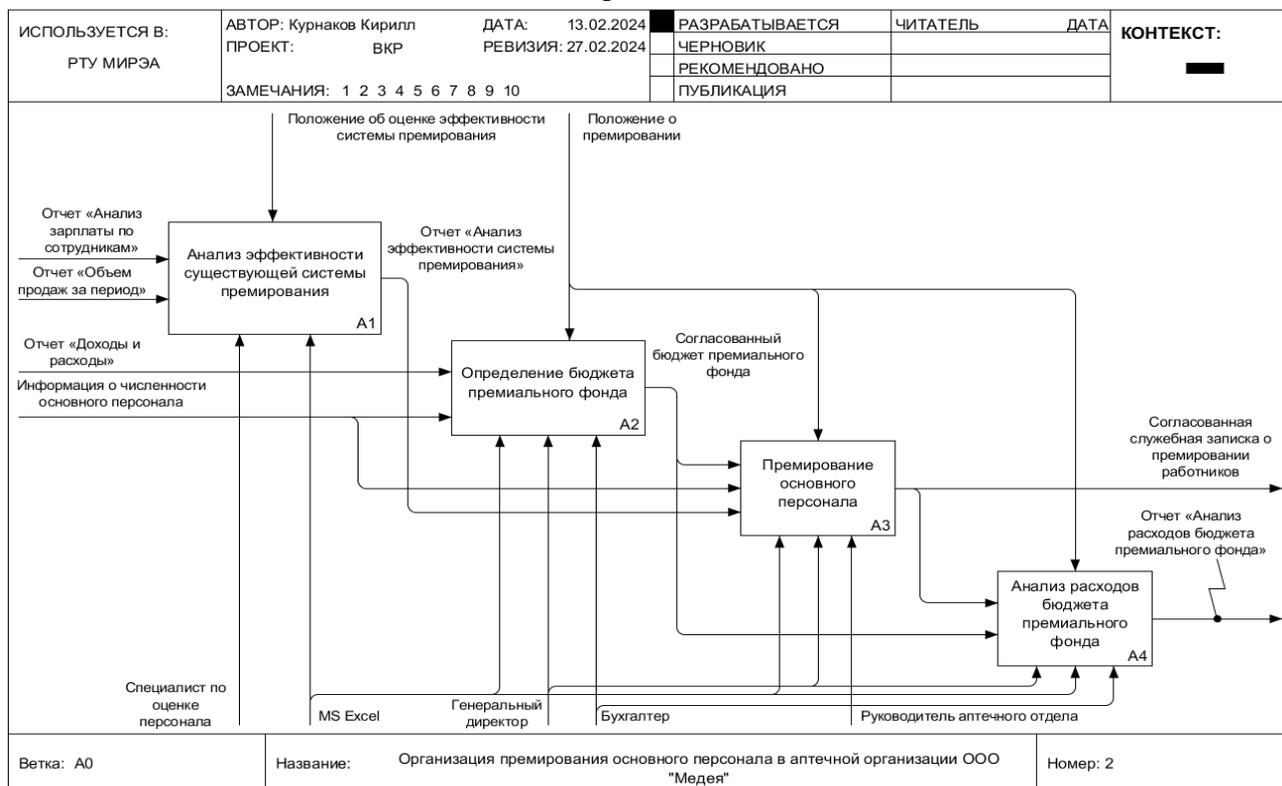


Рисунок 2 – Декомпозиция контекстной диаграммы бизнес-процесса «Организация премирования основного персонала»

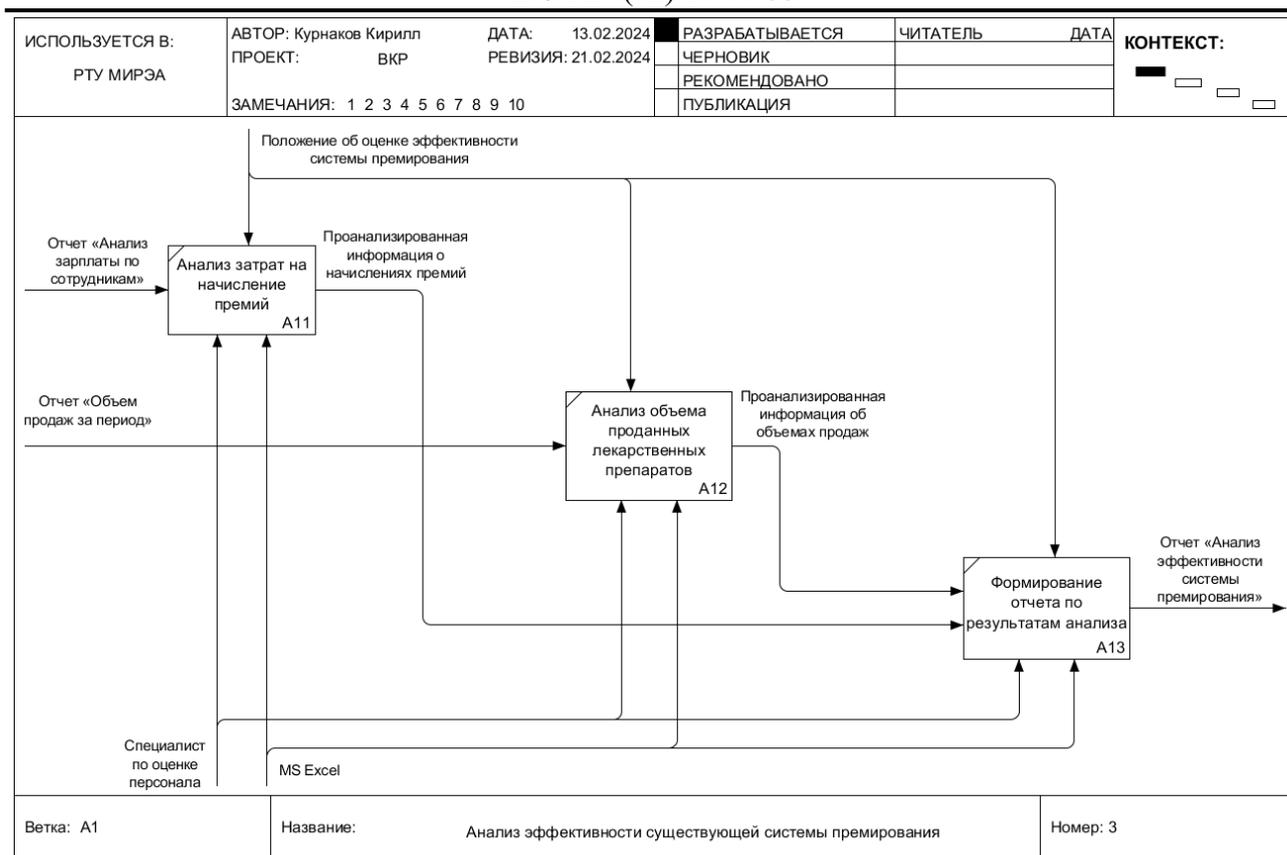


Рисунок 3 – Декомпозиция подпроцесса «Анализ эффективности существующей системы премирования»

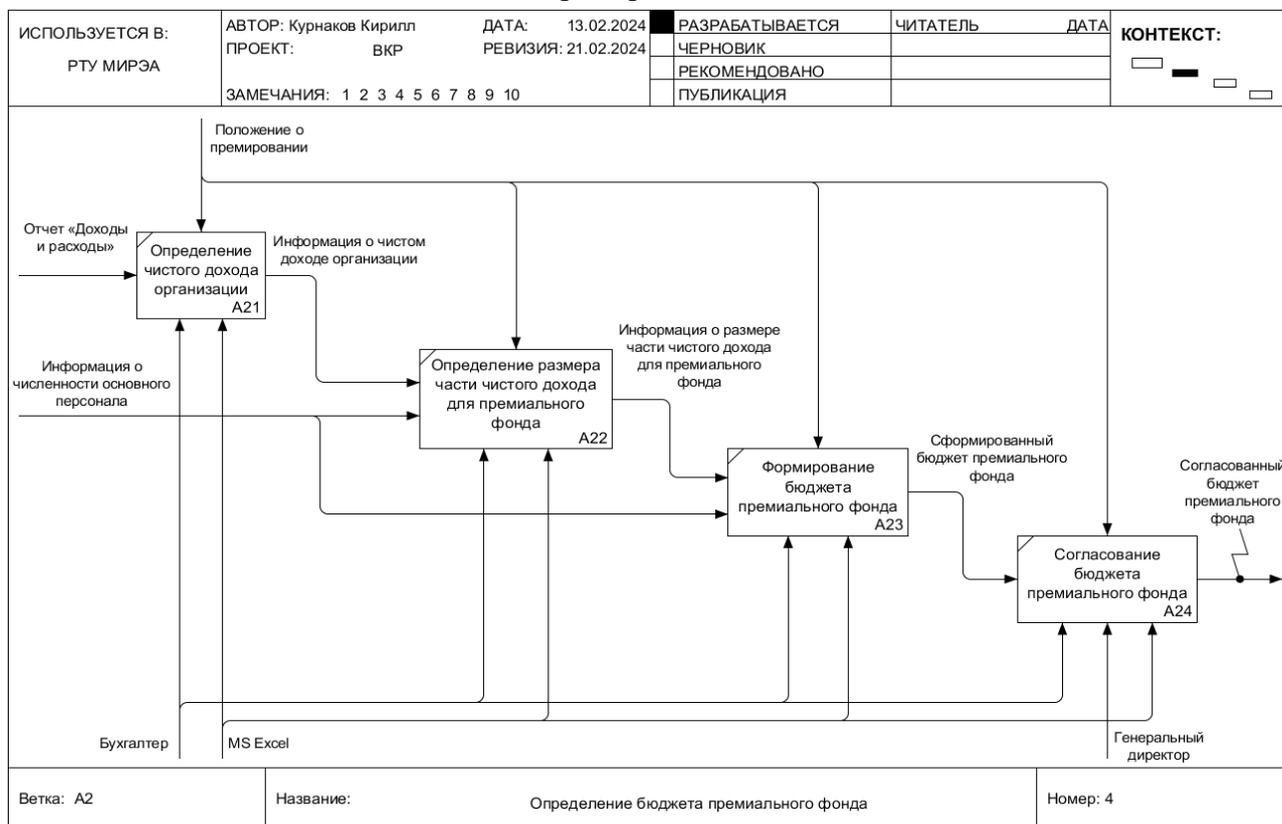


Рисунок 4 – Декомпозиция подпроцесса «Определение бюджета премиального фонда»

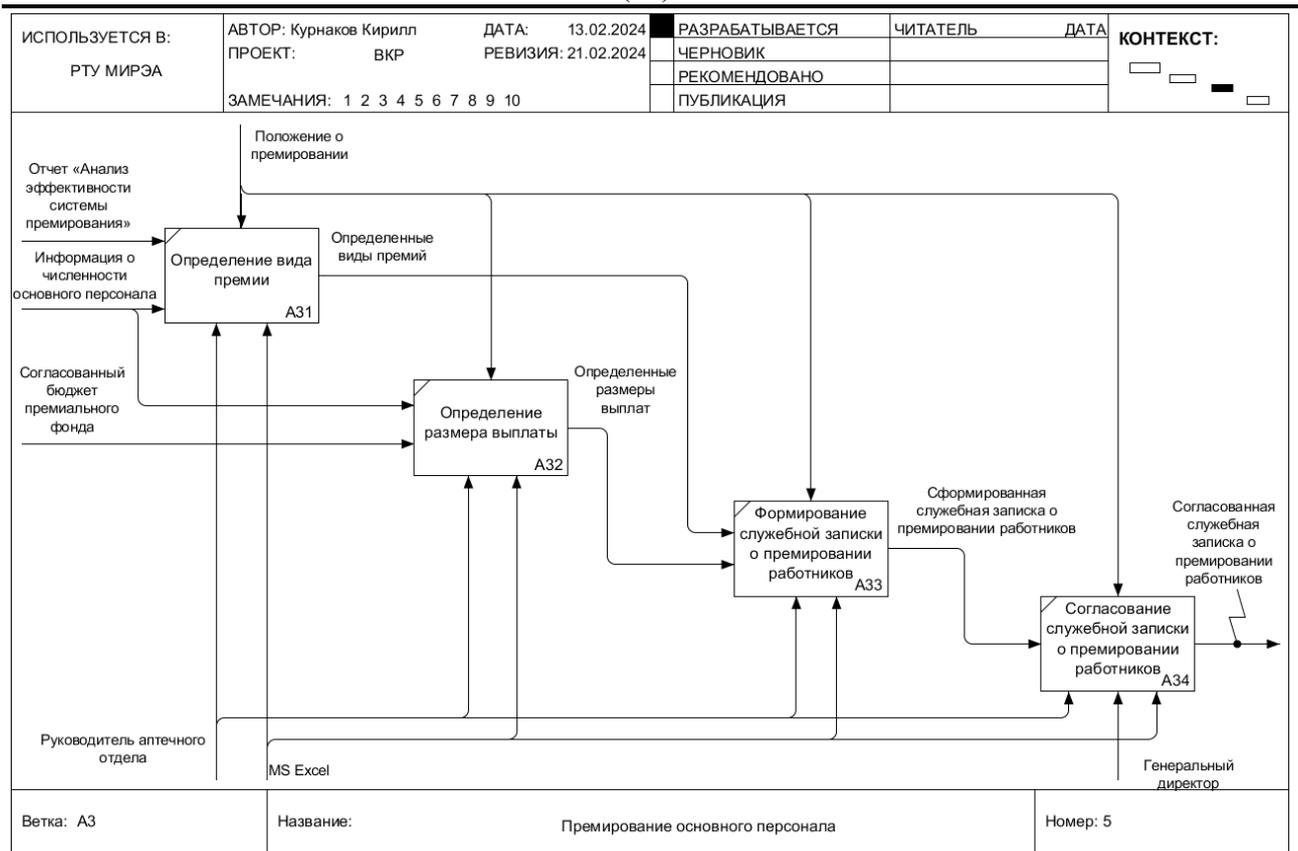


Рисунок 5 – Декомпозиция подпроцесса «Премирование основного персонала»

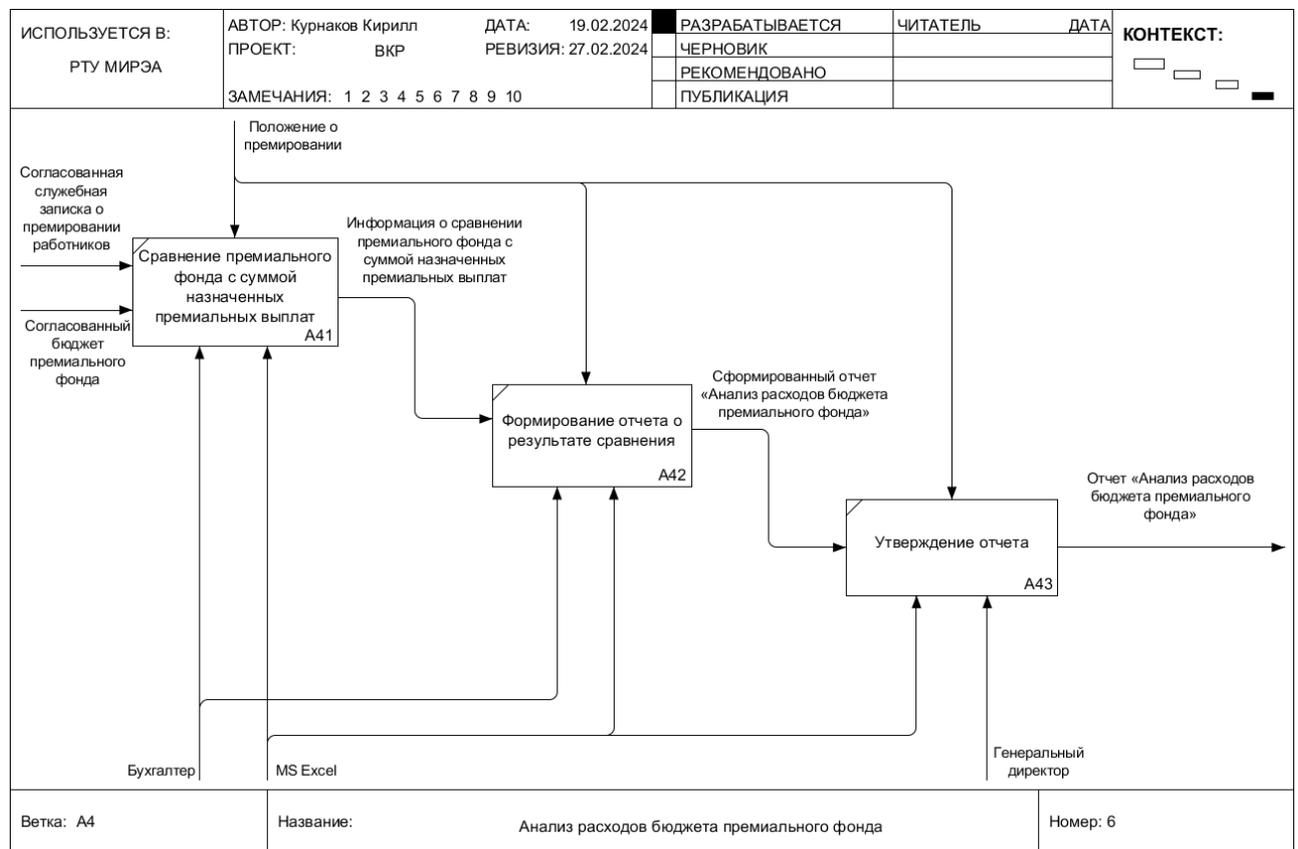


Рисунок 6 – Декомпозиция подпроцесса «Анализ расходов бюджета премиального фонда»

Графическая модель процесса "as is" бизнес-процесса «Организация премирования основного персонала» была подвергнута структурному анализу, который позволяет обнаружить «слабые места» в процессе.

В рамках структурного анализа проводится оценка целостности процесса с точки зрения согласования с его организационной структурой, информационным обеспечением и ИТ-системами с помощью так называемых точек перехода. Точка перехода — это смена одного из ресурсов процесса (человеческого, информационного, ИТ-системного и т.д.).

Организационный разрыв — это один из видов «точки перехода», когда происходит смена исполнителя при выполнении последовательных функций процесса [3, с. 206].

Основной вопрос анализа организационных разрывов — сколько их, как часто они происходят, насколько они оправданы и как отработаны интерфейсы при смене исполнителя.

В качестве механизма исполнения в процессе используется MS Excel, при этом внутренней системы для передачи файлов между сотрудниками в организации нет. Когда происходит смена исполнителя процесса, то все документы передаются следующему исполнителю посредством внешних носителей информации (USB-флеш-накопитель, внешний жесткий диск) или с использованием корпоративной почтовой системы. В связи с этим, могут возникать потери информации, также достаточно велик риск человеческой ошибки при заполнении документов, при формировании отчетов и при подсчетах экономических показателей. Все это замедляет бизнес-процесс, тем самым отражая несовершенство сбора, обработки, хранения и передачи информации в аптечной организации.

Существует два подхода к упрощению процесса и устранению организационных разрывов в нем. Это «горизонтальное сжатие процесса» и «вертикальное сжатие процесса». Суть сжатия состоит в том, чтобы сократить число участников, и за счет этого, соответственно, уменьшить количество организационных разрывов и петель в процессе, повысить его управляемость, сократить время выполнения.

В бизнес-процессе «Организация премирования основного персонала» существуют организационные разрывы между подпроцессами. Так подпроцесс «Анализ эффективности существующей системы премирования» выполняет специалист по оценке персонала. На выходе данного подпроцесса формируется документ, который далее передается руководителю аптечного отдела. Смена исполнителя процесса негативно влияет на ход исполнения процесса, тем самым замедляя его. Устранить выявленные организационные разрывы в бизнес-процессе «Организация премирования основного персонала» возможно через реинжиниринг посредством изменения технологии сбора, обработки, передачи и хранения информации, то есть путем автоматизации процесса.

В результате применения новой технологии сбора, обработки, передачи и хранения информации подпроцесс «Анализ эффективности существующей системы премирования» будет выполняться руководителем аптечного отдела. Руководитель аптечного отдела получив отчеты «Анализ зарплаты по сотрудникам» и «Объем продаж за период», с помощью информационной системы сможет проводить анализ заработной платы сотрудников и объема проданных лекарственных препаратов за период по каждому сотруднику. Информационная система будет автоматически подсчитывать уровень выполнения плана сотрудником за определенный период. Далее с помощью информационной системы руководитель аптечного

отдела сможет сформировать отчет о результатах анализа существующей системы премирования.

В свою очередь бухгалтер с помощью информационной системы сможет определять чистый доход аптечной организации за определенный период и бюджет премиального фонда.

Затем руководитель аптечного отдела, получив отчет «Анализ эффективности системы премирования», согласованный бюджет премиального фонда, информацию о количестве сотрудников, сможет с помощью информационной системы определить вид и размер премии для выплаты определенному сотруднику. Далее будет формироваться служебная записка о премировании работников, которая согласуется с генеральным директором аптечной организации.

В завершении процесса бухгалтер сможет сравнить премиальный фонд с суммой назначенных премиальных выплат и сформировать отчет с полученными результатами.

На Рисунках 7-12 представлена графическая модель бизнес-процесса «Организация премирования основного персонала» в аптечной организации в нотации IDEF0 после проведения реинжиниринга.

Новая технология выполнения бизнес-процесса «Организация премирования основного персонала» потенциально позволит снизить затраты на выполнение процесса, сократить время выполнения процесса и уменьшить вероятность человеческих ошибок.

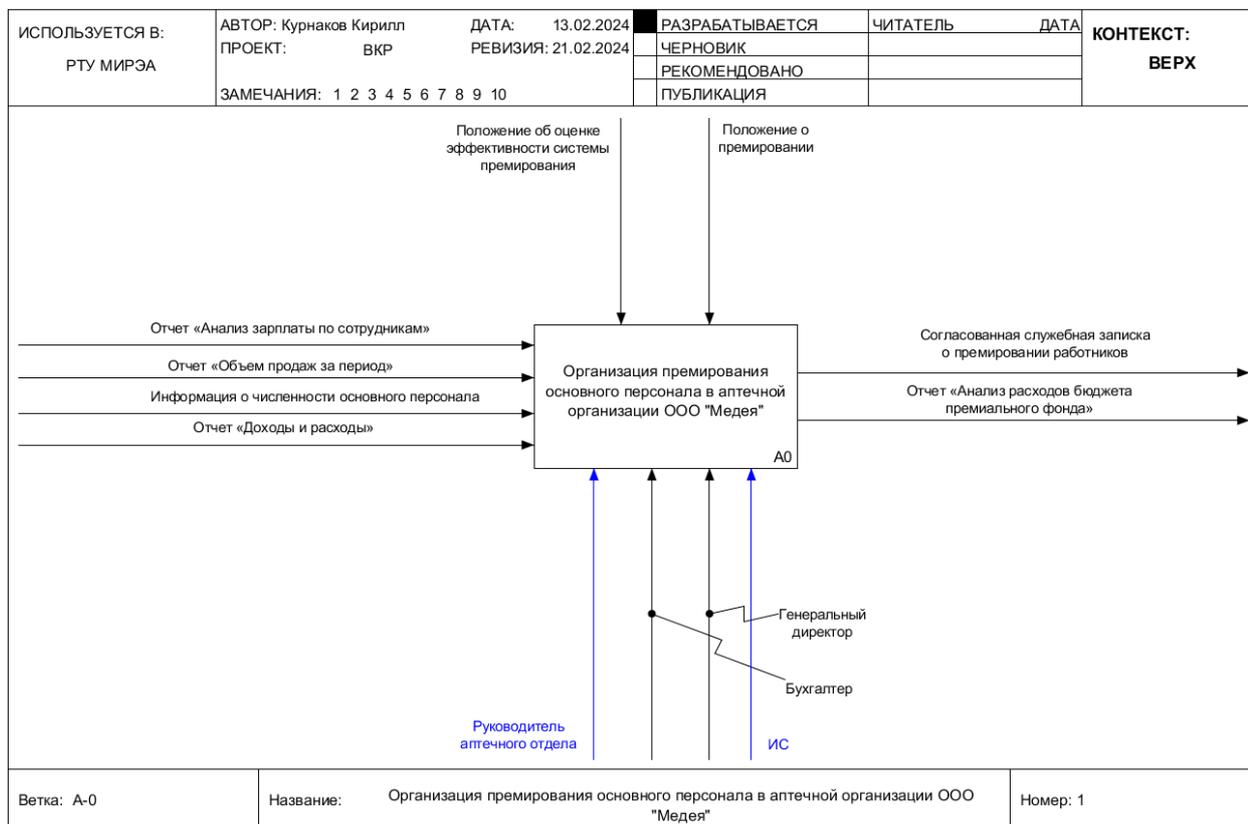


Рисунок 7 – Контекстная диаграмма бизнес-процесса «Организация премирования основного персонала». Модель "to be"

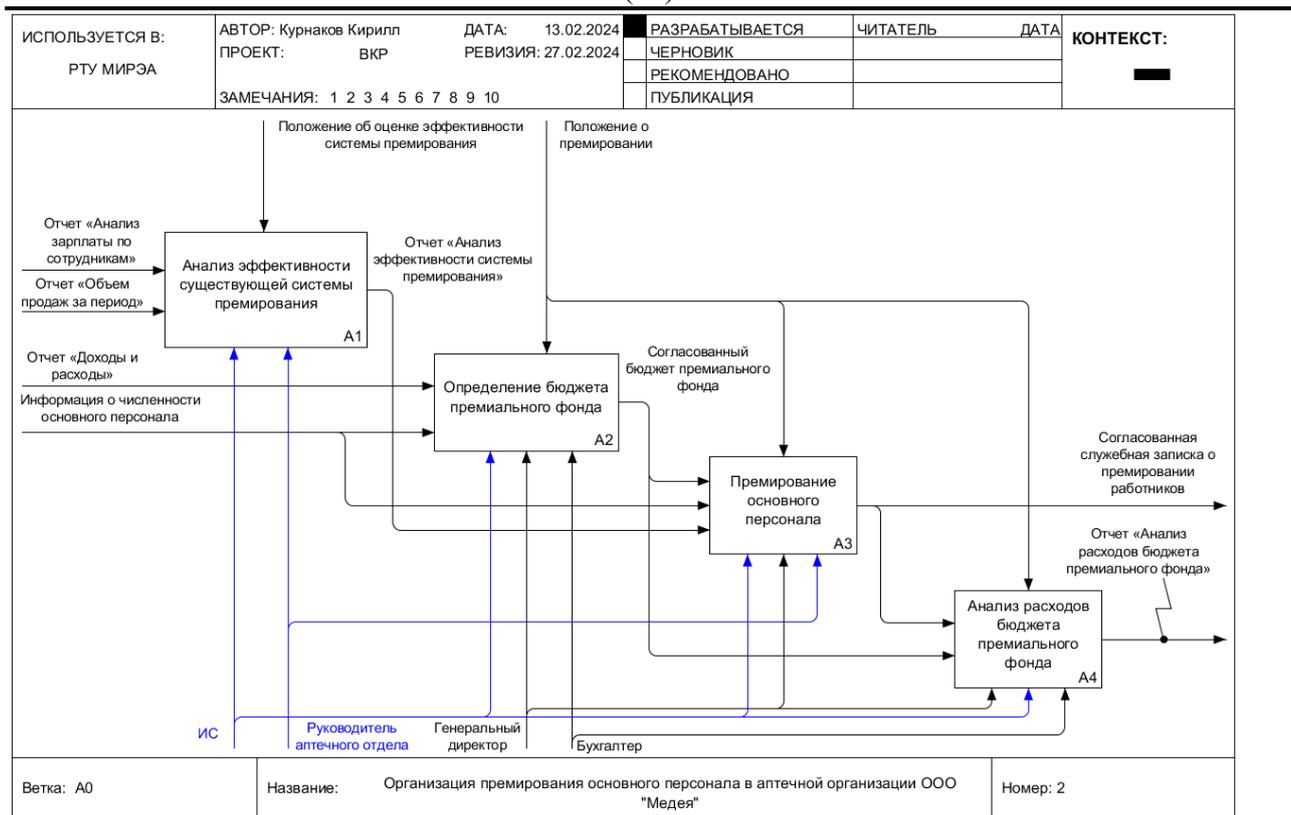


Рисунок 8 – Декомпозиция контекстной диаграммы бизнес-процесса «Организация премирования основного персонала». Модель "to be"

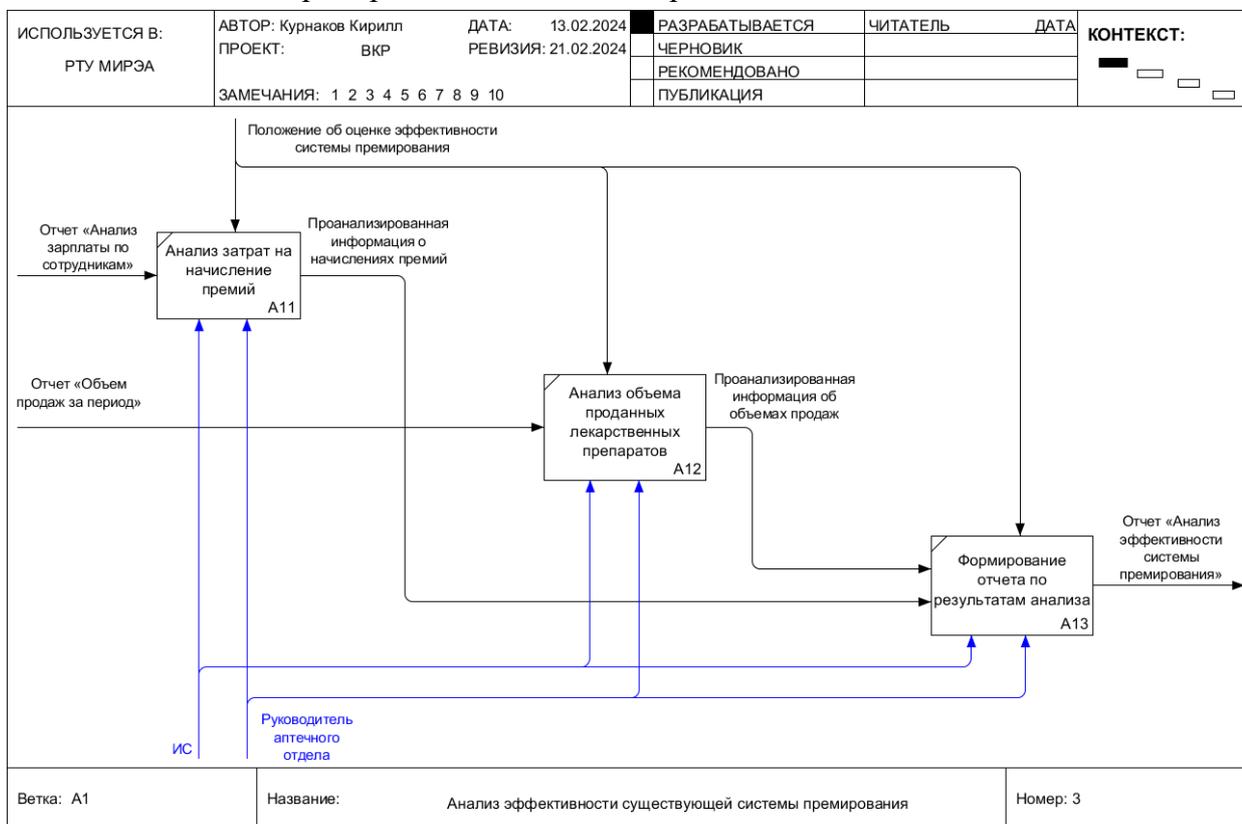


Рисунок 9 – Декомпозиция подпроцесса «Анализ эффективности существующей системы премирования». Модель "to be"

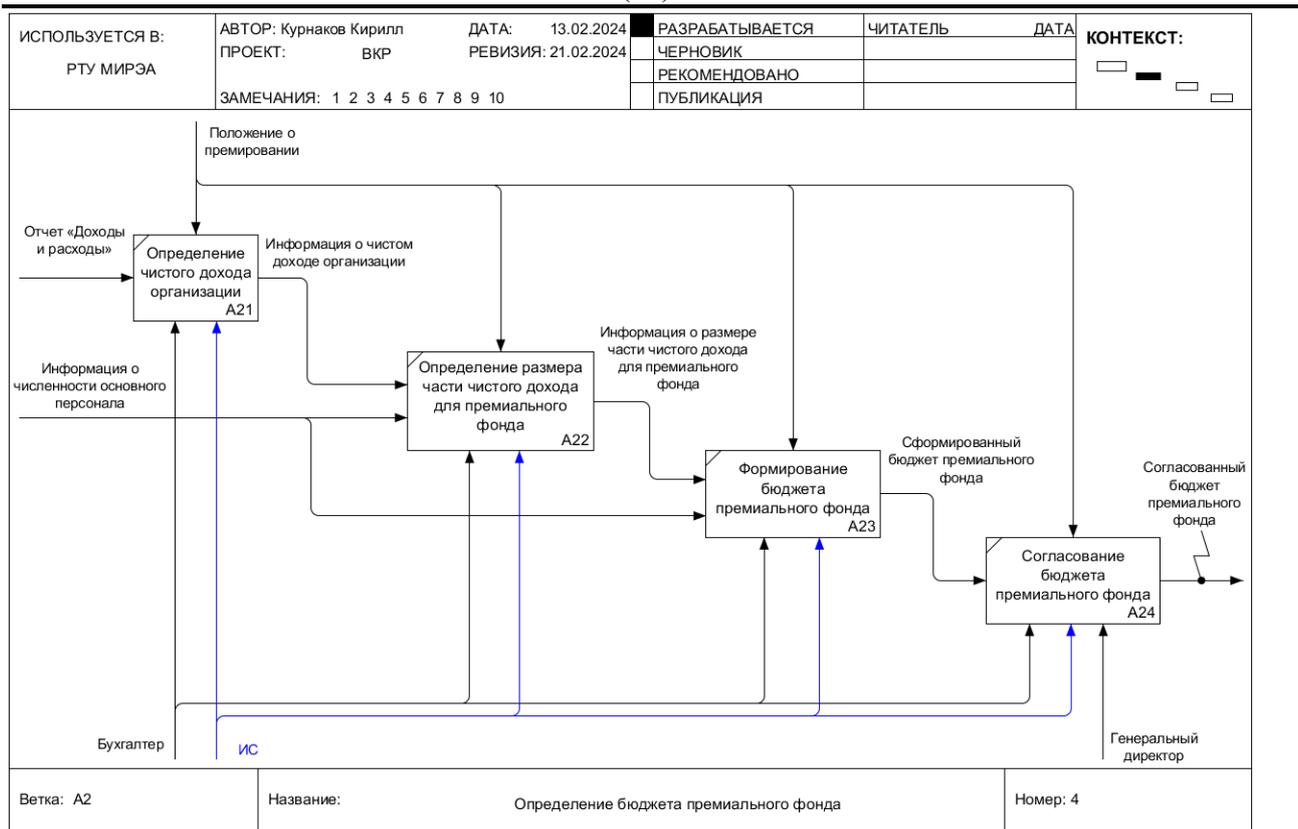


Рисунок 10 – Декомпозиция подпроцесса «Определение бюджета премиального фонда». Модель "to be"

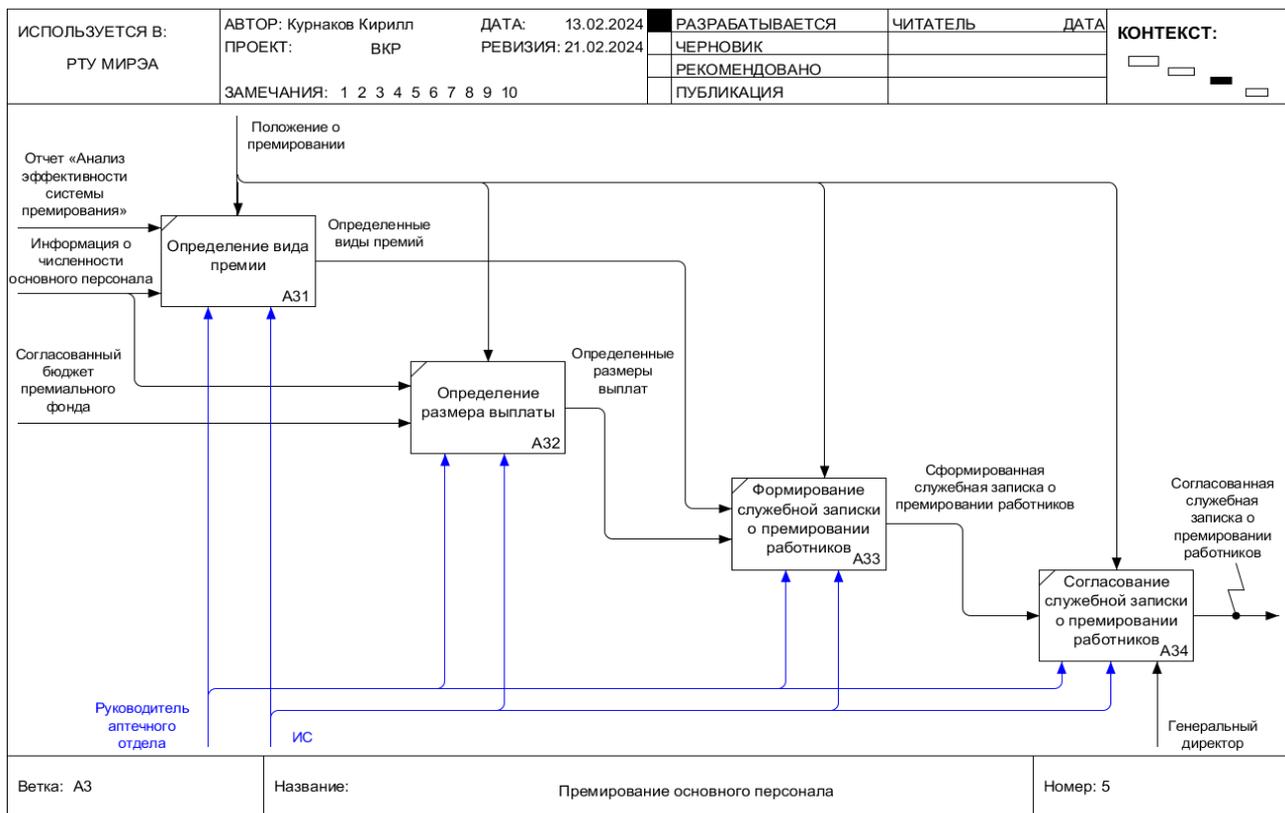


Рисунок 11 – Декомпозиция подпроцесса «Премирование основного персонала». Модель "to be"

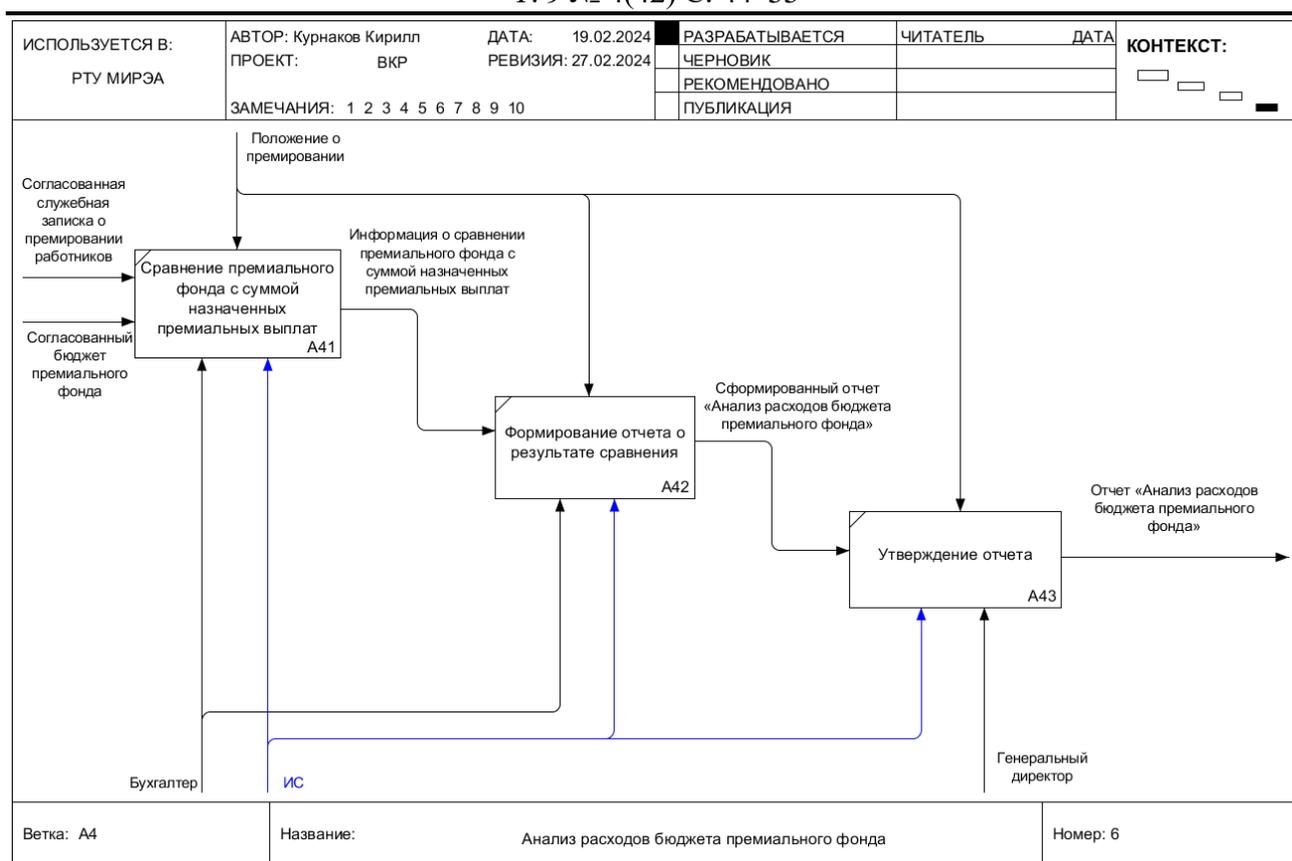


Рисунок 12 – Декомпозиция подпроцесса «Анализ расходов бюджета премиального фонда». Модель "to be"

Для оценки улучшений бизнес-процесса «Организация премирования основного персонала» аптечной организации был выбран количественный анализ, который использует «... абсолютные и относительные показатели, характеризующие время выполнения процесса, использование технологий, стоимость и качество» [1, с. 223].

В результате количественного анализа времени выполнения функций в бизнес-процессе «Организация премирования основного персонала» построена Таблицы 1, которая наглядно демонстрирует разницу во времени выполнения процесса в варианте исполнения "as is" и в варианте исполнения "to be".

Таблица 1 – Количественный анализ времени выполнения бизнес-процесса

Наименование функции	Время выполнения функции ("as is"), ч	Время выполнения функции ("to be"), ч
Анализ затрат на начисление премий	6	3
Анализ объема проданных лекарственных препаратов	6	3
Формирование отчета по результатам анализа существующей системы премирования	2	1
Определение чистого дохода аптечной организации	6	3

Определение размера части чистого дохода для премиального фонда	6	3
Формирование бюджета премиального фонда	2	1
Согласование бюджета премиального фонда	2	2
Определение вида премии	6	3
Определение размера выплаты	6	3
Формирование служебной записки о премировании работников	2	1
Согласование служебной записки о премировании работников	2	2
Сравнение премиального фонда с суммой назначенных премиальных выплат	6	3
Формирование отчета о результате сравнения	2	1
Итого	54	29

Таким образом, реинжиниринг бизнес-процесса «Организация премирования основного персонала» на основе уменьшения количества точек перехода, а также изменения технологии сбора, обработки, передачи и хранения информации с помощью внедрения информационной системы позволит снизить время выполнения процесса на 25 часов, и положительно повлияет на результаты выполнения процесса.

Список литературы

1. Долганова О. И, Виноградова Е. В., Лобанова А. М. Моделирование бизнес-процессов. М. : Юрайт, 2017. 289 с.
2. Зараменских Е. П. Управление жизненным циклом информационных систем. М. : Юрайт, 2019. 431 с.
3. Каменнова М. С., Крохин В. В, Машков И. В. Моделирование бизнес-процессов. Часть 1. М. : Юрайт, 2018. 282 с.
4. Ростик О. М., Стариков Е.М., Гамбург А.В., Костина Г.А., Кожевников М.В. Организация мотивации и оплаты труда. Екатеринбург : УФУ. 2019. 256 с.
5. Хаммер М., Чампи Дж. Реинжиниринг корпорации: Манифест революции в бизнесе. СПб. : Издательство С.-Петербургского университета. 1997. 332 с.

References

1. Dolganova O. I., Vinogradova E. V., Lobanova A.M. Modeling of business processes. Moscow : Yurayt, 2017. p.289
2. Zaramenskikh E. P. Information systems lifecycle management. Moscow : Yurait, 2019. p.431
3. Kamennova M. S., Krokhin V. V., Mashkov I. V. Modeling of business processes. Part 1. Moscow : Yurait, 2018. p.282

4. Rostik O. M., Starikov E.M., Hamburg A.V., Kostina G.A., Kozhevnikov M.V. Organization of motivation and remuneration. Yekaterinburg : Ufa. 2019. p. 256
 5. Hammer M., Champy J. Reengineering the corporation: A Manifesto for business revolution. St. Petersburg : St. Petersburg University Press. 1997. p.332
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

АНАЛИЗ ЦИФРОВЫХ СЛЕДОВ И СРЕДСТВ РАССЛЕДОВАНИЯ В ОБЛАСТИ КИБЕРПРЕСТУПНОСТИ

¹Куликова А.В., ²Богословский Ф.И.

ФГБОУ ВО "МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Н.Э. БАУМАНА (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)", Москва, Россия (105005, город Москва, 2-Я Бауманская ул, д. 5 стр. 1), e-mail: ¹kagamine_2000@mail.ru, ²f3dorasta@gmail.com

Настоящая научная статья посвящена анализу цифровых следов и средств расследования в области киберпреступности. В современном информационном обществе киберпреступность становится все более распространенной и серьезной угрозой. Цифровые следы, оставленные преступниками в сети, представляют собой ценный источник информации для правоохранительных органов и специалистов по кибербезопасности.

Статья рассматривает методы анализа цифровых следов, включая техники сбора и обработки данных, а также инструменты для выявления и атрибуции киберпреступных действий. Особое внимание уделяется использованию машинного обучения и искусственного интеллекта в процессе анализа цифровых следов, что позволяет повысить эффективность и точность расследования.

Исследование также охватывает актуальные проблемы и вызовы, с которыми сталкиваются специалисты по кибербезопасности при работе с цифровыми следами. В заключение, статья делает выводы о значимости дальнейших исследований в области анализа цифровых следов и развитии средств расследования для борьбы с киберпреступностью.

Ключевые слова: Цифровые следы, киберпреступность, расследование, машинное обучение, искусственный интеллект, кибербезопасность.

ANALYSIS OF DIGITAL TRACES AND INVESTIGATIVE TOOLS IN THE FIELD OF CYBERCRIME

¹Kulikova A.V., ²Bogoslovsky F.I.

BAUMAN MOSCOW STATE TECHNICAL UNIVERSITY (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia (105005, Moscow, 2nd Baumanskaya str., 5/1), e-mail: ¹kagamine_2000@mail.ru, ²f3dorasta@gmail.com

This scientific article is devoted to the analysis of digital traces and investigative tools in the field of cybercrime. In today's information society, cybercrime is becoming an increasingly common and serious threat. Digital traces left by criminals online provide a valuable source of information for law enforcement and cybersecurity professionals.

The article examines methods for analyzing digital traces, including techniques for collecting and processing data, as well as tools for identifying and attributing cybercriminal actions. Particular attention is paid to the use of machine learning and artificial intelligence in the process of analyzing digital traces, which makes it possible to increase the efficiency and accuracy of the investigation.

The study also covers current issues and challenges faced by cybersecurity professionals when dealing with digital footprints. In conclusion, the article draws conclusions about the significance of further research in the field of digital trace analysis and the development of investigative tools to combat cybercrime.

Keywords: Digital footprints, cybercrime, investigation, machine learning, artificial intelligence, cybersecurity.

Введение

В современном информационном обществе киберпреступность становится все более острой и актуальной проблемой, представляя серьезную угрозу для безопасности как государственных структур, так и обычных граждан. Киберпреступники все чаще используют цифровые технологии для осуществления атак на информационные системы, кражи конфиденциальных данных и финансовых средств, а также для совершения других противоправных действий в сети.

Одним из ключевых аспектов борьбы с киберпреступностью является анализ цифровых следов, оставленных преступниками в процессе совершения противоправных действий. Цифровые следы могут содержать ценную информацию о методах атаки, идентификации преступников, их мотивах и связях. Правильный анализ этих следов позволяет выявить уязвимости в системе безопасности, предотвратить новые атаки и привлечь к ответственности злоумышленников.

Целью данного исследования является рассмотрение современных методов анализа цифровых следов и средств расследования в области киберпреступности. Мы стремимся изучить техники сбора и обработки данных, применяемые при анализе цифровых следов, а также рассмотреть возможности использования машинного обучения и искусственного интеллекта для улучшения эффективности расследования. Кроме того, мы намерены выявить актуальные проблемы и вызовы, с которыми сталкиваются специалисты по кибербезопасности при работе с цифровыми следами, и предложить пути их решения.

Теоретические основы анализа цифровых следов

Цифровые следы [1] представляют собой информацию, оставленную в цифровой форме в процессе взаимодействия человека с компьютерными системами, мобильными устройствами, интернет-сервисами и другими электронными средствами. Эти следы могут включать в себя данные о действиях пользователя, его посещениях в сети, использованных программных средствах и многое другое. Анализ цифровых следов направлен на извлечение ценной информации из этих данных для целей

Методы сбора и анализа данных

Сбор данных. [2] Для успешного анализа цифровых следов необходимо правильно собирать данные. Это может включать в себя использование специализированных инструментов для извлечения информации с компьютеров, мобильных устройств, сетевых устройств и других источников. Также важно сохранить целостность данных и обеспечить их безопасность во время сбора.

Обработка данных. После сбора данных необходимо провести их обработку для выделения ключевой информации. Это может включать в себя фильтрацию, структурирование, классификацию и агрегацию данных. Техники обработки данных могут зависеть от конкретных задач расследования.

Анализ данных. [3] После обработки данные подвергаются анализу с целью выявления закономерностей, связей и паттернов, которые могут помочь в раскрытии киберпреступлений.

В этом этапе могут применяться методы статистического анализа, машинного обучения, искусственного интеллекта и другие техники.

Визуализация данных. [4] Для наглядного представления результатов анализа цифровых следов часто используется визуализация данных. Это позволяет лучше понять структуру информации, выделить ключевые элементы и обнаружить скрытые закономерности.

Методы анализа цифровых следов

Цифровые следы, оставленные пользователями в сети, представляют собой богатый источник информации для расследования киберпреступлений [5]. Для анализа цифровых следов используются различные методы и техники, позволяющие извлечь ценные данные и выявить закономерности. Ниже приведены основные методы анализа цифровых следов с примерами использования.

1. *Анализ IP-адресов.* Анализ IP-адресов позволяет идентифицировать и отслеживать действия конкретного пользователя в сети. Путем анализа IP-адресов можно определить местоположение пользователя, его интернет-провайдера, использованные устройства и другую важную информацию.

Пример использования: при расследовании киберпреступлений анализ IP-адресов может помочь выявить источник атаки, идентифицировать злоумышленника и связать его с конкретными действиями в сети.

2. *Анализ метаданных.* Метаданные содержат информацию о данных, например, дату создания, автора, местоположение и другие атрибуты. Анализ метаданных позволяет получить дополнительные сведения о файле или сообщении.

Пример использования: при расследовании утечек информации анализ метаданных файлов может помочь определить источник утечки, автора документа или дату его создания.

3. *Анализ социальных сетей.* Анализ социальных сетей позволяет изучить взаимосвязи между пользователями, их активность в сети, интересы и другие данные. Этот метод широко используется для выявления связей между участниками киберпреступных группировок.

Пример использования: при расследовании организованных преступных группировок анализ социальных сетей может помочь выявить лидеров, участников и структуру группы.

4. *Анализ шаблонов поведения.* Анализ шаблонов поведения пользователей в сети позволяет выявить аномалии или необычные действия, которые могут указывать на потенциальные киберпреступления.

Пример использования: при мониторинге корпоративных сетей анализ шаблонов поведения может помочь обнаружить несанкционированный доступ к данным или другие безопасные инциденты.

Успешные примеры расследований с использованием анализа цифровых следов

В современном цифровом мире, где киберпреступности становятся все более изощренными и сложными, анализ цифровых следов играет ключевую роль в расследованиях преступлений и обеспечении кибербезопасности. Эффективное использование технологий и методов анализа данных позволяет специалистам по кибербезопасности выявлять источники угроз, идентифицировать уязвимости и предотвращать потенциальные атаки. Далее

представлены успешные примеры расследований, в которых анализ цифровых следов сыграл ключевую роль в раскрытии преступлений и защите информационной безопасности.

1. *Расследование хакерской атаки на крупную финансовую организацию.* Специалисты по кибербезопасности провели анализ цифровых следов после того, как крупная финансовая компания стала жертвой масштабной хакерской атаки. Путем анализа IP-адресов, метаданных и шаблонов поведения удалось выявить источник атаки, идентифицировать использованные вредоносные программы и определить механизмы взлома. Эти данные помогли компании укрепить свою кибербезопасность и предотвратить будущие атаки.

2. *Расследование киберпреступления с использованием анализа социальных сетей.* Специалисты по киберпреступности провели расследование организованной преступной группировки, занимавшейся финансовыми мошенничествами через интернет. Путем анализа социальных сетей удалось выявить связи между участниками группировки, определить роли каждого участника и выявить способы общения и координации действий. Эта информация послужила основой для успешного задержания и судебного преследования участников группировки.

3. *Расследование утечки конфиденциальной информации в корпоративной среде.* Компания столкнулась с утечкой конфиденциальных данных, что привело к серьезным финансовым потерям. Специалисты по кибербезопасности провели анализ метаданных файлов, перехваченных сотрудниками компании, и выявили источник утечки. Также был проведен анализ шаблонов поведения сотрудников, что позволило выявить необычные действия, приведшие к утечке данных. Благодаря этим данным компания смогла усилить свои меры безопасности и предотвратить дальнейшие утечки.

Программное обеспечение для анализа цифровых следов

В настоящее время существует широкий спектр программных инструментов и технологий [6], специально разработанных для анализа цифровых следов и проведения расследований в области киберпреступности. Эти инструменты позволяют идентифицировать угрозы, анализировать данные, восстанавливать информацию и выявлять уязвимости в информационных системах. Ниже представлен обзор некоторых из наиболее популярных программных средств, используемых в данной области:

1. *EnCase Forensic.* Это одно из ведущих программных решений для цифрового расследования, которое предоставляет возможности по сбору, анализу и представлению цифровых данных. EnCase Forensic [7] позволяет проводить глубокий анализ файловой системы, реестра Windows, интернет-активности и других источников данных.

2. *Autopsy.* Это бесплатное и открытое программное обеспечение для цифрового расследования, основанное на платформе Sleuth Kit. Autopsy [8] предоставляет широкий спектр функций, включая анализ жестких дисков, извлечение метаданных файлов, восстановление удаленных файлов и многое другое.

3. *X-Ways Forensics.* Это мощное программное обеспечение для цифрового расследования, которое обладает широкими возможностями по анализу данных. X-Ways Forensics [9] позволяет проводить детальный анализ файловой системы, реестра Windows, структуры файлов и многое другое.

4. *Cellebrite UFED*. Это инструмент для извлечения данных с мобильных устройств, который широко используется в цифровых расследованиях. Cellebrite UFED [10] позволяет получать данные смартфонов, планшетов и других мобильных устройств, а также проводить анализ извлеченных данных.

Эти программные инструменты представляют лишь небольшую часть доступных на рынке средств для анализа цифровых следов в области киберпреступности. При выборе инструментов для проведения расследований необходимо учитывать особенности конкретной задачи, требования к безопасности данных и доступные ресурсы. Важно также следить за развитием технологий и выбирать инструменты, соответствующие последним трендам в области кибербезопасности.

Этические аспекты

Использование анализа цифровых следов для расследования киберпреступности поднимает ряд этических вопросов, которые необходимо учитывать при проведении исследований в данной области. Некоторые из ключевых этических аспектов, связанных с использованием анализа цифровых следов для расследования киберпреступности, включают следующее:

1. *Приватность и конфиденциальность данных*. При проведении анализа цифровых следов необходимо учитывать права и интересы частных лиц, чьи данные могут быть собраны и использованы в рамках расследования. Важно обеспечить защиту конфиденциальности информации и соблюдать законодательство о защите данных.

2. *Соблюдение процедур и стандартов*. При использовании средств анализа цифровых следов необходимо соблюдать установленные процедуры и стандарты, чтобы обеспечить точность и надежность результатов расследования. Нарушение процедур может привести к неправомерному использованию данных и ошибочным выводам.

3. *Принцип пропорциональности*. При сборе и анализе цифровых следов необходимо соблюдать принцип пропорциональности, то есть использовать только необходимую информацию для достижения целей расследования. Избегание излишнего сбора и использования данных поможет минимизировать нарушение приватности.

4. *Ответственность и честность*. Использование анализа цифровых следов для расследования киберпреступности требует от исследователей высокой степени ответственности и честности. Важно представлять результаты анализа точно и объективно, а также соблюдать этические нормы при работе с данными и участием в процессе расследования.

Эти этические аспекты играют важную роль в обеспечении справедливости, законности и эффективности процесса расследования киберпреступности с использованием анализа цифровых следов. Понимание и учет этических проблем помогут исследователям и специалистам в области кибербезопасности проводить свою работу в соответствии с принципами этики и законности.

Заключение

В ходе исследования была обсуждена значимость анализа цифровых следов и средств расследования в области киберпреступности. Было выявлено, что использование анализа

цифровых следов позволяет эффективно выявлять, анализировать и пресекать киберпреступные деяния, что является критически важным в современном цифровом мире.

Также были обсуждены несколько ключевых этических аспектов, связанных с использованием анализа цифровых следов для расследования киберпреступности, и подчеркнута важность соблюдения принципов приватности, конфиденциальности данных, процедур и стандартов, пропорциональности, ответственности и честности при работе в этой области.

Для дальнейших исследований в области анализа цифровых следов и средств расследования киберпреступности рекомендуется углубленное изучение методов и технологий анализа данных, разработка новых инструментов для выявления и предотвращения киберпреступности, а также проведение дополнительных исследований по этическим аспектам использования цифровых следов в расследованиях.

Список литературы

1. Семикаленова А. И. Цифровые следы: назначение и производство экспертиз // Вестник университета имени ОЕ Кутафина. – 2019. – №. 5 (57). – С. 115-120.
2. Цветков В. Я. Сбор данных и информации // Международный журнал прикладных и фундаментальных исследований. – 2016. – №. 4-3. – С. 646-647.
3. Мхитарян В. С. и др. Анализ данных // Учебник. М: Бакалавр. Академический курс (1-е изд.), Сер. – 2016. – Т. 58.
4. Нефедьева К. В. Инфографика визуализация данных в аналитической деятельности // Труды Санкт-Петербургского государственного института культуры. – 2013. – Т. 197. – С. 89-93.
5. Шевченко Е. С. Актуальные проблемы расследования киберпреступлений // Эксперт-криминалист. – 2015. – №. 3. – С. 29-30.
6. Тихобаев А. Г. Интерактивные компьютерные технологии обучения // Вестник Томского государственного педагогического университета. – 2012. – №. 8 (123). – С. 81-84.
7. Bunting S., Wei W. EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide. – John Wiley & Sons, 2006.
8. Burton J. L., Underwood J. Clinical, educational, and epidemiological value of autopsy // The Lancet. – 2007. – Т. 369. – №. 9571. – С. 1471-1480.
9. Rosalina V., Suhendarsah A., Natsir M. Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic // PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer. – 2016. – Т. 3. – №. 1.
10. Jain P., Mishra A. Extraction of Data using Cellebrite UFED 4PC // International Journal of Medical Toxicology & Legal Medicine. – 2023. – Т. 26. – №. 3and4. – С. 222-232.

References

1. Semikalenova A. I. Digital traces: purpose and production of examinations // Bulletin of the University named after OE Kutafin. – 2019. – No. 5 (57). – pp. 115-120.
2. Tsvetkov V. Ya. Collection of data and information // International Journal of Applied and Fundamental Research. – 2016. – No. 4-3. – pp. 646-647.

3. Mkhitarian V.S. et al. Data analysis // Textbook. M: Bachelor. Academic Course (1st ed.), Ser. – 2016. – Т. 58.
 4. Nefedeva K.V. Infographics, data visualization in analytical activities // Proceedings of the St. Petersburg State Institute of Culture. – 2013. – Т. 197. – pp. 89-93.
 5. Shevchenko E. S. Current problems in the investigation of cybercrimes // Expert criminologist. – 2015. – No. 3. – pp. 29-30.
 6. Tihobaev A. G. Interactive computer teaching technologies // Bulletin of Tomsk State Pedagogical University. – 2012. – No. 8 (123). – pp. 81-84.
 7. Bunting S., Wei W. EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide. – John Wiley & Sons, 2006.
 8. Burton J. L., Underwood J. Clinical, educational, and epidemiological significance of autopsy // The Lancet. – 2007. – Т. 369. – No. 9571. – pp. 1471-1480.
 9. Rosalina V., Suhendarsah A., Natsir M. Analisis Data Recovery Menggunakan Software Forensic: Winhex and X-Ways Forensic //PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer. – 2016. – Т. 3. – No. 1.
 10. Jain P., Mishra A. Extraction of Data using Cellebrite UFED 4PC //International Journal of Medical Toxicology & Legal Medicine. – 2023. – Т. 26. – No. 3and4. – pp. 222-232.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БИЗНЕС-ПРОЦЕССА «ОРГАНИЗАЦИЯ ПРЕМИРОВАНИЯ ОСНОВНОГО ПЕРСОНАЛА» НА ПРИМЕРЕ АПТЕЧНОЙ ОРГАНИЗАЦИИ

¹Кириллина Ю.В., ²Курнаков К.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: ¹jvk05@mail.ru, ²kurnakov.k.a@edu.mirea.ru

В данной статье рассматривается информационное обеспечение бизнес-процесса «Организация премирования основного персонала» в аптечной организации: логическая модель данных и макеты экранных форм проектируемой информационной системы. Логическая модель данных реализована в нотации IDEF1X с выделением одиннадцати сущностей предметной области. На основе логической модели данных построены макеты экранных форм для ввода нормативно-справочной информации, входной информации и получения результатной информации. Сформированное информационное обеспечение является основой для дальнейшего проектирования и разработки информационной системы поддержки организации премирования основного персонала в сети аптек.

Ключевые слова: информационная система, информационное обеспечение, нотации IDEF1X, бизнес-процесс, логическая модель данных, макет экранной формы.

INFORMATION SUPPORT OF THE BUSINESS PROCESS "ORGANIZATION OF BONUSES FOR KEY PERSONNEL" ON THE EXAMPLE OF A PHARMACY ORGANIZATION

¹Kirillina Yu.V., ²Kurnakov K.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ¹jvk05@mail.ru, ²kurnakov.k.a@edu.mirea.ru

This article discusses the information support of the business process "Organization of bonuses for key personnel" in a pharmacy organization: a logical data model and layouts of screen forms of the projected information system. The logical data model is implemented in the IDEF1X notation with the allocation of eleven entities of the subject area. On the basis of a logical data model, layouts of on-screen forms are built for entering normative reference information, input information and obtaining result information. The formed information support is the basis for further design and development of an information system to support the organization of bonuses for key personnel in the pharmacy chain.

Keywords: Information system, information support, IDEF1X notation, business process, logical data model, layout of the screen form

Бизнес-процессы являются основополагающей частью организации. Высокий уровень конкуренции и нестабильность внешней и внутренней среды требуют от компаний использования информационных систем, которые бы обеспечивали бизнес-процессы организации всеми необходимыми данными. В сфере экономики информация

рассматривается как данные, сведенные из экономических показателей организации, подлежащие обработке, передаче, анализу, хранению и использованию в процессе выполнения бизнес-процессов и при принятии управленческих решений. Информация является ресурсом, который используется организациями для обеспечения своей деятельности с целью увеличения прибыли.

Задачи информационного обеспечения заключаются в предоставлении какой-либо важной информации и возможности ее циркуляции для продуктивного функционирования всех подразделений организации. Таким образом, информационное обеспечение в значительной степени влияет на все производственно-хозяйственные и экономические процессы, выполняемые в организации [1].

Целью данной статьи является формирование предложений по информационному обеспечению для последующей автоматизации бизнес-процесса «Организация премирования основного персонала» в аптечной организации.

Информационная модель — это модель объекта, представленная в виде информации, описывающей существенные для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта. Информационная модель позволяет путем подачи на модель информации об изменениях входных величин моделировать возможные состояния объекта [2].

Бизнес-процесс «Организация премирования основного персонала» в сети аптек ООО «Медея» направлен на осуществление учета, контроля и анализа премиальных выплат и регулирование этих выплат исходя из экономических показателей деятельности организации. Для данного процесса и информационной системы определено 11 сущностей.

Главным объектом информационной системы будет являться сущность «Служебная записка о премировании работников», которая имеет связь со следующими сущностями «Бюджет премиального фонда», «Отчет об эффективности», «Отчет об анализе расхода бюджета премиального фонда», «Сотрудник» и «Вид премии».

Сущность «Бюджет премиального фонда» необходима для расчета размера премиальной выплаты для каждого сотрудника. Данная сущность должна содержать информацию о чистом доходе аптечной организации и размере части чистого дохода, которая будет являться бюджетом премиального фонда. Сущность «Бюджет премиального фонда» будет связана с сущностью «Отчет доходы и расходы», которая должна содержать информацию о доходах и расходах организации за определенный период времени.

Сущность «Отчет об эффективности» необходима для определения уровня выполнения плана каждым сотрудником аптечной организации. Данная сущность будет содержать информацию о начислениях премиальных выплат сотрудникам за прошедший период времени и информацию об уровне выполнения плана по продажам по каждому сотруднику аптечной организации, который относится к основному персоналу. Сущность «Отчет об эффективности» будет связана с сущностями «Отчет о затратах на выплату заработной платы», «Отчет об объемах продаж» и «Сотрудник».

Сущность «Отчет об объемах продаж» должна содержать информацию о плановых и выполненных объемах продаж по каждому сотруднику. На основании которой будет рассчитываться уровень выполнения плана каждого сотрудника за определенный период.

сотрудников аптечной организации за определенный период. Макет экранной формы отчета «Анализ зарплаты по сотрудникам» для проектируемой информационной системы представлен на Рисунке 2.

Organization: + Добавить

Start date: 📅 End date: 📅

Сотрудник	Структурное подразделение	Должность	Отработано (дней)	Оклад (руб.)	Премия (руб.)	Квартальная премия (руб.)	Всего начислено (руб.)

💾 Сохранить

Рисунок 2 – Макет экранной формы отчета «Анализ зарплаты по сотрудникам»

Входной документ отчет «Объем продаж за период» должен содержать информацию об объеме выполненных продаж сотрудниками аптечной организации за определенный период. Макет экранной формы отчета «Объем продаж за период» для проектируемой информационной системы представлен на Рисунке 3.

Входной документ отчет «Доходы и расходы» должен содержать информацию о выручке и затратах аптечной организации за определенный период. Макет экранной формы отчета «Доходы и расходы» представлен на Рисунке 4.

The screenshot shows a web application window titled "Организация премирования основного персонала". The main header contains a back arrow, the report title "Отчет 'Объем продаж за период'", and the user profile "Иванов А.А. Руководитель аптечного отдела". Below the header, there are input fields for "Организация:" with a "Добавить" button, and "Начало периода:" and "Конец периода:" with calendar icons. A table with five columns is displayed: "Сотрудник", "Структурное подразделение", "Должность", "Плановый объем продаж (руб.)", and "Выполненный объем продаж (руб.)". The table has seven empty rows. At the bottom right, there is a "Сохранить" button.

Сотрудник	Структурное подразделение	Должность	Плановый объем продаж (руб.)	Выполненный объем продаж (руб.)

Рисунок 3 – Макет экранной формы отчета «Объем продаж за период»

The screenshot shows a web application window titled "Организация премирования основного персонала". The main header contains a back arrow, the report title "Отчет 'Доходы и расходы'", and the user profile "Иванов А.А. Бухгалтер". Below the header, there are input fields for "Организация:" with a "Добавить" button, "Начало периода:" and "Конец периода:" with calendar icons, "Выручка (руб.):", and "Затраты (руб.):". At the bottom right, there is a "Сохранить" button.

Рисунок 4 – Макет экранной формы отчета «Доходы и расходы»

Справочник «Сотрудник» должен содержать информацию о сотрудниках аптечной организации. Макет экранной формы справочника «Сотрудник» представлен на Рисунке 5.

The screenshot shows a web application interface for an 'Employee Directory' (Справочник «Сотрудник»). The title bar at the top reads 'Организация премирования основного персонала'. The breadcrumb navigation shows '← Справочник «Сотрудник»'. The user profile in the top right is 'Иванов А.А. Руководитель аптечного отдела'. The form contains the following fields: 'Должность:' (Job Position) with a dropdown menu; 'Структурное подразделение:' (Structural Department) with a dropdown menu; 'Фамилия:' (Surname) and 'Телефон:' (Phone) as text input fields; 'Имя:' (Name) and 'Электронная почта:' (Email) as text input fields; and 'Отчество:' (Patronymic) as a text input field. A 'Сохранить' (Save) button is located in the bottom right corner.

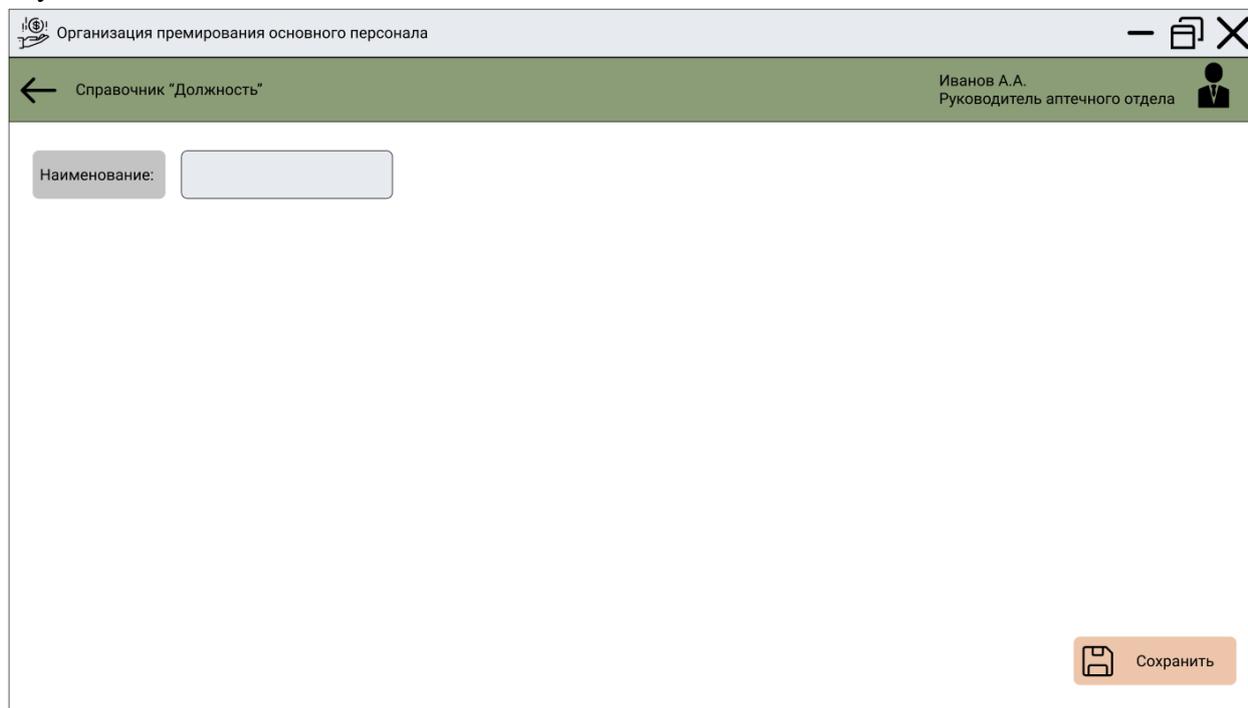
Рисунок 5 – Макет экранной формы справочника «Сотрудник»

Справочник «Структурное подразделение» должен содержать информацию о структурных подразделениях аптечной организации. Макет экранной формы справочника «Структурное подразделение» представлен на Рисунке 6.

The screenshot shows a web application interface for a 'Structural Department Directory' (Справочник «Структурное подразделение»). The title bar at the top reads 'Организация премирования основного персонала'. The breadcrumb navigation shows '← Справочник «Структурное подразделение»'. The user profile in the top right is 'Иванов А.А. Руководитель аптечного отдела'. The form contains a single 'Наименование:' (Name) text input field. A 'Сохранить' (Save) button is located in the bottom right corner.

Рисунок 6 – Макет экранной формы справочника «Структурное подразделение»

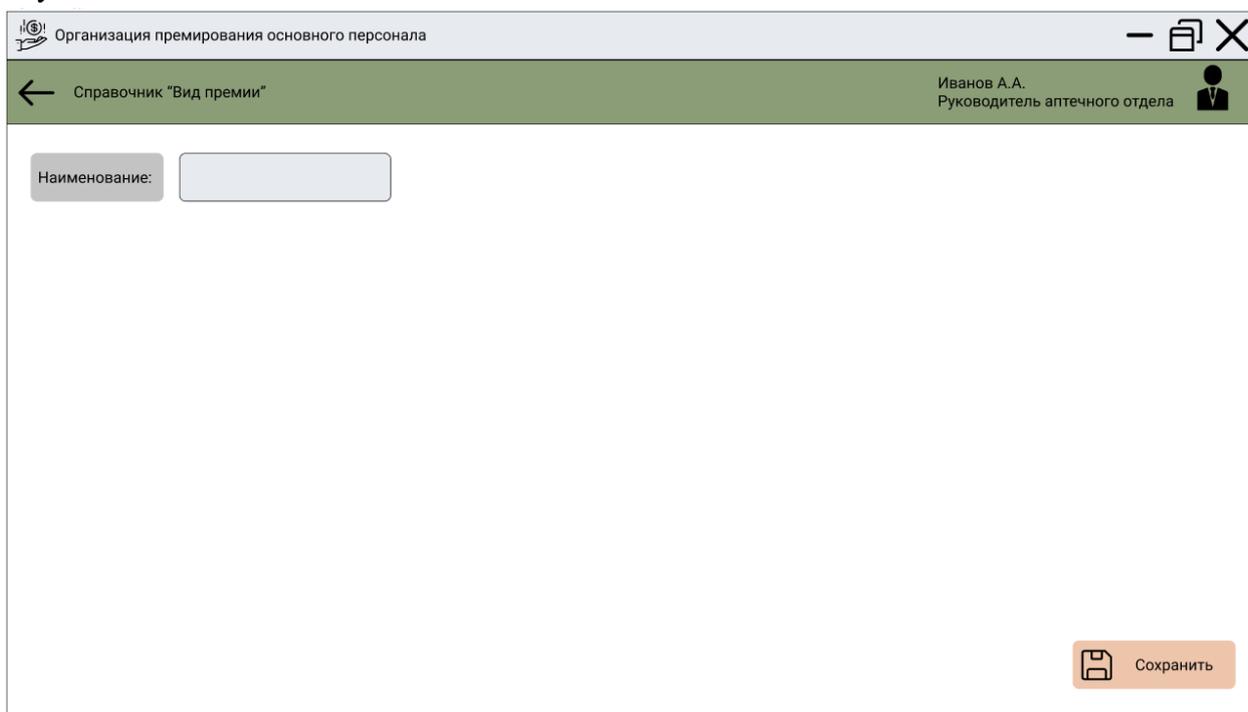
Справочник «Должность» должен содержать информацию о должностях сотрудников аптечной организации. Макет экранной формы справочника «Должность» представлен на Рисунке 7.



The screenshot shows a web application interface for a 'Job' reference form. At the top, there is a header bar with the text 'Организация премирования основного персонала' and a user profile for 'Иванов А.А. Руководитель аптечного отдела'. Below the header, there is a navigation bar with a back arrow and the text 'Справочник "Должность"'. The main content area contains a label 'Наименование:' followed by an empty text input field. In the bottom right corner, there is a 'Сохранить' (Save) button with a floppy disk icon.

Рисунок 7 – Макет экранной формы справочника «Должность»

Справочник «Вид премии» должен содержать информацию о видах премиальных выплат в аптечной организации. Макет экранной формы справочника «Вид премии» представлен на Рисунке 8.



The screenshot shows a web application interface for a 'Type of Bonus' reference form. At the top, there is a header bar with the text 'Организация премирования основного персонала' and a user profile for 'Иванов А.А. Руководитель аптечного отдела'. Below the header, there is a navigation bar with a back arrow and the text 'Справочник "Вид премии"'. The main content area contains a label 'Наименование:' followed by an empty text input field. In the bottom right corner, there is a 'Сохранить' (Save) button with a floppy disk icon.

Рисунок 8 – Макет экранной формы справочника «Вид премии»

В проектируемой информационной системе определено два выходных документа: «Служебная записка о премировании работников» и отчет «Анализ расходов бюджета премиального фонда».

Выходной документ «Служебная записка о премировании работников» должен содержать информацию о результативности сотрудников за определенный период, вид и размер премиальной выплаты сотруднику по итогу определенного периода. Макет экранной формы документа «Служебная записка о премировании работников» представлен на Рисунке 9.

Организация премирования основного персонала

← Служебная записка о премировании работников

Иванов А.А.
Руководитель аптечного отдела

Организация:

Дата создания:

Согласовано:

Сотрудник	Структурное подразделение	Должность	Уровень выполнения плана	Вид премии	Величина (руб.)	Условие получения

Сохранить

Рисунок 9 – Макет экранной формы документа «Служебная записка о премировании работников»

Выходной документ отчет «Анализ расходов бюджета премиального фонда» должен содержать информацию о фактическом остатке бюджета премиального фонда после назначения премиальных выплат. Макет экранной формы отчета «Анализ расходов бюджета премиального фонда» представлен на Рисунке 10.

Организация премирования основного персонала

← Отчет "Анализ расходов бюджета премиального фонда" Иванов А.А. Руководитель аптечного отдела

Организация:

Дата создания:

Бюджет премиального фонда (руб.): Результат анализа:

Расход бюджета премиального фонда (руб.):

Фактический остаток премиального фонда (руб.):

Сохранить

Рисунок 10 – Макет экранной формы отчета «Анализ расходов бюджета премиального фонда»

Таким образом, предложенный вариант логической модели данных совместно с макетами экранных форм будущей информационной системы позволит автоматизировать процесс обработки информации, реализуемого в рамках организации премирования основного персонала после разработки и внедрения информационной системы в деятельность аптечной сети.

Список литературы

1. Гвоздева В. А. Информатика, автоматизированные информационные технологии и системы: учебник. М. : ИД Форум, 2023. 542 с.
2. Новиков Б. А., Горшкова Е. А., Графеева Н.Г. Основы технологий баз данных: учебное пособие. М. : ДМК Пресс, 2020. 582 с.
3. Осипов Д. Л. Технологии проектирования баз данных. М. : ДМК Пресс, 2019. 498 с.
4. Стружкин Н. П., Годин В. В. Базы данных: проектирование: учебник для вузов. М. : Юрайт, 2024. 477 с.
5. Шилин А. С. Перспективные методы проектирования реляционных баз данных: учебное пособие. М. : Директ-Медиа, 2021. 136 с.

References

1. Gvozdeva V. A. Informatics, automated information technologies and systems: textbook. Moscow : ID Forum, 2023. p.542
2. Novikov B. A., Gorshkova E. A., Grafееva N.G. Fundamentals of database technologies: textbook. M. : DMK Press, 2020. p.582
3. Osipov D. L. Database design technologies. Moscow : DMK Press, 2019. 498 p.
4. Struzhkin N. P., Godin V. V. Databases: design: textbook for universities. M. : Yurait, 2024. p.477

Кириллина Ю.В., Курнаков К.А. Информационное обеспечение бизнес-процесса
«Организация премирования основного персонала» на примере аптечной организации
// Международный журнал информационных технологий и энергоэффективности. – 2024. –
Т. 9 № 4(42) С. 63–72

5. Shilin A. S. Promising methods of relational database design: textbook. М. : Direct-Media,
2021. p.136



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.42

АССЕМБЛЕР: ИСКУССТВО ПРОГРАММИРОВАНИЯ У САМЫХ ОСНОВ

Перевертун Д.Р.

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
danilaperevertun@gmail.com*

В статье рассматривается ассемблер как ключевой элемент в мире программирования, подчеркивая его важность для оптимизации программного обеспечения, разработки системного ПО и встраиваемых систем. Обсуждается роль ассемблера в обратном инжиниринге и его неоценимая ценность для глубокого понимания механизмов работы компьютеров. Освещаются технические аспекты написания ассемблерного кода, включая работу с регистрами, управление памятью и вводом-выводом, демонстрируя, как эти низкоуровневые операции предоставляют программистам уникальные возможности для контроля над аппаратным обеспечением. Статья мотивирует разработчиков изучать ассемблер как средство для улучшения своих навыков программирования и глубокого анализа программных и аппаратных систем.

Ключевые слова: Ассемблер, программирование, оптимизация кода, системное программное обеспечение, встраиваемые системы, обратный инжиниринг, архитектура компьютера, разработка ПО, машинный код, изучение ассемблера.

ASSEMBLER: THE ART OF PROGRAMMING AT THE VERY BASICS

Perevertun D.R.

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com*

The article considers assembler as a key element in the world of programming, emphasizing its importance for software optimization, system software development and embedded systems. The role of assembler in reverse engineering and its invaluable value for a deep understanding of the mechanisms of computer operation are discussed. Highlights the technical aspects of writing assembly code, including working with registers, memory management, and I/O, demonstrating how these low-level operations provide programmers with unique opportunities to control hardware. The article motivates developers to study assembler as a means to improve their programming skills and in-depth analysis of software and hardware systems.

Keywords: Assembler, programming, code optimization, system software, embedded systems, reverse engineering, computer architecture, software development, machine code, assembly language learning.

Ассемблер, часто воспринимаемый как реликвия эпохи зарождения компьютерной эры, на самом деле является мостом между мыслью программиста и железом машины. В этой статье мы раскроем не только историческую значимость ассемблера, но и его современное значение, продемонстрируем, как он продолжает формировать основы программирования,

давая разработчикам уникальные инструменты для решения задач оптимизации и понимания работы компьютеров на фундаментальном уровне.

Ассемблер тесно связан с архитектурой компьютера, на котором он исполняется, отражая особенности конкретного типа процессора, будь то x86, ARM или другие. Он позволяет управлять ресурсами машины напрямую, через регистры, команды управления памятью и прямые инструкции процессору, открывая двери в мир, где программист может максимально оптимизировать выполнение кода.

В основе ассемблера лежит принцип прямого управления машиной на самом низком уровне, где каждая команда переводится в машинный код, понятный процессору. Этот язык программирования уникален своей способностью максимально приближать разработчика к "железу", предоставляя возможность манипулировать базовыми функциями компьютера, такими как управление памятью, выполнение арифметических операций и прямое обращение к регистрам процессора.[5]

Каждая инструкция в ассемблере соответствует определенной операции, которую процессор может выполнить. Эти операции могут включать в себя перемещение данных между регистрами, выполнение математических расчетов, управление потоком выполнения программы через условные переходы и циклы. Хотя на первый взгляд кажется, что работа с ассемблером требует запоминания большого количества команд и регистров, на практике разработчики используют ограниченный набор инструкций для решения большинства задач.

На протяжении десятилетий ассемблер использовался для создания всего: от операционных систем до игр и встраиваемого ПО. Это демонстрирует его важность и гибкость как инструмента, который способен обеспечивать высокую производительность и тонкую настройку программного обеспечения.

В контексте программирования ассемблер представляет собой не просто язык, ограничивающийся академическими исследованиями или узкоспециализированными приложениями. Напротив, он играет ключевую роль в разработке множества систем, оставаясь актуальным и важным инструментом для определённых задач программирования, даже на фоне доминирования высокоуровневых языков.

Ассемблер выступает основой для создания и оптимизации операционных систем, драйверов устройств и прошивок для встраиваемых систем. В этих сферах требуется максимально эффективное использование ресурсов аппаратного обеспечения, к чему и стремится ассемблер, обеспечивая разработчикам возможность точного контроля над выполнением программы на уровне железа.

Операционные системы, такие как Linux и Windows, в своём ядре содержат компоненты, написанные на ассемблере, что позволяет им эффективно управлять аппаратными ресурсами и обеспечивать высокую производительность. Ассемблер используется для реализации критически важных функций, таких как управление памятью и процессами, обработка прерываний и низкоуровневая взаимодействие с аппаратурой.

В области разработки встраиваемых систем ассемблер остается неоценимым инструментом, поскольку позволяет создавать компактный и быстродействующий код для устройств с ограниченными вычислительными ресурсами и памятью.[3] Это особенно важно для микроконтроллеров и специализированного оборудования, где каждый байт на счету.

Кроме того, ассемблер находит применение в области обратного инжиниринга и анализа вредоносного ПО, где понимание машинного кода и способность читать

ассемблерный код являются ключевыми навыками. Анализ на этом уровне позволяет исследователям безопасности глубже понимать работу вредоносных программ и разрабатывать эффективные методы защиты.

Несмотря на кажущуюся сложность, изучение ассемблера доступно благодаря множеству ресурсов: от онлайн-курсов до эмуляторов и учебных пособий. Практический опыт и общение в специализированных сообществах позволяют глубже погрузиться в мир низкоуровневого программирования.

Процесс изучения ассемблера может быть увлекательным путешествием в мир низкоуровневого программирования. Начать стоит с выбора конкретной архитектуры, так как ассемблер тесно связан с инструкционным набором процессора. Для начинающих часто рекомендуется изучение ассемблера на базе архитектуры x86, поскольку она широко распространена и имеет обширное сообщество поддержки. ARM архитектура, в свою очередь, идеально подходит для тех, кто интересуется встраиваемыми системами и разработкой под мобильные платформы.

Изучение начинается с основ: понимания работы регистров, инструкций по перемещению данных, операций ввода-вывода и управления памятью. Существуют специализированные учебники и онлайн-курсы, которые шаг за шагом ведут ученика через все этапы обучения, от простых программ до сложных конструкций и алгоритмов.

Одним из ключевых ресурсов являются эмуляторы процессоров и ассемблеров, позволяющие практиковать написание и тестирование кода без необходимости доступа к физическому оборудованию.[1] Это особенно ценно в процессе обучения, когда экспериментирование и исправление ошибок являются неотъемлемой частью понимания.

Понимание ассемблера открывает новые горизонты для технического творчества и инноваций. Это не просто язык программирования, а способ мышления, который требует глубокого понимания и уважения к машине. Ассемблер предоставляет инструменты, которые позволяют разработчикам максимально приближаться к "железу", достигая высочайшей производительности и эффективности.

Помимо технических преимуществ, изучение ассемблера является также путешествием в историю компьютерных технологий, напоминая о корнях и эволюции программирования. Оно развивает не только умение писать эффективный код, но и формирует фундаментальное понимание работы компьютеров, что делает разработчика гораздо более грамотным в техническом плане.

Ассемблерный код является прямым отражением машинных инструкций, предоставляемых архитектурой конкретного процессора, и предлагает разработчикам возможность максимально точно контролировать поведение программы. На уровне ассемблера каждая строка кода соответствует отдельной операции, выполняемой процессором, что позволяет достигать высокой производительности и эффективности в управлении ресурсами системы. Это особенно важно в задачах, где критичны скорость выполнения и минимальное потребление ресурсов, например, в встраиваемых системах или при разработке драйверов устройств.

Ассемблерный код напрямую работает с регистрами процессора, операциями ввода-вывода и управления памятью, предоставляя программистам инструменты для непосредственного обращения к аппаратным средствам компьютера. Эта способность делает

ассемблер незаменимым в ситуациях, когда требуется точное и эффективное управление памятью, особенно в контексте ограниченных вычислительных ресурсов.[2]

Написание кода на ассемблере требует от разработчика глубоких знаний архитектуры целевого процессора и понимания низкоуровневой работы компьютерных систем. Несмотря на кажущуюся сложность и высокий порог входа, владение ассемблером позволяет не только улучшить производительность и оптимизировать программное обеспечение, но и дает комплексное понимание принципов работы компьютера.[6] Это знание становится особенно ценным при диагностике сложных программных проблем и в процессах обратного инжиниринга, когда требуется анализировать и понимать чужой или вредоносный код.

В современном программировании ассемблер не утратил своей актуальности, несмотря на широкое распространение высокоуровневых языков. Его применение в определенных областях, где важна каждая тактовая частота процессора и каждый байт памяти, подчеркивает значимость глубокого понимания машинного уровня работы компьютеров.[4] Ассемблер остается мощным инструментом в руках опытных разработчиков, стремящихся к максимальной оптимизации и эффективности своих проект

Ассемблер остается актуальным и важным языком в арсенале современного программиста. Он представляет собой уникальное сочетание искусства и науки, требующее от разработчика как технических навыков, так и творческого подхода. Изучение ассемблера не только улучшает понимание работы компьютера, но и открывает двери к оптимизации, которая может быть критически важна в высокопроизводительных и встраиваемых системах. Владение ассемблером позволяет программисту выходить за рамки стандартных решений, предлагаемых высокоуровневыми языками, и реализовывать инновационные подходы к решению задач.

Освоение ассемблера способствует развитию глубокого технического мировоззрения, формированию умения анализировать и понимать любые процессы на самом низком уровне. Это не просто навык программирования; это способность видеть и контролировать самые мелкие детали системы, превращая сложные задачи в управляемые и оптимизированные процессы.[7]

В мире, где технологии развиваются с невероятной скоростью, ассемблер остаётся напоминанием о том, что понимание базовых принципов работы компьютеров по-прежнему неопределимо. Для студентов, профессионалов и энтузиастов, стремящихся к пониманию этих принципов, ассемблер предлагает бесценное погружение в мир компьютерной архитектуры и программирования.

Таким образом, ассемблер не является устаревшим языком, предназначенным исключительно для академических исследований или специализированного использования. Это живой инструмент, который по сей день демонстрирует свою актуальность и эффективность в руках тех, кто готов освоить его мощь. Ассемблер открывает новые возможности для оптимизации, позволяет достигать высочайшей производительности и предоставляет глубокое понимание того, как на самом деле работают наши программы и компьютеры.

В заключительных словах этой статьи хочется подчеркнуть, что ассемблер — это не просто язык программирования. Это ключ к глубокому пониманию компьютерных технологий, мост между человеком и машиной, который позволяет не только создавать более эффективное ПО, но и лучше понимать технологический мир вокруг нас. Овладение

ассемблером — это путь к истинному мастерству в программировании, открывающий неограниченные горизонты для исследований, инноваций и творчества.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.
2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукофера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.

7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

УПРАВЛЕНИЕ СТРОИТЕЛЬСТВОМ КРУПНЫХ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ С ПРИМЕНЕНИЕМ ИНТЕГРИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

¹ Школьников П.Н., ² Белоусов А.В.

ФГБОУ ВО «ДАЛЬНЕВОСТОЧНЫЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ», Благовещенск, Россия, (675005, Амурская область, г Благовещенск, Политехническая ул, д. 86.), e-mail: ¹safronovaanastasiya2@gmail.com, ²belyiy2013@mail.ru

Данная статья посвящена глобальным переменам, которые ждут нас в будущем, а также рассмотрению и внедрению в проектирование, строительство и эксплуатацию интегрированных информационных систем уже сегодня. В ближайшем будущем эта технология будет играть ключевую роль в строительстве, что представляется увлекательным. Я считаю, что важно, чтобы все осознавали значение этой технологии. Вскоре она затронет каждый аспект строительства, поэтому сейчас самое подходящее время изучить работу интегрированных информационных систем. какие данные содержатся внутри них. В условиях растущей необходимости в повышении производительности и сокращении времени выполнения задач использование интегрированных информационных систем в управлении строительством крупных промышленных объектов приобретает особую важность.

Ключевые слова: Автоматизация процессов, внедрение интегрированных систем, развитие строительства, внедрение инновационных технологий.

CONSTRUCTION MANAGEMENT OF LARGE INDUSTRIAL FACILITIES USING INTEGRATED INFORMATION SYSTEMS

¹ Shkolnikov P.N., ² Belousov A.V.

FAR EASTERN STATE AGRARIAN UNIVERSITY, Blagoveshchensk, Russia, (675005, Amur Region, Blagoveshchensk, Polytechnic str., 86), e-mail: ¹safronovaanastasiya2@gmail.com, ²belyiy2013@mail.ru

This article focuses on the upcoming worldwide transformations we can expect to see in the near future, along with the examination and application of comprehensive information systems in the design, construction and operation today. Soon, this technology will become the driving force behind construction, and it will be exciting. I think it is very important that everyone understands this technology. At some point, this will affect the entire construction, so now is the time to find out how integrated information systems work, what set of source data they contain. In the light of increasing efficiency requirements and shortening work deadlines, the relevance of using integrated information systems in the construction management of large industrial facilities is becoming especially significant.

Keywords: Automated, integrated systems in construction, that incorporate, innovative technology.

Строительство и ранее считалось сферой, где важными были сила и выносливость. Однако в настоящее время значимость приобретают совершенно иные навыки.

Цель данного исследования заключается в обосновании и описании методологии использования интегрированных информационных систем для управления процессами строительства крупных промышленных объектов.

На основании поставленной цели выделены задачи, а именно, рассмотреть инструментарий в области управления строительством, а также разработать предложения по оптимизации строительных процессов с применением интегрированных информационных систем.

Строительные компании в основном применяют определенные типы информационных систем, каждая из которых играет свою роль в процессе строительства и эксплуатации зданий.

Основными участниками в процессе строительства крупных промышленных объектов являются: заказчик, строительный контроль от заказчика, генеральный подрядчик, ЕРС-подрядчик и субподрядчик. Строительные информационные системы предназначены для автоматизации основных и вспомогательных процессов строительных компаний, включая инженерные изыскания, строительное проектирование, управление строительством зданий и сооружений, снос и демонтаж объектов, а также контроль за выполнением работ. Для эффективного управления строительными проектами и выполнения различных задач в строительстве необходимо создать информационную систему, которая будет включать в себя определенный набор специализированных элементов. Этот набор включает в себя техническую поддержку, прикладные программы, информационное и программное обеспечение, а также ИТ-процессы информационной системы.



Рисунок 1 – Применение интегрированных информационных систем в строительстве

Технологии; BIM технологии; системы управления проектами и т.д. программное обеспечение; целостные информационные моделирования (технологии BIM).

САПР - это комплекс различных средств, включая технические и программные, которые предназначены для автоматизации процесса проектирования.

Система автоматизированного проектирования (САПР) играет ключевую роль в современной промышленной сфере, активно применяясь в различных отраслях, включая автомобильную, судостроительную, аэрокосмическую промышленность, а также в промышленном и архитектурном проектировании, разработке протезов и других областях.

CAD-система (компьютерная поддержка проектирования) – это программное обеспечение, которое используется для автоматизации процесса проектирования с использованием компьютерной техники. Она позволяет создавать проектную и технологическую документацию для отдельных изделий, зданий и сооружений.

CAD - это программное обеспечение, которое применяется не только для создания детальных 3D-моделей и 2D-чертежей физических компонентов, но и для всего процесса проектирования. От начального этапа концептуального проектирования и компоновки изделий до проведения прочностного и динамического анализа сборок и выбора методов изготовления компонентов, CAD играет ключевую роль. Кроме того, CAD можно применять

для разработки различных объектов, включая украшения, мебель, бытовую технику и многое другое.



Рисунок 2 – Применение интегрированных информационных систем в строительстве

САЕ (Computer-Aided-Engineering) представляет собой набор программных инструментов, способных предсказывать поведение в реальных условиях разработанной на компьютере модели изделия (системы инженерного анализа). Эти программы используют различные методы математических расчетов, такие как метод конечных элементов, метод конечных разностей и метод конечных объектов. Благодаря САЕ инженер может оценить производительность изделия, избегая значительных временных и финансовых затрат.

С помощью САЕ можно проводить:

- исследование прочности компонентов и узлов с использованием метода конечных элементов;
- изучение тепловых и гидродинамических процессов;
- кинематические исследования;
- симуляция процессов, таких как литье под воздействием давления;
- улучшение продуктов или процессов через оптимизацию;
- улучшение производительности компьютерных платформ с 64-битными и многоядерными процессорами путем оптимизации систем САЕ, что способствует более эффективному моделированию сложных конструкций с большим числом степеней свободы [1].

При изучении методов управления строительством можно предложить ряд мер по повышению эффективности строительных процессов с использованием интегрированных информационных систем:

- Согласование рабочей документации и выпуск обновлений.
- Улучшение процесса проверки поступающей продукции
- Увеличение уровня контроля операций для улучшения качества работы.
- Генерация исполнительной документации автоматически.
- Организация документации о прогрессе строительно-монтажных работ

- Автоматизированная проверка на наличие «STOP» факторов при освидетельствовании работ

Участие во всех бизнес-процессах целостной структуры системы, такой как составная часть, обеспечит полную прослеживаемость операций в процессе выполнения строительно-монтажных работ. Это необходимо как с технической точки зрения для четкого выполнения операций в определенной последовательности, так и с точки зрения статистического учета выполненных работ по необходимым критериям.

По результатам анализа можно заключить, что отрасль строительства, как одна из самых консервативных в экономике, не всегда открыта к новшествам. Однако внедрение интегрированных информационных систем играет важную роль в автоматизации процессов строительства. Предлагается использовать информационные модели для улучшения организации жилищного, промышленного, гражданского и других типов строительства (включая реконструкцию).

Список литературы

1. Fong P.S., Shen L.Y., & Yu J. (2009). An examination of the incorporation of electronic commerce in the Chinese construction sector. *Automation in Construction*, 18(8), pp. 1011-1024.
2. Shen Q., and Chung J. (2004) Enhancing e-commerce capabilities for construction firms. *Journal of Construction Engineering and Management*, 130(4), pp.590-598.
3. Учебное пособие "Основы организации и управления в строительстве" авторства Е.А.Гусаковой и А.С.Павлова, 2-е издание, переработано и дополнено. М.: Юрайт, 2023. 648 с., оно предназначено для использования в вузах и относится к категории учебной литературы "Высшее образование". ISBN 978-5-534-13821-4.
4. Зараменских Е. П. Учебник "Информационные системы: управление жизненным циклом" предназначен для среднего профессионального образования. М.: Юрайт, 2023, 497 с. – ISBN 978-5-534-16179-3.

References

1. Fong P.S., Shen L.Y., & Yu J. (2009). An examination of the incorporation of electronic commerce in the Chinese construction sector. *Automation in Construction*, 18(8), pp. 1011-1024.
 2. Shen Q., and Chung J. (2004) Enhancing e-commerce capabilities for construction firms. *Journal of Construction Engineering and Management*, 130(4), pp.590-598.
 3. Textbook "Fundamentals of Organization and Management in Construction" by E.A. Gusakova and A.S. Pavlov, 2nd edition, revised and supplemented. Moscow, Yurayt Publ., 2023. 648 p., it is intended for use in universities and belongs to the category of educational literature "Higher education". ISBN 978-5-534-13821-4.
 4. Zaramenskikh E. P. Textbook "Information Systems: Life Cycle Management" is intended for secondary vocational education. Moscow, Yurayt Publ., 2023, 497 p. – ISBN 978-5-534-16179-3.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

ВИРУСЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Перевертун Д.Р.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
danilaperevertun@gmail.com

В статье рассматриваются современные вызовы в области кибербезопасности, связанные с развитием вирусов программного обеспечения и методов их распространения. Освещаются основные типы вирусов и меры защиты, направленные на обеспечение безопасности информационных систем. Отдельное внимание уделяется современным технологиям и подходам в области обеспечения кибербезопасности, включая использование искусственного интеллекта и машинного обучения для предотвращения кибератак. Анализируются текущие и будущие перспективы развития в контексте международного сотрудничества и стандартизации в сфере кибербезопасности.

Ключевые слова: Кибербезопасность, вирусы программного обеспечения, защита информационных систем, искусственный интеллект, машинное обучение, международное сотрудничество, стандартизация в области кибербезопасности, троянские программы, компьютерные черви, шпионское ПО, рекламное ПО, вирусы-вымогатели.

SOFTWARE VIRUSES AND SECURITY MEASURES

Perevertun D.R.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com

The article examines modern challenges in the field of cybersecurity related to the development of software viruses and methods of their distribution. The main types of viruses and protection measures aimed at ensuring the security of information systems are highlighted. Special attention is paid to modern technologies and approaches in the field of cybersecurity, including the use of artificial intelligence and machine learning to prevent cyber attacks. The current and future development prospects in the context of international cooperation and standardization in the field of cybersecurity are analyzed.

Keywords: Cybersecurity, software viruses, protection of information systems, artificial intelligence, machine learning, international cooperation, standardization in the field of cybersecurity, Trojans, computer worms, spyware, adware, ransomware.

В современном мире, где цифровые технологии проникают в каждую сферу нашей жизни, вопросы кибербезопасности становятся все более актуальными. Вирусы программного обеспечения – одна из главных угроз, стоящих перед пользователями и организациями. Эти малициозные программы способны не только нарушить нормальную работу компьютерных систем, но и привести к значительным финансовым потерям, утечке конфиденциальной

информации и даже к разрушению критически важной инфраструктуры. В данной статье рассматриваются основные типы вирусов программного обеспечения и современные подходы к обеспечению кибербезопасности, направленные на защиту информационных систем от этих угроз.

Вирусы программного обеспечения могут быть классифицированы по различным признакам, включая способ распространения, тип наносимого вреда, и тактику скрытности. Среди наиболее распространенных типов можно выделить троянские программы, черви, шпионское ПО, рекламное ПО и вирусы-вымогатели. Каждый из этих типов имеет свои особенности и требует применения специфических мер безопасности.

На сегодняшний день каждый аспект нашей жизни все больше зависит от цифровых технологий, вопросы кибербезопасности становятся критически важными. Вирусы программного обеспечения представляют собой одну из самых значимых угроз для пользователей и организаций, способных не только нарушить нормальную работу компьютерных систем, но и привести к значительным финансовым потерям, утечке конфиденциальной информации и даже к разрушению критически важной инфраструктуры.[4]

Вирусы программного обеспечения охватывают широкий спектр малициозных программ, каждая из которых имеет свои уникальные характеристики и методы распространения. Некоторые из них маскируются под легитимное программное обеспечение, тем самым обманывая пользователей и получая доступ к их системам. Другие способны самостоятельно распространяться через сетевые соединения, нанося вред не только отдельным пользователям, но и целым сетям. Также существуют программы, специализирующиеся на сборе информации без ведома пользователя, что представляет серьезную угрозу конфиденциальности данных.

Защита от таких угроз требует комплексного подхода, который включает в себя использование передовых технологий и строгих организационных мер. Современные технологии обеспечения безопасности способны выявлять и блокировать вредоносное ПО, еще до того, как оно сможет нанести ущерб. Вместе с тем, организационные меры, такие как разработка и внедрение политик безопасности, регулярные аудиты и обучение персонала, играют не менее важную роль в обеспечении защиты информационных систем.

Однако с развитием технологий эволюционируют и угрозы кибербезопасности. В ответ на это, разрабатываются новые методы защиты, включая применение машинного обучения для обнаружения и предотвращения атак, усиление защиты облачных и распределенных систем, а также разработку международных стандартов кибербезопасности.

Защита в цифровой среде требует комплексного подхода, который включает в себя как технические средства, так и организационные меры. Среди ключевых технологий – антивирусное ПО, межсетевые экраны, системы обнаружения и предотвращения вторжений, а также средства шифрования данных.[3] Организационные меры включают в себя разработку и внедрение политик информационной безопасности, проведение регулярных аудитов и тренингов для сотрудников.

Обеспечение безопасности в цифровом пространстве — это непрерывный процесс, требующий применения многоуровневых стратегий защиты, включающих в себя как передовые технологии, так и строгие организационные меры. В основе защиты лежит идея создания надежного барьера, который сможет выявлять, предотвращать и минимизировать

вред от малициозных программ, обеспечивая тем самым целостность и конфиденциальность пользовательских данных.

Современные технологии обеспечения безопасности включают в себя разработку и внедрение программного обеспечения, способного анализировать поведение приложений и трафика в реальном времени, выявлять подозрительные действия и блокировать их до того, как они смогут нанести ущерб. Эти технологии постоянно совершенствуются, чтобы противостоять новым и более изощренным угрозам, что требует регулярных обновлений и адаптации к меняющимся условиям киберпространства.

Однако технологические средства защиты не могут обеспечить полную безопасность без должного уровня организационной подготовки. Важным аспектом является разработка и внедрение комплексной политики безопасности, которая включает в себя не только технические аспекты, но и обучение персонала основам кибергигиены, а также проведение регулярных аудитов безопасности. Эти меры позволяют не только своевременно выявлять и устранять уязвимости, но и повышать осведомленность сотрудников о потенциальных угрозах и способах их предотвращения.

В контексте быстро меняющегося цифрового мира, одной из ключевых задач является обеспечение адаптивности и гибкости систем безопасности. Это достигается за счет внедрения новейших технологических решений, таких как искусственный интеллект и машинное обучение, которые способны анализировать большие объемы данных и выявлять сложные угрозы, еще до того как они смогут проявить себя.[2]

Таким образом, обеспечение кибербезопасности требует комплексного подхода, сочетающего в себе использование передовых технологий, строгую организационную дисциплину и постоянное обновление знаний и навыков. Важно понимать, что защита информационных систем — это непрерывный процесс, который требует постоянного внимания и адаптации к постоянно меняющимся условиям и угрозам в киберпространстве.

С развитием технологий эволюционируют и угрозы кибербезопасности. В последние годы особенно актуальными стали атаки с использованием искусственного интеллекта, целенаправленные атаки типа "нулевой день" и атаки на цепочки поставок. В ответ на эти вызовы разрабатываются новые методы защиты, включая применение машинного обучения для обнаружения и предотвращения атак, усиление защиты облачных и распределенных систем, а также разработку стандартов и нормативов кибербезопасности на международном уровне.

В сфере кибербезопасности современные вызовы постоянно эволюционируют, требуя от специалистов не только внимания к текущим угрозам, но и антиципации будущих вызовов. Развитие технологий, таких как искусственный интеллект (ИИ) и машинное обучение, открывает новые горизонты для защиты информационных систем, однако в то же время создает возможности для более изощренных атак. Целенаправленные атаки типа "нулевой день", эксплуатирующие уязвимости, о которых еще не известно производителям программного обеспечения, ставят под угрозу даже самые защищенные системы.[7] Атаки на цепочки поставок, когда злоумышленники используют уязвимости в одном из звеньев для доступа к данным целого ряда организаций, становятся все более распространенными.

В ответ на эти вызовы, область кибербезопасности постоянно развивается, стремясь предвидеть и нейтрализовать потенциальные угрозы. Использование ИИ и машинного обучения для обнаружения и предотвращения атак становится нормой, позволяя

анализировать большие объемы данных в реальном времени и выявлять угрозы, которые могут оставаться незамеченными для традиционных систем безопасности.[6] Разработка и внедрение новых стандартов и нормативов на международном уровне также играет ключевую роль в укреплении общей защищенности цифрового пространства, позволяя координировать усилия различных стран и организаций в борьбе с киберпреступностью.

Важной перспективой в области кибербезопасности является развитие облачных и распределенных систем защиты. Эти технологии обеспечивают гибкость и масштабируемость решений для защиты данных, позволяя быстро адаптироваться к изменяющимся условиям и требованиям безопасности.[1] Также важно уделить внимание укреплению защиты личных данных пользователей, в контексте усиления законодательства в области защиты персональных данных по всему миру.

Однако прогресс в технологиях и методах защиты неизбежно сопровождается развитием новых методов атак. Поэтому в будущем сфера кибербезопасности будет продолжать развиваться, сталкиваясь с новыми вызовами и находя решения для обеспечения безопасности в постоянно меняющемся цифровом мире.[5] Такой подход требует не только технологических инноваций, но и глубокого понимания потенциальных угроз, а также сотрудничества между государствами, частным сектором и международными организациями.

В заключении можно отметить, что кибербезопасность в современном цифровом мире становится все более значимым и сложным аспектом, требующим непрерывного внимания и развития. Угрозы, исходящие от вирусов программного обеспечения, представляют собой серьезный вызов для индивидуальных пользователей, компаний и государственных организаций по всему миру. Многообразие и постоянное эволюционирование малициозных программ требуют от специалистов по кибербезопасности глубоких знаний, умения применять передовые технологии и разрабатывать комплексные стратегии защиты.

Применение современных технологий, таких как искусственный интеллект и машинное обучение, позволяет существенно повысить эффективность систем обнаружения и предотвращения кибератак. Однако технологические решения в одиночку не могут гарантировать полную безопасность. Важную роль играет развитие организационных мер, включая обучение персонала, разработку и внедрение политик информационной безопасности, а также проведение регулярных аудитов и тестирований на проникновение.

Сотрудничество на международном уровне и стандартизация в сфере кибербезопасности также являются ключевыми элементами в борьбе с глобальными киберугрозами. Разработка и внедрение общепризнанных стандартов и практик позволяют координировать усилия различных стран и организаций, способствуя созданию более безопасного цифрового пространства.

В перспективе, обеспечение кибербезопасности потребует от всех заинтересованных сторон адаптации к постоянно меняющейся среде угроз, развития новых подходов и технологий, а также глубокого понимания потенциальных рисков и стратегий их минимизации. Постоянное развитие в этой области не только защитит от текущих угроз, но и подготовит общество к противостоянию будущим вызовам в области кибербезопасности.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
 2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
 3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
 4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
 5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
 6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
 7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

СОВЕРШЕНСТВОВАНИЕ ЗАЩИТЫ ОТ СОЦИАЛЬНЫХ АТАК В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

¹Гельфанд А.М., ²Кузнецов С.А., ³Анучин К.Н.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: ¹amgelfand@mail.ru, ²Killingsprin@bk.ru, ³anucin221@gmail.com

Статья посвящена анализу роли человеческого фактора в информационной безопасности и методам противодействия атакам социальной инженерии. В условиях возрастающей численности и сложности кибератак основное внимание авторов сосредоточено на изучении влияния человеческого фактора и способах его минимизации как ключевого элемента в защите информации. Анализируются различные формы социальной инженерии и подходы к обучению персонала с целью повышения осведомленности о методах кибермошенников. Авторы делают акцент на необходимости разработки комплексного, ориентированного на человека подхода к информационной безопасности, который включал бы не только технологические решения, но и меры по увеличению осведомленности и подготовленности пользователей и персонала.

Ключевые слова: Информационная безопасность, социальная инженерия, кибератаки, противодействие мошенничеству.

IMPROVING PROTECTION AGAINST SOCIAL ATTACKS IN THE FIELD OF INFORMATION SECURITY

¹Gelfand A. M., ²Kuznetsov S. A., ³Anuchin K. N.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshhevikov, 22, bldg. 1), e-mail: ¹amgelfand@mail.ru, ²Killingsprin@bk.ru, ³anucin221@gmail.com

The article is devoted to the analysis of the role of the human factor in information security and methods of countering social engineering attacks. In the context of the increasing number and complexity of cyber attacks, the main attention of the authors is focused on studying the influence of the human factor and ways to minimize it as a key element in information protection. Various forms of social engineering and approaches to personnel training are analyzed in order to increase awareness of the methods of cyber fraudsters. The authors emphasize the need to develop a comprehensive, human-centered approach to information security that would include not only technological solutions, but also measures to increase the awareness and preparedness of users and staff.

Keywords: Information security, social engineering, cyber attacks, fraud mitigation.

Введение

Информационная безопасность является одной из основных причин беспокойства для многих компаний. С ростом числа кибератак и их обескураживающей изощренностью задача защиты информации стала еще более сложной. Хотя при обсуждении нарушений безопасности в средствах массовой информации преобладают технологические сбои, львиную долю которых занимают вредоносные программы и использование уязвимостей программного обеспечения, становится все более очевидным, что человеческий фактор может сыграть значительную роль в подрыве усилий организации по обеспечению безопасности. В данной статье мы попытаемся рассмотреть с теоретической точки зрения, как можно решить проблему человеческого фактора в безопасности. Основное внимание будет уделено социальной инженерии - атакам, которые основаны на взаимодействии с человеком для получения конфиденциальной информации. Эти атаки могут иметь различные формы и осуществляться в любой точке цепочки - от первоначальной разведки цели до попытки создания черного хода. Хочется надеяться, что благодаря расширению исследований в этой области и разработке теорий о том, как можно снизить эти риски, удастся сместить акцент с исключительно технологических решений по защите от информационных рисков и перейти к более значимой роли таких аспектов, как осведомленность и развитый, ориентированный на человека, многоуровневый подход к обеспечению информационной безопасности. В этом вступлении мы попытаемся дать краткую характеристику отчета в целом и затронуть некоторые ключевые моменты, которые будут обсуждаться далее [2,4].

1. Понимание атак социальной инженерии

Атаки с использованием социальной инженерии часто являются первым шагом на пути к более крупному и сложному вторжению в организационные системы. Социальная инженерия - это получение информации от людей, обычно той, которая должна быть секретной. Большинство пользователей компьютеров и мобильных устройств знают об угрозе безопасности, которую представляют вирусы и другие вредоносные программы, даже если они не очень хорошо разбираются в этих угрозах. В результате многие пользователи принимают меры по защите от этих угроз. Однако многие пользователи еще не знают о потенциальных рисках, связанных с социальной инженерией. В отличие от вредоносных программ, о которых часто предупреждают, угрозы социальной инженерии обычно не пытаются проникнуть в компьютер или мобильное устройство пользователя. Вместо этого тактика социальной инженерии часто используется для того, чтобы обманом заставить пользователя предоставить доступ или информацию, которая может быть использована для получения доступа к организационным системам. В последние годы сочетание большего количества атак, больших потенциальных выплат и все еще относительно низкой осведомленности пользователей об опасности социальной инженерии сделало эти виды атак все более популярными среди киберпреступников. В немалой степени это связано и с тем, что использование социальной инженерии для взлома систем обычно требует от злоумышленников наименьших усилий и ресурсов по сравнению с более техническими атаками. Многие люди еще не усвоили первый урок защиты от кибератак, который заключается в том, что каждый должен играть важную роль в обеспечении безопасности систем. Это особенно верно в отношении социальной инженерии; хотя обучение и подготовка пользователей очень важны, не только от них зависит, будут ли они распознавать и

предотвращать атаки. Организации также могут помочь защитить себя и своих сотрудников, используя соответствующие технологии и устанавливая эффективные физические барьеры безопасности. Однако, безусловно, без тщательного обучения пользователей и программ подготовки даже самые надежные технологии и решения безопасности могут быть легко обойдены теми, кто использует методы социальной инженерии для проникновения в систему организации. Поэтому в статье не только предлагаются различные решения в виде методов обучения пользователей и технологических средств защиты от социальной инженерии, но и в заключении говорится о крайне важности наличия соответствующего режима, направленного на оценку и постоянное совершенствование средств защиты для удовлетворения потребностей постоянно меняющихся угроз социальной инженерии [1, 4].

2. Повышение осведомленности и обучение пользователей

Как уже говорилось в предыдущих разделах, эффективными методами противодействия социальной инженерии являются программы обучения пользователей и повышения их осведомленности о безопасности. Пользователи часто являются самым слабым звеном в системе безопасности организации, просто потому, что злоумышленнику необходимо манипулировать ими для достижения своих целей. Обычно сотрудники имеют определенный уровень доступа к сетям и системам организации, и их восприимчивость к атакам - человеческая уязвимость - часто используется злоумышленниками в своих интересах. Поэтому проактивный подход к снижению рисков социальной инженерии заключается в формировании и поддержании у пользователей мышления, ориентированного на безопасность, а также в обучении их распознаванию атак социальной инженерии и защите от них. Это включает в себя понимание тактики социальных инженеров - например, предотвращение человеческой склонности доверять безоговорочно или распознавание различных форм обмана - и создание сообщества пользователей, в котором существует коллективная ответственность за безопасность, что часто называют "обороной вглубь". Это включает в себя не только повышение уровня осведомленности человека о безопасности во время работы, но и усиление его бдительности на всех этапах повседневной жизни, где он взаимодействует с информационными технологиями. Ведь социальная инженерия не только атакует информационные системы организаций, но и представляет собой серьезную угрозу личной конфиденциальности в киберсреде. Включение тематического контента по защите частной жизни в материалы по безопасности также может помочь расширить понимание людьми конфиденциальности на различных онлайн-платформах и в приложениях. Конечной целью программы повышения осведомленности и обучения пользователей является создание культуры безопасности в организации: культуры, которая будет поддерживаться и проявляться на протяжении многих лет при постоянной поддержке как сотрудников, так и высшего руководства. В следующем разделе я расскажу о последних инициативах и практиках, направленных на вовлечение сотрудников в деятельность по повышению осведомленности о безопасности и дальнейшее создание устойчивой культуры безопасности, ориентированной на пользователей [5].

3. Внедрение технических средств контроля

Как отмечает Янг в книге "Кибербезопасность для индустрии 4.0", постоянно меняющийся ландшафт киберугроз означает, что злоумышленники постоянно пытаются найти новые векторы атак. Именно поэтому так важны расширенные функции, которые предлагают межсетевые экраны нового поколения. Предоставляя разнообразные методы защиты сети с акцентом на выявление различных потенциальных атак и защиту от них, можно свести к минимуму шансы стать жертвой атаки нулевого дня.

Один из способов, с помощью которого злоумышленники постоянно пытаются обмануть защиту, - это использование уязвимостей "нулевого дня". Это недостатки в программном, аппаратном или микропрограммном обеспечении, которые еще не известны разработчикам и производителям. В результате отсутствуют патчи и исправления, а значит, злоумышленники могут использовать эти уязвимости в ущерб технологическим пользователям.

Современные решения в области кибербезопасности движутся в сторону внедрения более совершенных межсетевых экранов, таких как брандмауэры нового поколения. Такие брандмауэры часто включают в себя дополнительные функции поверх стандартных технологий, такие как глубокая проверка пакетов, защита и обнаружение вторжений, проверка на уровне приложений. Благодаря этим функциям, а также функциям блокировки и ограничения скорости для различных правил брандмауэра, они могут обеспечить более сложную защиту от социальной инженерии, поскольку весь спектр методов атак, используемых злоумышленниками, постоянно меняется и развивается [3.4].

Брандмауэр - важнейшая часть кибербезопасности. Он действует как барьер между доверенной и недоверенной сетью и контролирует трафик, разрешенный к передаче в сеть и из нее. В настоящее время большинство крупных организаций и корпораций используют ту или иную технологию брандмауэра. Однако не все брандмауэры построены одинаково. Некоторые организации могут выбрать брандмауэр, который использует только предопределенные правила для разрешения или блокирования трафика - такие брандмауэры называются статическими брандмауэрами с пакетной фильтрацией. Другие могут использовать динамическую фильтрацию пакетов, когда брандмауэр проверяет экземпляр соединения на предмет его валидности и затем создает динамическое правило, позволяющее пропускать дальнейший трафик. Аналогично, брандмауэры с проверкой состояния работают на транспортном уровне модели OSI и отслеживают состояние активных соединений. Это означает, что если соединение было установлено доверенным лицом, дальнейший трафик в течение сессии будет разрешен [2,5].

И IDS, и IPS могут обнаруживать целый ряд различных атак, но наиболее эффективны против конкретных типов атак. Например, сетевые IDS и IPS лучше всего выявляют угрозы, исходящие из Интернета или других сетевых устройств.

Существует множество различных типов технологий, которые при правильном применении повышают эффективность защиты от социальной инженерии. К ним относятся системы обнаружения вторжений (IDS), системы предотвращения вторжений (IPS) и межсетевые экраны. IDS - это пассивная система, которая способна обнаруживать возможные атаки, нарушения безопасности, а также отслеживать и вести журнал потенциальной вредоносной активности. IPS - это активная система, которая при обнаружении угрозы предпринимает заранее определенные действия. Например, она может отправить предупреждение системному администратору или закрыть порт.

В мире современных технологий каждый день создаются новые вредоносные программы и схемы социальной инженерии, которые используются злоумышленниками. Поэтому очень важно следить за современными технологиями и обеспечивать адекватную защиту от этих атак [3].

4. Оценка и совершенствование защиты

Теперь масштаб вашего проекта очевиден. Вы знаете, какие технологии используются в вашей среде, и осведомлены о потенциальных векторах атак с помощью социальной инженерии. Поэтому вам необходимо оценить, насколько хорошо данная технология способна предотвращать и обнаруживать социальные атаки. Как всегда, совершенствование технологий может оказаться непосильной задачей, однако изменения и улучшения можно начать с простых вещей. Необходимо регулярно устанавливать исправления и обновления по мере их появления. Многие производители выпускают патчи сразу после выхода своего продукта, потому что в нем есть определенная уязвимость. Когда патч выпущен, хакер может воспользоваться уязвимостью, поэтому важно поддерживать системы в актуальном состоянии по мере появления таких патчей. Также убедитесь, что технология имеет обновленные списки потенциально вредоносных сайтов и известных фишинговых сайтов, чтобы сотрудники не попали на них по ошибке. В большинстве случаев поставщики продуктов регулярно предоставляют обновления этих списков, поэтому важно следить за тем, чтобы технология обновлялась. Это особенно полезно при защите от программ-вымогателей, поскольку криптографические методы вымогателей меняются. Поскольку технология находится на стадии оценки, важно понимать, что плохие результаты не всегда связаны с неэффективностью технологии. Проблема может заключаться в том, что текущая технология не позволяет решить всю проблему, технология развернута неправильно или, возможно, не подходит для защиты организации. Вот почему важно начинать пересмотр и изменение технологии с мелочей, с изменений, которые можно внести без масштабных последствий, и с изменений, которые можно достаточно легко реализовать. Это может быть что угодно - от внедрения новой технологии безопасности до такой простой вещи, как более строгие политики паролей. Эффективность изменений можно регулярно проверять, проводя учения "красной команды", и предпочтительные исправления и улучшения должны быть основаны на результатах этих учений.

Список литературы

1. Белопахов А.С. Использование игры «CAPTURE THE FLAG» как инструмента формирования навыка отражения кибератак у профессиональных программистов//Вестник науки. – 2023. – Т. 3. – №. 5 (62). – С. 584-589.
2. Беляцкий Н.П., Подупейко А.А. Цифровая трансформация: время меняться. – 2020.
3. Гасанов З.З., Вардидзе Р.Т. Обеспечение безопасности JAVA-приложений//Неделя науки-2021. – 2021. – С. 66-67.
4. Понин Ф.Н. Трансформация области COMPUTER SCIENCE под влиянием новейших технологических инноваций//Universum: технические науки. – 2023. – №. 12-1 (117). – С. 59-64.

5. Shestakova L., Akhmetzyanov R. The use of E-learning elements by a mathematics teacher in work with schoolchildren //Mathematics at school. – 2023. – Т. 3. – №. 116. – С. 35-44.

References

1. Belopakhov A.S. Using the game "CAPTURE THE FLAG" as a tool for developing the skill of repelling cyber attacks among professional programmers //Bulletin of Science. – 2023. – Т. 3. – №. 5 (62). – pp. 584-589.
 2. Byalyatsky N.P., Podupeiko A.A. Digital transformation: time to change. – 2020.
 3. Hasanov Z.Z., Vardidze R.T. Ensuring the security of JAVA applications //Science Week-2021. – 2021. – pp. 66-67.
 4. Ponin F.N. Transformation of the field of computer science under the influence of the latest technological innovations //Universum: technical sciences. – 2023. – №. 12-1 (117). – pp. 59-64.
 5. Shestakova L., Akhmetzyanov R. The use of E-learning elements by a mathematics teacher in work with schoolchildren//Mathematics at school. – 2023. – Vol. 3. – No. 116. – pp. 35-44.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.056

ПСИХОЛОГИЧЕСКИЕ АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ

Перевертун Д.Р.

*ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
danilaperevertun@gmail.com*

В статье рассматриваются психологические аспекты кибербезопасности, подчёркивая значимость человеческого фактора в предотвращении киберугроз. Анализируется влияние доверия, восприятия риска, эмоциональных реакций и мотивации на поведение пользователей в сети. Освещаются стратегии повышения осведомлённости и обучения, направленные на формирование защитного поведения и культуры кибербезопасности в организациях и среди индивидов. Подчёркивается важность интеграции психологических принципов в разработку и внедрение мер кибербезопасности, а также обозначается роль социальной инженерии и эмоциональной уязвимости в контексте киберугроз.

Ключевые слова: Кибербезопасность, человеческий фактор, психологические аспекты, доверие в интернете, восприятие риска, эмоциональная уязвимость, мотивация защиты, обучение кибербезопасности, социальная инженерия, культура безопасности.

PSYCHOLOGICAL ASPECTS OF CYBERSECURITY

Perevertun D.R.

*ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: danilaperevertun@gmail.com*

The article examines the psychological aspects of cybersecurity, emphasizing the importance of the human factor in preventing cyber threats. The influence of trust, risk perception, emotional reactions and motivation on the behavior of users on the network is analyzed. Awareness-raising and training strategies aimed at developing protective behavior and a culture of cybersecurity in organizations and among individuals are highlighted. The importance of integrating psychological principles into the development and implementation of cybersecurity measures is emphasized, as well as the role of social engineering and emotional vulnerability in the context of cyber threats.

Keywords: Cybersecurity, human factor, psychological aspects, trust on the Internet, risk perception, emotional vulnerability, protection motivation, cybersecurity training, social engineering, security culture.

В эпоху цифровизации, когда технологии проникают в каждую сферу человеческой жизни, вопросы кибербезопасности становятся всё более актуальными. Однако, несмотря на техническую оснащённость и продвинутые методы защиты, человеческий фактор остаётся самым слабым звеном в цепи кибербезопасности. В этой статье мы рассмотрим психологические аспекты, лежащие в основе кибербезопасности, а также исследуем, как

понимание человеческой психологии может способствовать повышению уровня защищённости в информационном пространстве.

Одним из ключевых психологических аспектов в контексте кибербезопасности является принцип доверия. Человек по своей природе склонен доверять системам, процессам и другим людям. Мошенники и киберпреступники активно используют этот аспект, применяя социальную инженерию и фишинг для обмана жертв.[4] Важно понимать, что доверие в цифровом мире должно быть обоснованным и проверенным.

Следующий важный аспект — это восприятие риска. Многие пользователи не осознают реальной угрозы, которую представляют кибератаки, либо, наоборот, переоценивают свои способности к защите. Это приводит к тому, что меры безопасности либо игнорируются, либо применяются некорректно. Обучение и повышение осведомлённости могут сыграть ключевую роль в изменении этой ситуации.

В понимании психологических аспектов угроз кибербезопасности ключевую роль играет осознание того, что за каждым действием в сети стоит человек со своими убеждениями, страхами, ожиданиями и предрассудками. Эти индивидуальные характеристики в комплексе влияют на уровень уязвимости перед лицом киберугроз. Принцип доверия, например, является фундаментальным в построении межличностных отношений и взаимодействия с технологиями.[2] Однако в контексте кибербезопасности это доверие может быть использовано против человека. Мошенники и хакеры активно эксплуатируют доверчивость, прибегая к таким методам, как социальная инженерия и фишинг, чтобы манипулировать жертвами и выманивать у них конфиденциальную информацию.

Восприятие риска также играет существенную роль в том, как индивиды оценивают потенциальную угрозу своей кибербезопасности. Некоторые могут недооценивать риск, полагая, что они не представляют интереса для злоумышленников, или же переоценить свои способности защитить себя, что приводит к избыточной самоуверенности и игнорированию базовых мер безопасности. Эта дихотомия в восприятии угроз создаёт условия, при которых пользователи могут стать лёгкой добычей для киберпреступников.

Не менее важен эмоциональный аспект, включающий в себя такие чувства, как страх, жадность или чувство непобедимости. Эти эмоции могут облегчить злоумышленникам задачу манипулирования своими жертвами. Например, страх потери может побудить человека к поспешным действиям, таким как нажатие на вредоносную ссылку или предоставление конфиденциальных данных, если злоумышленник убедит его, что это необходимо для предотвращения ещё больших потерь.[7] Жадность может быть использована при различных схемах обмана, обещающих большую прибыль за минимальные усилия или вложения.

Таким образом, психологические аспекты угроз кибербезопасности заключаются в сложном взаимодействии между индивидуальными особенностями личности, её эмоциональным состоянием и способностью критически оценивать информацию и риски. Разумеется, эти аспекты не существуют в вакууме и взаимодействуют с техническими и социальными факторами, создавая сложную картину угроз и вызовов в области кибербезопасности.[5] В этой связи, понимание и учёт психологических аспектов могут значительно повысить эффективность предотвращения киберугроз и формирования культуры кибербезопасности как в организациях, так и среди индивидуальных пользователей. Осознание того, как эмоции и психологические настройки влияют на принятие решений в сети, может помочь в разработке более интуитивно понятных и пользовательски

ориентированных систем безопасности, которые учитывают человеческие слабости и стараются минимизировать их влияние.

Понимание психологии не только помогает выявить слабые места в защите, но и разработать более эффективные методы противодействия киберугрозам. К примеру, использование геймификации в процессах обучения может значительно повысить интерес и вовлечённость сотрудников в изучение вопросов кибербезопасности.

Мотивация является ключевым элементом в обеспечении кибербезопасности. Создание системы поощрений за соблюдение правил и протоколов безопасности может стимулировать более ответственное поведение пользователей и сотрудников.

В сфере кибербезопасности психология защиты занимает центральное место, исследуя, как человеческие факторы влияют на принятие и эффективность мер безопасности. Понимание того, что стоит за решением человека следовать или игнорировать рекомендации по кибербезопасности, может пролить свет на способы укрепления защитных механизмов в информационном пространстве. На уровне организаций и индивидов развитие защитного поведения в цифровом мире часто зависит от сложного взаимодействия между осознанием угрозы, восприятием собственной уязвимости и мотивацией к действию.

Защитное поведение в контексте кибербезопасности не сводится лишь к техническим навыкам и знаниям. Оно глубоко укоренено в психологических мотивациях и отношениях, влияющих на то, как люди воспринимают свою способность влиять на безопасность собственных данных и систем.[6] Это включает в себя уровень самоэффективности, то есть веры в свои способности осуществлять необходимые действия для защиты от киберугроз. Люди с высоким уровнем самоэффективности склонны активнее принимать меры по обеспечению кибербезопасности, поскольку они уверены в своих способностях успешно применять необходимые инструменты и стратегии.

Ключевым элементом психологии защиты является также мотивация к изменению и поддержанию безопасного поведения в интернете. Эта мотивация может быть усилена через различные стратегии, включая обучение, осведомлённость о рисках и последствиях кибератак, а также через системы поощрений и наказаний в организационной культуре. Понимание того, что действия индивида имеют значение и могут защитить как личные данные, так и корпоративные активы, способствует формированию глубоко укоренённого чувства ответственности и заинтересованности в кибербезопасности.

Помимо мотивации и самоэффективности, важную роль в психологии защиты играет и образовательный компонент. Обучение и повышение осведомленности не только передают необходимые знания и навыки, но и способствуют формированию правильного восприятия киберугроз и понимания ценности проактивного подхода к безопасности.[3] Информационные кампании и образовательные программы, направленные на развитие критического мышления и осознанного отношения к киберрискам, являются неотъемлемой частью стратегии защиты.

Психологические аспекты кибербезопасности играют ключевую роль в формировании эффективной стратегии защиты информационных систем и данных. Понимание того, как человеческий фактор влияет на безопасность, позволяет разработать более целенаправленные и эффективные подходы к её обеспечению.

Внедрение психологических знаний в практику кибербезопасности охватывает не только разработку технических решений, но и формирование корпоративной культуры, обучение и

повышение осведомлённости среди пользователей. Программы обучения должны быть направлены не только на передачу знаний о технических аспектах безопасности, но и на развитие критического мышления, способности оценивать риски и принимать обоснованные решения в условиях неопределённости.

Следует также обратить внимание на социально-психологические аспекты, такие как формирование доверия внутри организации, управление конфиденциальностью и приватностью, а также на механизмы противодействия социальной инженерии и манипуляциям. Инвестирование в развитие социального капитала и построение открытой, взаимоподдерживающей обстановки в коллективе может существенно повысить уровень кибербезопасности.

Необходимо также учитывать влияние новых технологий, таких как искусственный интеллект и машинное обучение, на психологические аспекты кибербезопасности. Автоматизация и применение алгоритмов для предотвращения кибератак может с одной стороны уменьшить человеческий фактор как источник угроз, но с другой — создать иллюзию полной безопасности, что также может быть рискованным.

Стоит подчеркнуть, что человеческий фактор играет критически важную роль в обеспечении защиты в цифровой эпохе. Понимание того, как психологические характеристики и поведенческие тенденции влияют на безопасность информационных систем, позволяет формировать более эффективные и адаптированные подходы к защите от киберугроз. Важность разработки и реализации образовательных программ, направленных на повышение осведомлённости и обучение безопасному поведению в интернете, не может быть переоценена. Такие программы должны учитывать психологические аспекты восприятия риска, доверия, эмоционального вовлечения и мотивации к защите, чтобы стимулировать формирование устойчивой культуры кибербезопасности среди пользователей и в организациях.

Кроме того, необходимо акцентировать внимание на том, что кибербезопасность — это не статичная дисциплина, а динамично развивающаяся область, требующая постоянной адаптации к новым угрозам и технологическим реалиям.[1] В этом контексте понимание психологических основ поведения пользователей и злоумышленников становится критически важным для предотвращения киберинцидентов и минимизации их последствий. Эффективная стратегия кибербезопасности должна включать в себя не только технические решения, но и активное участие пользователей, основанное на глубоком понимании психологических аспектов их взаимодействия с цифровым миром.

В заключение, интеграция психологических знаний в практику кибербезопасности открывает новые горизонты для разработки более эффективных методов защиты, обучения и профилактики киберугроз. Взаимодействие между техническими и человеческими аспектами безопасности должно стать основой для создания устойчивых и адаптируемых систем защиты в информационном обществе будущего.

Список литературы

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – С. 1-6.

2. Гельфанд А. М. и др. Интернет вещей (IoT): Угрозы безопасности и конфиденциальности//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 215-220.
3. Гельфанд А. М. и др. Исследование распределенного механизма безопасности для устройств интернета вещей с ограниченными ресурсами//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). – 2020. – С. 321-326.
4. Косов Н. А. и др. Анализ методов машинного обучения для детектирования аномалий в сетевом трафике//Цифровизация образования: теоретические и прикладные исследования современной науки. – 2021. – С. 33-37.
5. Косов Н. А., Тимофеев Р. С. Сравнение методов обучения свёрточных нейронных сетей//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 526-530.
6. Косов Н.А., Мазепин П.С., Гришин Н.А. Применение нейронных сетей для автоматизации тестирования программного обеспечения //Наукосфера. – 2020. – №. 6. – С. 152-156.
7. Штеренберг С.И. Методика построения защищенных систем искусственного интеллекта для проведения электроретинографии в офтальмологии //Офтальмохирургия. – 2022. – №. 4s. – С. 51-57.

References

1. Krasov A. et al. Using mathematical forecasting methods to estimate the load on the computing power of the IoT network //The 4th International Conference on Future Networks and Distributed Systems (ICFNDS). – 2020. – pp. 1-6.
 2. Gelfand A.M. et al. Internet of things (IoT): security and privacy threats//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 215-220.
 3. Gelfand A.M. et al. Investigation of a distributed security mechanism for Internet of Things devices with limited resources //Actual problems of infotelecommunications in science and education (APINO 2020). – 2020. – pp. 321-326.
 4. Kosov N. A. et al. Analysis of machine learning methods for detecting anomalies in network traffic //Digitalization of education: theoretical and applied research of modern science. – 2021. – pp. 33-37.
 5. Kosov N.A., Timofeev R.S. Comparison of training methods for convolutional neural networks//Actual problems of infotelecommunications in science and education (APINO 2021). – 2021. – pp. 526-530.
 6. KOSOV N.A., MAZEPIN P.S., GRISHIN N.A. Application of neural networks for software testing automation //The sciencosphere. - 2020. – No. 6. – pp. 152-156.
 7. Shterenberg S. I. Methods of constructing protected artificial intelligence systems for conducting electroretinography in ophthalmology //OPHTHALMOSURGERY. – 2022. – No. 4s. – pp. 51-57.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.77

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СРЕД ИСПОЛНЕНИЯ JAVASCRIPT КОДА NODE.JS, DENO И BUN ДЛЯ РАЗРАБОТКИ СЕРВЕРНОЙ ЧАСТИ ВЕБ-ПРИЛОЖЕНИЯ

¹ Смирнов А.А., ² Черенков А.В., ³ Подольский Е.А.

ФГАОУ ВО "НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ (ИТМО)", Санкт-Петербург, Россия (197101, город Санкт-Петербург, Кронверкский пр-кт, д. 49 литер а), e-mail: ¹smirnov.andrew.1999@yandex.ru, ²art.cherenkov@gmail.com, ³podolskijgor51@gmail.com

Актуальность исследования обусловлена стремительным развитием веб-технологий и повсеместным использованием JavaScript не только на клиентской стороне, но и на сервере. С увеличением сложности веб-приложений и переходом к разработке fullstack, вопросы эффективности и безопасности исполнения серверного JavaScript становятся ключевыми. Анализ зарубежных и отечественных научных источников по данной теме позволит выявить современные тенденции, проблемы и подходы к оптимизации выполнения серверного JavaScript кода, а также причины появления новых сред исполнения кода, что влияет на разработку высокопроизводительных и надежных веб-приложений. Целью работы является анализ зарубежных и отечественных научных источников, связанных со средами исполнения JavaScript кода Node.js, Deno и Bun, и сравнение этих сред между собой. В результате проделанного исследования были проанализированы зарубежные и отечественные источники по теме исследования. Найдены различия между средами выполнения и какие концепции привели к этим различиям. Составлена сравнительная таблица.

Ключевые слова: Веб-приложение, серверная часть, контент, производительность.

COMPARATIVE ANALYSIS OF THE JAVASCRIPT CODE EXECUTION ENVIRONMENTS OF NODE.JS, DEMO AND BAN FOR DEVELOPING THE BACKEND OF A WEB APPLICATION

¹ Smirnov A.A., ² Cherenkov A.V., ³ Podolsky E.A.

NATIONAL RESEARCH UNIVERSITY OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS (ITMO), St. Petersburg, Russia (197101, St. Petersburg, Kronverkskiy pr-kt, 49), e-mail: ¹smirnov.andrew.1999@yandex.ru, ²art.cherenkov@gmail.com, ³podolskijgor51@gmail.com

The relevance of the research is due to the rapid development of web technologies and the widespread use of JavaScript not only on the client side, but also on the server. With the increasing complexity of web applications and the transition to fullstack development, issues of efficiency and security of server-side JavaScript execution are becoming key. An analysis of foreign and domestic scientific sources on this topic will reveal current trends, problems and approaches to optimizing the execution of server-side JavaScript code, as well as the reasons for the emergence of new code execution environments, which affects the development of high-performance and reliable web applications. The purpose of the work is to analyze foreign and domestic scientific sources related to the execution environments of the JavaScript code Node.js, Deno and Bun, and comparing these environments with each other. As a result of the research, foreign and domestic sources on the research topic were analyzed.

Differences between runtimes have been found and which concepts have led to these differences. A comparative table has been compiled.

Keywords: Web application, backend, content, performance.

Объектом исследования являются программные среды для разработки серверной части веб-приложения.

Теоретической основой исследования стали труды авторов: И. В. Родыгина, А. Наливайко, М. С. Берьянов, Р. Ф. Фархутдинов, М. Хамидуллин, I. Kniazev, A. Fitiskin, M. Abbadini, J. J. Merelo-Guervós, M. Garcia-Valdez, P. A. Castillo, А. Моисеев, F. Doglio, D. Koper, M. Woda.

Информационная база исследования: eLIBRARY, Springer, CyberLeninka, ResearchGate, Google Scholar.

Задачи исследования:

1. Поиск зарубежных и отечественных научных источников, описывающих среды исполнения серверного JavaScript кода.
2. Изучение и анализ источников.
3. Написание заключения и выводов по анализированным источникам.

В статье авторов Родыгина И.В., Наливайко А.В. «Сравнительный анализ технологий для разработки серверной части системы управления продажами» [1] говорится, что быстрая скорость выдачи контента способствует удовлетворению пользователей, что может повысить конверсию и удержание клиентов. Поэтому такая цель как повышение производительности ещё долго будет актуальной, и инновационные инструменты, предлагающие такое улучшение, имеют все шансы развиться и стать трендовыми. Здесь интересны тесты производительности Node.js в сравнении с Java и PHP. В тесте на выдачу чистого текста и в тесте сериализации Node.js занимает второе место, уступая лишь Java библиотеке Vert.X, и в десятки раз обгоняя PHP. При этом Node.js обеспечивает минимальную задержку между ответами. В тесте на множественные запросы к базе данных Node.js уступает Java с фреймворком Spring, но обгоняет PHP с Laravel.

В контексте разработки программного обеспечения на языке JavaScript существуют средства, позволяющие внедрить строгую типизацию, такие как TypeScript. Одновременно, возможность использования асинхронного кода является встроенной функциональностью JavaScript, не требующей использования сторонних библиотек. Однако, при сравнительном анализе производительности, JavaScript на платформе Node.js показывает результаты, уступающие языку Java.

Для того чтобы увеличить конкурентоспособность языка JavaScript в этой области, были созданы новые инновационные решения, такие как Bun и Deno. Эти платформы интегрируют поддержку TypeScript "из коробки", заявляют о значительном улучшении производительности по сравнению с Node.js и предлагают инновационные решения некоторых проблем, рассматриваемых далее в работе.

Берьянов М. С. в статье «Исследование платформы Deno в сравнении с Node.js» [2] рассматривает вхождение Node.js в предпочтительный стек технологий для разработки приложений, обозначая его как ведущий тренд, который завоевал популярность, в значительной степени благодаря массовому сообществу разработчиков. В данной статье

уделяется внимание Deno как потенциальному конкуренту Node.js. Проводится краткий анализ двух платформ (таблица 1). В большей степени рассматриваются интересные аспекты инноваций, предложенных в Deno, особенно в сравнении с Node.js.

Таблица 1 – Сравнение Node.js и Deno при анализе [2]

	Node.js	Deno
Совместимость с браузером	В значительной степени	Полная
Поддержка TypeScript	Необходимо устанавливать библиотеку	Встроенная
Обеспечение безопасности	Не настраивается	Выдаются разрешения при запуске кода
Управлении модулями	В файле package.json задаются все зависимости и загружаются в папку node_modules	Зависимости задаются непосредственно в коде и загружаются при первом запуске

Инновационность в безопасности относительно Node.js проявляется в выполнении в Deno кода в «песочнице». Это означает, что у среды выполнения по умолчанию нет доступа к файловой системе, сети, выполнению других скриптов и к переменным окружения. Разрешения на эти действия выдаются при запуске с помощью флагов, например, флаги --allow-write и --allow-read позволяют более детально контролировать, к каким частям файловой системы может получить доступ процесс.

В работе авторов Фархутдинов Р. Ф., Хамидуллин М. Р. «PHP и NODE.JS в веб-разработке, анализ преимуществ, сравнение и пути развития» [3] предполагается, что Node.js вероятно будет развиваться в сторону увеличения производительности и улучшения работы на многоядерных машинах.

Чепегин, И.Д. в статье «Серверный JavaScript - преимущества и недостатки Node.js» [4] выделяет главное преимущество не столько Node.js, сколько JavaScript – использование единого языка как на стороне клиента, так и сервера (таблица 2). Преимуществом считается уже конкретно Node.js пакетный менеджер NPM, причём именно количество доступных через него модулей и пакетов, то есть огромное сообщество. Отмечено, что в NPM есть недостаток в виде сильной зависимости от пакетов, так как удаление зависимости может привести в нерабочее состояние уже разработанные сервисы. Недостатки Node.js покрываются решением другой платформы.

Таблица 2 – Сравнение Node.js с другими технологиями при анализе [4]

	JavaScript (Node.js)	Другие языки программирования
Использование единого языка для написания клиента и сервера при разработке веб приложения	Присутствует	Отсутствует у большинства
Пакетный менеджер	NPM с миллионами библиотек	Зависит от языка программирования

Тихонов Д.С., Черенков А.В., Долгов А.В. в работе «Сравнительный анализ технологий серверной разработки на платформах DENO и BUN» [5] проводят сравнительный анализ сред исполнения JavaScript кода Deno и Bun (таблица 3). Помимо общей информации о средах проводится ряд экспериментов, в которых сравнивается производительность технологий. На основании полученных данных можно сделать следующий вывод: Bun выделяется в производительности при обработке массивов и рекурсивных вычислениях, что делает его идеальным для сценариев, где требуется высокая скорость обработки данных и интенсивные вычисления.

Таблица 3 – Сравнение Deno и Bun при анализе [5]

	Deno	Bun
Рекомендуемый вариант использования	Веб-серверы или микросервисы	Обработка массивов и рекурсивных вычислениях

С другой стороны, Deno обеспечивает лучшую производительность в асинхронных задачах, что особенно важно для приложений, зависящих от асинхронного ввода-вывода, таких как веб-серверы или микросервисы.

В результате анализа установлено, что новые среды исполнения (Deno, Bun) являются не просто копиями Node.js, а каждая из них нацелена решить определённые проблемы и предоставить разработчикам альтернативы, в которых реализованы инновационные идеи (Таблица 4).

Таблица 4 – Итоговое сравнение Node.js, Deno и Bun [6-8]

	Node.js	Deno	Bun
Как проводится обновление среды исполнения	Сторонними инструментами, например, NVM	Встроенными инструментами	Встроенными инструментами
Обеспечение безопасности	Не настраивается	Выдаются разрешения при запуске кода	Не настраивается
Компиляция кода в исполняемый файл	Отсутствует	Присутствует	Присутствует
Совместимость с браузером	В значительной степени	Полная	В значительной степени
Поддержка TypeScript	Необходимо устанавливать библиотеку	Встроенная	Встроенная
Наличие дополнительных инструментов для разработки	Необходимо устанавливать библиотеки	Инструменты для сборки, тестирования, обновления	Инструменты для сборки, тестирования, обновления
Пакетный менеджер	NPM	Не нуждается в пакетном менеджере	NPM
Рекомендуемые модели облачного сервиса	Виртуальные машины	Виртуальные машины	Бессерверные вычисления
Стандартная библиотека	Часто требуются внешние библиотеки	Обширная	Часто требуются внешние библиотеки
Работа с пакетами	В файле package.json задаются все зависимости и загружаются в папку node_modules	Зависимости задаются непосредственно в коде и загружаются при первом запуске	В файле package.json задаются все зависимости и загружаются в папку node_modules
Используемый движок	V8	V8	JavaScriptCore
Дата выпуска версии 1.0.0	2015-01-14	2020-05-14	2023-09-08

Заключение

Deno будет лучшим выбором при акценте на безопасность, полной совместимости с браузером и удобстве работы с библиотеками.

Vip же стоит выбрать при необходимости быстрой сборки, а также при выполнении затратных синхронных вычислений, и в бессервисных вычислениях.

Node.js стоит выбрать для крупных проектов, в которых важны стабильность работы, проверенная временем, и наличие специальных, узконаправленных библиотек. Также намного больше разработчиков знакомо с Node.js, нежели чем с двумя другими средами.

Список литературы

1. Родыгина И. В., Наливайко А. В. Сравнительный анализ технологий для разработки серверной части системы управления продажами: статья в журнале - научная статья//Известия ЮФУ. Технические науки. №4(221). — 2021. — С. 256-266
2. Берьянов М. С. Исследование платформы Deno в сравнении с Node.js//Студенческий: электрон. научн. журн. 2022. № 40(210). — С. 45-48.
3. Фархутдинов Р. Ф., Хамидуллин М. Р. PHP и NODE.JS в веб-разработке, анализ преимуществ, сравнение и пути развития//Материалы 12-й Международной молодежной научной конференции. В 4-х томах. Том 3. Отв. редактор М.С. Разумов. Курск, 2022. — С. 122-124.
4. Чепегин, И. Д. Серверный JavaScript - преимущества и недостатки Node.js//Вестник науки и образования. – 2020. – № 12-1(90). – С. 18-20.
5. Тихонов Д.С., Черенков А.В., Долгов А.В. сравнительный анализ технологий серверной разработки на платформах DENO и BUN//Научно-технические инновации и веб-технологии. - 2023. - №2. - С. 55-59.
6. Kniazev I., Fitiskin A. Choosing the right javascript runtime: an in-depth comparison of NODE.JS and BUN//Norwegian Journal of Development of the International Science. — 2023. — С. 72-84.
7. Abbadini M. et al. NatiSand: Native Code Sandboxing for JavaScript Runtimes//Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. – 2023. – С. 639-653.
8. Koper D., Woda M. Performance Analysis and Comparison of Acceleration Methods in JavaScript Environments Based on Simplified Standard Hough Transform Algorithm //International Conference on Dependability and Complex Systems. – Cham: Springer International Publishing, 2022. – С. 131-142.

References

1. Rodygina I. V., Nalivaiko A.V. Comparative analysis of technologies for the development of the server part of the sales management system: an article in the journal - a scientific article // News of the Southern Federal University. Technical sciences. №4(221). — 2021. — pp. 256-266
2. Baranov M. S. Research of the Deno platform in comparison with Node.js // Student: electron. scientific Journal. 2022. № 40(210). — pp. 45-48.

3. Farkhutdinov R. F., Khamidullin M. R. PHP and NODE.JS in web development, analysis of advantages, comparison and development paths // Materials of the 12th International Youth Scientific Conference. In 4 volumes. Volume 3. Editor M.S. Razumov. Kursk, 2022. — pp. 122-124.
 4. Chepegin, I. D. Server-side JavaScript - advantages and disadvantages Node.js // Bulletin of Science and Education. – 2020. – № 12-1(90). – pp. 18-20.
 5. Tikhonov D.S., Cherenkov A.V., Dolgov A.V. comparative analysis of server development technologies on the DENO and BUN platforms // Scientific and technical innovations and web technologies. - 2023. - No. 2. - pp. 55-59.
 6. Kniازهv I., Fitiskin A. Choosing the right javascript runtime: an in-depth comparison of NODE.JS and BUN // Norwegian Journal of Development of the International Science. — 2023. — pp. 72-84.
 7. Abbadini M. et al. NatiSand: Native Code Sandboxing for JavaScript Runtimes //Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses. – 2023. – pp. 639-653.
 8. Koper D., Woda M. Performance Analysis and Comparison of Acceleration Methods in JavaScript Environments Based on Simplified Standard Hough Transform Algorithm //International Conference on Dependability and Complex Systems. – Cham: Springer International Publishing, 2022. – pp. 131-142.
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.052

МЕТОДИКА РАЗРАБОТКИ И ВНЕДРЕНИЯ ЗАЩИТНЫХ ПРОТОКОЛОВ ДЛЯ IOT УСТРОЙСТВ С УЧЕТОМ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ

Денисов Н.А.

ФГБОУ ВО «МИРЭА - РОССИЙСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ», Москва, Россия, (119454, г. Москва, просп. Вернадского, 78, стр. 4.), e-mail: ndenisoff@icloud.com

По мере того как устройства интернета вещей (IoT) становятся неотъемлемой частью повседневной жизни людей, важными элементами промышленности, медицины и других ключевых секторов экономики, они также начинают выступать целью для кибератак. Уязвимости в этих устройствах могут привести к серьезным последствиям, в том числе, утечке конфиденциальной информации, нарушению работы ключевых систем и даже физическим угрозам. Более того, характер и сложность уязвимостей в IoT устройствах часто отличаются от традиционных вычислительных систем. Недостатки в безопасности могут возникать на различных уровнях – аппаратном и прикладном обеспечении, сетевых протоколах и других элементах. Это означает, что подходы к защите, применяемые в традиционных ИТ-системах, не всегда применимы к IoT и создает потребность в разработке специализированных защитных протоколов для IoT. В связи с вышеизложенным, автором настоящей статьи, была предпринята попытка исследования методики разработки и внедрения защитных протоколов для iot устройств с учетом распространенных уязвимостей

Ключевые слова: Устройства интернета вещей (IoT), кибератаки, разработка и внедрение защитных протоколов, IoT устройства, распространенные уязвимости, разработка специализированных защитных протоколов для IoT.

METHODOLOGY FOR DEVELOPMENT AND IMPLEMENTATION OF SECURITY PROTOCOLS FOR IOT DEVICES, CONSIDERING COMMON VULNERABILITIES

Denisov N.A.

MIREA - RUSSIAN TECHNOLOGICAL UNIVERSITY, Moscow, Russia (119454, Moscow, avenue. Vernadsky, 78, b. 4), e-mail: ndenisoff@icloud.com

As Internet of Things (IoT) devices become an integral part of people's daily lives, important elements of industry, medicine and other key sectors of the economy, they also become a target for cyber attacks. Vulnerabilities in these devices can lead to serious consequences, including leakage of confidential information, disruption of key systems, and even physical threats. Moreover, the nature and complexity of vulnerabilities in IoT devices often differ from traditional computing systems. Security flaws can occur at various levels - hardware and application software, network protocols and other elements. This means that security approaches used in traditional IT systems are not always applicable to IoT and creates a need for the development of specialized security protocols for IoT. In connection with the above, the author of this article made an attempt to study the methodology for the development and implementation of security protocols for iot devices, taking into account common vulnerabilities.

Keywords: Internet of Things (IoT) devices, cyber attacks, development and implementation of security protocols, IoT devices, common vulnerabilities, development of specialized security protocols for IoT.

Введение

Интернет вещей (IoT) представляет собой растущую сеть физических объектов, оснащенных встроенными сенсорами, программным обеспечением и другими технологиями для подключения и обмена данными с другими устройствами и системами через Интернет. Данная концепция революционизирует способ взаимодействия людей с окружающим миром, предоставляя новые возможности для интеграции физического и цифрового пространств.

Традиционно Интернет использовался для соединения компьютеров и мобильных устройств. Однако, с появлением IoT, практически любой объект может быть оснащен способностью отправлять и получать данные. IoT способствует созданию "умных" домов и предприятий, где все устройства могут быть связаны и автоматически управляться. К возможностям IoT относят автоматизацию процессов (например, регулирование температуры, освещения и безопасности), предоставление пользователю возможности контролировать эти процессы удаленно через смартфоны или другие устройства и т.д.

В современную эпоху, когда технологии интернета вещей (IoT) стремительно интегрируются в повседневную жизнь, обеспечение безопасности этих устройств становится насущной необходимостью. Растущая зависимость от IoT в различных сферах (бытовая автоматизация, промышленное производство, здравоохранение и т.д.), подчеркивает значимость разработки и внедрения эффективных защитных протоколов. Особенно это актуально с учетом увеличения числа кибератак и уязвимостей, которые способны кардинально нарушить приватность, безопасность данных и функциональную надежность систем на основе IoT. Проблема обеспечения безопасности IoT устройств усугубляется многообразием существующих устройств и разнообразием способов их применения. Таким образом, разработка универсальных и одновременно специфических защитных протоколов, способных учитывать широкий спектр уязвимостей и атак, является важной и востребованной задачей.

Характеристика методики

Целью методики разработки и внедрения защитных протоколов для IoT устройств является предотвращение различных уязвимостей и обеспечение высокого уровня безопасности данных и функционирования устройств.

Основные задачи методики: анализ уязвимостей, разработка стратегии защиты, минимизация поверхности атаки, протоколирование и мониторинг, соблюдение нормативных требований.

Центральным элементом методики является комплексный подход к безопасности, который включает в себя технические аспекты защиты, а также управленческие, нормативные и процедурные меры. Методика учитывает не только непосредственно угрозы безопасности и уязвимости самих устройств, но и широкий спектр внешних и внутренних факторов, способных повлиять на безопасность системы в целом. Стратегия защиты, реализованная в рамках данной методики, определяет оптимальные способы защиты устройств и данных от различных видов атак путем выбора подходящих методов шифрования, управления доступом, аутентификации и других мер безопасности.

Методика также направлена на минимизацию поверхности атаки, что подразумевает ограничение возможностей для несанкционированного доступа и вмешательства в работу устройств и систем путем оптимизации конфигураций устройств и сетей, а также ограничения

доступа к некритичным функциям и сервисам. Для обеспечения возможности отслеживания и анализа безопасности в реальном времени, своевременного обнаружения и реагирования на инциденты безопасности, аудита и проверки соответствия систем безопасности установленным требованиям и стандартам, предусмотрено протоколирование и мониторинг.

С целью юридической защиты и повышения доверия пользователей и партнеров к системе IoT, предлагаемая методика предусматривает соблюдение нормативных требований в части соответствия законодательству и стандартам в области защиты данных и информационной безопасности.

Предлагаемая методика подразумевает интеграцию на четырех уровнях IoT устройств:

1. Уровень приложений занимает центральное место во взаимодействии пользователя с IoT-системой и включает в себя все программное обеспечение и приложения, которые позволяют пользователям управлять IoT-устройствами, а также собирать, анализировать и визуализировать данные, полученные от этих устройств. На уровне приложений обеспечивается защита пользовательского интерфейса и приложений, которые взаимодействуют с IoT устройствами. Предлагается использование SSL/TLS для защиты данных, передаваемых между приложениями и IoT устройствами; реализация многофакторной аутентификации и контроля доступа к приложениям; автоматизация процесса обновления приложений для устранения уязвимостей и поддержания актуальности защиты; отслеживание активности пользователей и запись событий безопасности.

2. Уровень служб касается сервисов и программного обеспечения, которое управляет IoT устройствами. На данном уровне планируется обеспечение безопасности API, через который приложения взаимодействуют с устройствами; разделение систем на разные сегменты для снижения рисков распространения угроз; реализация надежных процедур бэкапа и восстановления данных для предотвращения потерь информации.

3. Сетевой уровень в архитектуре Интернета вещей обеспечивает связь между IoT-устройствами и другими компонентами системы (серверы обработки данных или приложения уровня пользователя). Сетевой уровень отвечает за передачу данных, собранных устройствами, и является ключевым для обеспечения эффективности и безопасности всей IoT-системы. На сетевом уровне акцент сделан на обеспечении безопасности передачи данных между устройствами и через сетевые узлы. Будет реализовано использование VPN и шифрование сетевого трафика для защиты данных в процессе передачи; создание сетевых сегментов для изоляции критически важных устройств и данных; развертывание IDS/IPS для мониторинга и реагирования на подозрительную активность в сети.

4. Уровень элементов относится к физическим устройствам и компонентам, которые непосредственно выполняют сбор данных и взаимодействуют с внешней средой. На уровне элементов рассматривается защита физических устройств и компонентов. Будет организована защита устройств от несанкционированного физического доступа и повреждений; регулярное обновление прошивок, использование надежного аппаратного обеспечения; ограничение функционала устройств до необходимого минимума для уменьшения рисков.

Алгоритм реализации методики: [4, с. 725]

1. Оценка существующей инфраструктуры IoT, выявление и анализ уязвимостей на всех уровнях (аппаратное обеспечение, программное обеспечение, сетевые компоненты).
2. Анализ уязвимостей и выбор инструментов для тестирования безопасности.

3. Проектирование и разработка защитных протоколов, адаптированных под специфику IoT устройств:

- создание системы защиты, предусматривающей шифрование данных, управление доступом и аутентификации, авторизацию и обнаружение инцидентов;
- устранение ненужных функций, ограничение доступа, применение принципа наименьших привилегий;
- разработка процесса обновления программного обеспечения и прошивок, включая патчи безопасности.

4. Пилотное внедрение протоколов с последующим тестированием и оптимизацией: [1, с. 69]

- установка систем протоколирования и мониторинга для обнаружения и реагирования на инциденты;
- проведение тестов на проникновение и оценка рисков, связанных с уязвимостями.

5. Развертывание защитных протоколов на все IoT устройства, интеграция с существующими системами безопасности и настройка систем мониторинга и реагирования на инциденты.

6. Разработка программ обучения для разработчиков, администраторов и пользователей, проведение обучающих семинаров для сотрудников.

Основными программными модулями предлагаемого решения будут являться: [6, с. 59]

1. Модуль анализа уязвимостей. Отвечает за автоматическое сканирование уязвимостей в рамках интеграции с инструментами для обнаружения известных уязвимостей в аппаратном и программном обеспечении IoT, а также за ручную оценку уязвимостей в виде интерфейса для проведения экспертных аудитов и анализа сложных уязвимостей, которые не могут быть обнаружены автоматически.

2. Модуль шифрования и защиты данных. Обеспечивает за реализацию современных алгоритмов шифрования для защиты данных, передаваемых и хранимых на IoT устройствах, а также за безопасное хранение и обновление ключей шифрования.

3. Модуль управления доступом и аутентификации. Основные функции - управление доступом пользователей и устройств к IoT системам и возможность применения дополнительных мер аутентификации для повышения уровня безопасности.

4. Модуль минимизации поверхности атаки. Обеспечивает анализ текущей конфигурации с точки зрения ее оптимизации и управление настройками сети и устройств для ограничения доступа к неиспользуемым функциям и сервисам.

5. Модуль обновления и патчинга. Основные функции - автоматизация процесса обновления программного обеспечения, прошивок устройств и информирование администраторов о новых обновлениях безопасности.

6. Модуль мониторинга и протоколирования. Отвечает за обнаружение и предотвращение вторжений (IDS/IPS) путем мониторинга сетевого трафика на предмет подозрительной активности. Осуществляет запись важных событий безопасности для последующего анализа и расследования инцидентов (логирование и аудит).

7. Модуль тестирования на проникновение и оценки рисков. Обеспечивает интеграцию с инструментами для проведения тестов на проникновение и оценки уязвимостей и оценки и приоритизацию рисков, связанных с уязвимостями

Ожидаемые результаты: [3, с. 78]

- уменьшение количества уязвимостей и инцидентов безопасности в среде IoT;
- повышение уровня безопасности данных и надежности работы IoT устройств;
- соответствие современным стандартам и требованиям в области кибербезопасности.

Использование защитных протоколов для IoT устройств целесообразно в рамках системы Умный Дом и промышленных IoT систем.

В рамках системы Умный Дом внедрение защитных протоколов актуально для таких IoT устройств, как умные замки, системы безопасности, термостаты, и устройства для управления освещением и бытовой техникой.

Умные замки обеспечивают физическую безопасность дома; защитные протоколы здесь необходимы для предотвращения несанкционированного доступа, что важно для обеспечения безопасности жильцов. Системы безопасности включают в себя камеры видеонаблюдения, датчики движения и другие средства мониторинга; защита данных, передаваемых этими устройствами, минимизирует риски утечки информации о домашнем хозяйстве. Умные термостаты, контролирурующие климат в доме, должны быть защищены от несанкционированного управления, поскольку это может привести к неэффективному использованию энергии или даже повреждению системы отопления и охлаждения. Защита устройств для управления освещением и бытовой техникой обеспечивает удобство и экономию энергии, а также предотвращает потенциальные риски, связанные с перегрузкой электросети или неожиданным включением техники.

Таким образом, основная цель внедрения предлагаемой методики в системе Умный Дом - повышение безопасности и защиты личной информации, снижение риска несанкционированного доступа. Особенности реализации защитных протоколов: [7, с. 124]

- анализ уязвимостей каждого устройства в системе, особенно умных замков и систем безопасности;
- внедрение защитных протоколов, включающих двухфакторную аутентификацию для доступа к умному замку и шифрование данных между устройствами и центральным управляющим хабом;
- отключение неиспользуемых сетевых интерфейсов и сервисов для обеспечения минимизации поверхности атаки.
- установление процесса автоматического обновления программного обеспечения для всех устройств.

Промышленные IoT системы используются для мониторинга и управления производственными процессами. В данном случае, внедрение защитных протоколов актуально для сенсоров по измерению температуры, давления и других параметров.

Так, защита сенсоров и устройств от несанкционированного доступа и манипуляций обеспечивает получение более точных и надежных данных для производственных процессов. Предотвращение вмешательства в работу систем позволяет поддерживать стабильность и эффективность производства. С учетом того, что промышленные IoT системы часто связаны с интернетом, они могут стать целью для хакеров. Предлагаемая методика помогает предотвратить атаки, направленные на парализацию производственных процессов или кражу конфиденциальной информации, а внедрение комплексных мер безопасности (шифрование

данных, сетевая безопасность) защищает системы от внешних и внутренних угроз. Надежная защита IoT устройств снижает риск непредвиденных остановок в производственных процессах, что может быть вызвано как техническими сбоями, так и кибератаками, обеспечивая более высокую производственную эффективность и снижая потенциальные финансовые потери от простоев. Кроме того, использование предложенной методики дает возможность предприятиям соответствовать стандартам и нормативным требованиям в области кибербезопасности и защиты данных, повышая их репутацию и доверие со стороны клиентов и партнеров.

Таким образом, основная цель внедрения предлагаемой методики в управлении производственными процессами - повышение надежности и безопасности промышленных систем, защита от потенциальных кибератак и снижение риска простоев на производстве.

Особенности реализации защитных протоколов:

- оценка уязвимостей промышленных IoT устройств, особенно в области защиты данных от внешних атак;
- реализация защитных механизмов, в частности шифрование всех передаваемых данных и строгие процедуры аутентификации для доступа к управлению системами;
- удаление всех ненужных функций и ограничение сетевых подключений только до необходимых узлов;
- настройка автоматизированной системы для обновления программного обеспечения и прошивок.

Таким образом, разработка и внедрение защитных протоколов для устройств интернета вещей (IoT) – это процесс создания и применения комплекса мер безопасности, предназначенных для защиты IoT устройств от различных угроз кибербезопасности.

Данный процесс осуществляется через комплексный анализ уязвимостей IoT устройств, последующую разработку стратегии защиты, адаптированной к специфике этих устройств, и реализацию предложенных защитных мер. Целью разработки и внедрения защитных протоколов является обеспечение безопасности и конфиденциальности данных, передаваемых и обрабатываемых IoT устройствами, защита устройств от несанкционированного доступа и снижение риска кибератак. [2, с. 49]

Реализация данных мер обусловлена растущим использованием IoT устройств и их интеграцией в критически важные области жизни и экономики. Предлагаемая методика предназначена для производителей и разработчиков IoT устройств, а также для специалистов по кибербезопасности и ИТ-администраторов, работающих в компаниях и организациях, использующих IoT технологии. Кроме того, она актуальна для конечных пользователей этих устройств, поскольку повышает уровень их безопасности и надежности.

Данный процесс предполагает максимально оперативную реализацию, учитывая текущую динамику роста использования IoT и соответствующих угроз кибербезопасности, а также требует регулярного пересмотра и обновления в соответствии с появлением новых технологий, угроз и стандартов безопасности. [5, с. 26]

В заключение можно отметить, что в современную эпоху цифровизации разработка и внедрение защитных протоколов для IoT устройств является важным элементом стратегии кибербезопасности, и ее значимость будет только повышаться по мере дальнейшего развития и распространения технологий интернета вещей.

Список литературы

1. Бармин, С. Протоколы прикладного уровня для функций M2M и IoT / С. Бармин // Электронные компоненты. – 2021. – № 10. – С. 66-71.
2. Кычкин, А. В. Разработка программной системы для управления IoT-устройствами с использованием структурных и поведенческих паттернов / А. В. Кычкин, О. В. Горшков // Прикладная информатика. – 2020. – Т. 15, № 4(88). – С. 44-53.
3. Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения / М. М. Ковцур, Д. И. Кириллов, А. В. Михайлова, П. А. Потемкин // Техника средств связи. – 2020. – № 4(152). – С. 74-86.
4. Корзухин, С. В. Конфигурируемые IoT-устройства на основе SoC-систем ESP8266 и протокола MQTT / С. В. Корзухин, Р. Р. Хайдарова, В. Н. Шматков // Научно-технический вестник информационных технологий, механики и оптики. – 2020. – Т. 20, № 5. – С. 722-728.
5. Кумалатов, Р. Ш. Разнообразие устройств и протоколов в решении безопасности iot / Р. Ш. Кумалатов // Студенческий. – 2022. – № 34-1(204). – С. 25-26.
6. Харламов, М. А. Использование уязвимостей IOT-устройств при DDOS-атаках / М. А. Харламов, Е. Д. Никитин // Молодежная научная школа кафедры "Защищенные системы связи". – 2021. – Т. 1, № 2(4). – С. 57-60.
7. Горбенко, А. К. Анализ методов обнаружения уязвимостей в IoT-устройствах / А. К. Горбенко, А. А. Маринов // Научный альманах Центрального Черноземья. – 2022. – № 1-6. – С. 117-128.

References

1. Barmin, S. Application layer protocols for M2M and IoT functions / S. Barmin // Electronic components. - 2021. – No. 10. – pp. 66-71.
2. Kychkin, A.V. Development of a software system for controlling IoT devices using structural and behavioral patterns / A.V. Kychkin, O. V. Gorshkov // Applied Informatics. - 2020. – vol. 15, No. 4(88). – pp. 44-53.
3. Development of a methodology for implementing machine learning to improve the information security of a web application / M. M. Kovtsur, D. I. Kirillov, A.V. Mikhailova, P. A. Potemkin // Communication equipment. – 2020. – № 4(152). – pp. 74-86.
4. Korzukhin, S. V. Configurable IoT devices based on the ESP8266 SoC systems and the MQTT protocol / S. V. Korzukhin, R. R. Khaidarova, V. N. Shmatkov // Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. - 2020. – Vol. 20, No. 5. – pp. 722-728.
5. Kumalatov, R. S. A variety of devices and protocols in the iot security solution / R. S. Kumalatov // Studentskiy. – 2022. – № 34-1(204). – pp. 25-26.
6. Kharlamov, M. A. The use of vulnerabilities of IOT devices in DDOS attacks / M. A. Kharlamov, E. D. Nikitin // Youth Scientific School of the department "Secure communication systems". - 2021. – Vol. 1, No. 2(4). – pp. 57-60.

Денисов Н.А. Методика разработки и внедрения защитных протоколов для IoT устройств с учетом распространенных уязвимостей // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 4(42) С. 107–114

7. Gorbenko, A. K. Analysis of vulnerability detection methods in IoT devices / A. K. Gorbenko, A. A. Marinov // Scientific Almanac of the Central Chernozem region. - 2022. – No. 1-6. – pp. 117-128.



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.032.26

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ЯЗЫКОВОЙ МОДЕЛИ GPT-3.5 ДЛЯ ОБУЧЕНИЯ РУССКОМУ ЯЗЫКУ СТУДЕНТОВ СИСТЕМЫ СПО

Туманова И.В.

БПОУ ВОЛОГОДСКОЙ ОБЛАСТИ "ЧЕРЕПОВЕЦКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ АКАДЕМИКА И.П. БАРДИНА", Череповец, Россия, (162627, Вологодская область, город Череповец, ул. Сталеваров, д.26), e-mail: tumatops@mail.ru

В статье рассматривается возможность применения нейронных сетей, в том числе языковой модели GPT-3.5, в обучении русскому языку студентов среднего профессионального образования. Выделены основные преимущества использования нейронных сетей в учебном процессе, такие как индивидуализация обучения, автоматизация оценивания, обратная связь в реальном времени и расширение доступа к образованию. Особое внимание уделяется значимости дальнейших исследований и разработок в данной области для оптимизации учебных процессов и повышения эффективности использования нейронных сетей в образовании. Статья посвящена актуальной теме, так как в настоящее время нейросети набирают все большую популярность и активно интегрируются в образовательный процесс.

Ключевые слова: Нейронные сети, русский язык, обучение, среднее профессиональное образование, GPT-3.5, индивидуализация, автоматизация оценивания, обратная связь, безопасность данных, исследования, эффективность.

THE POSSIBILITIES OF USING THE GPT-3.5 LANGUAGE MODEL FOR TEACHING RUSSIAN TO STUDENTS OF THE EDUCATIONAL SYSTEM

Tumanova I.V.

"CHEREPOVETS METALLURGICAL COLLEGE NAMED AFTER ACADEMICIAN I.P. BARDIN", Cherepovets, Russia, (162627 Vologda region, Cherepovets, Stalevarov st., 26), e-mail: tumatops@mail.ru

The article considers the possibility of using neural networks, including the GPT-3.5 language model, in teaching Russian to students of secondary vocational education. The main advantages of using neural networks in the educational process are highlighted, such as individualization of learning, automation of assessment, real-time feedback and increased access to education. Special attention is paid to the importance of further research and development in this area for optimizing educational processes and increasing the effectiveness of the use of neural networks in education. The article is devoted to an urgent topic, as neural networks are currently gaining more and more popularity and are actively integrated into the educational process.

Keywords: Neural networks, Russian language, training, secondary vocational education, GPT-3.5, individualization, automation of assessment, feedback, data security, research, efficiency.

С развитием информационных технологий и искусственного интеллекта, нейронные сети стали играть значительную роль в образовательной сфере. Поскольку они способны обрабатывать и анализировать большое количество информации, их использование в образовании открывает новые горизонты для глубокой персонализации обучения и

автоматизации многих образовательных процессов. Это включает в себя адаптивное обучение, автоматическую проверку заданий, анализ успеваемости студентов и многое другое¹. В рамках этой статьи мы рассмотрим различные примеры использования нейронных сетей в образовательной среде и отметим их преимущества.

Один из ключевых аспектов применения нейронных сетей в образовании – это возможность персонализации обучения. Это означает, что каждый студент может получать индивидуальную программу обучения, учитывающую его уровень знаний, скорость обучения, профессиональные интересы и прочее. Примером такого подхода может служить приложение CogBooks, которое использует нейронные сети для адаптации учебных планов к уровню знаний каждого студента. Подобные технологии позволяют оптимизировать образовательный процесс, учитывая индивидуальные особенности каждого учащегося, что ведет к увеличению эффективности обучения.

Нейронные сети могут быть использованы для проверки домашних заданий и тестов, ускоряя этот процесс и увеличивая его точность. Например, приложение Gradescope, использует нейронные сети для проверки заданий студентов и предоставления им обратной связи. Это не только экономит время преподавателей, но и помогает студентам быстрее получать обратную связь о своем успехе и понимании материала.

Благодаря сложным алгоритмам обучения, нейронные сети могут выявлять уникальные способности каждого студента и адаптировать обучающие материалы с учетом этих способностей². Примером такого подхода является проект TALENT, который использует нейронные сети для определения талантов студентов в различных областях, таких как музыка, спорт и т.д. Информатика и компьютерные технологии — это еще одна область, в которой активно применяются нейронные сети. Глубокие нейронные сети используются для построения интеллектуальных тьюторов - программ, которые помогают студентам изучать информатику и компьютерные науки. Они могут быть использованы для обучения различным навыкам, таким как программирование, решение задач, проектирование баз данных, обучения верстке и многое другое. Образовательные платформы, такие как Coursera, уже активно используют нейронные сети и другие методы машинного обучения для предложения специализированных курсов

Наконец, нейронные сети также используются для автоматического перевода, что значительно облегчает изучение иностранных языков. С помощью этой технологии студенты могут переводить тексты, аудио и видео материалы на различных языках, что помогает им лучше понимать иностранный язык и усваивать новую информацию. Примерами таких систем являются Google Translate и Yandex.Translate, Deep L, которые используют глубокие нейронные сети для перевода материалов на разных языках.

Внедрение нейронных сетей в образовательную сферу открывает огромные возможности для повышения качества обучения, улучшения профессиональных навыков преподавателей и оптимизации времени обучения. Однако, несмотря на все преимущества, стоит отметить, что

¹ Кужель С.С., Кужель О.С. Информационные технологии - средство развития системного творческого мышления // Educational Technology & Society 5(1) 2002 pp. 264-275

² Актуальность использования нейросетей в образовательных целях / И. Р. Хабибуллин, О. В. Азовцева, А. Д. Гареев. — Текст: непосредственный // Молодой ученый. — 2023. — № 13 (460). — С. 176-178. — URL: <https://moluch.ru/archive/460/101127/> (дата обращения: 21.05.2023)

технология нейронных сетей все еще находится на начальном этапе своего развития. Системы, основанные на применении нейронных сетей, требуют дальнейших исследований, тестирования и совершенствования, чтобы устранить возможные ошибки и улучшить точность прогнозирования.

В будущем, правильное и обдуманное использование технологии нейронных сетей в образовании будет играть ключевую роль в создании наиболее подходящих условий для каждого студента. Это позволит учитывать индивидуальные потребности и интересы каждого ученика, создавая для них максимально благоприятную образовательную среду. Важно также понимать, что успех внедрения нейронных сетей в образование в значительной степени зависит от открытости и готовности образовательной системы к инновациям и новым подходам. Также требуется подходящий набор данных для обучения и тестирования нейронных сетей, чтобы они могли эффективно адаптироваться к специфике образовательного процесса. Это в свою очередь подчеркивает важность качественных данных и умения их правильно обрабатывать в контексте использования нейронных сетей в образовании.

Языковая Модель GPT-3.5, также известная как Generative Pretrained Transformer 3.5, разработанная OpenAI, представляет собой относительно новое достижение в области искусственного интеллекта и машинного обучения. Эта модель обладает уникальными способностями в генерации текста, её обучение базировалось на огромных массивах данных, что позволяет модели понимать и генерировать текст на различных языках, в 1 главе мы говорили об особенностях рекуррентных нейронных сетей, которые способны понимать даже речевые паттерны. Важно отметить, что GPT-3.5 в отличие от своих предшественников, демонстрирует улучшенное понимание контекста, более точное соблюдение заданных инструкций и повышенную способность к адаптации к различным видам текстов. Эти характеристики делают её идеальной для использования в образовательных целях, поскольку модель может быть адаптирована под специфические нужды обучения и оказывать помощь в изучении различных аспектов языка.

Модель GPT-3.5 имеет возможность генерации вопросов, ответов и упражнений, а также корректировки ошибок, что делает её ценным инструментом для обучения грамматике, орфографии и синтаксису русского языка. Благодаря своим аналитическим способностям, GPT-3.5 способна адаптироваться к индивидуальным уровням знания студентов и предлагать материалы, соответствующие их уровню понимания.

Для обучения русскому языку, GPT-3.5 также может быть использована для создания интерактивных модулей, включающих тексты для чтения, аудио- и видеоматериалы для слушания и просмотра, а также интерактивные упражнения для проверки понимания и закрепления материала.

Вместе с этим, GPT-3.5 предлагает ряд новых возможностей для обучения языку. Она способна на генерацию историй и диалогов на русском языке, которые могут быть использованы для обучения, а также предоставляет возможность для интерактивного обучения через диалоги в режиме реального времени, суть ее работы заключается в том, что она анализирует предыдущий контекст ввода, чтобы предсказать следующее слово или фразу. Модель обучается на огромном количестве текстовых данных, благодаря чему она способна генерировать связные и логические ответы на запросы пользователей, проиллюстрировать это можно следующим образом: если мы вводим вопрос "Кто был первым президентом

Российской Федерации?", модель анализирует контекст вопроса и, на основании своих предварительных знаний, генерирует ответ "Борис Ельцин". Таким образом, модель использует свои предварительные знания и понимание контекста для генерации текста.

Ключевой особенностью GPT-3.5 является ее способность учитывать больший контекст ввода по сравнению с предыдущими версиями модели. Это позволяет ей более точно интерпретировать запросы пользователей, еще GPT-3.5 обладает улучшенной способностью к адаптации, что позволяет ей эффективно применяться в обучении языков. Она способна адаптировать свои ответы в соответствии с уровнем знаний и понимания пользователя, что делает её полезным инструментом для индивидуализированного обучения.

Модель может быть использована для обучения следующим разделам русского языка:

- **Грамматика:** Модель может быть использована для обучения различных аспектов грамматики. Например, можно создать обучающий модуль, в котором модель будет представлять собой задачи на выбор правильной грамматической формы слова или построение предложений в определённом времени. Благодаря своим обучающим данным, модель может генерировать правильные грамматические структуры на основе контекста.
- **Лексика:** модель может генерировать примеры использования новых слов в контексте, помогая студентам лучше понять и запомнить новую лексику.
- **Структура предложений:** может объяснить студентам как строятся предложения в русском языке. Это может быть особенно полезно для обучения сложных конструкций, таких как сложноподчинённые предложения.
- **Практика навыков чтения и письма:** можно генерировать тексты на определённые темы, что позволяет студентам практиковать навыки чтения и письма.
- **Индивидуализация обучения:** модель способна подстраиваться. GPT-3.5 позволяет создавать индивидуализированные обучающие программы. Это может быть особенно полезно для студентов, которые имеют сложности с определёнными аспектами русского языка.

Таким образом, языковая модель GPT-3.5 представляет собой мощный инструмент для обучения русскому языку, позволяющий студентам улучшить свои языковые навыки в разнообразных аспектах.

Список литературы

1. Голицына И.Н. Эффективное управление учебной деятельностью с помощью компьютерных информационных технологий. - // Educational Technology & Society 6(2) 2003, С. 77-83.
2. Редько, В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики / В.Г. Редько. - М.: Ленанд, 2019. - 224 с
3. Хайкин, С. Нейронные сети: полный курс / С. Хайкин. - М.: Диалектика, 2019. - 1104 с
4. Кащенко, С. А. Модели волновой памяти / С.А. Кащенко, В.В. Майоров. - М.: Либроком, 2020. - 288 с.
5. Круглов, В. В. Искусственные нейронные сети. Теория и практика: моногр. / В.В. Круглов, В.В. Борисов. - М.: Горячая линия - Телеком, 2021. - 382 с.

6. Кужель С.С., Кужель О.С. Информационные технологии - средство развития системного творческого мышления // *Educational Technology & Society* 5(1) 2002 С. 264-275
7. Матвеева Н. Ю., Золотарюк А. В. Технологии создания и применения чат-ботов. Научные записки молодых исследователей. 2018, (1): С.28–30
8. Актуальность использования нейросетей в образовательных целях / И. Р. Хабибуллин, О. В. Азовцева, А. Д. Гареев. — Текст: непосредственный // *Молодой ученый*. — 2023. — № 13 (460). — С. 176-178.

References

1. Golitsyna I.N. Effective management of educational activities using computer information technologies. - // *Educational Technology & Society* 6(2) 2003, pp. 77-83.
 2. Redko, V.G. Evolution, neural networks, intelligence: Models and concepts of evolutionary cybernetics / V.G. Redko. - М.: Lenand, 2019. - p.224
 3. Khaykin, S. Neural networks: a complete course / S. Khaykin. - М.: Dialectics, 2019. - p.1104.
 4. Kashchenko, S. A. Models of wave memory / S.A. Kashchenko, V.V. Mayorov. - М.: Librocom, 2020. - 288 p.
 5. Kruglov, V. V. Artificial neural networks. Theory and practice: monograph / V.V. Kruglov, V.V. Borisov. - М.: Hotline - Telecom, 2021. - 382 p.
 6. Kuzhel S.S., Kuzhel O.S. Information technologies - a means of developing systemic creative thinking // *Educational Technology & Society* 5(1) 2002 pp. 264-275
 7. Matveeva N. Yu., Zolotaryuk A.V. Technologies for creating and using chatbots. Scientific notes of young researchers. 2018, (1): pp.28–30
 8. The relevance of using neural networks for educational purposes / I. R. Khabibullin, O. V. Azovtseva, A.D. Gareev. — Text: direct // *Young scientist*. — 2023. — № 13 (460). — pp. 176-178.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.052

СИСТЕМНЫЙ ПОДХОД В КАЧЕСТВЕ НАДЕЖНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Вахрушев А.В.

ФГБОУ ВО "КАЛУЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. К.Э. ЦИОЛКОВСКОГО", Калуга, Россия (248023, Калужская область, город Калуга, ул. Степана Разина, д.26), e-mail: ppetrov@yandex.ru

В данной статье исследуется системная инженерия и раскрывается суть системного подхода в обеспечении надежности информационных систем. Эта тема актуальна во всех областях применения информационных систем, включая стратегические и бизнес-процессы, где необходимо обеспечить высокое качество и надежность системы.

Ключевые слова: Оптимизация, надежность, информационная система.

A SYSTEMATIC APPROACH TO THE RELIABILITY OF INFORMATION SYSTEMS

Vakhrushev A. V.

KALUGA STATE UNIVERSITY. K.E. TSIOLKOVSKY", Kaluga, Russia (248023, Kaluga region, Kaluga city, Stepana Razina st., 26), e-mail: ppetrov@yandex.ru

This article explores system engineering and reveals the essence of a systematic approach to ensuring the reliability of information systems. This topic is relevant in all areas of information systems application, including strategic and business processes, where it is necessary to ensure high quality and reliability of the system.

Keywords: optimization, reliability, information system.

Введение

Суть системного подхода заключается в том, чтобы рассматривать каждый объект как часть более общей системы и в то же время как самостоятельную сложную систему. В современном мире развитие различных областей человеческой деятельности невозможно без широкого использования компьютеров и создания информационных систем. По мере возрастания сложности проектируемых систем, важное значение приобретают такие общесистемные вопросы, как выбор оптимальной структуры системы, определение наилучшего взаимодействия между ее элементами и оптимальных режимов их работы. Необходимость решения этих вопросов привела к появлению системного подхода к анализу больших систем. Основой системного подхода служит теория систем, разработанная биологом Л. фон Берталанфи. Кроме того, было разработано направление, названное исследованием операций, которое возникло в связи с военными задачами. Несмотря на широкое использование в других областях, первоначальная терминология этого направления часто сложно применима на практике.

Основная часть

Надежность - это способность объекта выполнять свои функции в течение определенного времени и в пределах установленных показателей. Объект может быть техническим изделием определенного назначения, которое рассматривается в процессе проектирования, производства, испытаний и эксплуатации. Эти объекты могут включать в себя различные системы и их элементы. Элемент - это простая составная часть изделия, которая в контексте надежности может быть составлена из множества деталей. Система - это совокупность взаимодействующих элементов, предназначенных для выполнения определенных функций в автономном режиме. Понятия элемента и системы могут меняться в зависимости от поставленной задачи. Например, станок может рассматриваться как система, состоящая из различных элементов, таких как механизмы и детали, при анализе его надежности, а при изучении надежности технологической линии он может рассматриваться как элемент.

Организации, которые стремятся к обеспечению надежности, обычно работают в средах, которые являются взаимодейственно сложными. Взаимодейственная сложность увеличивается, когда результаты неизвестны и могут быть потенциально неожиданными, когда социально-технические системы имеют несовместимые функции, и когда информационный поток является косвенным и неоднозначным. Тесная связь включает "процессы, зависящие от времени", "непрерывные последовательности операций", "единственный способ достичь цели" и "небольшую слабинку". Отказы являются "неотъемлемыми свойствами" взаимодейственно сложных и тесно связанных систем, так как аварии, которые невозможно предвидеть или предотвратить, неизбежны в таких системах. Это "нормальные несчастные случаи". Среда, такие как строительство или программы информационной безопасности, которые требуют значительного управления технологиями и инфраструктурой, имеют высокий уровень социальной и технической взаимосвязи. В таких условиях люди, сложные технологии и материальные активы становятся критически зависимыми друг от друга. Эта взаимосвязь означает, что ошибка в любом конкретном процессе или деятельности может быстро привести к более серьезным событиям и потенциально привести к дестабилизации или сбою в целом, особенно в непредсказуемых процессах, таких как разработка программного обеспечения и управление.

Делоне и Маклин (1992 г.) предложили шесть критериев для оценки успешной работы информационной системы:

1. Качество информационной системы;
2. Качество предоставляемой информации;
3. Уровень использования информационной системы;
4. Удовлетворенность пользователей;
5. Влияние информационной системы на поведение пользователей;
6. Воздействие информационной системы на организацию.

Для полноценной оценки успешности информационной системы необходимо учитывать критерии, такие как качество самой информационной системы, качество предоставляемых ею данных, использование системы, удовлетворенность пользователей, воздействие системы на пользователей и ее влияние на организацию и ее эффективность.

Акцент на надежности также крайне важен, особенно в условиях конкуренции между организациями и на стратегически значимых объектах. Часто организации предпочитают не жертвовать надежностью ради повышения производительности. Если организации сосредотачиваются только на текущей прибыли, не учитывая издержек, связанных с обеспечением надежности информационных систем, они, скорее всего, столкнутся с потерей прибыли и значительными затратами при внедрении систем информационной безопасности.

Модель успешности информационных систем не может быть полной без надежной и устойчивой работы систем. В связи с повторяющимися сбоями в информационных системах, обеспечение надежности программного обеспечения может стать важной составляющей задач управления проектами. Разработка концепции надежности программного обеспечения может помочь менеджерам проектов не только выполнить поставленные задачи быстрее, но и обеспечить надежность программных продуктов, а также бесперебойную работу систем через резервирование и возможность многократного дублирования.

Общее понимание системного подхода в контексте информационных систем

Подход системы в информационных системах означает, что мы рассматриваем информационную систему в целом, а не как отдельные части, и учитываем, как их взаимодействие друг с другом и с внешней средой. Это помогает нам понять, что информационная система не только состоит из компонентов, таких как оборудование, программное обеспечение, сети и базы данных, но также включает процессы обработки информации, управления и безопасности данных. Мы видим информационную систему в ее полной сложности и динамике.

Другим важным аспектом системного подхода для информационных систем является учет влияния внешних факторов, таких как угрозы безопасности, изменения в бизнес-процессах или технологические новшества. Мы понимаем информационную систему как открытую систему, взаимодействующую со внешней средой, и учитываем эти внешние воздействия, чтобы приспособлять систему к изменяющимся условиям.

Таким образом, системный подход для информационных систем предполагает рассмотрение системы в целом и ее взаимосвязи с внешним миром. Это помогает нам понимать систему в ее целостности и разрабатывать эффективные стратегии обеспечения ее надежности и устойчивости.

Анализ системы как целого

Анализ системы в целом - это метод и процесс изучения всех ее компонентов, процессов и взаимосвязей с точки зрения цельности. Этот подход помогает понять, как части системы взаимодействуют друг с другом и как эти взаимодействия влияют на работу системы в целом.

Анализ системы в целом включает в себя несколько аспектов:

1. Исследование структуры: изучение всех компонентов системы, их функций и взаимосвязей, включая аппаратное и программное обеспечение, структуру данных и сетевые элементы.
2. Процессы: изучение процессов, происходящих внутри системы, таких как обработка данных, взаимодействие между компонентами и управление ресурсами.
3. Взаимодействие с окружающей средой: учет взаимодействия системы с внешней средой, другими системами, пользователями, а также окружающими технологическими и бизнес-процессами.

4. Оценка производительности: изучение производительности системы, включая скорость работы, надежность и масштабируемость.

Цель анализа системы в целом заключается в создании полного и точного представления о ее работе в естественной среде, выявлении уязвимостей, рисков и проблем, а также разработке стратегий для улучшения работы системы, ее надежности и безопасности.

Обеспечение безопасности информационной системы

Обеспечение безопасности информационной системы означает защиту информации от несанкционированного доступа, вирусов, вторжений и утечек. Вот что включает в себя обеспечение безопасности информационной системы:

1. Защита от внешних угроз:

- Используются технологии, такие как брандмауэры и прокси-серверы, для обнаружения и предотвращения вторжений и вирусов.

2. Управление доступом:

- Разрабатываются стратегии управления правами доступа, аутентификация пользователей и мониторинг активности для предотвращения несанкционированного доступа.

3. Шифрование данных:

- Для защиты конфиденциальности и целостности данных используются криптографические методы.

4. Контроль целостности информации:

- Осуществляется контроль изменений в данных для обнаружения несанкционированного доступа или модификаций.

5. Аудит и мониторинг:

- Устанавливаются системы аудита и мониторинга для отслеживания действий пользователей и системных событий.

6. Физическая безопасность:

- Обеспечивается безопасность оборудования и помещений, где хранится критическая информация.

7. Обучение персонала:

- Сотрудники проходят обучение по безопасности информации и знакомятся с политикой безопасности.

Обеспечение безопасности информационных систем требует комплексного подхода, начиная от технических мер безопасности и заканчивая обучением персонала и разработкой стратегий реагирования на инциденты.

Анализ рисков и уязвимостей

Анализ рисков и уязвимостей в информационных системах - это процесс выявления и оценки потенциальных опасностей, которые могут негативно повлиять на работоспособность, конфиденциальность, целостность и доступность информации. Ниже приведены основные аспекты этого процесса:

1. Идентификация уязвимостей:

- Определение слабых мест в информационной системе, которые могут быть использованы злоумышленниками для несанкционированного доступа или атак.

2. Оценка вероятности и последствий:

- Оценка вероятности возникновения определенной угрозы и возможных последствий для информационной системы, включая финансовые потери, ухудшение репутации, нарушение бизнес-процессов и другие негативные последствия.
- 3. Разработка стратегий управления рисками:
 - После выявления уязвимостей и оценки рисков, разрабатываются стратегии управления рисками, включая выбор технических, организационных и процедурных мер для смягчения рисков до приемлемого уровня.
- 4. Улучшение безопасности:
 - На основе анализа рисков и уязвимостей принимаются меры по устранению или снижению уязвимостей, повышению защищенности и улучшению реагирования на угрозы.
- 5. Постоянный мониторинг и обновление:
 - Процесс анализа рисков и уязвимостей должен быть постоянным, включая систематический мониторинг, обновление методов и технологий безопасности, а также адаптацию стратегий управления рисками к изменяющимся условиям и угрозам.

Анализ рисков и уязвимостей является важным этапом управления информационной безопасностью, направленным на предотвращение возможных проблем и минимизацию потенциальных угроз для информационной системы.

Восстановление и реагирование

Восстановление и реагирование в информационной безопасности - это процессы, которые направлены на восстановление работоспособности информационной системы после возникновения инцидента или нарушения безопасности, а также на предотвращение развития инцидента и минимизацию ущерба. Вот некоторые ключевые аспекты восстановления и реагирования:

1. Разработка плана реагирования на инциденты:
 - Необходимо иметь четкий план действий, описывающий процедуры реагирования на различные виды инцидентов.
2. Обнаружение инцидентов:
 - Разработка механизмов для быстрого обнаружения инцидентов безопасности.
3. Меры по устранению инцидента:
 - Принятие мер по прекращению инцидента и минимизации его воздействия на информационную систему и бизнес-процессы.
4. Восстановление работоспособности:
 - Восстановление систем и данных до нормального состояния после инцидента.
5. Анализ инцидента:
 - Оценка последствий инцидента для выявления уязвимостей и организационных уроков, а также для предотвращения подобных инцидентов в будущем.
6. Улучшение процессов и профилактические меры:
 - Внедрение улучшений в процессы реагирования и проактивные меры по предотвращению возможных угроз и инцидентов.

Восстановление и реагирование в информационной безопасности играют важную роль в обеспечении безопасности информационных систем и минимизации последствий возможных инцидентов. Реагирование на инциденты, оперативное восстановление и обучение на основе

анализа инцидентов позволяют улучшить защиту и повысить надежность информационных систем.

Заключение

Рассмотрение информационной системы с системным подходом имеет ряд преимуществ и является критически важным для обеспечения безопасности, эффективности и устойчивости информационных систем. Вот почему:

1. **Целостность:** Системный подход учитывает информационную систему как целое, что помогает предотвратить изоляцию уязвимых мест и улучшить целостность системы.

2. **Комплексный анализ:** Определение уязвимостей и рисков путем комплексного анализа всех компонентов и процессов системы.

3. **Предотвращение каскадных отказов:** Использование системного подхода позволяет выявить возможные каскадные отказы, что позволяет принимать меры для их предотвращения.

4. **Обоснованные решения:** Системный подход обеспечивает полное понимание информационной системы, что помогает принимать обоснованные решения, направленные на улучшение безопасности и надежности.

5. **Улучшение управления рисками:** Анализ системы как целого дает более точную оценку рисков и уязвимостей, что способствует разработке стратегий управления рисками и принятию мер для уменьшения уровня рисков.

Таким образом, системный подход играет важную роль в обеспечении надежности информационных систем, позволяя комплексно рассматривать систему, выявлять уязвимости, разрабатывать стратегии управления рисками и обеспечивать подходящее управление безопасностью.

1. **Исследования:** Для дальнейших исследований следует обратить внимание на следующие аспекты:

- Разработка методов системного анализа и моделирования информационных систем с учетом их надежности и безопасности.
- Проверка эффективности системного подхода в реальных условиях эксплуатации информационных систем различных масштабов.
- Исследование влияния различных видов угроз на надежность информационных систем и создание методов для обнаружения, предотвращения и управления рисками.

2. **Практическое применение:** Для практического применения следует обратить внимание на следующие моменты:

- Внедрение системного подхода в стратегии обеспечения информационной безопасности и управления рисками на уровне организации.
- Интеграция системного подхода в процессы управления информационной безопасностью, включая разработку обучающих программ для персонала и оценку эффективности управления рисками.

3. **Развитие технологий:** Необходимо следить за развитием технологий и инструментов, поддерживающих системный подход в обеспечении надежности информационных систем, включая средства мониторинга, системы управления уязвимостями, технологии обнаружения вторжений и другие.

Продвижение исследований и разработка практической реализации системного подхода помогут эффективнее обеспечивать надежность и безопасность информационных систем, что в свою очередь способствует защите конфиденциальности, целостности и доступности информации.

Список литературы

1. "Information Security Management Handbook" (Хэндбук управления информационной безопасностью) от Tipton, Harold F., и Micki Krause.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems" ("Инженерия безопасности: Руководство по созданию надежных дистрибутивных систем") от Ross J. Anderson.
3. "Computer Security: Principles and Practice" ("Компьютерная безопасность: принципы и практика") от William Stallings и Lawrie Brown.
4. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies" ("Руководство по информационной безопасности: эффективные стратегии компьютерной безопасности и управления рисками") от Corey Schou и Steven Hernandez.
5. "Introduction to System Safety Engineering" ("Введение в инженерии систем безопасности") от Phil Hughes.
6. Делоне, В. Х.; Маклин, Э. (1992). «Успех информационных систем: поиски зависимой переменной». Информационные системы исследования. 3 (1): С.60–95. Дои:10.1287 / isre.3.1.60.
7. Делоне, В. Х. и Маклин, Э. (2002). Возвращение к успеху информационных систем. Материалы 35-й Гавайской международной конференции по системным наукам (HICSS), Большой остров, Гавайи, С.238-249.
8. Делоне, В. Х.; Маклин, Э. (2003). «Модель успеха информационных систем Делона и Маклина: последние десять лет». Журнал информационных систем управления. 19 (4): С.9–30.
9. Евдокимов О.Г., Гавдан Г.П., Резниченко С.А. Подход к оценке эффективности системы обеспечения информационной безопасности распределенной системы передачи данных // Безопасность информационных технологий. 2022. Т. 29. № 2. С. 57-70.
10. Забелина В.А., Ахвердиев В.И., Гоголь И.В., Овчинников С.С., Нестеров Ю.Г., Кротов Ю.Н. Создание рекомендательной системы для интернетмагазина на основе гибридной интеллектуальной информационной системы // Труды Международного научно-технического конгресса "Интеллектуальные системы и информационные технологии - 2022" ("ИС & ИТ-2022", "IS&IT'22"). Таганрог, 2022. С. 254-262

References

1. "Information Security Management Handbook" by Tipton, Harold F., and Mickey Krause.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross J. Anderson.
3. "Computer Security: Principles and Practice" ("Computer security: principles and practice") by William Stallings and Lawrie Brown.
4. "Information Assurance Handbook: Effective Computer Security and Risk Management Strategies" ("Information Security Handbook: Effective Computer Security and Risk

- Management Strategies") from Corey Schou and Steven Hernandez.
5. "Introduction to System Safety Engineering" by Phil Hughes.
 6. Delaunay, V. H.; McLean, E. (1992). "The success of information systems: the search for a dependent variable." *Research information systems*. 3 (1): 60–95. Doi:10.1287 / isre.3.1.60.
 7. Delaunay, V. H. and McLean, E. (2002). Return to the success of information systems. *Proceedings of the 35th Hawaii International Conference on Systems Sciences (HICSS)*, Big Island, Hawaii, pp. 238-249.
 8. Delaunay, V. H.; McLean, E. (2003). "Delon and McLean's Information Systems Success Model: The last Ten Years." *Journal of Management Information Systems*. 19 (4): pp. 9–30.
 9. Evdokimov O.G., Gavdan G.P., Reznichenko S.A. An approach to evaluating the effectiveness of the information security system of a distributed data transmission system // *Information technology security*. 2022. Vol. 29. No. 2. pp. 57-70
 10. Zabelina V.A., Akhverdiev V.I., Gogol I.V., Ovchinnikov S.S., Nesterov Yu.G., Krotov Yu.N. Creation of a recommendation system for an online store based on a hybrid intelligent information system // *Proceedings of the International Scientific and Technical Congress "Intelligent Systems and Information Technologies - 2022" ("IS & IT-2022", "IS&IT'22")*. Taganrog, 2022. pp. 254-262
-



Международный журнал информационных технологий и энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/iicse/>



УДК 004.021

АНАЛИЗ ЭФФЕКТИВНОСТИ АЛГОРИТМА МУРАВЬИНОЙ КОЛОНИИ В ЗАДАЧЕ МАРШРУТИЗАЦИИ ТРАНСПОРТНЫХ СРЕДСТВ С ОГРАНИЧЕННОЙ ВМЕСТИМОСТЬЮ

Гергедава Д.А.

ФГБОУ ВО «МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ (НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)», Москва, Россия, (125080, город Москва, Волоколамское ш., д. 4), e-mail: pusher123toxic@gmail.com

В условиях современной транспортной логистики, где эффективность и оптимизация играют ключевую роль, задача маршрутизации транспортных средств с ограниченной вместимостью представляет актуальную проблему. С увеличением объема грузов и строгих временных ограничений поиск оптимальных маршрутов становится сложной задачей.

В данном контексте алгоритмы, вдохновленные природными процессами, привлекают внимание исследователей. Алгоритм муравьиной колонии, основанный на коллективном поведении муравьев при поиске пищи, представляет перспективный подход к решению задач маршрутизации.

Статья направлена на анализ эффективности алгоритма муравьиной колонии в решении задачи маршрутизации транспортных средств с ограниченной вместимостью, а также анализ параметров, влияющих на эффективность алгоритма.

Ключевые слова: Популяционные алгоритмы, муравьиный алгоритм, автоматизация, задача маршрутизации транспорта, комбинаторная оптимизация.

ANALYSIS OF THE ANT COLONY ALGORITHM'S EFFICIENCY IN THE CAPACITY VEHICLE ROUTING PROBLEM

Gergedava D.A.

MOSCOW AVIATION INSTITUTE (NATIONAL RESEARCH UNIVERSITY), Moscow, Russia, (4, Volokolamskoye shosse, Moscow, 125080, Russian Federation), e-mail: pusher123toxic@gmail.com

In the context of modern transportation logistics, where efficiency and optimization play a crucial role, the problem of routing vehicles with limited capacity is a pertinent issue. With the increasing volume of cargo and strict time constraints, finding optimal routes becomes a challenging task.

In this context, algorithms inspired by natural processes attract researchers' attention. The ant colony algorithm, based on the collective behavior of ants in search of food, represents a promising approach to solving routing problems.

The article aims to analyze the efficiency of the ant colony algorithm in solving the problem of routing vehicles with limited capacity, as well as to analyze the parameters influencing the algorithm's effectiveness.

Keywords: Population algorithms, ant algorithm, automation, vehicle routing problem, combinatorial optimization.

Проблема оптимизации маршрутов транспортных средств представляет собой сложный класс задач комбинаторной оптимизации, возникающих в контексте логистических и снабженческих систем, где требуется эффективное перемещение товаров и услуг от

поставщиков до конечных потребителей. Эта проблема становится особенно актуальной в современной экономической среде, где динамичность рынка и быстрое развитие технологий создают необходимость в оптимизации процессов доставок [1].

Существует большое количество разновидностей задачи маршрутизации транспорта (VRP), отличающихся количеством и природой накладываемых ограничений [2]. Наиболее известные из них задача динамической маршрутизации транспортных средств (DVRP), иногда называемая задачей онлайн-маршрутизации, относительно недавно возникшая в связи с достижениями в области информационных технологий, которые позволяют получать и обрабатывать информацию в режиме реального времени, в DVRP некоторые заказы известны заранее, до начала рабочего дня, однако в течение дня системе приходится включать в изменяющийся график новые поступающие заказы, задача маршрутизации с ограниченными временными окнами (VRPTW), целью задачи VRPTW также является обслуживание клиентов с минимизацией общего пройденного расстояния, но при наличии дополнительного ограничения в виде заранее определенных временных интервалов, не нарушая ограничений по вместимости для каждого транспортного средства.

В этой статье мы сосредоточим внимание на задаче маршрутизации с ограниченной вместимостью (CVRP), являющейся усложнением классической VRP, но более простой чем VRPTW ввиду отсутствия временных окон. Любые из вариантов задачи маршрутизации представляют собой NP-сложную задачу комбинаторной оптимизации, поскольку так или иначе являются обобщением задачи коммивояжера [3]. Точные алгоритмы в 100% случаев позволяют получить оптимальное решение, однако крайне вычислительно затратны для NP-сложных задач, полный перебор имеет сложность $O(n!)$.

Ни один даже самый современный компьютер не способен в разумные сроки произвести такой объем вычислений, который привел бы к точному решению, уже даже для пары десятков вершин (Таблица 1).

Таблица 1 – Зависимость числа операций от размера задачи

n	$\frac{(n-1)!}{2}$	n	$\frac{(n-1)!}{2}$
3	1	8	2.520
4	3	9	20.160
5	12	10	181.440
6	60	20	6.082E+16
7	360	30	4.420E+30

Приведем математическую формулировку задачи маршрутизации с ограниченной грузоподъемностью (CVRP). Одним из основных ограничений является то, что суммарная масса груза на каждом маршруте грузовика не должна превышать его максимальной грузоподъемности. Кроме того, каждый клиент должен быть обслужен ровно один раз.

Пусть $G = (V, E)$ – граф, в котором $V = \{1 \dots n\}$ – набор вершин, задающих города (или клиентов) с центральным хабом, который без ограничения общности можно считать расположенным в вершине 1. А E – набор ребер, соответствующий дорогам, соединяющим города (клиентов). Вводится также матрица расстояний $C = (c_{ij})$, часто значения этой матрицы могут интерпретироваться в более общем смысле, как стоимость поездки из вершины i в j .

Минимизируем

$$\sum_{i \neq j} c_{ij} x_{ij} \rightarrow \min \quad (1)$$

Со следующими ограничениями

$$\left\{ \begin{array}{l} \sum_{e \in \delta(\{i\})} x_e = 2 \quad \forall i \in V \quad (2) \\ \sum_{e \in \delta(\{0\})} x_e = 2K \quad (3) \\ \sum_{e \in \delta(S)} x_e \geq 2k(S) \quad \forall S \subseteq V \quad (4) \\ x_e \leq 1 \quad \forall e \in E \quad \delta(\{0\}) \quad (5) \\ x_e \geq 0 \quad \forall e \in E \quad (6) \end{array} \right.$$

Здесь S – подмножество V , т.е. множество вершин, входящих в конкретный маршрут, $\delta(S)$ – множество ребер в маршруте с вершинами из S , K – количество доступных транспортных средств, $k(S)$ – это целая часть от деления суммы спросов вершин в множестве S на максимальную грузоподъемность грузовика C .

Ограничение (2) утверждает, что каждый клиент посещается каким-либо транспортным средством один раз, тогда как ограничение (3) утверждает, что K транспортных средств должны выезжать и въезжать на территорию склада. Ограничение (4) — это неравенство пропускной способности, которое требует, чтобы все подмножества обслуживались достаточным количеством транспортных средств. Ограничения (5), (6) требуют, чтобы каждое ребро, не примыкающее к депо, могло использоваться дважды, когда маршрут обслуживает только одного клиента.

Как было сказано ранее, для решения задачи будет использоваться алгоритм муравьиной колонии, дополнительно модифицированный таким образом, чтобы учитывать введенные ограничения, приведем математическую формулировку алгоритма.

Фактически алгоритм использует набор искусственных муравьев (особей), которые сотрудничают в решении задачи путем обмена информацией с помощью феромонов, нанесенных на ребра графа.

Вероятность перехода муравья из i –ой вершины в j –ую определяется следующей формулой

$$P_{ij} = \frac{\tau_{ij}^\alpha \eta_{ij}^\beta}{\sum_{m \in A} \tau_{im}^\alpha \eta_{im}^\beta} \quad (7)$$

τ_{ij} – количество феромона между городами i и j

η_{ij} – величина обратная расстоянию между городами, т.е. вероятность выбора города пропорциональна близости этого города и количеству феромона по дороге в него

A – все доступные для посещения города из текущей позиции муравья

Константы α и β определяют степень влияния близости следующей вершины и количества феромонов на пути на выбор муравья о переходе в новую вершину.

Распределение феромона для муравья с индексом k по граням (дорогам), описывается следующими формулами

$$\Delta\tau_{ij,k}(t) = \begin{cases} \frac{Q}{L_k(t)}, & \text{если } (i, j) \in T_k(t), \\ 0, & \text{если } (i, j) \notin T_k(t), \end{cases} \quad (8)$$

$$\tau_{ij}(t+1) = (1-p) \cdot \tau_{ij}(t) + \sum_{k=1}^m \Delta\tau_{ij,k}(t), \quad (9)$$

Добавка феромона, которую делает муравей k между i -ым и j -ым городом на итерации t равна отношению некоторой константы Q к длине маршрута $L_k(t)$, пройденного муравьем k , при условии, что эти два города являются частью пройденного муравьем маршрута $(i, j) \in T_k(t)$.

Количество феромона между городами i и j на новой итерации $\tau_{ij}(t+1)$ равно сумме количества феромона между городами на предыдущей итерации $\tau_{ij}(t)$, умноженной на коэффициент испарения $(1-p)$ и суммы всех новых порций феромона, которые были отложены всеми муравьями на данном участке $\sum_{k=1}^m \Delta\tau_{ij,k}(t)$.

Временная сложность этого алгоритма зависит от времени жизни колонии t (число итераций), количества вершин графа n и числа муравьев m , и определяется как $O(tn^2m)$.

Алгоритм был реализован на языке программирования Python 3.9 с использованием аппаратного обеспечения на базе четырехъядерного процессора Intel Core I3-12100F с частотой 3.5 ГГц и оперативной памятью Kingston KF426C16BB2A объемом 16 Гб 2666 МГц.

Основные методы, определенные в классе:

- **solutionOfOneAnt(vertices, edges, capacityLimit, demand, pheromones, depot)** - метод строит маршрут для каждого транспортного средства из депо для одной особи из колонии, поочередно выбирая следующий город с учетом вероятности, зависящей от феромонов и стоимости перемещения, маршрут завершается, когда транспортное средство достигает своей максимальной вместимости;
- **updatePheromones(pheromones, solutions)** – этот метод обновляет матрицу феромонов, сначала происходит испарение феромонов в соответствии с коэффициентом испарения для всех элементов матрицы. Затем, для каждого маршрута в каждом решении, обновляются феромоны на соответствующих ребрах графа. Количество отложенных феромонов обратно пропорционально длине маршрута. Таким образом, более оптимальные маршруты вносят больший вклад в увеличение феромонов;

- **rateTour(solution)** – в этом методе для каждого маршрута в решении вычисляется общая стоимость, учитывая стоимость перемещения между городами, возвращает список маршрутов и соответствующих им затрат.

Данные тестовых экземпляров считываются из текстового документа, содержащем евклидовы координаты вершин на плоскости, ограничение вместимости, количество доступных транспортных средств и величину спроса для каждой вершины, для экспериментальных вычислений используются общедоступные экземпляры из CVRPLIB. Алгоритм инициализируется со следующими параметрами (Таблица 2).

Таблица 2 – Начальные параметры алгоритма

Параметр	Значение
α	2.4
β	2.4
ρ	0.1
Q	5
Количество итераций	1000

Для проведения вычислительных экспериментов используется группа экземпляров Set E (Christofides and Eilon, 1969) (Рисунок 1), выбор обоснован широкой вариативностью размерности задач, количества используемых транспортных средств и грузоподъемности, что позволит сделать более комплексные выводы о производительности алгоритма.

Instance	n	K	Q	UB	Opt
E-n13-k4	12	4	6000	247	yes
E-n22-k4	21	4	6000	375	yes
E-n23-k3	22	3	4500	569	yes
E-n30-k3	29	3	4500	534	yes
E-n31-k7	30	7	140	379	yes
E-n33-k4	32	4	8000	835	yes
E-n51-k5	50	5	160	521	yes
E-n76-k7	75	7	220	682	yes
E-n76-k8	75	8	180	735	yes
E-n76-k10	75	10	140	830	yes
E-n76-k14	75	14	100	1021	yes
E-n101-k8	100	8	200	815	yes
E-n101-k14	100	14	112	1067	yes

Рисунок 1 – Экземпляры набора Set E

Далее приводятся результаты вычислительных экспериментов в двух разных сценариях, в первом из них количество особей муравьев в популяции полагается равным количеству вершин в графе, во втором фиксируется значение 100 особей для всех экземпляров, что значительно больше количества вершин большей части из них и совпадает с ним для E-n101-k8 и E-n101-k14, нотация X-nxx-kxx означает следующее: X-буквенное наименование набора

данных из CVRPLIB, n – количество вершин, k – количество транспортных средств, обслуживающих клиентов.

Таблица 3 – Количество особей совпадает с количеством муравьев

Экземпляр	Муравьиный алгоритм	Верхняя граница	Погрешность %
E-n22-k4	383	375	2.14
E-n23-k3	579	569	2.03
E-n30-k3	522	534	-2.17
E-n33-k4	882	835	5.70
E-n51-k5	635	521	21.90
E-n76-k7	836	682	20.42
E-n76-k14	1174	1021	14.98
E-n101-k8	964	815	18.28
E-n101-k14	1272	1067	19.21

Таблица 4 – Количество особей равно 100

Экземпляр	Муравьиный алгоритм	Верхняя граница	Погрешность %
E-n22-k4	378	375	0.80
E-n23-k3	574	569	0.87
E-n30-k3	519	534	-2.89
E-n33-k4	862	835	3.23
E-n51-k5	619	521	18.80
E-n76-k7	824	682	20.82
E-n76-k14	1158	1021	13.41
E-n101-k8	958	815	17.54
E-n101-k14	1244	1067	16.58

Итоговое решение гораздо в меньшей степени выглядит как формализация естественной логики, маршруты, построенные АСО, в целом кажутся более беспорядочными, хотя разрыв остается удовлетворительным, на Рисунке 2. приведено сравнение решения полученного муравьиным алгоритмом с оптимальным решением.

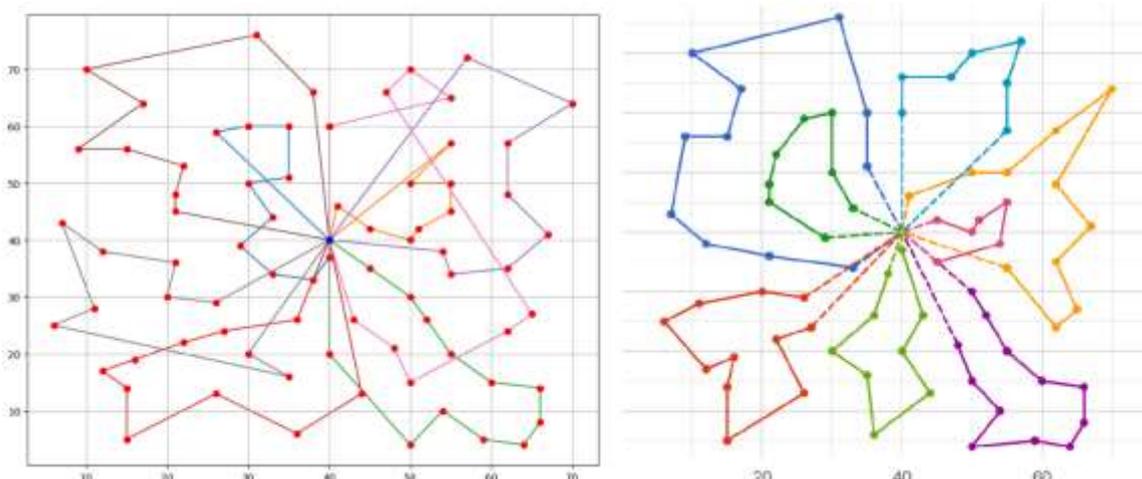


Рисунок 2 – Решения АСО и оптимальное решение для экземпляра E-n76-k10

Можно также заметить, что для экземпляра E-n30-k3 АСО достигает значительного улучшения, однако это объясняется увеличением количества используемых транспортных средств на одно, в связи с чем мы видим отличающиеся по структуре решения на Рисунке 3.

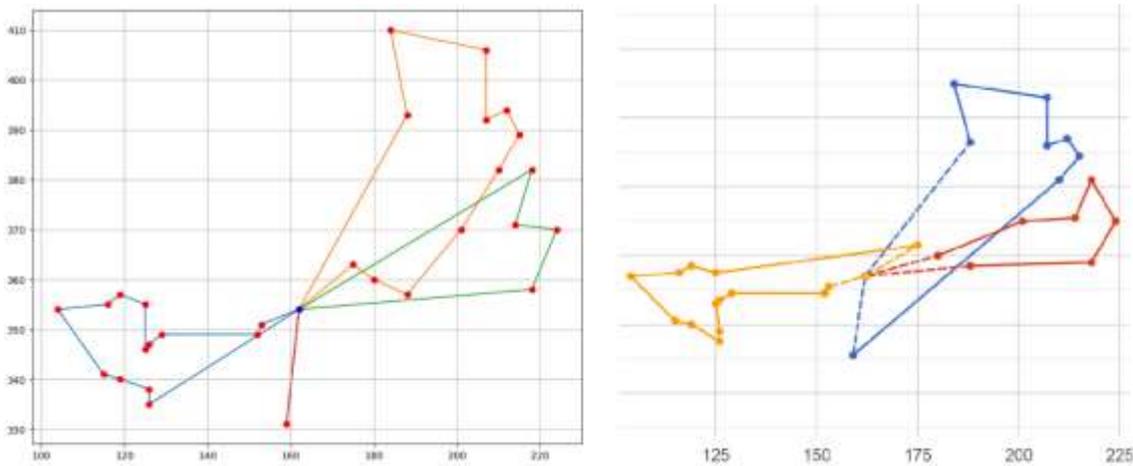


Рисунок 3 – Решения АСО и оптимальное решение для экземпляра E-n30-k3

При большем количестве муравьев алгоритм демонстрирует гораздо лучшие показатели сходимости, что можно наблюдать на графиках сходимости от числа итераций для некоторых экземпляров (Рисунок 4.)

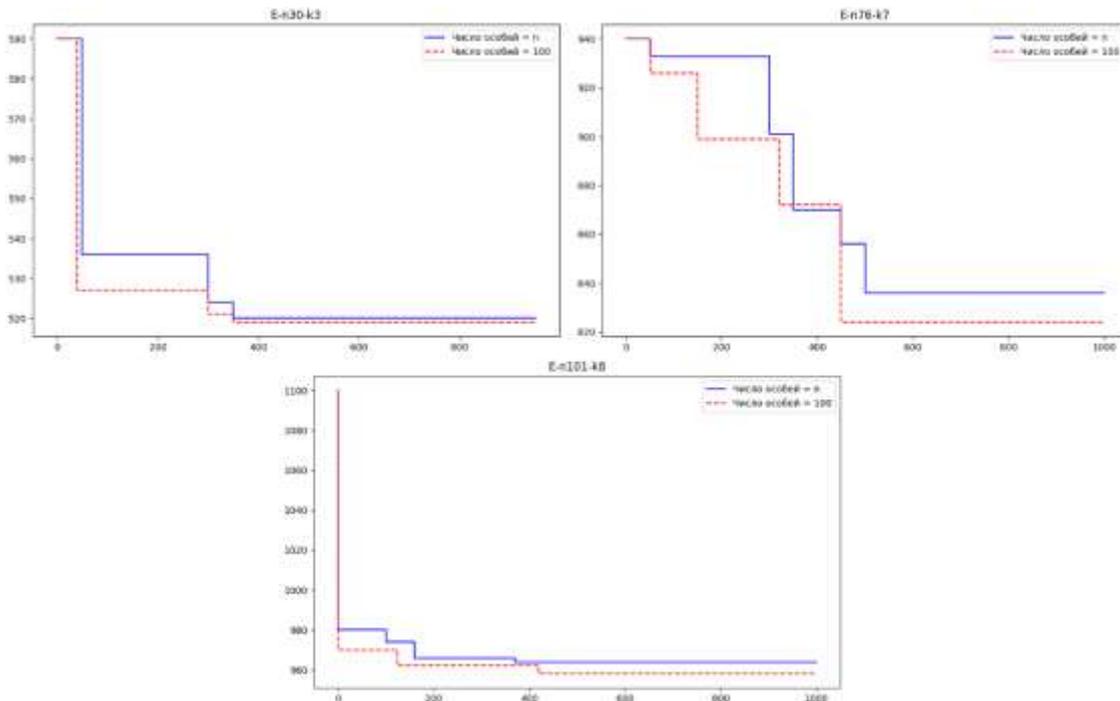


Рисунок 4 – Сходимость от числа итераций

Параметр количества муравьев сильно влияет на уровень сходимости и результирующее решение. Однако следует отметить, что увеличение количества муравьев влияет на время поиска решения (Рисунок 5.)

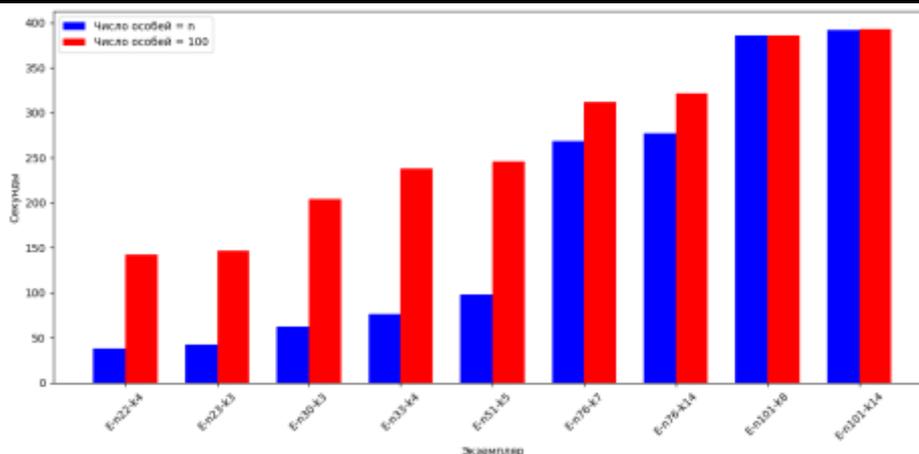


Рисунок 5 – Сравнение времени сходимости

Незначительное влияние значение параметра числа особей оказывает также на использование памяти, расход которой увеличивается примерно экспоненциально с увеличением размерности задачи (Рисунок 6.)

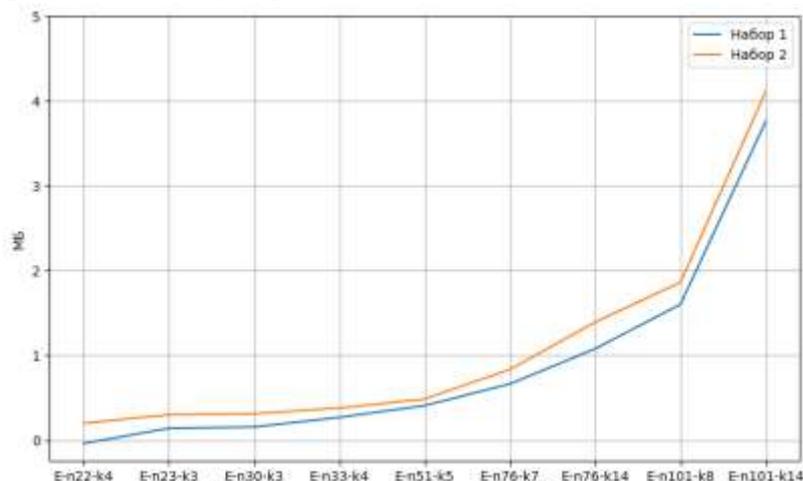


Рисунок 6 – Расход памяти при разном количестве особей

Далее анализирует степень влияния различных настраиваемых параметров на сходимость алгоритма, в изначальной конфигурации попеременно изменяется значение каждого из параметров в большую и меньшую сторону (Таблицы 5, 6.).

Таблица 5 – Влияние значений параметров на точность решения

Экземпляр	Муравьиный алгоритм								Верхняя граница
	$\alpha = 2$	$\alpha = 5$	$\beta = 2$	$\beta = 5$	$Q = 3$	$Q = 9$	$\tau_0 = 0.1$	$\tau_0 = 1$	
E-n22-k4	383	378	411	378	378	380	378	383	375
E-n23-k3	580	578	659	578	578	580	578	576	569
E-n30-k3	522	519	572	519	519	520	519	518	534
E-n33-k4	882	879	956	879	879	880	879	872	835
E-n51-k5	635	620	841	620	620	622	620	616	521
E-n76-k7	821	811	1172	811	811	812	620	616	682

Таблица 6 – Влияние значений параметров на точность решения

Экземпляр	Потребление памяти (МБ)		Время выполнения (сек)		Потребление памяти (МБ)		Время выполнения (сек)		Верхняя граница
	$Q = 3$	$Q = 9$	$Q = 3$	$Q = 9$	$\tau_0 = 0.1$	$\tau_0 = 1$	$\tau_0 = 0.1$	$\tau_0 = 1$	
E-n22-k4	0.12	0.1	29.82	29.94	0.1	0.14	28.78	31.5	375
E-n23-k3	0.12	0.13	32.51	32.98	0.13	0.18	31.44	32.79	569
E-n30-k3	0.23	0.24	73.47	73.84	0.22	0.29	62.78	67.14	534
E-n33-k4	0.25	0.25	80.07	80.62	0.24	0.33	80.07	85.62	835
E-n51-k5	0.57	0.57	254.28	254.37	0.57	0.68	247.62	289.28	521
E-n76-k7	3.51	3.53	853.5	855.19	3.6	4.2	849.4	897.34	682

Заключение

Полученные результаты экспериментальных вычислений дают возможность сделать вывод, что муравьиный алгоритм (ACO) представляет собой мощный инструмент для решения задач комбинаторной оптимизации, в частности, задачи маршрутизации с ограниченной грузоподъемностью (CVRP). Параметры Q и ρ – степень испарения, не оказывают существенного влияния на потребление памяти или время работы алгоритма, однако влияют на сходимость алгоритма и точность полученного решения, разница по потребляемой памяти варьируется в пределах 0,01 – 0,02 Мб, значительное влияние на точность оказывают параметры α и β , как и число итераций и число муравьев, однако системности не наблюдается, алгоритм требует точной настройки под конкретную задачу с учетом структуры имеющихся данных.

Список литературы

1. Мартин Кристофер. Логистика и управление цепочками поставок: создание сетей, создающих добавленную стоимость. Пирсон, 2016.

2. Саид Латераль, Карим Абу эль Мехди б, Мохаммед Саид Риффи. Проблема маршрутизации транспортных средств за последнее десятилетие: варианты, таксономия и метаэвристика, 2023.
3. Дахия С. & Сангван С. (2018). Обзор литературы по проблеме коммивояжера. Международный исследовательский журнал 5(16), С.1152-1155. Проверено 18 марта 2022 г.
4. Као Ю., Чен М. Х. и Хуан Ю. Т. (2012). Гибридный алгоритм, основанный на АСО и PSO для задач маршрутизации транспортных средств с емкостью. Математические проблемы в инженерии, 2012.
5. Нин Дж., Чжан К., Чжан С. & Чжан Б. (2018). Алгоритм оптимизации колонии муравьев, основанный на обновлении информации по наилучшему пути. Информационные науки, С.433-434.

References

1. Martin Christopher. Logistics and Supply Chain Management: Creating Value-Adding Networks. Pearson, 2016.
 2. Said Elatara, Karim Abouelmehdib, Mohammed Essaid Riffi. The vehicle routing problem in the last decade: variants, taxonomy and metaheuristics, 2023.
 3. Dahiya C. & Sangwan S. (2018). Literature Review on Travelling Salesman Problem. International Journal of Research 5(16), pp.1152-1155. Retrieved March 18, 2022
 4. Kao, Y., Chen, M. H., & Huang, Y. T. (2012). A Hybrid Algorithm Based on ACO and PSO for Capacitated Vehicle Routing Problems. Mathematical Problems in Engineering, 2012.
 5. Ning, J., Zhang, Q., Zhang, C., & Zhang, B. (2018). A Best-Path-Updating Information-Guided Ant Colony Optimization Algorithm. Information Sciences, pp.433–434.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

ЦИФРОВЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ЖИЛИЩНО-КОММУНАЛЬНЫМ ХОЗЯЙСТВОМ

Друзьяка Д.В.

ФГБОУ ВО «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ МОСКОВСКИЙ
ГОСУДАРСТВЕННЫЙ СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ», Москва, Россия, (129337, город
Москва, Ярославское ш., д. 26), e-mail: d.v.druziaka@gmail.com

В статье проводится обзор и анализ цифровых технологий, которые применяются в управлении жилищно-коммунальным хозяйством. Также рассматриваются цифровые инструменты и решения в жилищно-коммунальном секторе: автоматизация процессов учета и платежей, мониторинг состояния инженерных систем, повышение оперативности и качества обслуживания жильцов, улучшение управления энергопотреблением и экологический аспект. Кроме того, в статье обсуждаются наиболее перспективные инновационные решения в данной области.

Ключевые слова: Цифровые технологии, управление, жилищно-коммунальное хозяйство, автоматизация, учет, платежи, мониторинг, обслуживание, энергопотребление, инновации.

DIGITAL TECHNOLOGIES IN HOUSING AND COMMUNAL SERVICES MANAGEMENT

Druzyaka D.V.

NATIONAL RESEARCH MOSCOW STATE UNIVERSITY OF CIVIL ENGINEERING, Moscow,
Russia, (129337, Moscow, Yaroslavskoye shosse, 26), e-mail: d.v.druziaka@gmail.com

The article provides an overview and analysis of digital technologies that are used in housing and communal services management. Digital tools and solutions in the housing and communal sector are also considered: automation of accounting and payment processes, monitoring of the state of engineering systems, improving the efficiency and quality of service to residents, improving energy consumption management and the environmental aspect. In addition, the article discusses the most promising innovative solutions in this area.

Keywords: Digital technologies, management, housing and communal services, automation, accounting, payments, monitoring, maintenance, energy consumption, innovations.

Для начала необходимо рассмотреть преимущества автоматизации процессов учета. Она позволяет устранить возможные ошибки, связанные с ручным вводом данных. Ручной учет требует значительных временных и ресурсных затрат. Автоматизация сокращает время и усилия, затрачиваемые на сбор и обработку информации. Цифровые системы учета позволяют проводить быстрый анализ данных и генерировать детализированные отчеты. Это помогает улучшить понимание текущего состояния и эффективности управления жилищно-коммунальным хозяйством. Также автоматизация позволяет жильцам упростить процесс оплаты коммунальных услуг. Цифровые решения предлагают удобные онлайн-платформы,

где жильцы могут легко управлять своими платежами, просматривать и проверять свои счета, а также получать уведомления об изменениях в тарифах и услугах.

Применение цифровых решений для упрощения платежей и взаимодействия с жильцами:

1. Онлайн-платежи: Цифровые технологии позволяют жильцам оплачивать коммунальные услуги онлайн с помощью банковских карт, мобильных платежных приложений или электронных кошельков.

2. Автоматическое уведомление о задолженностях.

3. Интерактивные платформы для взаимодействия.

4. Учет индивидуальных предпочтений: Цифровые системы могут хранить информацию о предпочтениях жильцов, например, о выбранных способах оплаты или предпочтительном способе связи [1].

Необходимо упомянуть мониторинг состояния инженерных систем. Это совокупность технических и программных средств, позволяющая осуществлять сбор и обработку информации о различных параметрах работы системы инженерно-технического обеспечения здания (сооружения) с целью контроля возникновения в ней дестабилизирующих факторов и передачи.

Применение датчиков и систем удаленного мониторинга является одной из ключевых составляющих эффективного мониторинга. Датчики установлены на различных системах и оборудовании, чтобы контролировать и регистрировать температуру, влажность, давление, энергопотребление и другие. Системы удаленного мониторинга позволяют получать информацию с этих датчиков удаленно и в реальном времени. Это позволяет оперативно реагировать на любые отклонения и принимать меры по предотвращению поломок или проблем.

Анализ данных и прогнозирование возможных проблем - это важная задача, которую выполняет мониторинг. Путем сбора и анализа данных, полученных из датчиков и систем удаленного мониторинга, можно выявить тренды, паттерны и аномалии, которые могут указывать на возможные проблемы или отклонения от нормальной работы. На основе этих данных можно проводить прогнозирование возможных поломок или проблем и принимать соответствующие меры заранее. Это позволяет избежать неожиданных сбоев и значительно снизить риски операционных проблем.

На сегодняшний день страны-лидеры мира активно внедряют цифровые технологии в сфере жилищно-коммунального хозяйства. Это происходит путем сбора метаданных и создания цифровых платформ, сервисов и приложений в разных сегментах и отраслях ЖКХ. В основе этих ИТ-решений лежат разработки и технологии искусственного интеллекта [2].

По прогнозам экспертов, в текущем году затраты передовых стран на цифровизацию городской инфраструктуры превысят 185 миллиардов долларов. Среди самых востребованных цифровых технологий, направленных на повышение эффективности городской инфраструктуры, можно выделить мониторинг коммунальных сетей и инженерной инфраструктуры, систему контроля и движения транспортных мусоровозов, а также управление аварийно-диспетчерской службой жилищно-коммунальных организаций.

Растущая потребность в цифровых ИТ-решениях для жилищно-коммунальной сферы способствовала увеличению числа мировых стартапов, разрабатывающих решения для ЖКХ,

до 146 за период с 2010 по 2021 год. Особенно динамичный рост компаний, занимающихся цифровыми решениями для ЖКХ, начался с 2015 года.

Ведущие страны являются мировыми лидерами в развитии современных информационных технологий и количестве стартапов, использующих компоненты искусственного интеллекта в сфере ЖКХ. На рынке цифровых технологий преобладают ИТ-решения для ресурсоснабжающих компаний, предоставляющих коммунальные услуги по тепло-, водо-, газо- и электроснабжению, водоотведению и обращению с бытовыми отходами (55%), в то время как доля цифровых стартапов для управляющих компаний по жилищным услугам составляет 45% [3].

Управляющие компании активно внедряют различные цифровые платформы и приложения, которые облегчают коммуникацию между жильцами и управляющей компанией. Жильцы могут напрямую обращаться в службу поддержки через мобильные приложения, электронную почту или онлайн-чаты. Это упрощает процесс передачи информации и позволяет быстро получать обратную связь от жильцов.

С использованием цифровых технологий они также могут эффективно отслеживать и обрабатывать заявки жильцов. Жильцы отправляют свои заявки через онлайн-формы или мобильные приложения, что позволяет им сохранять время и избегать очередей в офисах управляющей компании. Благодаря цифровым инструментам также обеспечивается быстрое назначение исполнителей работ, мониторинг их выполнения и своевременное информирование жильцов об этапах решения их проблем.

Компания "LawnTap Technologies" разработала цифровое решение для ухода за придомовой территорией. Система отслеживает высоту травы на газонах и автоматически отправляет запросы компаниям, предлагающим услуги по уходу за газоном. Цифровое решение использует виртуального помощника "AI-бот", который анализирует предложения и находит оптимального исполнителя для выполнения работ. После завершения работ система самостоятельно оценивает их качество и проводит оплату с банковского счета управляющей компании, предоставляя полный комплекс первичных документов. В настоящее время разрабатывается адаптированная цифровая платформа для работы с управляющими компаниями, запуск которой запланирован на 2024-2025 годы [4].

В российской отрасли ЖКХ уже начинают проявляться первоначальные шаги в информатизации и цифровизации. Однако эти процессы идут медленно и с трудностями. Доля предприятий ЖКХ, которые внедряют цифровые технологии в свои бизнес-процессы, составляет крайне незначительное число в общей отрасли. Даже в подотрасли электроснабжения, которая считается наиболее успешной в сравнении с другими подотраслями ЖКХ, процент автоматизированного учета не превышает 9%.

С трудностями внедрения новых технологий в сферу жилищно-коммунального хозяйства связано несколько причин. Одна из них заключается в том, что сама система тарифообразования не стимулирует организации к внедрению новых технологий и обновлению оборудования. Тарифы ограничивают возможность увеличения затрат на капитальную модернизацию и замену оборудования на более современное и эффективное. Еще одной причиной является устаревание технических стандартов, которые до сих пор используются совместно с наследием СССР. По данным Росстата, в 2022 году лишь 65% ресурсоснабжающих организаций применяли базовые информационные технологии, такие как локальные сети, системы электронного документооборота и другие решения - не более 5%.

Отсутствие бюджетных средств и стремление получить более выгодную оплату по нормативам также являются факторами, затрудняющими цифровизацию ресурсоснабжающих организаций.

Внедрение комплексных цифровых технологий и ИТ-решений в сфере жилищнокоммунального хозяйства оказывается сложным из-за недостатка легкомасштабируемых альтернатив. Также ключевым фактором является отсутствие инициатив и заинтересованности со стороны национальных государств. Важно отметить, что на данный момент лишь 14% цифровых ИТ-решений, разработанных мировыми компаниями, успешно применяются в отрасли ЖКХ в некоторых странах, в то время как 44% стартапов в области цифровизации ЖКХ находятся на стадии пилотирования.

Современное использование цифровых технологий в управлении жилищно-коммунальным хозяйством имеет огромный потенциал для повышения оперативности и качества обслуживания жильцов. Внедрение цифровых платформ и приложений позволяет упростить коммуникацию с жильцами и оперативно реагировать на их заявки и проблемы. Персонализированное обслуживание и учет индивидуальных потребностей каждого жильца также становятся возможными благодаря цифровым инструментам.

Перспективы дальнейшего развития цифровых технологий в управлении жилищно-коммунальным хозяйством огромны. Постоянное совершенствование цифровых платформ и приложений, а также внедрение новых технологий, таких как интернет вещей (IoT) и искусственный интеллект (ИИ), позволят автоматизировать процессы, улучшить аналитику и прогнозирование, а также повысить эффективность управления ресурсами.

Список литературы

1. Кириллова А.Н. Стратегический потенциал и ключевые факторы развития жилищно-коммунального развития жилищнокоммунального хозяйства // Недвижимость: экономика, управления. 2018. №3. С.12-16.
2. Кислякова Ю.Г., Казакова О.Ю. Инновационные технологии «Умного города» в сфере жилищно-коммунального хозяйства // Социально-экономическое управление: теория и практика. №3 (38). 2019. С.57-58.
3. Лычагина А.А., Деменев А.В. Оптимизация сферы ЖКХ посредством технологических инноваций // Сервис в России и за рубежом. 2020. Т14. №5. С.164-174.
4. Открытые данные электронного портала «Мировые инновационные проекты и стартапы» – <https://www.Crunchbase.com>

References

1. Kirillova A.N. Strategic potential and key factors in the development of housing and communal development of housing and communal services // Real estate: economics, management. 2018. No.3. pp.12-16.
2. Kislyakova Yu.G., Kazakova O.Yu. Innovative technologies of the "Smart city" in the field of housing and communal services // Socio-economic management: theory and practice. No.3 (38). 2019. pp.57-58.
3. Lychagina A.A., Demenev A.V. Optimization of the housing and communal services sector through technological innovations // Service in Russia and abroad. 2020. T14. No.5. pp.164-174.

4. Open data of the electronic portal "Global innovative projects and startups" –
<https://www.Crunchbase.com>
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.08

СПОСОБ ФОРМАЛИЗАЦИИ ЦЕЛЕЙ И ЗАДАЧ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ

¹Балашов О.В., ²Букачев Д.С.

¹СМОЛЕНСКИЙ ФИЛИАЛ АО «РАДИОЗАВОД», Смоленск, Россия, (214027, г. Смоленск, улица Котовского, 2), e-mail: smradio@mail.ru

²ФГБОУ ВО «СМОЛЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Смоленск, Россия (214000, г. Смоленск, ул. Пржевальского, 4), e-mail: dsbuka@yandex.ru

При разработке средств автоматизации управления организационно-техническими системами возникает необходимость формализованного представления их целей и задач. Рассматривается подход, позволяющий формализовать цели и задачи сложных многоуровневых систем в виде взаимосвязанных графов целей, задач и результатов их выполнения. Это позволяет автоматизированно сгенерировать план предстоящих действий сложных иерархических систем, который представляет собой совокупность развернутых во времени, взаимоувязанных по отношению к общей цели и сбалансированных по ресурсам и логике применения перечней задач для каждого объекта, синхронизированных горизонтально и вертикально в соответствии со структурой системы.

Ключевые слова: Средства автоматизации управления, организационно-техническая система, цель, задача, формализация, план предстоящих действий.

A WAY TO FORMALIZE THE GOALS AND OBJECTIVES OF ORGANIZATIONAL AND TECHNICAL SYSTEMS

¹Balashov O.V., ²Bukachev D.S.

¹SMOLENSK BRANCH OF JOINT-STOCK COMPANY "RADIO FACTORY", Smolensk, Russia, (214027, Smolensk, street Kotovskogo, 2), e-mail: smradio@mail.ru

²SMOLENSK STATE UNIVERSITY, Smolensk, Russia (214000, Smolensk, street Przewalski, 4), e-mail: dsbuka@yandex.ru

When developing means of automation of management of organisational and technical systems, there is a need for formalised representation of their goals and tasks. We consider an approach that allows formalising the goals and tasks of complex multilevel systems in the form of interconnected graphs of goals, tasks and results of their implementation. This allows to automatically generate a plan of the future actions of complex hierarchical systems, which is a set of task lists for each object, synchronised horizontally and vertically in accordance with the system structure, deployed in time, interconnected in relation to the common goal and balanced in terms of resources and logic of application.

Keywords: Control automation tools, organisational and technical system, goal, task, formalisation, plan of forthcoming actions.

подавляющее большинство организационно-технических систем (ОТС) состоит из типовых объектов, имеющих множество реализаций и обладающих общими свойствами для

всех своих возможных реализаций [2, 5]. Под объектом понимается элемент ОТС, предназначенный для выполнения определенного перечня работ (имеющий конкретное функциональное предназначение), имеющий собственную структуру и ресурсы, и находящийся в определенных отношениях с другими объектами ОТС (прежде всего – подчинительных, часть-целое).

В качестве реализаций типового объекта рассматриваются реальные или виртуальные объекты, соответствующие рассматриваемому типовому объекту. Например, типовому объекту «экскаватор» может соответствовать 2-3 реальных экскаватора на строительной площадке. Множество объектов ОТС, находящихся в определенных подчинительных отношениях, образуют иерархическую структуру ОТС.

Формализация целей ОТС

В качестве цели функционирования объекта рассматривается требуемый результат, которого объект должен достичь, выполнив какую-либо задачу [1]. Каждому объекту ОТС (и ОТС в целом) соответствует два класса целей. К первому классу относятся цели, определяющие функциональное предназначение объекта и формируемые на этапе проектирования, реорганизации/модификации и непосредственно в процессе функционирования объекта (стратегические цели). Ко второму классу относятся цели, формируемые при планировании предстоящих действий ОТС на этапе ее функционирования (тактические и текущие цели).

Стратегические цели имеют иерархическую структуру [1, 7], вершиной которой является глобальная цель функционирования ОТС, отражающая её функциональное предназначение. На Рисунке 1 рассмотрен пример дерева целей системы.

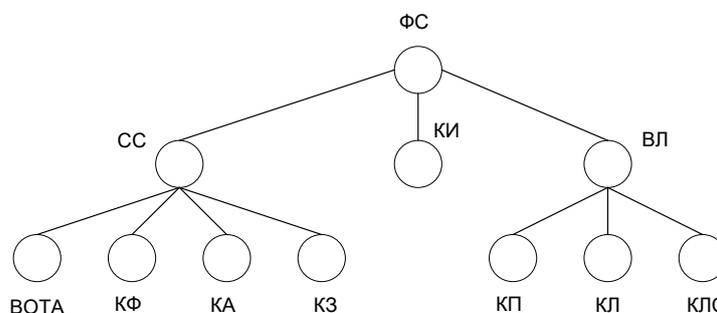


Рисунок 1 – Пример дерева целей системы (фрагмент)

Содержательная формулировка наименований вершин дерева целей приведена в Таблице 1.

Таблица 1 - Расшифровка наименований вершин дерева целей

№ уровня	Код цели	Цель	№ уровня	Код цели	Цель
1	ФС	Обеспечить высокий уровень финансовой стабильности предприятия	2	СС	Обеспечить эффективное использование собственных средств
			2	КИ	Создать благоприятный инвестиционный климат
			2	ВЛ	Обеспечить высокую ликвидность
2	СС	Обеспечить эффективное использование собственных средств	3	ВОГА	Снизить волатильность текущих активов
			3	КФ	Стабилизировать коэффициент финансирования
			3	КА	Увеличить коэффициент автономии
			3	КЗ	Уменьшить коэффициент задолженности
	ВЛ	Обеспечить высокую ликвидность	3	КП	Повысить коэффициент покрытия
			3	КЛ	Повысить коэффициент ликвидности
			3	КЛС	Повысить коэффициент средней ликвидности

В качестве локальных целей рассматриваются требуемые свойства и характеристики ОТС, обеспечивающие достижение глобальной цели. Как правило, свойства и характеристики ОТС, рассматриваются относительно предназначения функциональных подсистем и объектов ОТС.

Тактические (текущие) цели также имеют иерархическую структуру и представляют собой требуемые результаты выполнения задач объектов ОТС, образующих содержание планов предстоящих действий [1, 2]. Глобальная цель ОТС в предстоящих действиях представляет собой совокупность требуемых результатов выполнения задач объектами ОТС на момент окончания этих действий (рисунок 2). Локальные цели ОТС представляют собой требуемые результаты выполнения задач объектов ОТС в предстоящих действиях.

Формализованное представление стратегических целей может иметь следующий вид:

$$\Gamma_{GQ^I} = (Q_i, G_{Q^I}, b), \quad (1)$$

где Γ_{GQ} – соответствие между объектом Q_i и структурой G_{Q^I} цели этого объекта;
 b – правила установления соответствия между Q_i и G_{Q^I} .

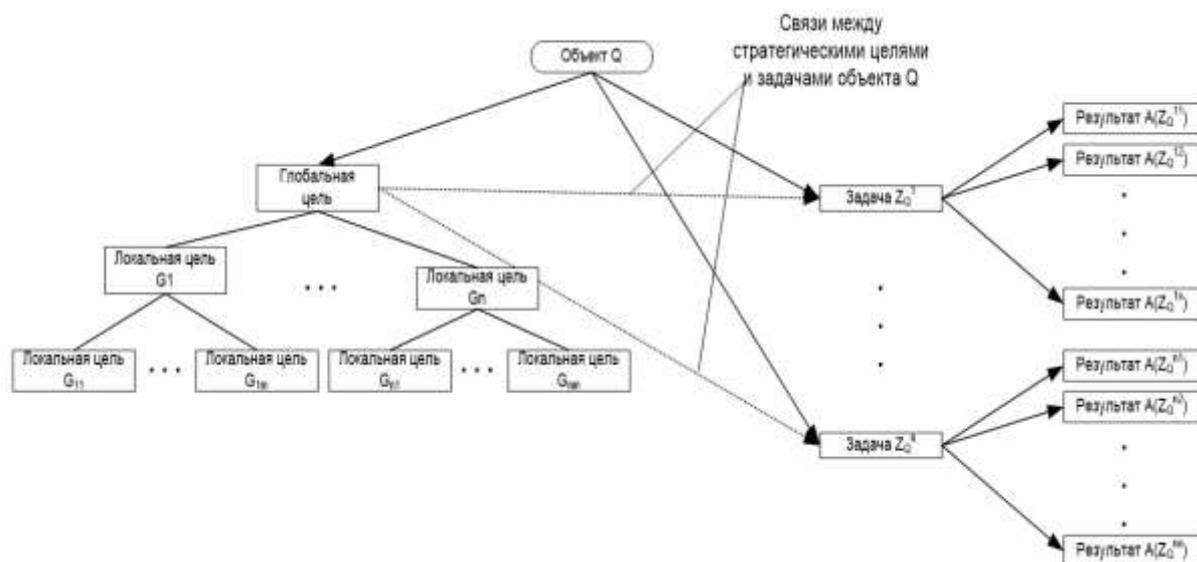


Рисунок 2 – Графическое представление соответствия целей и соответствующих им задач

Цель объекта G^I может иметь иерархическую структуру G_{Q^I} и быть представлена в виде

$$G_{Q^I} = G_{Q_i} r^x \{G_{Q(i-1)^1}, G_{Q(i-1)^2}, \dots, G_{Q(i-1)^m}\}, \quad (2)$$

где G_{Q_i} – глобальная цель объекта Q_i ;

r^x – отношение между глобальной целью и множеством локальных целей первого уровня $\{G_{Q(i-1)^1}, G_{Q(i-1)^2}, \dots, G_{Q(i-1)^m}\}$;

x – тип отношения между целями.

В структуре цели могут быть выделены различные классы целей (приоритетные, доминирующие и ряд других). Выделение подобных целей в структуре глобальной цели объекта производится посредством соответствующих типов отношений.

Стратегической цели каждого объекта соответствует некоторое множество характеристик. К рассматриваемым характеристикам относятся: лингвистическая формулировка цели, оценочные характеристики (вероятность достижения цели объектом, возможности объекта по достижению цели), вспомогательные характеристики (вариант цели, класс цели – глобальная, локальная, текущая, плановая).

Формализованное представление соответствия Γ_{GH} цели первого класса G_i^I множеству характеристик H_{G_i} представляется в виде

$$\Gamma_{GH} = (G_i^I, H_{G_i}, b), \quad (3)$$

где $H_{G_i} = \{(H_{G(i-1)1}, H_{G(i-1)2}, \dots, H_{G(i-1)v})\}$ – множество характеристик цели;

b – правила установления соответствия между G_i^I и H_{G_i} .

Формализованное представление текущих целей основано на формализованном представлении планов, задач и результатов их выполнения [2, 3].

Каждой глобальной и локальной цели объекта Q может быть поставлено в соответствие определенное множество задач этого объекта

$$\Gamma_{GZ} = (G_i^I, Z_{Q_i}, b). \quad (4)$$

Через соответствие (4) может быть установлена связь между стратегическими целями объекта Q и множеством возможных результатов выполнения задач, которые этот объект может выполнять, исходя из своего функционального предназначения.

Каждой цели первого класса ставится в соответствие множество ее параметров, в качестве которых могут рассматриваться:

- множество объектов Q^B , на которые оказывается то или иное воздействие со стороны объекта Q_i в процессе достижения цели;
- множество продукции V^B , которая производится объектом Q_i в процессе достижения цели;
- множество документов D , разрабатываемых объектом в процессе достижения цели (характерно для целей органов управления);
- множество задач, выполнение которых необходимо для достижения цели Z^G ;
- множество параметров отображения S , обеспечивающих «привязку» объекта в процессе достижения цели к участку пространства;
- множество ресурсов P , которые выделяются или необходимы для достижения цели.

Соответствие между целью G_i^I и множеством ее параметров может быть представлено в виде

$$\Gamma_G = (G_i^I, (Q^B, V^B, D, Z^G, S, P), b). \quad (5)$$

Формализация задач ОТС

Каждый объект ОТС, исходя из своего функционального предназначения, способен выполнить конечное множество задач [2, 4]. Под *задачей* понимается основная единица деятельности ОТС, направленная на получение заданного результата и требующая выделения определенных объемов ресурсов (людских, энергетических, финансовых, материальных и др.). В результате выполнения объектом задачи может иметь место преобразование информации или материальных ресурсов, а также изменение состояния рассматриваемого объекта и/или других объектов. Примерами задач объектов являются: освоение новой технологии, изготовление продукции, оказание услуги, оценка рынка, разработка плана и др.

Графическое представление соответствия задач объектов (Q_i) и результатов показано на Рисунке 3.

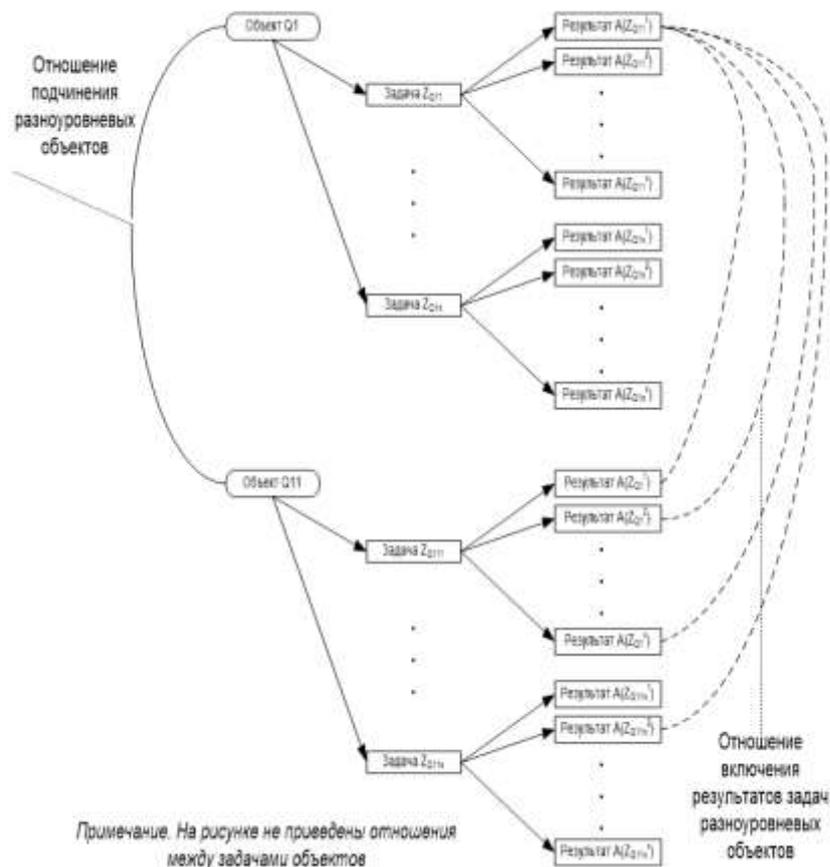


Рисунок 3 – Графическое представление соответствия задач и их результатов

Рассматриваемое соответствие может быть представлено в виде

$$\Gamma_{QZ} = (Q_i, Z_Q, b), \quad (6)$$

где b – правила установления соответствия между Q_i и Z_Q .

Каждой задаче Z_{Q_i} соответствует множество ее параметров. В качестве параметров задачи рассматриваются:

- множество объектов Q^B , на которые оказывается то или иное воздействие со стороны объекта Q_i в процессе выполнения задачи;
- множество продукции V^B , которая производится объектом Q_i в процессе выполнения рассматриваемой задачи, под продукцией также понимается какая-либо услуга или работа;
- множество документов D , разрабатываемых объектом в процессе выполнения задачи (характерно для управленческих задач должностных лиц и органов управления);
- множество результатов A , являющихся множеством возможных фактов (событий) выполнения (невыполнения) рассматриваемой задачи;
- множество параметров отображения S , обеспечивающих «привязку» объекта, выполняющего задачу к участку пространства, на котором проводится выполнение этой задачи ($S = \{S_1, \dots, S_n\}$);

- множество ресурсов P , которые выделяются/необходимы для выполнения задачи ($P = \{P_1, \dots, P_n\}$).

Соответствие между Z_Q и множеством параметров (Q^B, V, D, A, S, P) может быть представлено в виде

$$\Gamma_{QZ} = (Z_Q, (Q^B, V^B, D, A, S, P), b). \quad (7)$$

Среди множества задач Z , соответствующих объекту Q_i , для каждой задачи Z_{Q_i} может быть выделено множество $Z_{Q_i}^{\text{посл}}$ «последующих» задач, то есть задач, выполнение которых возможно объектом Q_i только после выполнения задачи Z_{Q_i} . Выделение рассматриваемого множества для каждой задачи Z_{Q_i} проводится посредством отношения $r^{\text{посл}}$ на множестве задач Z_Q объекта Q_i . Множество последующих задач для задачи Z_{Q_i} объекта Q_i может быть представлено в виде

$$Z_{Q_i}^{\text{посл}} = Z_{Q_i} r^{\text{посл}} \{Z_{Q_i}^n\}, Z_{Q_i} \in Z_Q, \{Z_{Q_i}^n\} \in Z_Q, \quad (8)$$

где n – идентификатор последующих задач.

Каждой задаче Z_{Q_j} объекта Q_j соответствует множество задач $\{Z_{Q_i}\}$, выполняемых множеством объектов $\{Q_i\}$, входящих в состав объекта Q_j . Множество задач $\{Z_{Q_i}\}$ может входить в технологию выполнения задачи Z_{Q_j} .

Для каждой задачи Z_{Q_i} объекта Q_i может существовать множество $Z_{Q_i}^{\text{несовм}}$ несовместных задач других объектов, одновременное выполнение которых невозможно (нежелательно) с выполнением задачи Z_{Q_i} .

Необходимо отметить, что множество несовместных задач определяется логикой выполнения этих задач (предопределенная несовместность). Вместе с тем, множество $Z_{Q_i}^{\text{несовм}}$ может быть расширено за счет задач, являющихся совместными по логике выполнения, но не являющимися таковыми по значениям своих параметров. Например, несовместными по логике выполнения для строительства являются такие задачи, как одновременное выполнение закладки фундамента и возведение стен.

Каждой задаче объекта ОТС соответствует некоторое множество характеристик этой задачи. К рассматриваемым характеристикам относятся: лингвистическая формулировка задачи, временные характеристики (время начала и конца выполнения, время фиксации обстановки и т.д.); оценочные характеристики (возможности объекта по выполнению задачи, оценка степени выполнения задачи и т.д.).

Формализованное представление соответствия Γ_{ZH} задаче Z_j множества характеристик H_{Z_i} представляется в виде

$$\Gamma_{ZH} = (Z_j, H_{Z_j}, b), \quad (9)$$

где $H_{Z_i} = \{(H_{Z(i-1)1}, H_{Z(i-1)2}, \dots, H_{Z(i-1)v})\}$ – множество характеристик задачи;

b – правила установления соответствия между Z_j и H_{Z_j} .

Процесс реализации задач, выполняемых объектами ОТС, особенно транспортной отрасли, «привязывается» к пространству. Процесс привязки производится посредством

определения значений пространственных параметров. Под *пространственным параметром* понимается совокупность формализованных координат и элементов действительности, относительно которых осуществляется ориентация объекта в пространстве. В качестве элементов действительности могут рассматриваться топогеодезические и гидрографические объекты.

С целью формализации связей между задачами объектов, располагающихся на разных иерархических уровнях ОТС, введены понятия общих и частных задач объектов ОТС (рисунок 4).

Под *общей задачей* объекта ОТС, состоящего из подобъектов, понимается задача, для выполнения которой должно быть выполнено множество задач подобъектов, исходя из своего функционального предназначения [2].

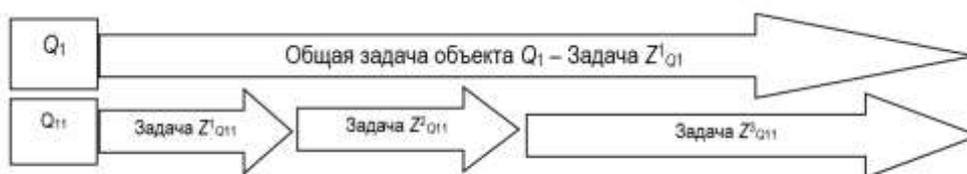


Рисунок 4 – Иллюстрация смысла общих и частных задач

Под *частной задачей* объекта ОТС понимается одна из задач, которые может выполнять один из его подобъектов. Каждой общей задаче объекта можно поставить в соответствие множество его частных задач, образующих технологию выполнения рассматриваемой общей задачи.

Рассмотренный подход к формализации целей и задач ОТС позволяет автоматизированно сгенерировать план предстоящих действий [2, 6] для сложных иерархических ОТС, который представляет собой совокупность развернутых во времени, взаимосвязанных по отношению к общей цели и сбалансированных по ресурсам и логике применения перечней задач для каждого объекта, синхронизированных горизонтально и вертикально в соответствии со структурой системы.

Список литературы

1. Балашов О.В., Букачев Д.С. Метод автоматизированного оперативного управления социально-экономическими системами//Международный журнал информационных технологий и энергоэффективности. – 2018. – Т.1, № 2(8). – С. 2-10.
2. Балашов О.В., Букачев Д.С. Подход к разработке технологии автоматизированного планирования и оперативного управления организационно-техническими системами//Международный журнал информационных технологий и энергоэффективности. – 2020. – Т. 5, № 4(18). – С. 21-32.
3. Балашов О.В., Букачев Д.С. Искусственный интеллект в автоматизации процессов планирования и оперативного управления//Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7, № 1(23). – С. 25–30.

4. Балашов О.В., Букачев Д.С. Об одном способе формализованного представления ситуаций и задач//Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8, № 9(35). – С. 30–36.
5. Булатов, М. А. Проблемы оптимизации и выбора вариантов создания и применения сложных организационно-технических комплексов / М.А.Булатов, Б.В.Соколов// Информатизация и связь. – 2023. – № 1. – С. 64-74. – DOI 10.34219/2078-8320-2023-14-1-64-74.
6. Мистров, Л. Е. Методологические основы формализации процесса разработки плана применения организационно-технических систем /Л.Е.Мистров//Информационные системы и технологии. – 2022. – № 5(133). – С. 73-82.
7. Попов, А. В. Реализация метода структурно-параметрической оптимизации графовых моделей организационно-технических систем /А.В.Попов//Вестник Югорского государственного университета. – 2023. – № 3. – С. 35-45. – DOI 10.18822/byusu20230335-45.

References

1. Balashov O.V., Bukachev D.S. Metod avtomatizirovannogo operativnogo upravleniya social'no-ekonomicheskimi sistemami // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2018. – Т.1, № 2(8). – pp. 2-10.
 2. Balashov O.V., Bukachev D.S. Podhod k razrabotke tekhnologii avtomatizirovannogo planirovaniya i operativnogo upravleniya organizacionno-tekhnicheskimi sistemami // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2020. – Т. 5, № 4(18). – pp. 21-32.
 3. Balashov O.V., Bukachev D.S. Iskusstvennyj intellekt v avtomatizacii processov planirovaniya i operativnogo upravleniya // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2022. – Т. 7, № 1(23). – pp. 25–30.
 4. Balashov O.V., Bukachev D.S. Ob odnom sposobe formalizovannogo predstavleniya situacij i zadach // Mezhdunarodnyj zhurnal informacionnyh tekhnologij i energoeffektivnosti. – 2023. – Т. 8, № 9(35). – pp. 30–36.
 5. Bulatov, M. A. Problemy optimizacii i vybora variantov sozdaniya i primeneniya slozhnyh organizacionno-tekhnicheskikh kompleksov / M. A. Bulatov, B. V. Sokolov // Informatizaciya i svyaz'. – 2023. – № 1. – S. 64-74. – DOI 10.34219/2078-8320-2023-14-1-64-74.
 6. Mistrov, L. E. Metodologicheskie osnovy formalizacii processa razrabotki plana primeneniya organizacionno-tekhnicheskikh sistem / L. E. Mistrov // Informacionnye sistemy i tekhnologii. – 2022. – № 5(133). – pp. 73-82.
 7. Popov, A. V. Realizaciya metoda strukturno-parametricheskoj optimizacii grafovyyh modelej organizacionno-tekhnicheskikh sistem / A. V. Popov // Vestnik YUgorskogo gosudarstvennogo universiteta. – 2023. – № 3. – pp. 35-45. – DOI 10.18822/byusu20230335-45.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.021

АЛГОРИТМЫ И СТРУКТУРЫ ДАННЫХ: ОСНОВЫ ДЛЯ НАЧИНАЮЩИХ ПРОГРАММИСТОВ

Удальцов К.Р.

ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург,
Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail:
2003.06.10kr@gmail.com

Статья представляет базовые понятия алгоритмов и структур данных, необходимые для понимания программирования начинающими разработчиками. В ней рассматриваются основы алгоритмов, структур данных и их применение в реальных проектах.

Ключевые слова: Алгоритмы и структуры данных.

ALGORITHMS AND DATA STRUCTURES: BASICS FOR BEGINNER PROGRAMMERS

Udaltsov K.R.

ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER
PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave.
Bolshevikov, 22, bldg. 1), e-mail: 2003.06.10kr@gmail.com

The article presents basic concepts of algorithms and data structures necessary for understanding programming by beginner developers. It covers fundamentals of algorithms, data structures and their application in real projects.

Keywords: Algorithms and data structures.

Введение:

Для начинающего программиста важно освоить основы алгоритмов и структур данных, так как они являются основой программирования. Понимание этих концепций позволит эффективно решать задачи, оптимизировать код и создавать более качественные программы.

Алгоритмы и структуры данных: Основы для начинающих программистов

В мире программирования алгоритмы и структуры данных играют ключевую роль в разработке эффективных и [1] оптимизированных программ. Понимание основных понятий и принципов работы алгоритмов и структур данных является фундаментом для любого начинающего программиста.

Алгоритмы представляют собой набор инструкций, которые выполняют определенную задачу. Эффективные алгоритмы помогают решать задачи быстро и оптимально, что особенно важно при работе с большими объемами данных. Структуры данных, в свою очередь, определяют способ организации и хранения данных в компьютере.

Одной из основных структур данных является массив. Массив представляет собой набор элементов, расположенных в памяти компьютера последовательно. Каждому элементу массива присваивается уникальный индекс, что позволяет быстро получать доступ к нужному элементу.

Кроме массивов, существует множество других структур данных, таких как списки, стеки, очереди, деревья и графы. Каждая из них имеет свои особенности и применения. Например, списки позволяют хранить элементы в произвольном порядке, стеки используются для реализации принципа Last In First Out (LIFO), а очереди - первый пришел, первый обслужен (FIFO).

Для работы с алгоритмами и структурами данных программистам необходимо знать основные операции, такие как вставка, удаление, поиск и сортировка данных. [2] Многие популярные алгоритмы, такие как сортировка пузырьком, сортировка выбором, сортировка вставками, быстрый поиск и др., основаны на этих операциях.

Понимание основных принципов работы алгоритмов и структур данных поможет начинающим программистам разрабатывать более эффективные и оптимизированные программы. Постоянное изучение и практика помогут улучшить навыки программирования и делать программы более производительными.

Итак, основы [3] алгоритмов и структур данных являются неотъемлемой частью обучения любого начинающего программиста и помогут создавать более качественное программное обеспечение.

Кроме основных алгоритмов и структур данных, существует множество продвинутых концепций, которые могут быть полезны для разработчика. Одним из таких концептов является рекурсия. Рекурсия - это процесс, при котором функция вызывает саму себя. Она может быть полезной для решения задач, которые могут быть разбиты на более простые подзадачи. Однако, при использовании [4] рекурсии необходимо быть внимательным, чтобы избежать бесконечной рекурсии и переполнения стека вызовов.

Еще одним важным аспектом, который стоит изучить, является анализ амортизированной сложности. Амортизированная сложность позволяет оценить среднюю производительность операций в структуре данных на протяжении длительного времени.

Помимо этого, разработчику стоит изучить алгоритмы поиска и обхода графов. Графы широко применяются в различных областях, таких как социальные сети, логистика, анализ данных и другие. Алгоритмы поиска в графе, такие как поиск в ширину и поиск в глубину, позволяют находить пути и связи между вершинами графа. Алгоритмы обхода графа, такие как обход в глубину и обход в ширину, позволяют перебирать все вершины графа.

Важно также упомянуть о различных структурах данных для работы с текстом, таких как строки, деревья суффиксов и хэш-таблицы. Эти структуры данных позволяют эффективно хранить и обрабатывать текстовую информацию, что является важным аспектом во многих приложениях.

Наконец, необходимо упомянуть о важности тестирования алгоритмов и структур данных. Тестирование помогает убедиться, что реализация работает корректно и соответствует ожидаемым результатам. [5] Существуют различные методы тестирования, такие как модульное тестирование, функциональное тестирование и тестирование производительности. Регулярное тестирование поможет выявить ошибки и улучшить качество программного обеспечения.

В заключение, разработчику важно не только понимать основы алгоритмов и структур данных, но и продолжать изучение и применение продвинутых концепций. Это поможет создавать более эффективные и масштабируемые программы. Регулярная практика, изучение новых алгоритмов и структур данных, а также тестирование помогут развивать навыки программирования и достигать успеха в области разработки программного обеспечения.

Список литературы

1. Котенко И. В. и др. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей //Региональная информатика" РИ-2018". – 2018. – С. 149-149.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Казанцев А. А. и др. Создание и управление Security Operations Center для эффективного применения в реальных условиях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 590-595.
4. Красов А. В. и др. Программная реализация средств предотвращения вторжений и аномалий сетевой инфраструктуры.
5. Сахаров Д. В. и др. Использование математических методов прогнозирования для оценки нагрузки на вычислительную мощность IOT-сети //Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2020. – №. 2. – С. 86-94.
6. Гельфанд А. М. Способы выбора стежоконтейнеров для передачи данных//Региональная информатика и информационная безопасность. – 2020. – С. 260-262.
7. Волкоготов В. Н. и др. Анализ безопасности wi-fi сетей //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 270-275.
8. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему//Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411.

References

1. Kotenko I. V. et al. A human-machine interaction model based on touchscreens for monitoring the security of computer networks //Regional Informatics"RI-2018". – 2018. – pp. 149-149.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Kazantsev A. A. et al. Creating and managing a Security Operations Center for effective use in real-world environments//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 590-595.
4. Krasov A.V. et al. Software implementation of intrusion prevention tools and network infrastructure anomalies.
5. Sakharov D. V. et al. Using mathematical forecasting methods to assess the load on the computing power of the IOT network //Scientific and analytical journal "Bulletin of the St.

- Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia". - 2020. – No. 2. – pp. 86-94.
6. Gelfand A.M. Methods of choosing stegocontainers for data transmission//Regional informatics and information security. – 2020. – pp. 260-262.
 7. Volkogonov V. N. et al. Wi-fi network Security Analysis//Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 270-275.
 8. Budarny G. S. and others. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала: <http://www.openaccessscience.ru/index.php/ijcse/>



УДК 629.783

РАЗРАБОТКА МОДЕЛИ ФУНКЦИИ ФАЗОМАНИПУЛИРОВАННОГО СИГНАЛА ДЛЯ УЛУЧШЕНИЯ РАЗРЕШАЮЩЕЙ СПОСОБНОСТИ БРЛС (БОРТОВАЯ РАДИОЛОКАЦИОННАЯ СТАНЦИЯ)

Урамбеков Э.Б.

*ФГАОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ", Санкт-Петербург, Россия (190121, город
Санкт-Петербург, Большая Морская ул., д.67 лит. а), e-mail: yra_517@mail.ru*

Проведенный анализ эффективности обнаружения позволяет сделать вывод о том, что повышение разрешающей способности и дальности до цели наиболее эффективным является использование внутриимпульсной модуляции. Причем из всех известных методов модуляции самыми эффективными являются фазоманипулированные сигналы (ФМнС).

Ключевые слова: Радиолокационный сигнал, ЭПР, числодискретов, ФМС, точность по дальности, генератор-кода, согласованный фильтр.

DEVELOPMENT OF A PHASE-MANIPULATED SIGNAL FUNCTION MODEL TO IMPROVE RADAR RESOLUTION

Urambekov E.B.

*ST. PETERSBURG STATE UNIVERSITY OF AEROSPACE INSTRUMENTATION, St. Petersburg,
Russia (190121, Bolshaya Morskaya str., 67 letter a), e-mail: yra_517@mail.ru*

The analysis of the detection efficiency allows us to conclude that increasing the resolution and range to the target is most effective using intra-pulse modulation/ Moreover, of all known modulation methods, phase-manipulated signals (FMNs) are the most effective.

Keywords: Radar signal, EPR, number of samples, FMS, range accuracy, code generator, matched filter.

Радиолокационный фазоманипулированный сигнал (ФМнС) относится к классу дискретно кодированных сигналов (ДКС), в которых кодирование выполняется по фазе (ФДКС), обладающих большой длительностью и широким спектром. Рассматриваемый ФМнС представляет собой импульс с внутриимпульсной фазовой манипуляцией, повторяющийся с некоторым периодом. Манипуляция фазы осуществляется последовательностью примыкающих друг к другу N простых импульсов одинаковой (обычно прямоугольной) формы, начальные фазы высокочастотного заполнения которых принимают

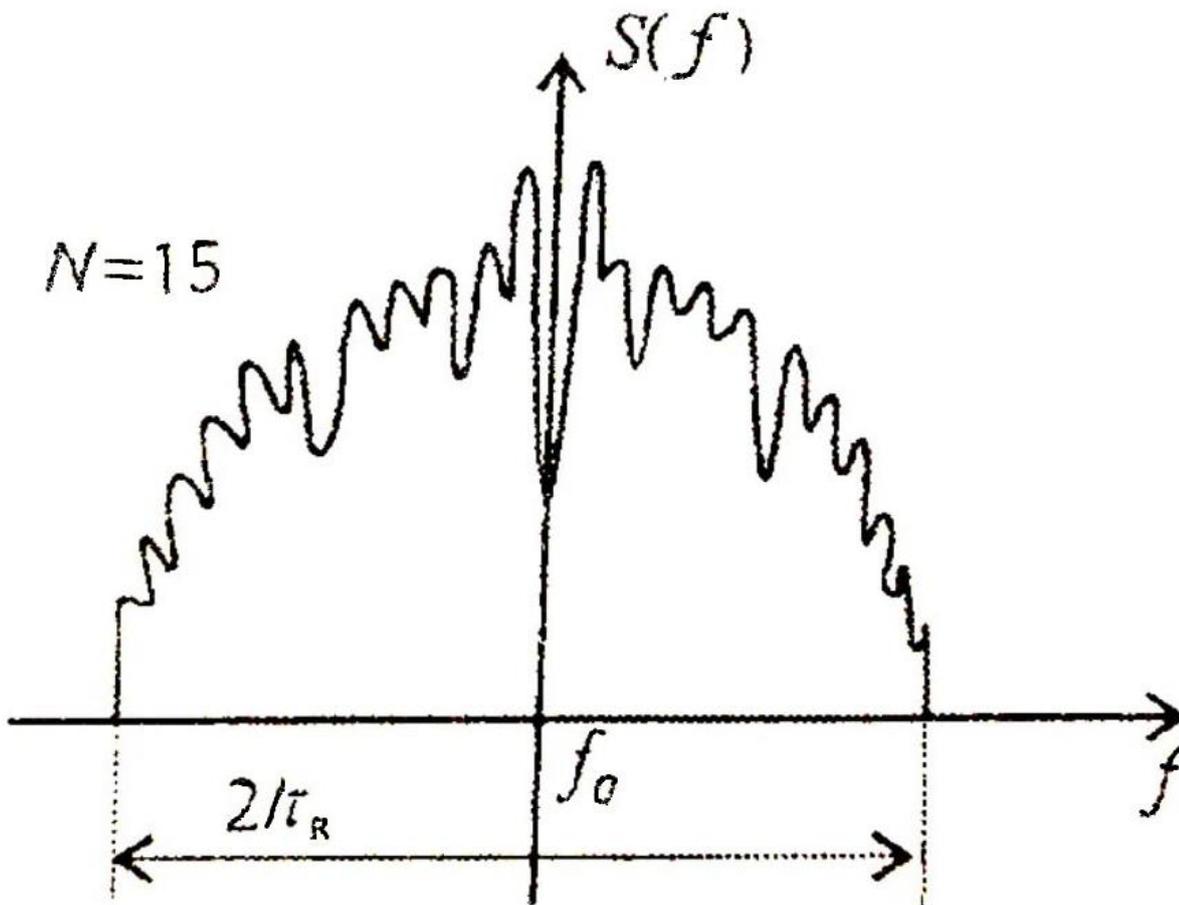


Рисунок 1 – Спектр ФМнС

При оптимальной обработке ФМнС имеется возможность разделения сигналов на выходе, импульсы которых на входе перекрываются. Это позволяет увеличивать длительность импульса τ без ухудшения разрешающей способности по дальности. Функция неопределенности ФМС соответствует характеризует влияние временного τ и частотного F сдвигов принимаемого сигнала по отношению к ожидаемому и может быть представлена моделью, показанной на Рисунке 2[1].

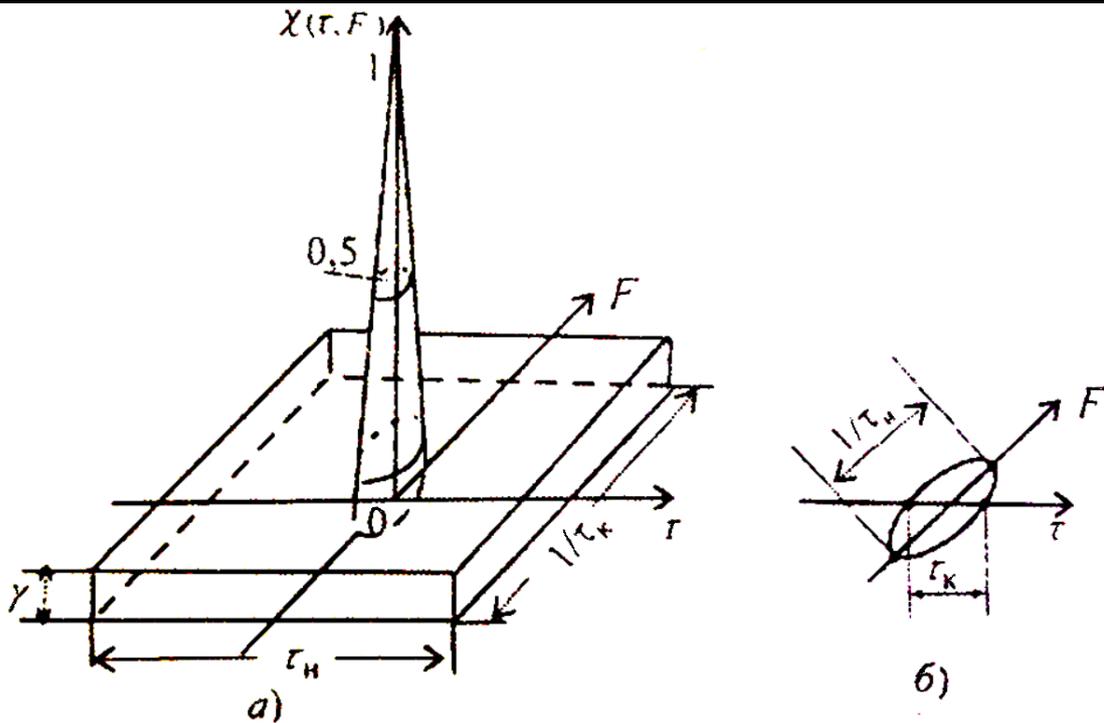


Рисунок 2 – Модель функции (а) и диаграммы неопределенности ФМнС (б)

Ширина спектра сигнала на выходе оптимального приемника по нулевому уровню будет тем меньше, чем больше длительность τ_n импульса ФМнС. Поэтому, чем больше τ_n , тем лучше разрешающая способность радиолокатора ФМнС по скорости.

Корреляционная функция импульса ФМнС имеет боковые лепестки, уровень которых тем меньше, чем больше число дискретов в импульсе ФМнС. Эти боковые лепестки могут затруднить обнаружение слабого ФМнС если вблизи от обнаруживаемой цели имеется другая цель с большей ЭПР. Из сказанного выше следует, что последовательность (код) надо выбирать таким образом, чтобы получить узкий пик корреляционной функции и малый уровень боковых лепестков последней. Для увеличения коэффициента сжатия, а, следовательно, улучшения разрешающей способности и точности при измерении дальности необходимо использовать импульс ФМнС с большим количеством дискретов N т.е. осуществлять манипуляцию фазы более эффективным кодом, чем код Баркера. С этой целью на практике наиболее часто используют коды на основе M -последовательностей (коды максимальной длины), строящихся как линейные рекуррентные двоичные последовательности [2].

Фазоманипулированные M - последовательностями сигналы по своим свойствам приближаются к «шумоподобным», параметры которых модулируются по случайному закону. Последние близки к идеальному сигналу, имеющему единственный узкий пик тела неопределенности в точке $\tau = 0, F = 0$ и равномерные остатки над остальной частью плоскости $\tau \theta F$, что обеспечивает высокую разрешающую способность и точность по дальности и скорости.

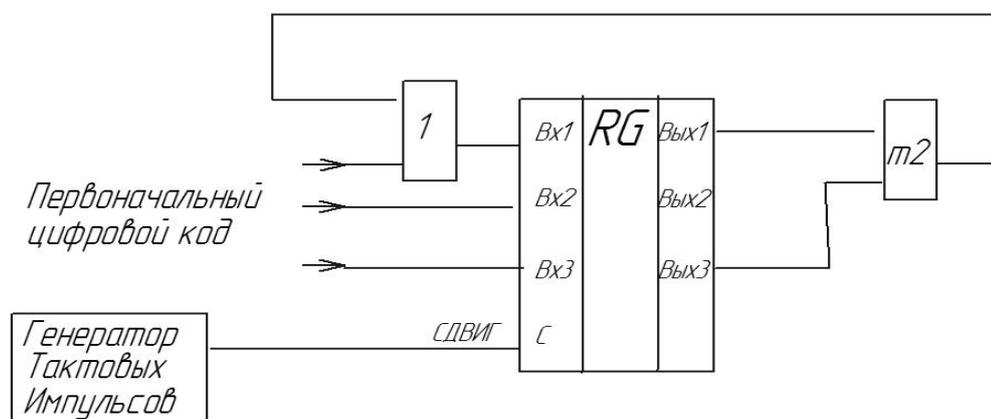


Рисунок 4 – Схема формирования M-последовательности

3. коэффициент взаимной корреляции $R_{ij} = (\text{числу совпадающих символов (дискретов)} - \text{число несовпадающих символов}) / \text{общее число символов} = -1/M$, т.е. сигналы квазиортогональны. Подобные сигналы, имеющие высокий коэффициент автокорреляции и низкий – взаимной корреляции, получили название «псевдошумовые» или «шумободобные», имея ввиду тот факт, что по корреляционным свойствам рассматриваемые сигналы близки к белому шуму;

4. ансамбль M-последовательностей $Q = M$;

5. форма любой M-последовательности отличается от любой другой временным сдвигом на один-два-три- и т.д. дискрета, что подтверждается формулой для периода $T_M = M \cdot \tau_0$, т.е. длительность M-последовательности определяется числом разрядов регистра: $T_M = M \cdot \tau_0 = 2^m - 1 = 7$.

Функциональная схема передающей части устройства представлена на Рисунке 5.

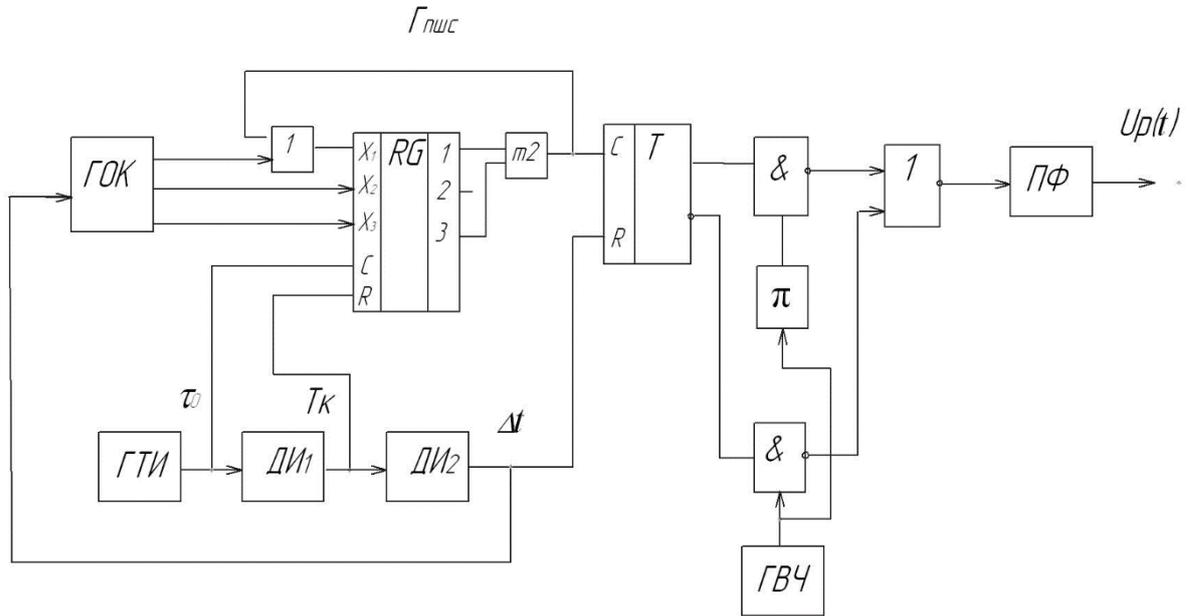


Рисунок 5 – Функциональная схема формирователя ФМн - сигнала

В состав передающей части формирователя входят генератор псевдошумовых ПШС - сигналов $\Gamma_{пшс}$, вырабатывающий одну из M – последовательностей M_1 из ансамбля, равного $M=7$, генераторное оборудование для формирования импульсных последовательностей:

1. с периодом τ_0 тактовой частоты (частота дискретов ПШС),
2. с длительностью T_k (длительность зондирования объекта) и периодом

$\Delta t = T_{изм}$ (период измерения), генератор опорного кода ГОК, управляющий триггер Т и высокочастотный передатчик, состоящий из модулятора М, генератора высокой частоты ГВЧ и полосового фильтра ПФ. В состав модулятора входят две схемы совпадения и фазовращатель на π .

Работу устройства формирования обеспечивает генераторное оборудование, в состав которого входят генератор тактовых импульсов ГТИ и делители импульсов ДИ1 и ДИ2. Сигналы задающего генератора тактовых импульсов ГТИ подаются на делитель частоты ДИ1 с коэффициентом деления, равном базе $M=7$. На выходе ДИ1 образуется сигнал, длительность которого определяется базой ПШС, и равна $7\tau_0$. Второй делитель ДИ2 (Рисунок 5) с коэффициентом деления равном скважности зондирующих импульсов, обеспечивает получение интервала $T_{изм}$, соответствующего дальности однозначного измерения R_{max} .

Генератор M -последовательности собран на 3-х разрядном регистре сдвига RG с обратной связью, объединяющей с помощью сумматора $m2$ два выхода регистра (1-й и 3-й) с входом первого триггера.

Генератор опорного кода ГОК формирует $m = 3$ символа (по числу триггеров регистра),

которые по сигналу $T_{изм}$, образованному на выходе ДИ2, записываются в триггеры регистра T1–T2 – T3, например 101. Далее, через $2^m - 1 = 7$ тактов образуется последовательность вида 1001110, которая и поступает через управляющий триггер на модулятор ФМн.

Генерируемая М-последовательность может сниматься с любого триггера или с любого сумматора по модулю 2. При этом вид ПШС не меняется, а лишь возникает сдвиг между М-последовательностями на целое число тактов τ_0 .

Триггер Т управляет схемами совпадений И2, открывая одну из них и закрывая другую. На одну схему И2 поступает сигнал с генератора высокой частоты ГВЧ непосредственно, на другую – через фазосдвигающую на 180^0 цепь. Выходное (результатирующее) напряжение $U_p(t)$ представляет собой непрерывный фазоманипулированный сигнал высокой частоты.

Для получения импульсов ФМнС необходимо замыкать цепь обратной связи в генераторе $\Gamma_{пшс}$ только на время, соответствующее длительности импульса τ_k .

На выходе высокочастотной части формирователя ставятся полосовой фильтр ПФ и антенна WA (на схеме не показаны).

Заключение.

Оптимальная обработка ФМн – сигналов предусматривает формирование на выходе устройства обработки корреляционного интеграла и может осуществляться фильтровыми или корреляционными схемами. С помощью этих схем производится сжатие импульса ФМнС, т.е. получение корреляционной функции $R(t,f)$ в виде узкого пика в начале координат t,f и минимального уровня боковых лепестков этой функции.

Список литературы

1. Информационные технологии в радиотехнических системах/В.А.Васин, И.Б.Власов, Ю.М.Егоров и др. МГТУ им.Баумана, 2004.
2. Варакин Л.Е. Системы связи с шумоподобными сигналами. М., Радио и связь, 1985.
3. Анализ функционирования бортовых радиолокационных комплексов мониторинга наземной обстановки в интересах поиско-спасательных служб./ Урамбеков Э.Б., Филиппов А.А., Сазанов И.Н. Инновации.Наука.Образование. 2020.№12. С. 510-520.

References

1. Information technologies in radio engineering systems/V.A.Vasin, I.B.Vlasov, Yu.M.Egorov and others.Bauman, 2004.
 2. Varakin L.E. Communication systems with noise-like signals. M., Radio and Communications, 1985.
 3. Analysis of the functioning of airborne radar systems for monitoring the ground situation in the interests of search and rescue services./ Urambekov E.B., Filippov A.A., Sazanov I.N. Innovations.Science.Education. 2020.No.12. pp. 510-520.
-



Международный журнал информационных технологий и
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.94

АНАЛИЗ АЭРОДИНАМИЧЕСКИХ ПОКАЗАТЕЛЕЙ ГОНОЧНОГО АВТОМОБИЛЯ КЛАССА FORMULA STUDENT

¹Гулин М.С., Куркин А.А., Кулагин А.Л., Кузмичёв В.А., Капустин А.Г.
ФГБОУ ВО "НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМ. Р.Е. АЛЕКСЕЕВА", Нижний Новгород, Россия (603155, Нижегородская область, город
Нижний Новгород, ул. Минина, д.24), e-mail: ¹ Gylin103@mail.ru

Предлагаемая работа описывает процесс подбора оптимальной конфигурации для автомобиля команды Sapienza Fast Charge. Для достижения поставленной цели был проведен анализ с несколькими испытаниями на трассе, сравнимой с трассой для заезда на выносливость. Тесты проводились с различными конфигурациями кузова и аэродинамических элементов, а также с различными вариантами управления энергопотреблением, реализованными в схеме питания инвертора. Наилучший результат, с соблюдением правил Formula Student 2020, был достигнут, благодаря сочетанию наилучшего времени на трассе и меньшего энергопотребления. Данная работа начинается с описания прототипа автомобиля, деталей силового агрегата и аккумулятора, установленных на борту. Далее приложена информация о спроектированных и построенных аэродинамических элементы, и представлен CFD-анализ их характеристик. Также рассмотрено описание тестовой трассы и проведено сравнение традиционной трассы для теста на выносливость в Formula Student. Описаны параметры, измеренные экспериментально и все проведенные тесты, чтобы определить оптимальную конфигурацию автомобиля. Ключевые слова: Цифровые подстанции, МЭК 61850, автоматизация, энергетические системы, стандарты, сети связи, передача данных, эффективность, надежность, инновации, современные требования, технологические решения.

Ключевые слова: Транспортное средство, электрический, аэродинамика, энергетический, экспериментальный.

ANALYSIS OF AERODYNAMIC PARAMETERS OF A FORMULA STUDENT CLASS RACING CAR

¹Gulin M.S., Kurkin A.A., Kulagin A.L., Kuzmichev V.A., Kapustin A.G
"NIZHNY NOVGOROD STATE TECHNICAL UNIVERSITY" R.E. ALEKSEEVA", Nizhny Novgorod,
Russia (603155, Nizhny Novgorod region, Nizhny Novgorod city, Minina str., 24), e-mail:
¹Gylin103@mail.ru

The proposed work describes the process of selecting the optimal configuration for the Sapienza Fast Charge team car. To achieve this goal, an analysis was conducted with several tests on a track comparable to an endurance race track. The tests were carried out with various body configurations and aerodynamic elements, as well as with various energy management options implemented in the inverter power supply circuit. The best result, in compliance with the rules of Formula Student 2020, was achieved by combining the best time on the track and lower energy consumption. This work begins with a description of the prototype car, the parts of the power unit and the battery installed on board. Next, information about the designed and built aerodynamic elements is attached, and a CFD analysis of their characteristics is presented. The description of the test track is also considered and a comparison of the traditional track for the endurance test in Formula Student is carried out. The

parameters measured experimentally and all the tests performed to determine the optimal configuration of the car are described.

Keywords: Vehicle, electric, aerodynamic, energy, experimental.

Описание

Formula Student Electric - это научно-образовательное соревнование, которое требует разработки и изготовления полностью электрического прототипа автомобиля с открытыми колесами. Автомобили оцениваются как по производительности, так и по общей энергоэффективности. Например, в заезде на выносливость, который является одним из важнейших этапов соревнований. Оптимизация производительности и экономичности автомобилей затрагивает как силовой агрегат, так и кузов автомобиля. Поэтому можно выделить три важнейшие темы для разработки автомобилей: карты мощности, с помощью которых инвертор управляет электродвигателем, аэродинамический обвес, и общие технические характеристики автомобиля. Для достижения лучших показателей не обязательно использовать максимальную мощность, разрешенную правилами технического регламента, для силового агрегата (80 кВт). Также не обязательно устанавливать все компоненты аэродинамического обвеса (переднее антикрыло, заднее антикрыло и подкрылки с диффузорами). Стоит отметить, что наилучшей конфигурацией может оказаться не самая легкая машина. Все вышесказанное приводит к тому, что необходимо найти оптимальный баланс между различными характеристиками автомобиля.

Многоэлементные крылья широко используются в автоспорте для создания более высокого коэффициента подъемной силы (CL. На гоночных автомобилях области установки этих крыльев ограничены, но все же многие команды используют от 6 до 7 элементов только на переднем антикрыле. Конструкция многоэлементных крыльев очень сложна из-за ряда параметров. В многоэлементных крыльях представляет интерес область, где поток покидает первый элемент и перемещается ко второму элементу. Конструктивные параметры включают профили аэродинамического профиля, длину хорды, угол атаки, зазор между пазами и перекрытие.

Непосредственным преимуществом реализуемой модели k-epsilon является то, что она более точно предсказывает скорость распространения как плоских, так и круглых потоков. Также она обеспечивает превосходные характеристики для потоков, включающих вращение, пограничных слоев при сильных градиентах давления, разделение и рециркуляцию. Как реализуемая, так и RNG модели k-epsilon показали существенные улучшения по сравнению со стандартной моделью k-epsilon, где характеристики потока включают сильную кривизну линии обтекания, вихри и вращение. Одним из ограничений реализуемой модели k-epsilon является то, что она создает нефизическую турбулентную вязкость в ситуациях, когда вычислительная область содержит как вращающиеся, так и неподвижные зоны текучей среды (например, несколько систем отсчета, вращающиеся скользящие сетки). Это связано с тем фактом, что реализуемая модель k-epsilon включает эффекты среднего вращения при определении турбулентной вязкости. Этот эффект дополнительного вращения был протестирован на системах с одной вращающейся системой отсчета и показал превосходство по сравнению со стандартной моделью k-epsilon. Однако из-за характера этой модификации к ее применению к системам с несколькими системами отсчета следует относиться с некоторой осторожностью.

Модель SST обеспечивает превосходные характеристики для пограничного слоя, ограниченного стенками, потоков со свободным сдвигом и с низким числом Рейнольдса. Модель SST учитывает перенос турбулентного напряжения сдвига и дает высокоточные прогнозы возникновения и величины отрыва потока при неблагоприятных градиентах давления. Модель SST рекомендуется для высокоточного моделирования пограничного слоя. Однако ее зависимость от расстояния до стенки делает эту модель менее подходящей для свободных сдвиговых течений по сравнению со стандартным методом k-epsilon. Кроме того, модель SST требует более мелкую сетку вблизи стенки.

Таким образом, моделью, которую мы выбрали для нашего CFD-моделирования, представляла реализацию метода k-эпсилон.

Анализ

Первоначально для 2D-случаев данные о профилях были собраны из www.airfoiltools.com. Затем эти профили были смоделированы и протестированы с использованием ANSYS Fluent для анализа сетки; однако в этом исследовании представлен и обсуждается только 3D-пример проверки для анализа сетки. Вместо аэродинамического профиля на Ahmed было выполнено 3D-моделирование Кузова, который изображает упрощенную форму транспортного средства и в прошлом неоднократно тестировался в аэродинамической трубе, что делает его популярным инструментом для многих инженеров CFD. Тело Ahmed было смоделировано с помощью программного обеспечения Pro-Engineer и экспортировано в Design Modeler для pre mesh. Тело было разделено пополам, поскольку это задача с симметричным состоянием в стационарном режиме. Вокруг кузова было создано ограждение тех же размеров, что и испытательный участок в аэродинамической трубе (1,87 м x 1,4 м). Были смоделированы первый кузов, занимающий объем немного больше, чем само транспортное средство, и два других кузова; один снизу, а другой сзади. Эти тела были позже использованы при создании сетки в качестве объектов влияния (зон с максимальным размером элемента, определенным пользователем). Эти функции определения размеров тел использовались для точного моделирования потока, таких как области с высокими завихрениями, турбулентностью и разделением потока. Построение сетки для этой области было выполнено с использованием ANSYS Workbench. Были сгенерированы различные сетки с различными настройками, которые позже были смоделированы, а затем были отмечены ошибки экспериментальных значений. Следовательно, анализ сетки был выполнен на теле Ahmed. Три зафиксированных тела, которые были представлены в Design Modeler, затем использовались для определения размеров тела. В этих областях плотность сетки поддерживается постоянной путем указания максимального размера элемента в области. Всего было использовано 5 различных сеток. Решателем, использованным для анализа тела Ahmed, был ANSYS Fluent, использующий реализуемую модель турбулентности k-epsilon, гибридные и связанные схемы для инициализации и решения соответственно. Для пространственной дискретизации используется подветренный импульс второго порядка, турбулентная кинетическая энергия и скорость турбулентного рассеяния.

Численные результаты, полученные для пяти различных настроек сетки, были сопоставлены с испытаниями в аэродинамической трубе, проведенными в Техническом университете Граца, Австрия, и были признаны хорошо согласующимися. Это обеспечило

наиболее подходящий размер сетки для анализа чувствительности. Коэффициент лобового сопротивления (C_d) был рассчитан с использованием силы ветра 40 м/с, угла вылета 25 градусов и числа Рейнольдса $2,78 \times 10^6$. Это значение C_d также сравнивалось с аналитическими значениями, полученными с помощью различных методов моделирования CFD (вычислительной гидродинамики), чтобы подтвердить результаты.

После завершения процесса детального моделирования, анализа сетки и валидации была разработана стратегия анализа и внедрена в пакет аэродинамической прижимной силы. Результаты анализа подробно обсуждаются ниже. Для случая 1 максимальный CL (коэффициент подъемной силы), равный 3,63, был рассчитан путем выбора 1-го и 2-го элементов как 122-155 с соотношением хорд ($C1/C2$), равным 1,42, и L/D (отношение подъемной силы к лобовому сопротивлению), равным 21,5, где C1 обозначает 1-ю хорду, а C2 обозначает 2-й аккорд. Для случая 2 максимальное значение L/D, равное 54,1, было рассчитано путем выбора только 1-го элемента (BE 122-155), а 2-м элементом был E385 с другим соотношением хорд, равным 2,5, и был получен CL, равный 2,83.

Анализ также проводится с помощью закрылков или плетеных накладок (тонкая плоская пластина на конце, ориентированная под углом 90° к поверхности задней кромки второго элемента), которые являются простыми дополнениями к крылу. Это добавление толщиной ($0,05 C1$) привело к увеличению общей прижимной силы на 5,8%, т.е. к резкому повышению производительности.

После завершения проектирования крыльев было выполнено CFD-моделирование для всей установки с использованием скорости на входе = 20 м/с; среднего относительного давления на выходе = 0 Па, вращающейся стенки (шины) при $\omega = 82,88$ рад/с и скорости движущейся стенки (грунт) = 20 м/с. Сначала был смоделирован и протестирован базовый автомобиль без каких-либо аэродинамических устройств. Из-за высокой сложности было выполнено всего несколько итераций сборки диффузора. Затем крылья были добавлены ко всей установке и смоделированы, чтобы определить эффективную подъемную силу и лобовое сопротивление при скорости 20 м/с при лобовой площади транспортного средства 0,82 м².

Вывод

На основе подробных параметрических вычислений сделан вывод, что с увеличением количества элементов, создающих прижимную силу, общая прижимная сила увеличивается. Почти 60% прижимной силы создается передними и задними антикрыльями. По мнению экспертов, диффузор создает 30% общей прижимной силы, однако в этом исследовании разница объясняется некоторыми упрощениями при моделировании диффузора. Возможны различные улучшения в секции диффузора, которые рекомендуется провести в следующих исследованиях.

Список литературы

1. Ланфрит М. (2005) Рекомендации по наилучшей практике управления внешней аэродинамикой автомобилей с помощью FLUENT. Fluent Deutschland GmbH Биркенвег Дармштадт/Германия. Версия 1.2.
2. Профессионал/инженер. (2009) Wildfire Release 4.
3. Справочное руководство по ANSYS CFX. (2009). Выпуск 11.

4. Гильмино Э. (2008) Вычислительное исследование обтекания упрощенного кузова автомобиля, Журнал ветроэнергетики и промышленного применения, 96: С.1207-1217.
5. Кац Дж. (1996) Аэродинамика гоночных автомобилей: проектирование для скорости (инженерия и эксплуатационные характеристики). Издательство Bentley; 2-е издание. ISBN: 978-0837601427
6. Мингес М., Паскетти Р., Серре Э. (2008) Моделирование потока с большими вихрями высокого порядка над моделью автомобиля с кузовом Ahmed. Физика жидкостей. Том 20, 095101/17.
7. Байрактар И., Дэвид Л., Байсал О. (2001) Экспериментальное и вычислительное исследование корпуса Ахмеда для аэродинамики наземного транспортного средства, Технический университет Граца, документ SAE 2001-01-2742.
8. Кападия С., Рой С., Вурцлер К. (2003) Моделирование отдельных вихрей на эталонной модели автомобиля Ahmed, AIAA. Документ № 2003-0857.
9. Морел Т. (1978) Влияние наклона основания на характер обтекания и лобовое сопротивление трехмерных тел с тупыми концами, в: Совран Г., Морел Т., Мейсон У.Т. (ред.) Механизмы аэродинамического сопротивления кузовов с тупыми концами и дорожных транспортных средств. Пленум Пресс, Нью-Йорк, С. 191-226.

References

1. Lanfrith M. (2005) Recommendations on the best practice of controlling the external aerodynamics of cars using FLUENT. Fluent Deutschland GmbH Birkenweg Darmstadt/Germany. Version 1.2.
 2. Professional/engineer. (2009) Wildfire Release 4.
 3. The ANSYS CFX Reference Guide. (2009). Issue 11.
 4. Gilmino E. (2008) Computational Flow Study of a simplified car body, Journal of Wind Energy and Industrial Applications, 96: pp. 1207-1217.
 5. Katz J. (1996) Aerodynamics of racing cars: design for speed (engineering and performance). Bentley Publishing House; 2nd edition. ISBN: 978-0837601427
 6. Minges M., Paschetti R., Serre E. (2008) Modeling of a flow with large high-order vortices over a model of a car with an Ahmed body. Physics of liquids. Volume 20, 095101/17.
 7. Bayraktar I., David L., Baysal O. (2001) Experimental and computational study of the Ahmed hull for Ground Vehicle Aerodynamics, Technical University of Graz, SAE document 2001-01-2742.
 8. Kapadia S., Roy S., Wurzler K. (2003) Modeling of individual vortices on a reference model of an Ahmed, AIAA car. Document No. 2003-0857.
 9. Morel T. (1978) The effect of base tilt on the flow pattern and drag of three-dimensional bodies with blunt ends, in: Sovran G., Morel T., Mason U.T. (eds.) Mechanisms of aerodynamic drag of bodies with blunt ends and road vehicles. Plenum Press, New York, pp. 191-226.
-