16+

ISSN 2074-1707

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2021
№ 1 (53)

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

Группа специальностей 05.11.00 «Приборостроение, метрология и информационно-измерительные приборы и системы»:

05.11.01 – Приборы и методы измерения (по видам измерений) (технические науки);
05.11.16 – Информационно-измерительные и управляющие системы (по отраслям) (технические науки);
05.11.17 – Приборы, системы и изделия медицинского назначения (технические науки).

Группа специальностей 05.13.00 «Информатика, вычислительная техника и управление»:

05.13.01 – Системный анализ, управление и обработка информации (по отраслям) (технические науки);
05.13.05 – Элементы и устройства вычислительной техники и систем управления (технические науки);
05.13.10 – Управление в социальных и экономических системах (технические науки);
05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей (технические науки);
05.13.18 – Математическое моделирование, численные методы и комплексы программ (технические науки);
05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки).

Журнал входит в базу данных Ulrich’s Periodicals Directory.

Астрахань
Издательский дом «Астраханский университет»
2021

ББК 30
П75

Рекомендовано к печати редакционно-издательским советом
Астраханского государственного университета

ПРИКАСПИЙСКИЙ ЖУРНАЛ: управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2021
№ 1 (53)

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

ISSN 2074-1707

ASTRAKHAN STATE UNIVERSITY

PRIKASPIYSKIY ZHURNAL:
Upravlenie i Vysokie Tekhnologii

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2021
No. 1 (53)

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

Group of specialties 05.11.00 "Instrument engineering, measurement science, information and measuring devices and systems":

05.11.01 – Instruments and measurement methods (by measurement types) (technical sciences);
05.11.16 – Information-measuring and control systems (by branches) (technical sciences);
05.11.17 – Medical instruments, systems and items (technical sciences).

Group of specialties 05.13.00 "Informatics, computer technique and control":

05.13.01 – System analysis, information control and processing (by branches) (technical sciences);
05.13.05 – Components and devices of computational tools and control systems (technical sciences);
05.13.10 – Management in social and economic systems (technical sciences);
05.13.11 – Mathematical software and software for computing machines, computer systems and networks (technical sciences);
05.13.18 – Mathematical modelling, numerical methods and complexes of programms (technical sciences);
05.13.19 – Information security methods and systems, information security (technical sciences).

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

Astrakhan
Publishing House "Astrakhan University"
2021

Recommended by the Editorial and Publishing Board
of Astrakhan State University

**CASPIAN JOURNAL:
Control and High Technologies**

A SCIENTIFIC AND TECHNICAL JOURNAL

**2021
No. 1 (53)**

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

СОДЕРЖАНИЕ

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

CONTENTS

INFORMATICS, COMPUTER TECHNIQUE AND CONTROL

SYSTEM ANALYSIS, CONTROL AND INFORMATION PROCESSING

MATHEMATICAL MODELLING, NUMERICAL METHODS AND PROGRAM SYSTEMS

INFORMATION SAFETY AND INFORMATION PROTECTION

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

INFORMATION-MEASURING AND CONTROL SYSTEMS

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2021.53.1.009-017
УДК 004.4

СТРУКТУРА ПРОГРАММНОГО ПРОДУКТА ДЛЯ СЕМАНТИЧЕСКОГО АНАЛИЗА ТЕКСТОВОЙ ИНФОРМАЦИИ

Статья поступила в редакцию 15.09.2020, в окончательном варианте – 13.01.2021.

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

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

Зорин Кирилл Андреевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

ассистент кафедры информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0003-1614-8168, e-mail: kirocan95@gmail.com

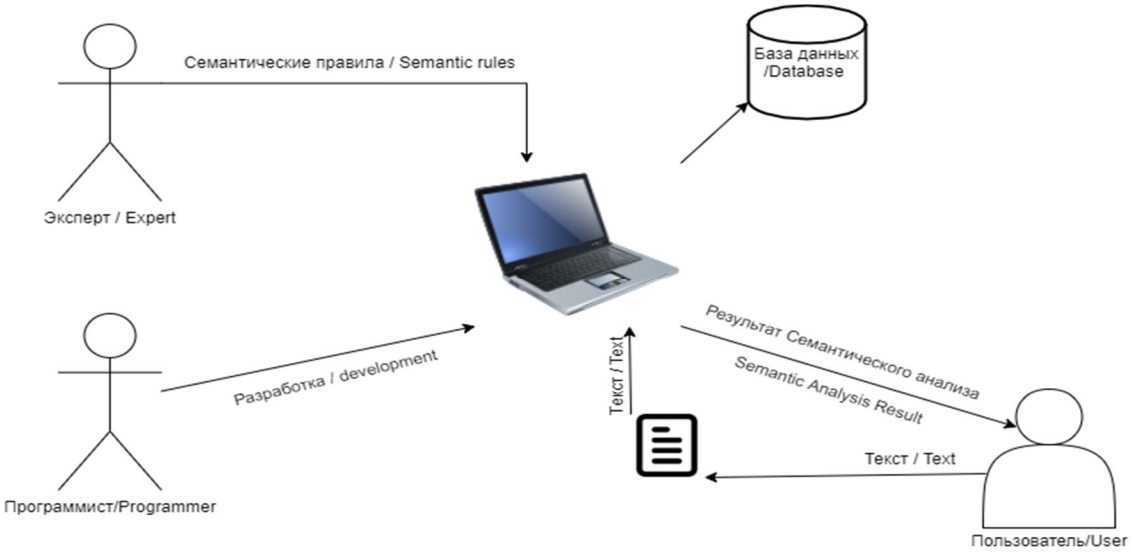
Кузнецова Валентина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

ассистент кафедры информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

Статья посвящена методике семантического анализа текста и реализующего ее программного обеспечения. Описывается общая логика работы разработанного web-приложения, которое осуществляет классификацию текстовой информации по заданным экспертом семантическим категориям. Для иллюстрации функционирования программного продукта приведены диаграммы использования, развертывания, а также общая схема работы алгоритма. Применение разработанного программного продукта позволяет обрабатывать текстовую информацию любого содержания, а также проводить семантический анализ текста. Реализованный метод актуален во многих сферах деятельности, где приходится работать с текстовой информацией: правоохранительная деятельность по выявлению незаконного контента, маркетинг, бренд-менеджмент, скоринг.

Ключевые слова: семантический анализ, алгоритм, методы классификации, программное обеспечение, оптимизация, текстовая информация, web-сервис

Графическая аннотация (Graphical annotation)



STRUCTURE OF A SOFTWARE PRODUCT FOR SEMANTIC ANALYSIS OF TEXTUAL INFORMATION

The article was received by the editorial board on 15.09.2020, in the final version – 13.01.2021.

Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

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

Zorin Kirill A., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

assistant of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0003-1614-8168, e-mail: kirocan95@gmail.com

Kuznetsova Valentina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

assistant of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

The article is devoted to the development of software for semantic text analysis. Describes the General logic of the developed web application, which implements the classification of textual information by previously pre-defined semantic categories. This article provides usage and deployment diagrams, as well as a General diagram of the algorithm. The methods implemented in the app allow you to increase the speed of processing text information. The use of the developed software product allows you to quickly process text information of any content, as well as conduct a deeper semantic analysis of the text. The implemented method is relevant in many areas of activity where you have to work with text information: monitoring of emotional mood towards the company, marketing, social network analysis.

Keywords: semantic analysis, algorithm, classification methods, software, optimization, text information, web service

Введение. Процесс обмена информации в социальной среде является одним из основополагающих процессов, который предопределяет развитие общества. Без постоянной передачи знаний прогресс в сфере науки, бизнеса, искусства, медицины практически невозможен. Передача информации, как и ранее, является основным фактором нормального функционирования и развития общества. В подавляющем большинстве случаев такой обмен происходит посредством применения текстового формата. Поэтому автоматизированный анализ текстовой информации является актуальной на сегодняшний день технологией для решения различных прикладных задач – в банковской, туристической, рекламной, правоохранительной и других сферах жизни общества.

Существуют различные методы анализа текста на выявление его семантической направленности. В статье Д.Ю. Турдакова «Семантический анализ текстов с использованием системы Texterra» [9] приводится метод анализа текста с использованием баз знаний, в частности Википедии. Также описан процесс построения семантической модели в Texterra, где на основе данных из открытых источников система обнаруживает термины и устойчивые выражения в тексте, что позволяет автоматически наполнять базу данных и улучшать качество для семантического распознавания текста. А.С. Епрев в статье «Автоматическая классификация текстовых документов» приводит обзор методов, которые возможно применить для классификации текстовых документов [3]. Т.В. Батура в статье «Методы автоматической классификации текстов» [2] приводит сравнение современных подходов решения задачи классификации текстов, показывает тенденцию развития данного направления, а также выбор наилучших алгоритмов для применения в исследовательских и коммерческих задачах. В работе также произведены анализ и сравнение качества работы различных методов классификации по таким характеристикам, как точность, полнота, время работы алгоритма, возможность осуществлять каждый анализ документа без выполнения полного цикла вычислений, количество предварительной информации, необходимой для классификации, независимость от языка. Однако методы, описанные в вышеуказанных статьях, не позволяют определить семантическую направленность текстов, а лишь классифицируют документы, отличая их по частоте вхождения слов или иным признакам. Текстовая информация, представленная на русском языке, отличается сложностью анализа, так как в отличие от английского языка порядок слов в русском языке не определяет смысл предложения. Также присутствуют категории рода, падежи, что напрямую влияет на представленную в тексте информацию. Предложенные методы показывают недостаточную эффективность при больших объемах текстовой информации, поэтому задача семантического анализа русскоязычного текста является не до конца решеной.

Предлагаемая методика. В рамках решения задачи была предложена автоматизация методики анализа русскоязычной текстовой информации путем выделения семантических единиц-индикаторов и их поиска в исследуемом тексте (на примере материалов экстремистской направленности). Для этого была подробно проанализирована и описана последовательность действий эксперта при проведении лингвистической экспертизы, что позволило выявить основные маркеры, которые позволяют сделать обоснованные предположения о принадлежности текста к той или иной смысловой категории. После выделения групп слов и присвоения весов Фишберна в рамках каждой из групп производится анализ текста [1].

Описанная в работе [1] методика была реализована в виде web-приложения. Данный подход к реализации дает возможность пользователю применять указанное программное обеспечение с любого устройства, которое имеет доступ к интернету. Приложение является многопользовательским. Обновлять web-приложение необходимо только на серверной части, что упрощает обслуживание и избавляет пользователя от установочных процедур на рабочей станции. Разработанный программный продукт позволяет обработать большое количество текстовых фрагментов за достаточно небольшой промежуток времени и на выходе получить результат в виде числа, которое отражает вероятность отнесения текста к определенной «смысловой» категории, например, категории текстов, связанных с политикой, религией, насилием и другие [1].

В основе семантического анализа текста лежит процесс определения принадлежности текстового фрагмента к выделенным смысловым группам. Каждая группа содержит в себе набор слов и устойчивых выражений, схожих по семантике.

В словесной форме алгоритм семантического анализа текста состоит из следующих этапов:

1) создание базы знаний, состоящей из слов-токенов;
2) определение семантических характеристик токенов;
3) создание групп – категорий на основе семантического значения;
4) расчет численного значения – веса, каждого токена в категории;
5) в зависимости от заданных экспертом правил на основании рассчитанных весов устанавливается семантическая направленность текста.

База слов составляется экспертами – лингвистами на основе известных публикаций, а также общих правил семантического анализа. Каждое слово может существовать в различных формах, с разными окончаниями, в различных падежах. Для того чтобы привести слово к первоначальному словарному значению, применяется метод лемматизации слова. Лемматизация – метод морфологического анализа, который сводится к приведению слова к первоначальной словарной форме (лемме) [5].

Каждому лемматизированному слову – токену эксперт ставит в соответствие численное значение его веса в категории от 0 до 1. Вес определяет значимость данного токена в категории. Чем выше вес – тем значимее употребление данного слова в тексте для категории, в которой присутствует данный токен. Токен может использоваться в различных категориях, однако вес токена в каждой категории будет разный, в зависимости от семантического значения, т.е. одно и то же слово может по-разному влиять на конечный результат семантического анализа.

Описание структуры разработанного программного продукта.

Пользователи системы. В системе предусмотрено 3 вида пользователей:

- Администратор системы;
- Эксперт;
- Пользователь.

Администратор системы осуществляет полный контроль над системой: подтверждает регистрацию новых пользователей, регистрирует новых экспертов. Имеет возможность редактировать категории, в том числе и удалять их. Зарегистрированный администратором эксперт имеет возможность создавать новые категории для анализа текстовой информации, добавлять новые токены в общий словарь, добавлять или обновлять список токенов в различных категориях, настраивать веса токенов в категориях. Диаграмма вариантов использования приведена на рисунке 1.

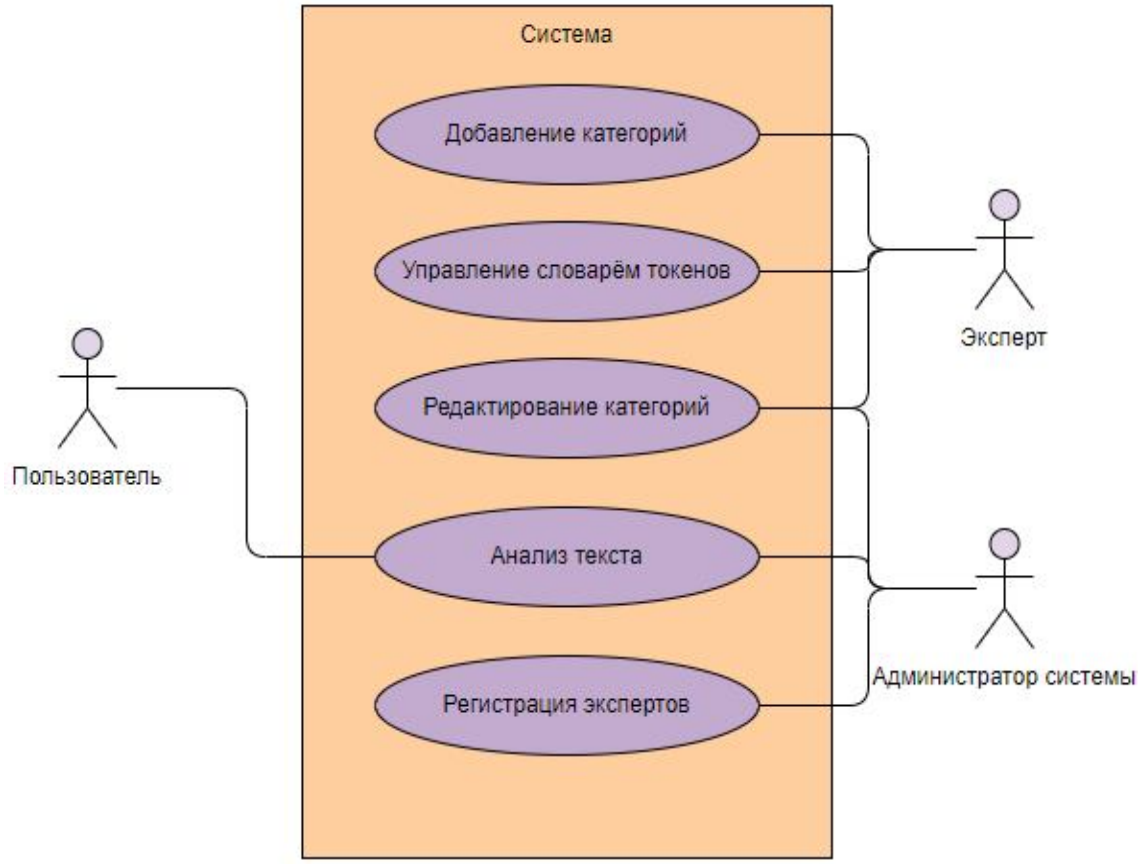


Рисунок 1 – Диаграмма вариантов использования

Пользователь может работать в системе только после подтверждения его учетной записи администратором системы. Пользователю доступно просматривать категории слов и веса токенов. Главный раздел для пользователя – анализ текстовой информации по доступным категориям, а также получение результатов.

Общий алгоритм работы программы при семантическом анализе текста. Эксперт составляет базу слов-токенов. После того как база токенов готова, эксперту необходимо создать категории. В каждую категорию эксперт добавляет токены с заданными весами. После того как базы данных заполнены – можно приступать к анализу текста.

Анализ текста включает следующие этапы:

1. Удаление знаков препинания из текстовой информации.
2. Лемматизация всех слов в тексте.
3. Поиск полученных токенов в категориях.
4. Анализ и вычисление результатов.
5. Вывод результата работы алгоритма семантического анализа текста.

Рассмотрим этапы предложенного алгоритма более подробно.

1. Удаление знаков препинания из текстовой информации. Удаление пробелов, запятых, точек и т.д. из исходного текста необходимо для сокращения объема анализируемого текста, а также правильного распознавания словосочетаний в тексте. Слова в тексте могут быть представлены в различной форме.

2. Лемматизация слова. Для приведения слова в словарную форму используется процесс лемматизации. Лемматизация слова позволяет привести все слова в тексте в начальную форму, после чего производить быстрый поиск необходимых слов – токенов во всех категориях. Для процесса лемматизации слова используется нейронная сеть, которая построена и обучена на фреймворке tensorflow [8]. В качестве датасета используется словарь, полученный в результате выполнения проекта по созданию размеченного текста – OpenCorpora. Словарь доступен бесплатно и в полном объёме по ссылке [7]. Он представляет набор морфологически, синтаксически и семантически размеченных текстов на русском языке.

3. Поиск токена слова в категориях. После процесса лемматизации система начинает поиск токенов слов в заранее сформированной экспертами базе данных категорий и токенов. Реляционная база данных представляет собой набор данных, организованных в виде таблиц, которые состоят из строк и столбцов. Общая схема алгоритма поиска токенов представлена на рисунке 2.

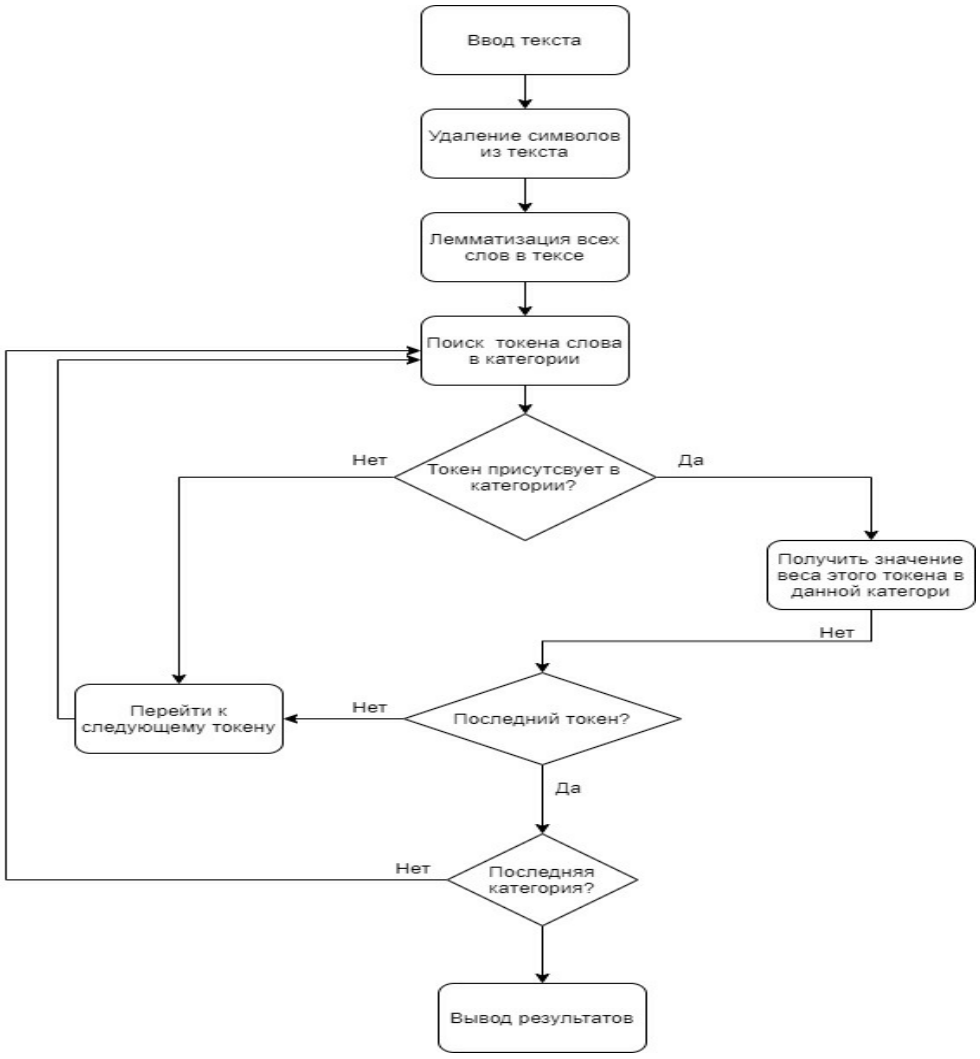


Рисунок 2 – Схема алгоритма для поиска токенов в категориях

4. Анализ и вычисление результатов. Для каждого найденного *i*-го токена в категории вычисляется нормированное значение (*V*) веса с применением метода Фишберна по следующей формуле [1]:

$$V_i = \frac{B_i}{\sum_{k=1}^{z} n_k B_k},$$

где *n* – количество слов в категории; B_i – оценка существенности слова в категории, так как одно и то же слово может иметь разный вес в различных категориях; *k* – индекс категории слов.

После вычисления нормированного значения веса для каждого найденного токена в категории необходимо рассчитать параметр γ_m (принадлежность текста к категории *m*), который характеризует принадлежность текстовой информации к m-й категории по следующей формуле:

$$\gamma_m = \sum_{i=1}^{n} s_i V_i,$$

где s_i – частота повтора *i*-го слова в тексте; m – номер категории, в которой имеется рассматриваемый токен.

Описание структуры разработанного приложения. Приложение имеет серверную часть, написанную на языке программирование C# 8.0 с использованием платформы .net core 3.1. Одно из основных преимуществ данной платформы – возможность использовать любую операционную систему для установки приложения. Для работы с базой данных используется Entity Framework, который позволяет абстрагироваться от используемой базы данных и работать с моделями данных вне зависимости

от типа хранилища. Таким образом мы получаем гибкую информационную систему, которая позволяет запустить приложение с использованием различных баз данных и операционных систем.

Для разработки клиентской части приложения использовались технологии Razor и библиотека Bootstrap. Razor легко интегрируется в среду разработки и позволяет гибко использовать данные, полученные от серверной части приложения. В качестве компонентов веб-интерфейса используются элементы библиотеки Bootstrap.

Схема взаимодействия компонентов разработанной системы представлена на рисунке 3.

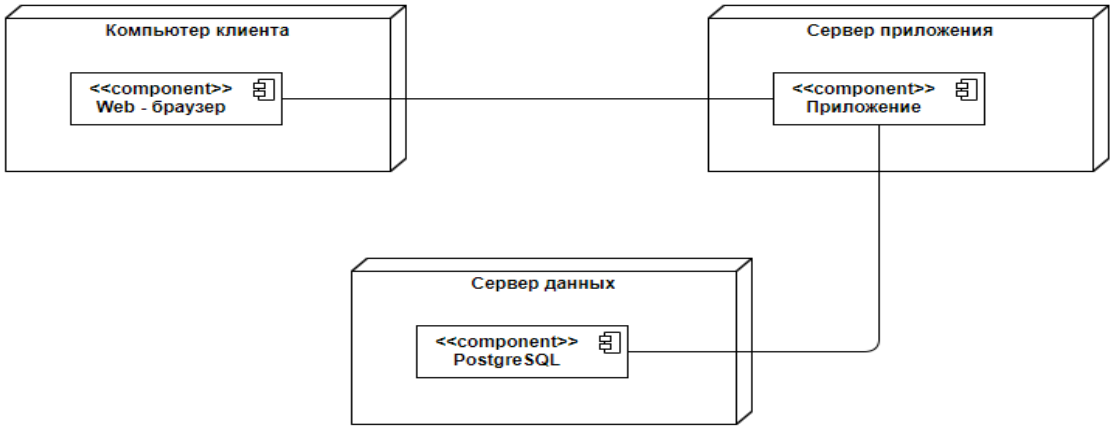


Рисунок 3 – Схема взаимодействия компонентов

В качестве хранилища данных была выбрана свободная объектно-реляционная система управления базами данных PostgreSQL.

Структура базы данных. Разработанное приложение использует реляционную базу данных, преимущество использования которой заключается в том, что при доработке функционала системы изменения в структуре базы данных сводятся к минимуму и не затрагивают хранимые данные. Данные создаются и обновляются с помощью структурированных запросов – sql. Запросы могут извлекать из базы как информацию из одной таблицы, так и связанные сущности из разных таблиц. Такой подход позволяет быстро обрабатывать результаты выборки, что для семантического анализа текста является важной составляющей. Модель данных приведена на рисунке 4.

Для работы программы эксперту необходимо создать категории, а также добавить в них токены, по которым будет производиться анализ текста. В схеме базы данных присутствует таблица токенов, которая связана с таблицей категорий, благодаря чему один токен может принадлежать к разным категориям.

Эксперт добавляет слова в любой форме, после чего при помощи нейронной сети определяется лемма данного слова – токен. При добавлении токена в категорию необходимо задать его вес в категории.

Вес токена в категории представляет собой целочисленное значение, которое указывает на то, насколько наличие слова-токена в тексте относит его к категории m. Чем выше это значение, тем выше вероятность употребления слова в рассматриваемой категории. Добавление новых токенов происходит на вкладке «Управление словарем». Добавляя новое слово, пользователю необходимо добавить краткое описание, которое может состоять как из морфологического значения, так и примеров употребления данного токена в тексте.

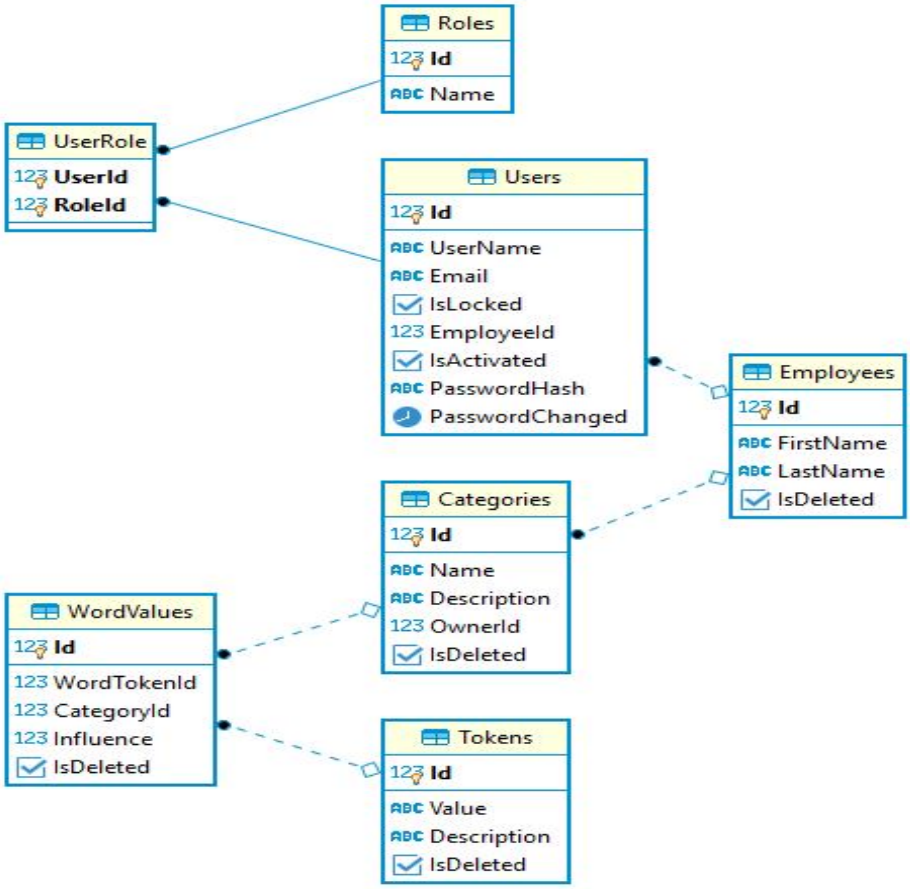


Рисунок 4 – Модель данных

Существует два способа добавления новой категории в систему:

1) можно на вкладке «Управление категориями» добавить название и описание новой категории. После этого при помощи поиска добавить в нее новые слова и установить значение веса для каждого слова в данной категории;

2) можно заполнить заранее структурированный файл в формате *JSON (рис. 5), в который эксперт добавляет новую категорию вместе с набором слов-токенов, которые ее характеризуют.

```
{
  "categoryName": "Экспрессивность",
  "categoryDescription": "Возможны негативные эмоции значительной интенсивности",
  "words": [
    {
        "tokenValue" : "Избавиться",
        "tokenDescription" : "Поможет избавиться",
        "tokenInfluence" : 3
    },
    {
        "tokenValue" : "Захлебнуться",
        "tokenDescription" : "Мир захлебнулся в крови",
        "tokenInfluence" : 2
    },
    {
        "tokenValue" : "Распоряжаться",
        "tokenDescription" : "Распоряжаться судьбами других",
        "tokenInfluence" : 1
    },
```

Рисунок 5 – Структура файла импорта категории

Для проведения анализа по существующим категориям пользователь на главной странице приложения вводит текст любого объема в соответствующее поле. После чего необходимо нажать на кнопку «Анализировать». Будет запущен процесс для семантического анализа текстовой информации. После проведения анализа пользователь получит результат анализа.

Результатом работы программного продукта является список категорий с указанием параметра γ_m (принадлежность текста к категории), который характеризует принадлежность текстовой информации к определенной категории.

Пример работы приложения. Для использования приложения пользователю необходимо выполнить вход в систему с помощью подтвержденной администратором учетной записи. На главной странице web-сервиса присутствует поле для ввода текстовой информации, куда пользователю нужно ввести текстовую информацию. После нажатия кнопки «Анализировать» запустится процесс анализа. Скриншот работы программного продукта приведен на рисунке 6.

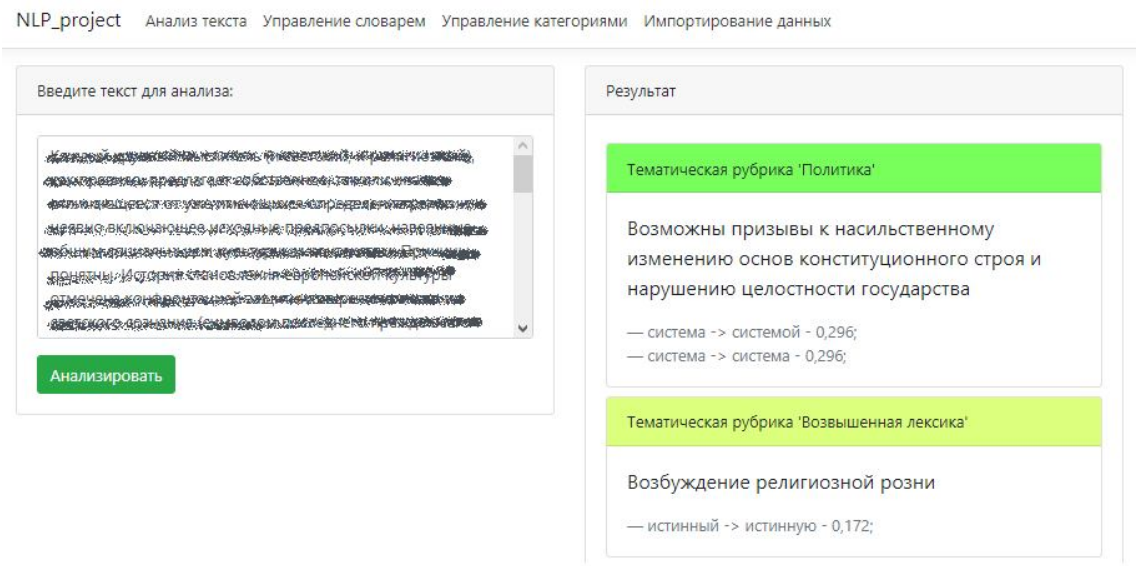


Рисунок 6 – Скриншот результатов работы программного продукта для семантического анализа текстовой информации

Особенность данного визуального представления результатов дает возможность анализирующему увидеть, наличие какого именно слова в тексте способствовало тому, что он был отнесен к той или иной смысловой категории, и самостоятельно принять решение о том, есть ли необходимость более детальной проверки подозрительного текста.

Заключение. Реализация предложенной ранее методики в виде web-сервиса дает возможность анализировать текстовую информацию на русском языке для определения ее семантической направленности. Автоматизация анализа текстовой информации позволяет экономить время на проведение сложной работы по определению семантической направленности полученной информации. Так как данное решение можно использовать для анализа любой текстовой информации, используя различные подготовленные экспертами категории, это позволит сэкономить бюджет различных компаний и государственных организаций за счет сокращения времени и затрат на услуги экспертов-лингвистов.

Библиографический список

1. Ажмухамедов И. М. Методы автоматизации анализа текстовой информации на русском языке с целью выявления ее семантической направленности / И. М. Ажмухамедов, Е. Е. Завьялова, В. Ю. Кузнецова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 2. – С. 118–126.

2. Батура Т. В. Методы автоматической классификации текстов / Т. В. Батура // Программные продукты и системы. – 2017. – № 1. – С. 3–6.

3. Епрев А. С. Автоматическая классификация текстовых документов / А. С. Епрев // Математические структуры и моделирование. – 2010. – № 21. – С. 65–81.

4. Ерхов Р. В. Преимущества разработки веб-приложения на платформе asp.net core / Р. В. Ерхов // Новые информационные технологии в научных исследованиях. – Рязань : Рязанский гос. радиотехнический ун-т, 2017. – С. 128–130.

5. Многофункциональный многоязычный словарь «Викисловарь». – Режим доступа: https://ru.wiktionary.org, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 02.08.2020).

6. Ожегов С. И. Толковый словарь русского языка: 100 000 слов, терминов и выражений / С. И. Ожегов ; под общ. ред. Л. И. Скворцова. – Москва : Мир и образование, 2015. – 1375 с.

7. Проект по созданию размеченного корпуса текстов «OpenCorpora». – Режим доступа: http://opencorpora.org, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 02.08.2020).

8. Сервис с открытым исходным для машинного обучения. – Режим доступа: https://www.tensorflow.org, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.08.2020).

9. Турдаков Д. Ю. Семантический анализ текстов с использованием системы Texterra / Д. Ю. Турдаков, И. А. Андрианов, Н. А. Астраханцев, В. Д. Майоров, Я. Р. Недумов, А. А. Сысоев, Д. Г. Федоренко. – Режим доступа: http://www.dialog-21.ru/digests/dialog2014/materials/pdf/TurdakovDY.pdf, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.08.2020).

10. Шарапов Н. Р. Архитектура технологии разработки веб-приложений asp.net core mvc / Н. Р. Шарапов // Вопросы науки и образования. – 2018. – № 13 – С. 30–31.

11. Юркин С. Ю. Авторизация и аутентификация пользователей в веб-приложениях на основе asp.net core identity / С. Ю. Юркин, Д. Е. Турчин // Сборник материалов IX Всероссийской научно-практической конференции молодых ученых с международным участием «Россия молодая» / Кузбасский гос. тех. ун-т имени Т.Ф. Горбачева. – Кемерово, 2017. – 420 с.

References

1. Azhmukhamedov I. M., Zavyalova Ye. Ye., Kuznetsova V. Yu. *Metody avtomatizatsii analiza tekstovoy informatsii na russkom yazyke s tselyu vyyavleniya ee semanticheskoy napravlennosti* [Methods for automating the analysis of textual information in Russian in order to identify its semantic orientation]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 2, pp. 118–126.

2. Batura T. V. Metody avtomaticheskoy klassifikatsii tekstov [Methods for automatic classification of texts]. *Programmnye produkty i sistemy* [Software products and systems], 2017, no. 1, pp. 3–6.

3. Eprev A. S. Avtomaticheskaya klassifikatsiya tekstovykh dokumentov [Automatic classification of text documents]. *Matematicheskie struktury i modelirovanie* [Mathematical structures and modeling], 2010, no. 21, pp. 65–81.

4. Erkhov R. V. Preimushchestva razrabotki veb-prilozheniya na platforme asp.net core [Advantages of developing a web application on the ASP.NET CORE platform]. *Novye informatsionnye tekhnologii v nauchnykh issledovaniyakh* [New information technologies in scientific research]. Ryazan, Ryazan State Radioengineering University, 2017, pp. 128–130.

5. *Mnogofunktsionalnyy mnogoyazychnyyslovar «Vikislovar»* [Multifunctional multilingual dictionary "Wiktionary"]. Available at: https://ru.wiktionary.org (accessed 02.08.2020).

6. Ozhegov S. I., Skvortsova L. I. (ed.) *Tolkovyy slovar russkogo yazyka: 100 000 slov, terminov i vyrazheniy* [Explanatory dictionary of the Russian language: 100,000 words, terms and expressions]. Moscow, Mir i obrazovanie Publ., 2015. 1375 p.

7. *Proekt po sozdaniyu razmechennogo korpusa tekstov «OpenCorpora»* [Project for the creation of a marked-up text corpus "Opensorpore"]. Available at: http://opencorpora.org (accessed 02.08.2020).

8. *Servis s otkrytym iskhodnym dlya mashinnogo obucheniya* [Open-source service for machine learning]. Available at: https://www.tensorflow.org (accessed 12.08.2020).

9. Turdakov D. Yu., Andrianov I. A., Astrakhantsev N. A., Mayorov V. D., Nedumov Ya. R., Sysoev A. A., Fedorenko D. G. *Semanticheskiy analiz tekstov s ispolzovaniem sistemy Texterra* [Semantic analysis of texts using the Texterra system]. Available at: http://www.dialog-21.ru/digests/dialog2014/materials/pdf/TurdakovDY.pdf (accessed 10.08.2020).

10. Sharapov N. R. Arkhitektura tekhnologii razrabotki veb-prilozheniy asp.net core mvc [Architecture of web application development technology asp.net mvc core]. *Voprosy nauki i obrazovaniya* [Issues of Science and Education], 2018, no. 13, pp. 30–31.

11. Yurkin S. Yu., Turchin D. E. Avtorizatsiya i autentifikatsiya polzovateley v veb-prilozheniyakh na osnove asp.net core identity [User authorization and authentication in web-based applications asp.net core identity]. *Sbornik materialov IX Vserossiyskoy nauchno-prakticheskoy konferentsii molodykh uchenykh s mezhdunarodnym uchastiem "Rossiya molodaya"* [Collection of Materials of the IX All-Russian Scientific and Practical Conference of Young Scientists with the International Participation "Rossiya molodaya"]. Kemerovo, 2017. 420 p.

DOI 10.21672/2074-1707.2021.53.1.018-027
УДК 004.4:004.62

РАЗРАБОТКА МОДУЛЯ УПРАВЛЕНИЯ ДАННЫМИ ОБ ОБЪЕКТАХ НА ОНЛАЙН-КАРТЕ ГОРОДА*

Статья поступила в редакцию 11.01.2021, в окончательном варианте – 29.01.2021.

Бурова Алена Алексеевна, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 28,
магистрант, e-mail: ata343@mail.ru
Буров Сергей Сергеевич, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 28,
магистрант, e-mail: sergey.burovic@gmail.com
Парыгин Данила Сергеевич, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 28,
кандидат технических наук, доцент, ORCID 0000-0001-8834-5748, e-mail: dparygin@gmail.com
Финогеев Антон Алексеевич, Пензенский государственный университет, 440026, Российская Федерация, г. Пенза, ул. Красная, 40,
кандидат технических наук, доцент, e-mail: fanton3@ya.ru
Рент Вячеслав Эдуардович, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. Ленина, 28,
магистрант, e-mail: vyacheslav61g@gmail.com

Решение широкого спектра задач, направленных на обеспечение устойчивого функционирования городской инфраструктуры, требует всестороннего прогнозирования развития ситуации. Работа распределенных технических систем в условиях урбанизированной территории непосредственно связана с множественными субъектно-объектными взаимодействиями, так как компоненты систем чаще всего расположены вблизи от практически непрерывной активности людей, имеющих отношение к их обслуживанию или занятых своей повседневной деятельностью. Поэтому построение точных моделей городских процессов зависит от обширной информационной базы об объектах инфраструктуры территории. В первую очередь это касается агрегирования и унификации данных разрозненных источников, а также последующей верификации, дополнения и обновления исходных данных. В статье описываются этапы разработки программного модуля управления данными, производящего парсинг данных из файла с форматом OSM XML, преобразующего их к необходимой структуре для работы в рамках единой платформы пространственного моделирования Live.UrbanBasis.com и производящего процедурную генерацию недостающих данных. Подход к генерации дополнительных данных по объектам инфраструктуры продемонстрирован на примере подъездов, этажей и квартир. В статье раскрываются подходы и технологии, примененные для работы с данными веб-картографического проекта OpenStreetMap.

Ключевые слова: OpenStreetMap, NetTopologySuite, объект инфраструктуры, пространственные данные, процедурная генерация, преобразование данных, онлайн-карта, город

DEVELOPMENT OF THE MODULE FOR DATA MANAGEMENT ON OBJECTS FOR ONLINE MAP OF A CITY

The article was received by the editorial board on 11.01.2021, in the final version – 29.01.2021.

Burova Alena A., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
post-graduate student, e-mail: ata343@mail.ru
Burov Sergey S., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
post-graduate student, e-mail: sergey.burovic@gmail.com
Parygin Danila S., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID 0000-0001-8834-5748, e-mail: dparygin@gmail.com
Finogeev Anton A., Penza State University, 40 Krasnaya St., Penza, 440026, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, e-mail: fanton3@ya.ru

* *Исследование выполнено в рамках гранта Российского научного фонда (РНФ, проект № 20-71-10087). Авторы выражают благодарность коллегам по лаборатории UCLab, особенно Русиновой Алле Викторовне за участие в разработке проекта Live.UrbanBasis.com.*

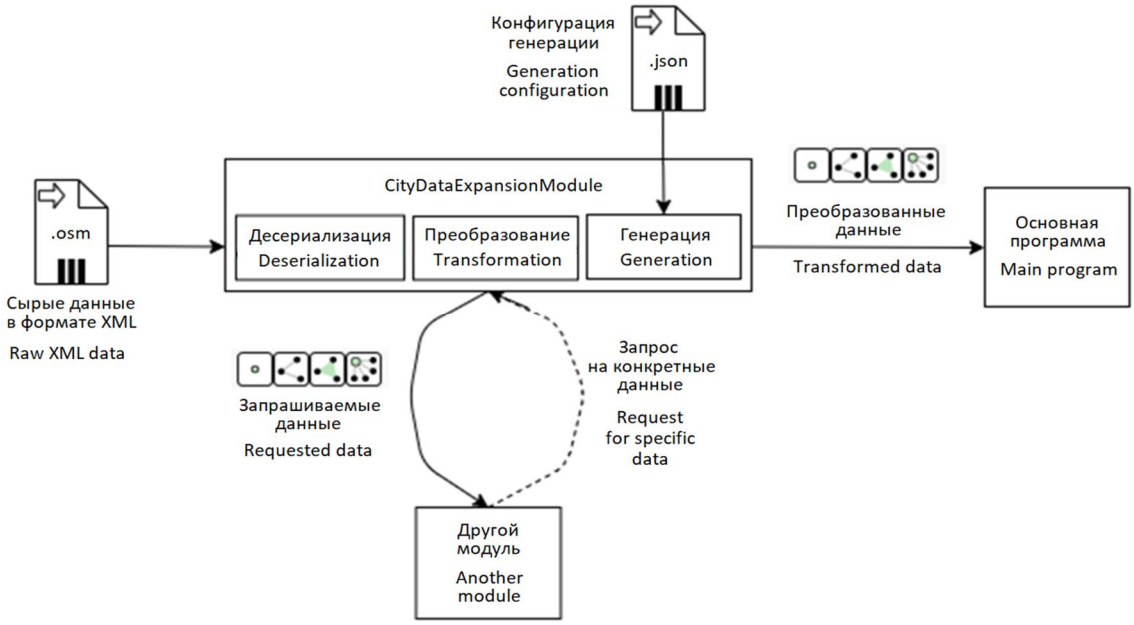
Rent Vyacheslav E., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,

post-graduate student, e-mail: vyacheslav61g@gmail.com

The solution of a wide range of tasks aimed at ensuring the sustainable functioning of urban infrastructure requires a comprehensive forecast of the development of the situation. The operation of distributed technical systems in an urbanized area is directly related to multiple subject-object interactions, since system components are most often located close to the almost continuous activity of people related to their maintenance, or just engaged in their daily routine. Therefore, the construction of urban processes models requires an extensive information base about the area infrastructure objects. First of all, this is associated with the aggregation and unification of data from disparate sources, and further verification, addition and updating of the original data is required. The paper describes the stages of development of a data management software module that parses data from a file with OSM XML format, transforms them into the necessary structure for working within a single spatial modeling platform Live.UrbanBasis.com and makes procedural generation of missing data. The approach to additional data generation of infrastructure objects is demonstrated using the example of entrances, floors, and apartments. The paper reveals the approaches and technologies used to work with the data of the OpenStreetMap web mapping project.

Keywords: OpenStreetMap, NetTopologySuite, infrastructure object, spatial data, procedural generation, data conversion, simulation, online map, city

Graphical annotation (Графическая аннотация)



Введение. Решение производственных задач различными учреждениями и организациями, обеспечивающими функционирование городской инфраструктуры, связано с учётом состояния и характеристик большого количества объектов территории [1]. Еще большую значимость имеет возможность оценивать их количественные и качественные изменения в результате их эксплуатации городским населением или обслуживания коммунальными службами. Для реализации такой предиктивной аналитики в лаборатории городских вычислений UCLab была создана клиент-серверная платформа OsmLifeSimulation (OSMLS) для моделирования перемещений и взаимодействий в рамках участка карты города [8]. Изначально программная система разрабатывалась с учётом потребностей служб управления транспортом, экологического мониторинга и управления отходами, однако в дальнейшем была расширена для учёта широкого спектра запросов потенциальных пользователей. Платформа получила возможность расширения функционала моделирования за счет подключаемых к ней модулей.

Связано это решение было также и с тем, что одной из проблем взаимодействия городских служб является множественность систем учёта информации, а также геоинформационных подоснов, используемых для работы с пространственными данными. Для нивелирования этих противоречий и снижения входного порога при создании собственных модулей было решено использовать в качестве картографической основы открытые данные проекта OpenStreetMap. Актуальные геоданные этого проекта поставляются в файле формата OSM XML.

В итоговой модели городских процессов стили отображаемых на карте объектов могут быть изменены отдельными модулями платформы [4]. Так как каждый модуль должен иметь возможность производить дополнительные действия с данными об объектах, то на этом этапе возникала необходимость структурирования данных для всех модулей системы. Исходный файл нуждался в парсинге и приведении полученных данных к новой структуре, совместимой с основной программой. При наличии в общей системе всего лишь нескольких отраслевых модулей, каждый из них мог решать эту задачу самостоятельно. Но при масштабировании платформы такая организация работы с данными становилась менее эффективной. В связи с этим целью представленного в данной статье исследования была выработка подхода к управлению данными об объектах городской инфраструктуры от их получения в источнике до генерации недостающей информации.

1. Анализ существующих подходов к работе с открытой базой картографических данных OpenStreetMap. OpenStreetMap (OSM) является некоммерческим веб-картографическим сервисом, поддерживающим множество данных об объектах инфраструктуры по всему миру. Для создания карт используются данные с персональных GPS-трекеров, аэрофотографии, видеозаписи, спутниковые снимки и панорамы улиц, предоставленные некоторыми компаниями, а также знания человека, рисующего карту [10].

Популярные сервисы с миллионами пользователей по всему миру используют данные OpenStreetMap в своих разработках. «Tesla Smart Summon», получившая широкое распространение в США, использует данные OSM для автономной навигации транспортных средств на парковках без водителя [11]. «Geotab» использует данные OpenStreetMap в своей платформе программного обеспечения для отслеживания транспортных средств MyGeotab [9]. Множество аналитических проектов и задач в сфере управления инфраструктурой реализуется основываясь на данных OSM [3].

Базовым элементом структуры данных OSM является точка (node) с географическими координатами – широтой (latitude) и долготой (longitude). Точка может быть отдельным объектом или входить в состав других объектов (линий, полигонов, мультиполигонов).

Линия (way) – это последовательности точек. Менять последовательность нельзя. Несколько линий логически могут представлять один объект. Например, длинная дорога состоит из нескольких линий.

Полигон – это замкнутая линия, у которой совпадают первая и последняя точки. Полигон не является самостоятельным элементом OSM.

Отношение – это логическое объединение точек, линий и других отношений в единый объект.

Каждый объект имеет набор тегов, описывающих его. Тег (tag) определён как k = «ключ» v = «значение». Если элемент не имеет тегов, то он не является объектом, а входит в состав других объектов, как и некоторые элементы с тегами.

В целом, всю структуру данных OSM можно представить схематично (рис. 1).

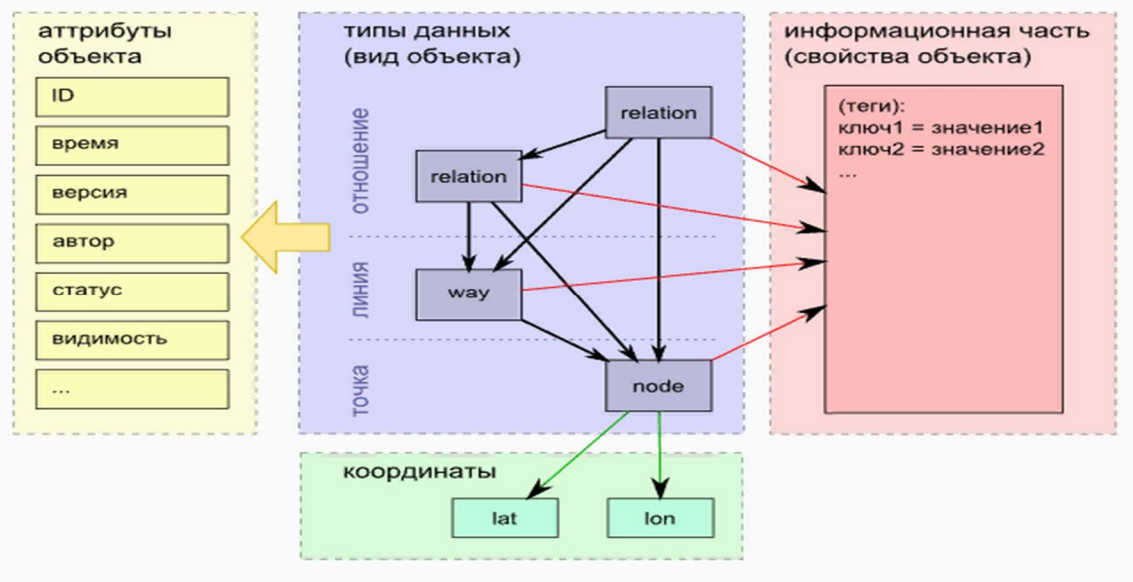


Рисунок 1 – Структура данных OpenStreetMap [5]

Все данные можно разбить на три группы:

1) типы данных (вид объекта) – основная группа, описывающая геометрические типы объектов на карте и их иерархию по отношению друг к другу, где основная единица точка (node) обязательно включает в себя координаты (lat, lon) и может входить во все остальные типы объектов;

2) атрибуты объектов – описывает формальные данные об авторах, времени добавления/правки, статусе, видимости, организует структуру типов объектов за счет присваивания к ним ID;

3) информационная часть (свойства объектов) – описательная группа, формирующая представление об объекте и его свойствах путем добавления определенных тегов к объекту.

Существует ряд решений для парсинга данных из osm-файла. Например, библиотека «BasicOSMParser» (доступна на GitHub в репозитории аккаунта PanierAvide/BasicOSMParser) – это набор классов Java, позволяющий анализировать необработанные XML-файлы OSM. Также библиотека позволяет экспортировать данные в виде файлов CSV. Он использует Java по умолчанию SAX parser (org.xml.sax). Тесты приложения используют платформу JUnit 4 framework.

Библиотека «osm4routing» (доступна на GitHub в репозитории аккаунта Tristramg/osm4routing) – инструмент, предоставляющий парсер данных из OpenStreetMap, чтобы превратить их в узлы-ребра, приспособлено для применений трассы. Входными данными является XML-файл OpenStreetMap. Выходными данными библиотеки могут быть CSV-файл или база данных (postgres, mysql, sqlite, postgis).

Библиотека «Libosmium» (доступна на GitHub в репозитории аккаунта osmcode/libosmium) – быстрая и гибкая библиотека C++ для работы с данными OpenStreetMap. Библиотека может прочитать OSM XML данные или в двоичном формате (PBF) и может вызывать различные обработчики для каждого OSM-объекта. Libosmium доступен под лицензией на программное обеспечение Boost.

Тем не менее существующие решения оказались не применимы к разрабатываемой платформе, так как соответствующие ее модули после парсинга из файла «.osm» принимают данные определенной структуры точек, линий и отношений, наследующихся от классов библиотеки NetTopologySuite (доступна на GitHub в репозитории аккаунта NetTopologySuite /NetTopologySuite).

2. Подход к подготовке данных для формирования среды моделирования городских процессов. Информационным обеспечением основной программы и других модулей является файл формата OSM XML (экспортированные данные участка карты OpenStreetMap). В основном файле содержится список экземпляров примитивных данных, таких как узлы, пути и отношения («nodes», «ways» и «relations»), а также их описание и связи.

Для корректной работы с коллекцией основной программы необходимо все полученные данные из файла приводить к структуре (точек, линий и отношений) при помощи библиотеки NetTopologySuite.

Коллекция основной программы MapObjects передается с сервера на клиент в формате GeoJSON. Для преобразования данных из объектов типа Geometry в GeoJSON используется GeoJsonWriter – средство библиотеки NetTopologySuite.

Соотношение структур полученных объектов из файла OSM XML и приведенных к структуре Geometry при помощи библиотеки NetTopologySuite представлено в таблице.

Таблица 1 – Соотношение структур объектов

Объект OSM XML	**Наследуемый объект NetTopologySuite.Geometries**
Точка (node)	Point
Линия (way)	LineString
Замкнутая линий (closed way)	LinearRing
Отношение (relation)	GeometryCollection

Для каждого из типов данных необходимо хранить его теги, описывающие объект карты и его свойства. Для типа «relation» помимо тегов необходимо хранить ещё и роль каждого из объектов.

Структура данных, которая должна быть получена после преобразования и использоваться в дальнейшем другими модулями и базовыми компонентами платформы, представлена на рисунке 2.

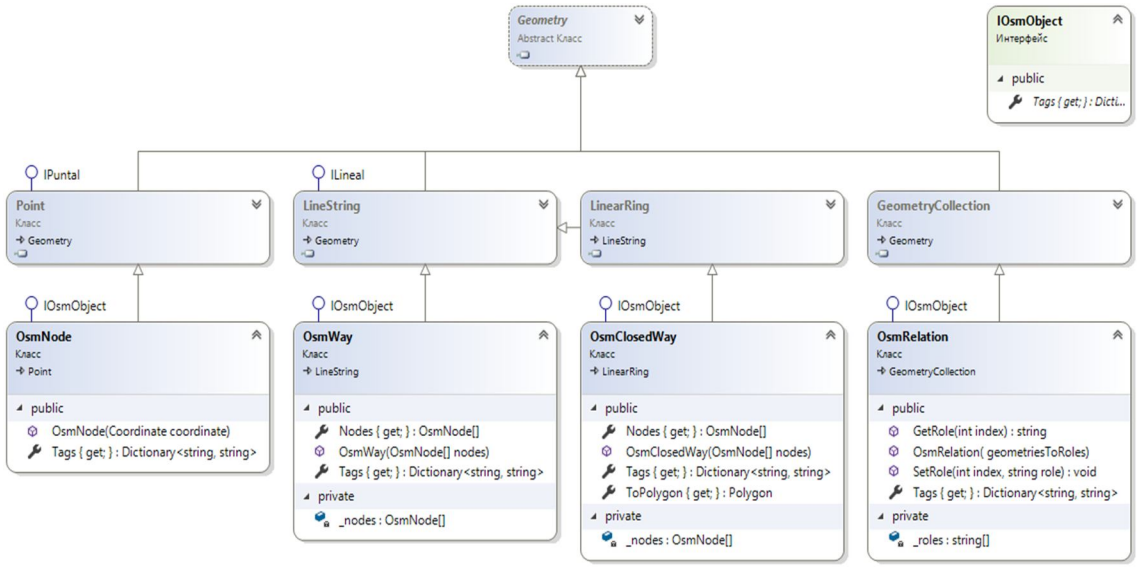


Рисунок 2 – Диаграмма классов OSM

В связи с этим программный модуль управления данными об объектах на онлайн-карте города должен соответствовать следующим требованиям: наследоваться от класса базового модуля; как и остальные модули, должен наследоваться от класса OSMLSModule и инициализироваться основной программой; производить парсинг данных из файла с форматом OSM XML, используя стандартные инструменты десериализации платформы DOT NET; преобразовывать полученные данные к новой структуре точек, линий и отношений при помощи библиотеки NetTopologySuite.

Кроме того, необходимо осуществлять процедурную генерацию недостающих данных (например, подъездов, этажей, квартир). Этих данных об объектах в исходном файле может быть недостаточно для дальнейшего моделирования процессов взаимодействия с объектами на карте города [2]. Генерация данных должна быть основана на данных конфигурации генерации, находящихся в файле «.json».

Помещать преобразованные и дополненные данные необходимо в коллекцию основной программы OSMLS. Основная программа хранит эти данные у себя в оперативной памяти и предоставляет их другим модулям. Выборка преобразованных данных (все замкнутые линии зданий, границы карты, все незамкнутые линии рельсовых путей и велодорожек) должна быть предоставлена по запросам другим модулям.

В общем виде всю работу данного модуля можно описать схемой, представленной в графической аннотации.

3. Реализация модуля управления данными об объектах инфраструктуры. Для реализации программного модуля в качестве интегрированной среды разработки программы была использована многофункциональная интегрированная среда разработки Microsoft Visual Studio 2017 community edition, позволяющая разрабатывать проекты для научных исследований или проекты с открытым исходным кодом.

Исходные коды программного модуля были реализованы на языке C# 7.3 с использованием модульной платформы .NET Core 2.1 [12]. Версия .NET Core 2.1. была обязательным условием для разработки модулей, в связи с требованием платформы.

Все объекты в программе наследуются от геометрических примитивов библиотеки NetTopologySuite версии 2.0.0.

3.1. Преобразование данных исходной базы. Класс OsmObjectsConverter реализует преобразование данных типа OsmXml, считанных из файла к коллекции osmObjects. Класс включает в себя функцию ConvertObjectsOSM(), которая, в первую очередь, находит и преобразует координаты границы используемой карты из классических Lat/Lon-координат в сферическую проекцию меркатора. Создает объект типа LinearRing с этими координатами.

Дальше идет основная часть работы класса, где поэтапно создаются словари OsmNode, OsmWays, OsmClosedWay и OsmRelations, где ключ – Id объекта, значение – преобразованный объект.

Словарь со значением типа OsmNode включает в себя преобразованные координаты (границы карты преобразуются, как и координаты) и теги для определенной точки.

Словари со значением типа OsmWays и OsmClosedWay отличаются лишь тем, что первая и последняя точка в OsmClosedWay должны быть одинаковы, когда в OsmWays они разные и не образуют замкнутую линию. В остальном OsmWays и OsmClosedWay образуются по одному принципу: из имеющегося словаря точек OsmNode берутся те, чьи Id (ключи словаря) совпадают со списком Id точек в OsmXml.Way и добавляются в словарь.

Словари со значением типа OsmRelations могут содержать в себе любые объекты: точки, линии и другие отношения. Следовательно, в отношениях указывается не только Id объекта, но и его тип (member.Type). Id текущего OsmRelations записывается в ключ словаря. По типу и Id объекта находится сам объект и добавляется в значение словаря.

После завершения преобразования все словари сливаются в один mapNodes, который возвращает данная функция. Отдельно возвращаются преобразованные данные о границах карты в виде полигона (Polygon).

3.2. Генерация дополнительных данных об инфраструктуре города. Также было выявлено, что для решения некоторых задач моделирования, связанных с объектами инфраструктуры, данных исходного файла может быть недостаточно. Для устранения этой проблемы необходима дополнительная генерация различных типов объектов, таких как подъезды, квартиры, строения и т.п. на основе существующих данных карты.

Для генерации недостающих данных квартир, этажей и подъездов используется класс OsmObjectsGenerator. В него подаются преобразованные данные osmObjects и данные конфигурации.

Данные конфигурации содержатся в объекте класса GeneratorConfiguration в следующих полях:

1) BuildingsTypesToLevelsCount – словарь, в котором ключ = количество этажей здания, значение = лист типов зданий, которые имеют данное количество этажей;

2) DefaultLevelsCount – дефолтное значение количества этажей, присваивается в случае, если тип здания не совпадает со значением из листа;

3) IsLevelsGenerationEnabled – отключает/включает генерацию этажей в зданиях;

4) BuildingsTypesToEntrancesCount – словарь, в котором ключ = количество подъездов в здании, значение = лист типов зданий, которые имеют данное количество подъездов;

5) DefaultEntrancesCount – дефолтное значение количества подъездов, присваивается в случае, если тип здания не совпадает со значением из листа;

6) IsEntrancesGenerationEnabled – отключает/включает генерацию подъездов в зданиях;

7) BuildingsTypesToFlatsCount – словарь, в котором ключ = количество квартир в здании, значение = лист типов зданий, которые имеют данное количество квартир;

8) DefaultFlatsCountForEveryEntranseLevels – дефолтное значение количества квартир в здании, присваивается в случае, если тип здания не совпадает со значением из листа;

9) IsFlatsGenerationEnabled – отключает/включает генерацию квартир в зданиях.

Данные конфигурации берутся из файла generatorConfig.json [6], если он существует. Если программа не может найти файл, она создает новый файл с дефолтными значениями для генерации. Конфигурация может задаваться или обновляться самим пользователем через файл.

При генерации этажей учитывается тип зданий. Если тип здания или данные конфигурации для такого типа здания не указаны, то берется значение этажности соседнего здания. В случае если в соседних зданиях этажность не указана или здания не были найдены, то берется дефолтное значение количества этажей.

Генерация подъездов исходит не из площади, а из длины фасада здания. Берется самый длинный из фасадов для дальнейшей генерации. Подъезды генерируются на одинаковом друг от друга расстоянии. При генерации подъездов зданий учитывается тип зданий. Если тип здания или данные конфигурации для такого типа здания не указаны, то берется дефолтное значение количества подъездов.

Для вычисления расположения точек-подъездов на линии фасада здания использовалась формула деления отрезка в данном отношении на плоскости $xM = (xA + \lambda \cdot xB) / (1 + \lambda)$ и $yM = (yA + \lambda \cdot yB) / (1 + \lambda)$, где A(xA; yA) и B(xB; yB) являются точками плоскости, а точка M(xM; yM) делит отрезок AB в отношении $\lambda = AM / MB$.

Генерация количества квартир в здании происходит в случае, если для здания указано количество подъездов и этажей. Генерация квартир в доме происходит по формуле «количество квартир на этаже * количество подъездов * количество этажей», где значение количества квартир на этаже берется по типу здания из конфигурации. Если тип здания или данные конфигурации для такого типа здания не указаны, то берется дефолтное значение количества квартир на этаже.

Наглядно результат работы генерации подъездов можно увидеть на рисунке 3, где точками обозначаются подъезды, а здания выделяются рамками. На рисунке 3 слева видно, что в исходном файле до генерации подъездов очень мало и они охватывают не все дома на карте. После генерации (рис. 3, справа) многие здания уже имеют подъезды, расположенные вдоль фасадов.

Рисунок 3 – Отображение подъездов на карте до генерации (слева) и после генерации (справа)

3.3. Тестирование работы модуля с данным для онлайн-карты. Для интеграционного тестирования [7] работы программного модуля был создан отдельный модуль CityDataExpansionTestModule, который должен со стороны другого модуля показать работу с предоставляемыми данными модуля CityDataExpansionModule. Данный модуль обращается к коллекции основной программы и глобальным переменным (AllBuildings, AllRailways, AllCycleways, MapBorders) модуля CityDataExpansionModule для дальнейшего отображения этих данных на карте с помощью инструментов основной программы.

Для отображения магазинов на онлайн-карте города были взяты объекты из коллекции основной программы OSMLS и из них выбраны объекты с тегом «shop». Для изменения отображения точек магазинов был создан класс «Shop», в котором был прописан стиль точки (красная непрозрачная точка). Также в стиле можно изменить цвет точки, ее границы, ширину и даже добавить ссылку на изображение, которое будет отображаться вместо точки.

Для отображения границы участка карты, с объектами которой сейчас работает модуль, достаточно обратиться к глобальной переменной MapBorders в модуле CityDataExpansionModule и просто вывести полигон с помощью инструмента основной программы.

Для вывода зданий тоже достаточно просто обратиться к глобальной переменной AllBuildings в модуле CityDataExpansionModule. Также эти данные можно взять из коллекции основной программы. Объекты представляют собой замкнутые линии с тегом «building» и могут включать в себя точки-подъезды с тегом «entrance».

На рисунке 4 отображены объекты зданий, магазинов и границы моделируемой области на онлайн-карте города, вывод которых был описан выше.

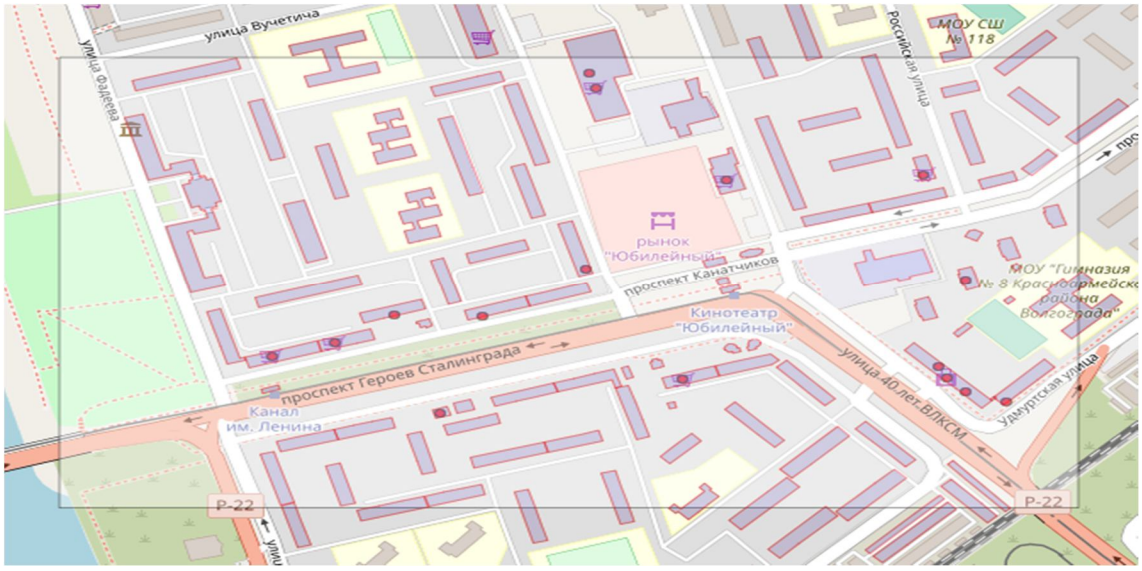


Рисунок 4 – Пример отображения данных на карте

Также можно отобразить все дороги на выбранном участке карты. Из коллекции основной программы берутся все линии (OsmWay), имеющие тег «highway». Для изменения стиля был создан класс «Roads» для отображения дорог в виде синей линии с шириной 3 пикселя.

После данные выводятся на участок карты (рис. 5). Для наглядного представления дорог было отключено отображение всех других объектов и оставлены лишь границы карты.

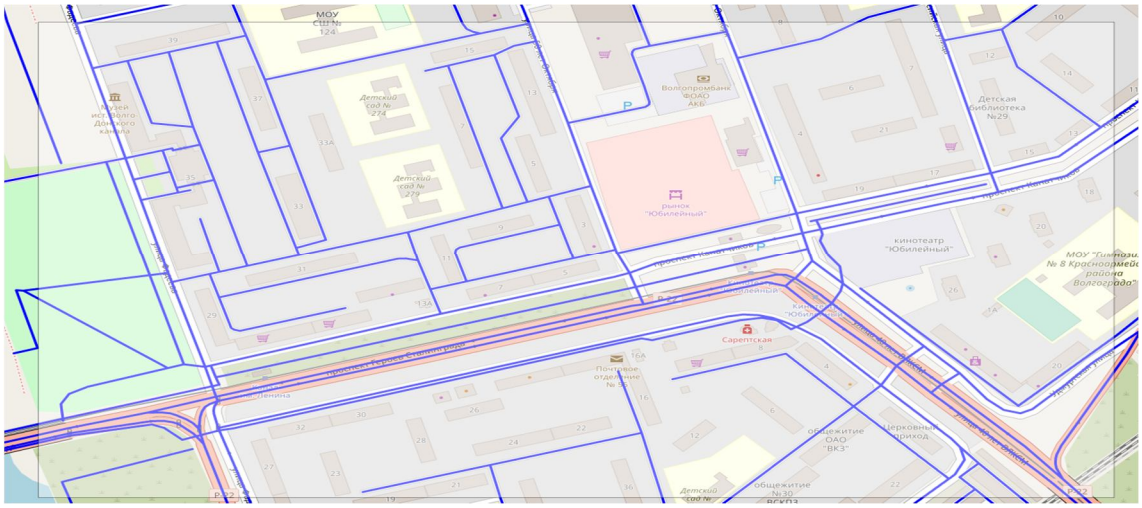


Рисунок 5 – Отображение дорог на выбранном участке карты

На рисунках можно заметить, что некоторые объекты, с которыми работает модуль, выходят за границу области карты, с которой ведется работа. Такой результат получается за счет того, что во время экспорта участка карты с OpenStreetMap объекты, которые лишь наполовину вошли в область экспорта, берутся полностью и со всеми тегами.

Заключение. В результате проведенной работы были сформулированы проблемы работы с открытыми картографическими данными. Сформирован подход к управлению данными в рамках платформы для моделирования городских процессов. Спроектирован и реализован программный модуль управления данными об объектах на онлайн-карте города.

Для реализации программного модуля в качестве интегрированной среды разработки программы была использована Microsoft Visual Studio 2017 community edition, позволяющая разрабатывать проекты для научных исследований или проекты с открытым исходным кодом. Это особенно важно в условиях развития проекта, предполагающего возможность создания специализированных модулей для моделирования отдельных процессов в городской среде силами обособленных разработчиков в учреждениях и организациях муниципальных образований.

Кроме того, в процессе исследования качества открытых геоданных была выявлена проблема их неполноты. В целях решения данной проблемы был предложен подход к генерации различных типов объектов инфраструктуры. В этом же направлении предполагается в дальнейшем проводить исследования и совершенствовать информационную базу платформы. Для этого планируется использовать нейросетевые модели обработки данных дистанционного зондирования Земли. Они позволят с необходимой регулярностью обновлять и дополнять информацию по территориям мониторинга и моделирования, а также станут основой для более точной генерации данных в местах с отсутствующими исходными источниками.

Библиографический список

1. Алешкевич А. А. Оценка доступности территории города / А. А. Алешкевич // XXII Региональная конф. молод. ученых Волгоградской области. Волгоград, 21–24 нояб. 2017 г. : тезисы докл. – Волгоград, 2017. – С. 210–211.

2. Архипова А. С. Визуализация поведения акторов в модели города / А. С. Архипова // Конкурс научно-исследовательских работ студентов Волгоградского государственного технического университета. Волгоград, 19–22 мая 2020 г. : тезисы докл. – Волгоград, 2020. – С. 175–176.

3. Зеленский И. С. Интеллектуальная поддержка решений по использованию объектов недвижимости для управления урбанизированными территориями / И. С. Зеленский, Д. С. Парыгин, О. В. Савина, А. А. Финогеев, А. А. Шуклин, А. Ю. Антюфеев // International Journal of Open Information Technologies. – 2020. – Т. 8, № 11. – С. 13–29.

4. Анохин А. О. Моделирование поведения агентов для реализации игрового искусственного интеллекта / А. О. Анохин, Н. П. Садовникова, А. В. Катаев, Д. С. Парыгин // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 2 (50). – С. 85–99. – DOI: 10.21672/2074-1707.2020.50.2.096-110.

5. Структура данных проекта OpenStreetMap. – 2020. – Режим доступа: https://habr.com/ru/post/146503/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 01.05.20).

6. How to serialize and deserialize (marshal and unmarshal) JSON in .NET. – 2020. – Режим доступа: https://docs.microsoft.com/en-us/dotnet/standard/serialization/system-text-json-how-to#additional-resources, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 21.04.20).

7. Integration tests in ASP.NET Core. – 2020. – Режим доступа: https://docs.microsoft.com/en-us/aspnet/core/test/integration-tests?view=aspnetcore-3.1, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 23.04.20).

8. Parygin D. Multi-agent Approach to Modeling the Dynamics of Urban Processes (on the Example of Urban Movements) / D. Parygin, A. Usov, S. Burov, N. Sadovnikova, P. Ostroukhov, A. Pyannikova // Communications in Computer and Information Science. – 2020. – Vol. 1135. – P. 243–257. – DOI : 10.1007/978-3-030-39296-3_18.

9. MyGeotab. – 2020. – Режим доступа: https://www.geotab.com/blog/smart-fleet-management-road-speed-information/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 10.12.20).

10. OpenStreetMap. – 2020. – Режим доступа: https://www.openstreetmap.org/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.11.20).

11. Tesla Smart Summon. – 2020. – Режим доступа: https://teslamotorsclub.com/tmc/threads/openstreetmaps-and-smart-summon.170675/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 15.12.20).

12. What's new in .NET Core. – 2020. – Режим доступа: https://docs.microsoft.com/en-us/dotnet/core/whats-new/dotnet-core-2-1, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.04.20).

References

1. Aleshkevich A. A. Otsenka dostupnosti territorii goroda [Urban area accessibility assessment]. *Tezisy dokladov XXII Regionalnoy konferentsii molodykh uchenykh Volgogradskoy oblasti* [Abstracts of the XXII Regional Conference of Young Scientists of the Volgograd Region], Volgograd, 21–24 November 2017. Volgograd, 2017, pp. 210–211.

2. Arkhipova A. S. Vizualizatsiya povedeniya aktorov v modeli goroda [Visualization of actor's behavior in a city model]. *Tezisy dokladov konkursa nauchno-issledovatel'skikh rabot studentov Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta* [Abstracts of the competition of research works of students of Volgograd State Technical University], Volgograd, 19–22 May 2020. Volgograd, 2020, pp. 175–176.

3. Zelenskiy I. S., Parygin D. S., Savina O. V., Finogeev A. A., Shuklin A. A., Antyufeev A. Yu. Intellektualnaya podderzhka resheniy po ispolzovaniyu obektov nedvizhimosti dlya upravleniya urbanizirovannymi territoriyami [Intelligent Support to Real Estate Use Decisions for Urbanized Areas Management]. *International Journal of Open Information Technologies*, 2020, vol. 8, no. 11, pp. 13–29.

4. Anokhin A. O., Sadovnikova N. P., Kataev A. V., Parygin D. S. Modelirovaniye povedeniya agentov dlya realizatsii igrovogo iskusstvennogo intellekta [Modeling of agent's behavior to implement gaming artificial intelligence]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 2 (50), pp. 85–99. DOI: 10.21672/2074-1707.2020.50.2.096-110.

5. *Struktura dannykh proyekta OpenStreetMap* [Data structure of the OpenStreetMap project]. Available at: https://habr.com/ru/post/146503/ (accessed 01.05.20).

6. *How to serialize and deserialize (marshal and unmarshal) JSON in .NET*. Available at: https://docs.microsoft.com/en-us/dotnet/standard/serialization/system-text-json-how-to#additional-resources (accessed 21.04.20).

7. *Integration tests in ASP.NET Core*. Available at: https://docs.microsoft.com/en-us/aspnet/core/test/integration-tests?view=aspnetcore-3.1 (accessed 23.04.20).

8. Parygin D., Usov A., Burov S., Sadovnikova N., Ostroukhov P., Pyannikova A. Multi-agent Approach to Modeling the Dynamics of Urban Processes (on the Example of Urban Movements). *Communications in Computer and Information Science*, 2020, vol. 1135, pp. 243–257. DOI: 10.1007/978-3-030-39296-3_18.

9. *MyGeotab*. Available at: https://www.geotab.com/blog/smart-fleet-management-road-speed-information/ (accessed 10.12.20).

10. *OpenStreetMap*. Available at: https://www.openstreetmap.org/ (accessed 28.11.20).

11. *Tesla Smart Summon*. Available at: https://teslamotorsclub.com/tmc/threads/openstreetmaps-and-smart-summon.170675/ (accessed 15.12.20).

12. *What's new in .NET Core*. Available at: https://docs.microsoft.com/en-us/dotnet/core/whats-new/dotnet-core-2-1 (accessed 28.04.20).

УДК 004.832.2

К ВОПРОСУ О ПОДДЕРЖКЕ ПРОЦЕССА ПРИНЯТИЯ РЕШЕНИЯ ОБ УЛУЧШЕНИИ ДЕЯТЕЛЬНОСТИ В ИСПЫТАТЕЛЬНОЙ ЛАБОРАТОРИИ

Статья поступила в редакцию 29.10.2020, в окончательном варианте – 12.11.2020.

Аль-Бусаиди Саид Султан Саид, Тамбовский государственный технический университет, 392000, Российская Федерация, г. Тамбов, ул. Советская, 106,

аспирант, ORCID: www.orcid.org/0000-0003-3990-8123, e-mail: al-busaidi2020@hotmail.com

Воякина Юлия Николаевна, Тамбовский государственный технический университет, 392000, Российская Федерация, г. Тамбов, ул. Советская, 106,

магистрант, ORCID: www.orcid.org/0000-0003-1654-4232, e-mail: miss.voyakina2011 @yandex.ru

Пономарев Сергей Васильевич, Тамбовский государственный технический университет, 392000, Российская Федерация, г. Тамбов, ул. Советская, 106,

доктор технических наук, профессор, ORCID: www.orcid.org/0000-0003-0228-912X, e-mail: svponom@yahoo.com

Рассмотрены вопросы поддержки процесса принятия решения с применением функций принадлежности на основе нормального закона распределения Гаусса. Обсуждаются рекомендации по осуществлению процедурной модели для определения параметров функций принадлежности путем статистической обработки результатов, полученных в процессе работы экспертной группы. Приведен пример применения разработанной процедурной модели при оценке показателя «Приоритетное число возможности улучшения» (по результатам работы экспертной группы) при подготовке принятия решения по улучшению деятельности в испытательной лаборатории.

Ключевые слова*:* экспертные оценки, статистическая обработка, доверительный интервал, функции принадлежности: трапециевидные, треугольные, гауссова типа, определение параметров, поддержка принятия решений

TO THE QUESTION OF SUPPORTING THE DECISION-MAKING PROCESS ON PERFORMANCE IMPROVEMENT IN THE TESTING LABORATORY

The article was received by the editorial board on 29.10.2020, in the final version – 12.11.2020.

Al-Busaidi Said SultanSaid, Tambov State Technical University, 106 Sovetskaya St., Tambov, 392000, Russian Federation,

post-graduate student, ORCID: www.orcid.org/0000-0003-3990-8123, e-mail: al-busaidi2020@hotmail.com

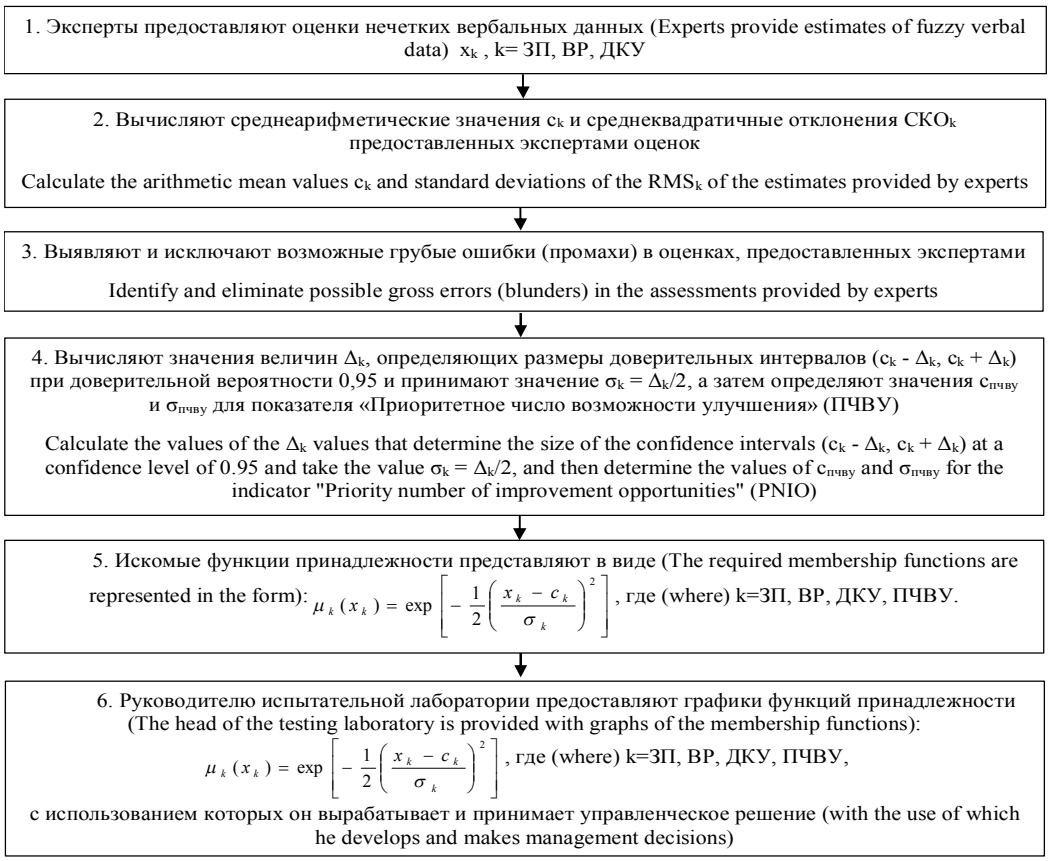
Voyakina Yuliya N., Tambov State Technical University, 106 Sovetskaya St., Tambov, 392000, Russian Federation,

undergraduate student, ORCID: www.orcid.org/0000-0003-1654-4232, e-mail: miss.voyakina2011 @yandex.ru

Ponomarev Sergey V., Tambov State Technical University, 106 Sovetskaya St., Tambov, 392000, Russian Federation,

Doct. Sci. (Engineering), Professor, ORCID: www.orcid.org/0000-0003-0228-912X, e-mail: svponom@yahoo.com

Graphical annotation (Графическая аннотация)



Введение. При осуществлении деятельности в системе менеджмента (СМ), сертифицированной по требованиям стандарта ГОСТ ISO/IEC 17025-2019 [1], руководители подразделений испытательной лаборатории (ИЛ) – в рамках процесса «8.6 Улучшение» [1] – регулярно подают генеральному директору ИЛ заявки на финансирование проектов улучшения работ в своих подразделениях. Нередко бывает так, что при поступивших заявках на выполнение 7–8 проектов улучшения у генерального директора (лица, принимающего решение (ЛПР)) имеются средства на финансирование только одной или двух заявок. В таких случаях генеральный директор по требованиям процесса «8.5 Действия, связанные с рисками и возможностями» [1] обычно создает экспертную группу с целью определения того, какому из заявленных проектов улучшения следует в первую очередь выделить финансовые и/или материальные средства.

Перспективными вариантами сравнения результативности и эффективности рассматриваемых проектов улучшения является использование широко известной FMEA-методологии [2–6] (от английских слов «Failure Mode Effect Analysis», что на русский язык можно перевести в виде «Анализ последствий режима отказа») либо недавно предложенной IOMEA-методологии [7–9] (от английских слов «Improvement Opportunity Mode Effect Analysis» или «Анализ последствий режима возможного улучшения»). В случае использования IOMEA-методологии, генеральный директор ИЛ обычно требует наглядно представить результаты работ экспертной группы, например, в виде графических материалов, иллюстрирующих результаты работы экспертов.

В испытательных лабораториях (ИЛ), внедривших систему менеджмента (СМ) по требованиям [1], при поддержке процессов принятия решений (с использованием IOMEA-методологии) широко применяют методы наглядной иллюстрации результатов работы экспертных групп в виде графиков функций принадлежности (ФП) треугольной и/или трапециевидной формы [10]. При этом неясным остается вопрос о том, каким образом следует определять параметры таких ФП (особенно параметры так называемого «спреда», характеризующего разброс ФП относительно среднего значения) по результатам работы экспертной группы.

В последнее время все чаще находят применение ФП в виде колоколообразных кривых, обычно задаваемые на основе нормального закона распределения Гаусса [11–14]. Скорее всего, это обусловлено следующим обстоятельством: «Гауссова ФП является уникальной с той точки зрения, что при ее использовании наиболее просто решаются задачи определения двух основных параметров, определяющих как среднее значение ФП, так и величину «спреда», характеризующего размах ФП относительно среднего значения [12]». В статье [14] достаточно подробно рассмотрены вопросы, связанные с выбором между ФП трапециевидного и Гауссова типа. Мы согласны с мнением автора статьи [14] о том, что ФП Гауссова типа во многих случаях являются предпочтительными по сравнению с трапециевидными или треугольными ФП.

Апробированная в испытательной лаборатории ФГБОУ ВО ТГТУ процедурная модель предусматривает выполнение следующих действий:

1) в результате работы экспертов (путем использования, например, десятибалльных нечетких шкал, применяемых в процессах FMEA-анализа [2–6] или IOMEA-анализа [7–9]) появляются количественные оценки x_i нечетких (вербальных) данных и к ним применяются известные методы статистической обработки [15–17];

2) вычисляют среднее арифметическое значение c и среднеквадратичные отклонения (СКО) предоставленных экспертами данных;

3) выявляют и исключают возможные промахи в оценках, предоставленных экспертами;

4) с использованием распределения Стьюдента вычисляют значение величины Δ, определяющее размер доверительного интервала ($c - \Delta$; $c + \Delta$) для среднего арифметического значения c предоставленных экспертами оценок и принимают значение параметра $\sigma = \Delta/2$; именно этот параметр σ определяет так называемый «спред» ФП;

5) искомую ФП представляют в виде

$$\mu(x) = \exp\left[-\frac{1}{2}\left(\frac{x-c}{\sigma}\right)^2\right]. \quad (1)$$

1. Основные виды функций принадлежности, применяемые при поддержке процесса принятия управленческого решения. В настоящее время при практическом использовании методов информационной поддержки процесса выработки проектов управленческих решений наиболее часто применяют следующие виды ФП:

- ФП треугольной формы [10, 11, 14, 18] (рис. 1а):

$$\mu(x;a,b,c) = \begin{cases} 0, \text{ если } x \le a, \\ (x-a)/(b-a), \text{ если } a < x \le b, \\ (c-x)/(c-b), \text{ если } b < x \le c, \\ 0, \text{ если } x > c, \end{cases} \quad (2)$$

где a, b, c – параметры, определяющие узловые точки ФП треугольной формы;

- ФП трапециевидной формы [10, 14, 18] (рис. 1б):

$$\mu(x;a,b,c,d) = \begin{cases} 0, \text{ если } x \le a, \\ (x-a)/(b-a), \text{ если } a < x \le b, \\ 1, \text{ если } b < x \le c, \\ (d-x)/(d-c), \text{ если } c < x \le d, \\ 0, \text{ если } x > d, \end{cases} \quad (3)$$

где a, b, c, d – параметры, определяющие узловые точки ФП трапециевидной формы;

- ФП в виде колоколообразных кривых [11–14, 18–23] (рис. 1в):

$$\mu(x;c,\sigma) = \exp\left[-\frac{1}{2}\left(\frac{x-c}{\sigma}\right)^2\right], \quad (4)$$

где c – параметр, определяющий значение абсциссы максимального значения ФП (4); σ – параметр, определяющий так называемый «спред» ФП (4).

Следует отметить, что возможно использование функций принадлежности, например, S-образной формы [18] (рис. 1г):

$$S(x;a,b,c) = \begin{cases} 0, \text{ если } x \le a, \\ 2[(x-a)/(b-a)]^2, \text{ если } a < x \le b, \\ 1-2[(x-a)/(b-a)]^2, \text{ если } b < x \le c, \\ 0, \text{ если } x > c, \end{cases} \quad (5)$$

где a, b, c – параметры, определяющие конфигурацию ФП S-образной формы, причем b = (a+c)/2, а также и других форм, которые рассмотрены в [11, 18–23].

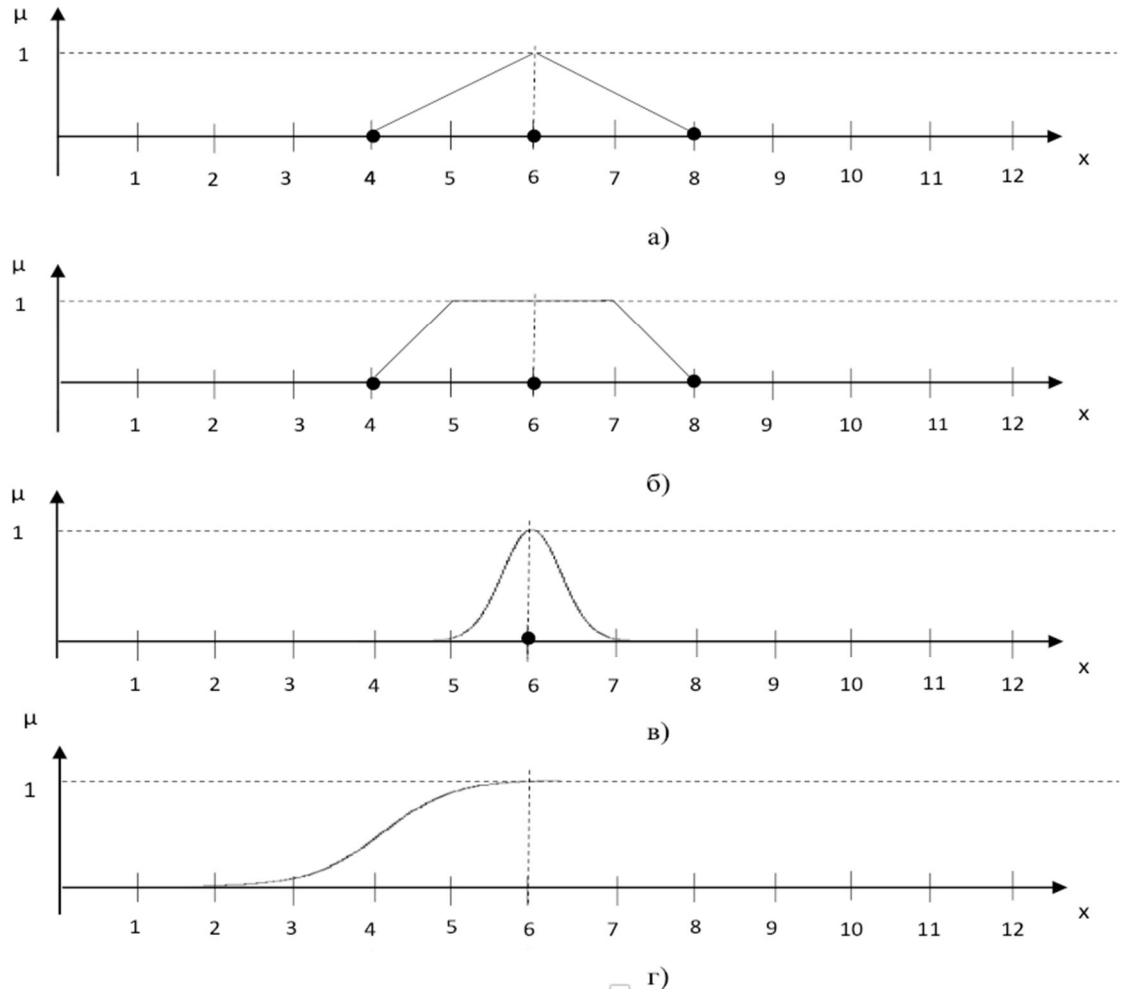


Рисунок 1 – Типичные формы функций принадлежности: а) треугольные; б) трапециевидные; в) Гауссова типа в виде колоколообразных кривых; г) в виде S-образной кривой

В статье [14] детально рассмотрены двенадцать соображений о свойствах ФП, определяющих выбор между трапециевидными и Гауссовыми ФП в качестве предпочтительного вида функции принадлежности, а именно:

1) представительность (способность отобразить имеющиеся данные);
2) конструирование (определение параметров по наблюдающимся данным);
3) оптимальность для целей решения задач подготовки принятия решений и последующего управления;
4) адаптивность к рассмотрению многообразных задач;
5) полезность для достижения инновационных целей;
6) аналитическая структура;
7) непрерывность и, желательно, гладкость;
8) монотонность на основных участках области определения;
9) стабильность при решении задач;
10) робастность (нечувствительность к небольшим изменениям входных данных);
11) невысокие затраты времени при вычислениях на компьютерах;
12) работоспособность при использовании в системе управления.

Автор статьи [14] считает, что функции принадлежности Гауссова типа проще по конструкции, их легче представлять и оптимизировать, они всегда непрерывны и гладки. Однако трапециевидные ФП проще в анализе [14].

По нашему мнению, главным достоинством ФП Гауссова типа является то, что значительно более понятно, каким образом можно определить их параметры по имеющимся данным, например, по предоставленным командой экспертов оценкам, полученным с применением квалиметрических шкал.

2. Опыт применения экспертных методов при оценке значений показателей в виде нечетких чисел с функциями принадлежности треугольной формы с применением десятибалльных квалиметрических шкал [7].

Разработанный нами подход к применению экспертных методов при оценке значений показателей в виде нечетких чисел с функциями принадлежности треугольной формы (с применением десятибалльных квалиметрических шкал [7, 8]) ранее был подробно рассмотрен в статье [9].

Предложенные в статье [7] десятибалльные квалиметрические шкалы для перехода от предоставленных экспертами вербальных оценок к балльным оценкам частных показателей-концептов:

1. «Значимость положительных последствий ЗП предлагаемого улучшения».

2.«Вероятность реализации ВР предлагаемого улучшения».

3. «Доступность (легкость) контроля и управления ДКУ процессами после внедрения предлагаемого улучшения», приведены в этой статье [7] в виде таблицы.

В результате работы каждого *i*-го эксперта, входящего в составы команды из *m* экспертов, чаще всего получаются целочисленные значения балльных оценок частных показателей-концептов $ЗП_i$, $ВР_i$ и $ДКУ_i$*(i*= 1,…,m*)*. Однако при агрегировании предоставленных экспертами только целочисленных оценок частных показателей-концептов $ЗП_i$, $ВР_i$ и $ДКУ_i$ (с применением аддитивной свертки, рассмотренной в [9]), чаще всего получаются дробные значения усредненных балльных оценок частных показателей-концептов $\overline{ЗП}$, $\overline{ВР}$ и $\overline{ДКУ}$.

В работе [9], с целью повышения достоверности получаемых интегральных оценок индикатора возможности улучшения деятельности в виде приоритетного числа возможности улучшения $\overline{ПЧВУ}$, подсчитываемого по формуле

$$\overline{ПЧВУ} = \overline{ВР} \cdot \overline{ЗП} \cdot \overline{ДКУ}, \qquad (6)$$

усредненным балльным оценкам частных показателей-концептов $\overline{ЗП}$, $\overline{ВР}$, $\overline{ДКУ}$ и $\overline{ПЧВУ}$ ставятся в соответствие нечеткие числа (НЧ) с функциями принадлежности треугольной формы, примерный вид которых приведен на рисунке 2.

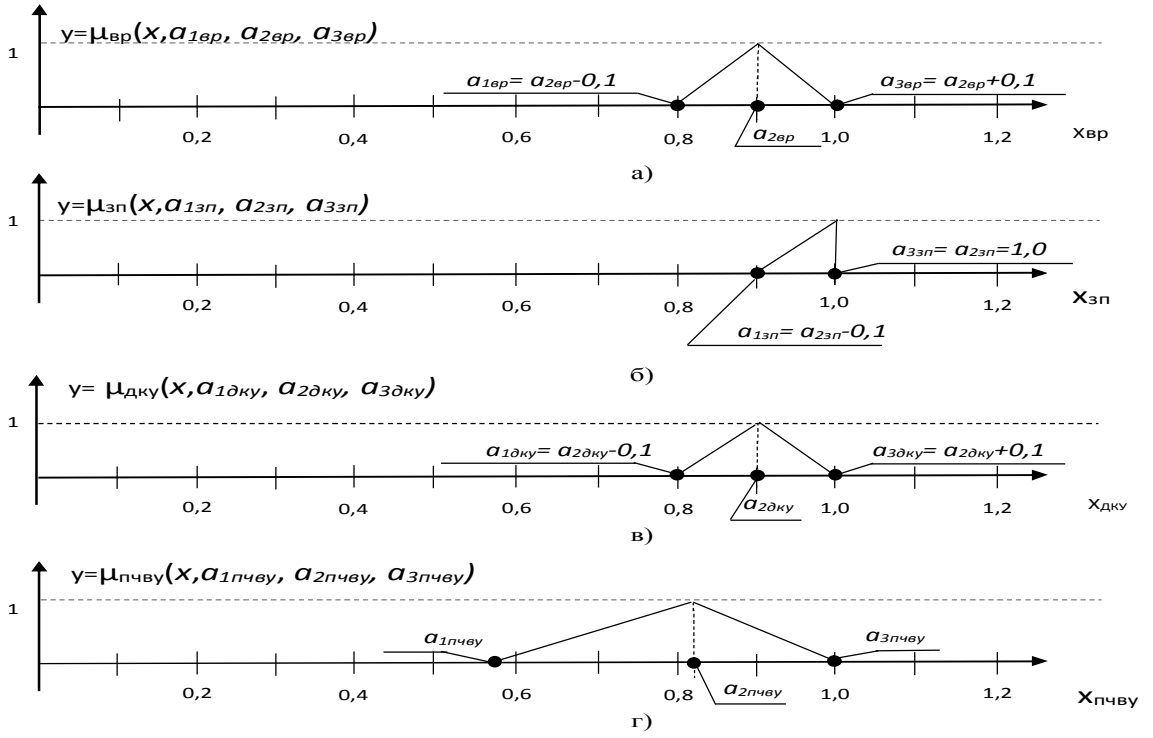


Рисунок 2 – Параметры функций принадлежности треугольных нечетких чисел, используемых для представления результатов формализации вербальных оценок экспертов в виде усредненных балльных оценок частных показателей-концептов: а – для $x_{вр}$; б – для$x_{зп}$; в – для $x_{дку}$; *г* – для $x_{пчву}$

На каждом графике (рис. 2а, б, в, г) под аргументами хвр, хзп, хдкуихпчву понимаются безразмерные величины: хвр =$\overline{ВР}$ / ВРmax, хзп =$\overline{ЗП}$ / ЗПmax, хдку =$\overline{ДКУ}$ / ДКУmахихпчву = $\overline{ПЧВУ}$/ ПЧВУmax, где ВРmax = ЗПmax = ДКУmax = 10, а значение ПЧВУmax = 1000, так как в соответствии с [7] ПЧВУmax = ВРmax · ЗПmax · ДКУmax.

Из рисунка 2а, б, в видно, что максимальные значения каждой функции принадлежности (ФП), соответствующие полученным усредненным балльным оценкам $\overline{ВР}$, $\overline{ЗП}$ и $\overline{ДКУ}$ частных показателей-концептов *а2вр,, а2зп , а2дку* и *а2пчву* , равны единице, а величины отклонения основания каждой треугольной ФП (от абсцисс максимальных значений ФП) были приняты в статье [9] численно равными 0,1 единиц аргументов *хвр, хзп, хдку* и *хпчву*. Отметим, что в работе [9] при *а2вр, а2зп* и *а2дку* более *0,9*, значения правых абсцисс оснований ФП задаются в виде *а3вр = 1,0, а3зп = 1,0, а3дку = 1,0*. Причем в работе [9] значения параметров *а1пчву, а2пчву, а3пчву* функции принадлежности треугольного нечеткого числа $\overline{ПЧВУ}$ вычисляли по формулам:

$$a1пчву = a1вр \cdot a1зп \cdot a1дку, \quad (7)$$

$$a2пчву = a2вр \cdot a2зп \cdot a2дку, \quad (8)$$

$$a3пчву = a3вр \cdot a3зп \cdot a3дку. \quad (9)$$

Приведенный в [9] подход к представлению результатов работы экспертной группы (в виде нечетких чисел с треугольными функциями принадлежности) при поддержке процесса принятия управленческого решения руководителем ИЛ (лицом, принимающим решение (ЛПР)) позволяет достаточно просто находить параметры *а1вр, а2вр, а3вр, а1зп, а2зп, а3зп, а1дку, а2дку, а3дку, а1пчву, а2пчву, а3пчву* треугольных функций принадлежности, представленных на рисунке 2. Однако при этом остается открытым вопрос о том, каким образом следует объективно оценить величину так называемого «спреда», характеризующего разброс ФП нечетких чисел *хвр, хзп, хдку* и *хпчву* относительно абсцисс *а2вр, а2зп, а2дку* и *а2пчву*.

Для приведенных на рисунке 2 графиков экспертная группа [9] приняла (на свое заседании) решение о том, что «спреды» для усредненных балльных оценок частных показателей-концептов $\overline{ЗП}$, $\overline{ВР}$ и $\overline{ДКУ}$ следует задать в виде ±10 % от максимальных возможных значений ВРmax = ЗПmax = ДКУmax = 10, а величина «спреда» для нечеткого числа хпчву определилась в процессе вычислений по формулам (7), (8) и (9). Такое волюнтаристское решение членов экспертной группы, принятое в [9], имеет субъективный характер и его недостатком является то, что при этом не были использованы возможности произвести объективную оценку величин «спредов» для нечетких чисел $\overline{ВР}$, $\overline{ЗП}$ и $\overline{ДКУ}$ по уже имевшимся экспертным балльным оценкам частных показателей-концептов ЗПi, ВРi и ДКУi *(i = 1,...,m)*. Ниже рассматривается предложенный в данной статье метод определения параметров ФП Гауссова типа в виде формул (4).

3. Применение статистических методов при обработке предоставленных экспертами данных о результатах оценки показателей ЗПi, ВРi и ДКУi *(i= 1,…,m).*

3.1. Предварительные сведения об оценке среднего арифметического значения и среднеквадратичного отклонения (СКО) путем статистической обработки результатов наблюдений [15–17, 24]. При наблюдениях любой величины X (например, показателей-концептов ЗП, ВР и ДКУ, определенных в процессе работы экспертной группы), истинное значение которой X_0, теоретически мыслимо получить бесконечный набор значений X_1, X_2, ⋯ , X_n, ⋯ , который принято называть генеральной совокупностью значений. Обозначим погрешности (ошибки) каждого отдельного независимого измерения через

$$\Delta X_i = X_0 - X_i . \quad (10)$$

Если среднее арифметическое значение погрешностей ΔX_i для генеральной совокупности равно нулю, т.е.

$$\lim_{n\to\infty} \frac{\sum_{i=1}^{n} \Delta X_i}{n} = 0 , \quad (11)$$

то такие погрешности являются случайными. Вероятность их появления тем большая, чем меньше их значения ΔX_i . Вероятность появления случайных погрешностей одной и той же величины, но разного знака одинакова. Для генеральной совокупности среднее арифметическое значение $\overline{X}$ (математическое ожидание) равно истинному значению X_0 наблюдаемой величины X, т.е.

$$\overline{\mathrm{X}} = \lim_{n\to\infty} \frac{\sum_{i=1}^{n} \mathrm{X}_i}{n} = \mathrm{X}_0 . \tag{12}$$

Рассеяние измеренных значений X_i вблизи истинного X_0 характеризуется дисперсией $D(\mathrm{X})$, определяемой соотношением

$$D(\mathrm{X}) = \sigma_{\mathrm{X}}^2 = \lim_{n\to\infty} \frac{\sum_{i=1}^{n} (\mathrm{X}_i - \overline{\mathrm{X}})^2}{n} . \tag{13}$$

Величина $\sigma\mathrm{X}$ называется среднеквадратичным отклонением (СКО) генеральной совокупности.

На самом деле в распоряжении экспертной группы имеется не бесконечная, а ограниченная совокупность – ряд $x1$, $x2$, … , x_i, … , x_n полученных (экспертным методом) значений величины X. Задача состоит в том, чтобы, пользуясь ограниченным числом наблюдений (выборкой объема n из генеральной совокупности), наилучшим образом оценить $\overline{\mathrm{X}}$, $D(\mathrm{X})$ и дисперсию $D(\overline{\mathrm{X}})$ для среднего арифметического значения $\overline{\mathrm{X}}$, характеризующие генеральную совокупность. Такими оценками являются соответственно:

- среднее арифметическое выборки

$$\overline{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{\sum_{i=1}^{n} x_i}{n}, \tag{14}$$

- исправленное среднеквадратичное отклонение (СКО) выборки для каждого отдельного наблюдения, рассчитываемое по формуле

$$\sigma_x = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{n-1}}, \tag{15}$$

- исправленное среднеквадратичное отклонение (СКО) выборки для среднего арифметического значения $\overline{x}$, вычисляемое по формуле

$$\sigma_{\overline{x}} = \sqrt{\frac{\sigma_x^2}{n}} = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{n(n-1)}} . \tag{16}$$

3.2. Выявление грубых ошибок (промахов) в экспертных оценках [15, 16]. Может оказаться, что некоторые экстремальные величины $x_э$ из значений x_i кажутся слишком большими или слишком малыми по сравнению с другими. Чтобы ответить на вопрос, следует ли учитывать такие величины при расчете $\overline{x}$, σ_x и $\sigma_{\overline{x}}$, необходимо для экстремального $x_э$ рассчитать сначала значение

$$S_n = \sqrt{\frac{1}{n} \sum_{i=1}^{n} (x_i - \overline{x})^2}, \tag{15а}$$

затем для экстремального $x_э$ вычислить значение

$$r = \frac{|x_э - \overline{x}|}{S_n} \tag{17}$$

и сравнить полученное значение r с величиной критерия ζ_1 при заданной величине доверительной вероятности. В таблице 2 приведены значения критерия ζ_1 при доверительной вероятности $\alpha = 0{,}95$ по данным [15, 16].

Таблица 2 – Зависимость величины критерия $\zeta 1$ от объема выборки n при доверительной вероятности $\alpha = 0{,}95$

n	ζ_1	n	ζ_1	n	ζ_1
3	1,41	9	2,24	20	2,62
4	1,69	10	2,29	25	2,72
5	1,87	12	2,39	30	2,88
6	2,00	14	2,46	35	2,96
7	2,09	16	2,52	40	3,00
8	2,17	18	2,58	45	3,08

Если $r > \zeta 1$, то $x_э$ должно быть исключено из выборки, а ее объем n соответственно уменьшен, после чего по формулам (14)–(16) следует рассчитать новые значения $\bar{x}$, σ_x, $\sigma_{\bar{x}}$, s_n и r.

3.3. Определение величины доверительного интервала при заданной доверительной вероятности [15, 16]. Оценки $\bar{x}$, σ_x и $\sigma_{\bar{x}}$ являются наилучшими, так как они не смещены, эффективны и состоятельны. Понятно, что ограниченный объем информации не позволяет в общем случае ожидать, что $X_0 = \bar{x}$, $\sigma_X^2 = \sigma_{\bar{x}}^2$ и $\sigma_{\bar{X}} = \sigma_{\bar{x}}$. Можно лишь утверждать, что с некоторой заранее заданной (доверительной) вероятностью

$$|X_0 - \bar{x}| < \Delta_{\bar{x}},$$

где число $\Delta_{\bar{x}}$ характеризует погрешность полученной оценки $\bar{x}$ при заранее заданной доверительной вероятности. Интервал $(\bar{x} - \Delta_{\bar{x}},\ \bar{x} + \Delta_{\bar{x}})$, по ширине равный $2 \cdot \Delta_{\bar{x}}$ и заключающий в себе $X = X_0$, называется доверительным.

При расчетах погрешности $\Delta_{\bar{x}}$ усредненных экспертных оценок доверительная вероятность должна быть заранее задана. Действуя по аналогии с обработкой результатов технических измерений и основываясь на практике экспертных оценок, в дальнейшем в данной статье всегда будем считать, что заданная доверительная вероятность равна $\alpha = 0{,}95$.

Для расчета доверительного интервала необходимо знать не только доверительную вероятность, но и закон распределения случайной величины. Этот закон, вообще говоря, должен быть установлен для каждого конкретного ряда измерений. Исследования [15, 16, 24] показали, что случайные величины (наблюдения) в большинстве случаев подчиняются нормальному закону распределения Гаусса. В дальнейшем будем считать, что случайная величина распределена по нормальному закону при большом числе экспертных оценок и по закону распределения Стьюдента [15, 16, 24] – при малом количестве наблюдений. Следует отметить, что на практике в состав экспертных групп чаще всего включают от 3 до 7 специалистов. Поэтому при вычислениях ширины доверительного интервала обычно используют так называемый коэффициент Стьюдента, определяемый при доверительной вероятности α=0,95.

При вышеизложенных допущениях погрешность Δ_x каждого отдельного результата наблюдения (при доверительной вероятности α=0,95) равна половине ширины доверительного интервала, и ее рассчитывают по формуле

$$\Delta_x = \zeta_2 \sigma_x = \zeta_2 \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n-1}}, \qquad (18)$$

для которой коэффициент Стьюдента (параметр ζ_2) берут из таблицы 3.

Таблица 3 – Зависимость коэффициента Стьюдента ζ_2 от объема выборки n при доверительной вероятности $\alpha = 0{,}95$ по данным [15, 16, 24]

n	ζ_2	n	ζ_2
3	4,30	9	2,31
4	3,18	10	2,26
5	2,78	15	2,15
6	2,57	20	2,09
7	2,45	50	2,01
8	2,37	100	1,96

Абсолютная погрешность $\Delta_{\bar{x}}$ среднего арифметического значения $\bar{x}$ результатов наблюдений вычисляют по формуле

$$\Delta_{\bar{x}} = \frac{\Delta_x}{\sqrt{n}} = \zeta_2 \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n(n-1)}}\,. \qquad (19)$$

Если σ_X и $\sigma_{\bar{X}}$ известны, то

$$\Delta_X = 1{,}96\sigma_X \approx 2{,}0\sigma_X,$$
$$\Delta_{\bar{X}} = 1{,}96\sigma_{\bar{X}} \approx 2{,}0\sigma_{\bar{X}},$$

т.е. значение характерного размера (половины ширины) доверительного интервала примерно в два раза превышает величину СКО для среднего арифметического значения, рассчитанную по формуле (16).

Исходя из предоставленных экспертами данных, полученный результат экспертной оценки величины X_0 должен быть записан в виде

$$X_0 = \bar{x} \pm \Delta_{\bar{x}} \text{ при доверительной вероятности } \alpha = 0{,}95$$

или в виде

$$\text{Вер}\,(\bar{x} - \Delta_{\bar{x}} < X_0 < \bar{x} + \Delta_{\bar{x}}) = \alpha = 0{,}95. \qquad (20)$$

3.4. Пример применения методов статистической обработки при определении параметров функции принадлежности Гауссова типа [15–17]. *Дано:* в результате работы экспертной группы было получено $m = 6$ оценок нечеткого числа «Значимость последствий» *($ЗП_i$, i= 1, 2, ..., m),* а именно: $ЗП_1 = 4$, $ЗП_2 = 8$, $ЗП_3 = 9$, $ЗП_4 = 9$, $ЗП_5 = 8$, $ЗП_6 = 8$.

Требуется найти: 1) значение абсциссы нечеткой переменной $c = x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{max}$, соответствующее максимальному значению функции принадлежности (4); 2) величину параметра σ, входящего в функцию принадлежности (4) и характеризующего так называемый «спред» ФП Гауссова типа.

Решение: Значение $ЗП_1$ резко отличается от других, проверим, следует ли оставить его в выборке при расчете $\overline{ЗП}$ и $\sigma_{\overline{ЗП}}$. С этой целью по формулам (14) и (15а) рассчитаем $\overline{ЗП}$ и $S_{n\,ЗП}$ в предположении, что результат $ЗП_1$ является доброкачественным, а затем по формуле (17) рассчитаем параметр r и сравним его с ζ_1 (табл. 2):

$$\overline{ЗП} = \frac{4+8+9+9+8+8}{6} = 7{,}667,$$

$$S_{n\,ЗП} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(ЗП_i - \overline{ЗП}\right)^2} = 1{,}6997,$$

$$r = \frac{7{,}667 - 4{,}0}{1{,}6997} = 2{,}157 > 2{,}00\,.$$

Таким образом, значение $ЗП_1 = 4$ из дальнейшего рассмотрения должно быть исключено. После этого дальнейшей обработке подвергает выборку объемом $n = 5$.

По формуле (14) находим

$$\overline{ЗП} = \frac{8+9+9+8+8}{5} = 8{,}4,$$

что определяет значение абсциссы $c = x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{max}$ (при $ЗП_{max} = 10$), соответствующее максимальной величине искомой ФП, равное $c = \overline{ЗП} / ЗП_{max} = 8{,}4/10 = 0{,}84$.

Из выражения (16) получаем $\sigma_{\overline{ЗП}} = \sqrt{\frac{\sum_{i=1}^{n}\left(ЗП_i - \overline{ЗП}\right)^2}{n(n-1)}} = 0{,}2191$.

Наконец, расчет по формуле (19), для которой параметр $\zeta 2 = 2{,}78$ взят из таблицы 3 при n = 5, дает величину абсолютной погрешности определения среднего арифметического значения показателя $\overline{ЗП}$, равную

$$\Delta_{\overline{ЗП}} = 2{,}78 \cdot 0{,}2191 \approx 0{,}6091,$$

что соответствует значению абсолютной погрешности $\Delta_{\bar{x}_{ЗП}}$ определения среднего арифметического значения $c = x_{\overline{ЗП}}$ нечеткой величины $x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{\max}$ (при $ЗП_{max} = 10$), равному

$$\Delta_{x_{\overline{ЗП}}} = 0{,}6091/10 = 0{,}06091.$$

В соответствии с выражением (20) полученный результат оценки показателя «Значимость последствий» ЗП определяется доверительным интервалом

$$\overline{ЗП} = 8{,}4 \pm 0{,}6091 \text{ вт/(м. град)},$$

а для нечеткой величины $x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{\max}$ соответствующий доверительный интервал имеет вид

$$x_{\overline{ЗП}} = 0{,}84 \pm 0{,}06091.$$

В связи с тем, что половина ширины доверительного интервала $\Delta_{\overline{ЗП}} \approx 0{,}6091$, а также с учетом сказанного во введении к данной статьи, в качестве параметров c и σ ФП Гауссова типа (4) для нечеткого показателя-концепта ЗП следует принять первый параметр равным

$$c = \overline{ЗП} = 8{,}4,$$

а в качестве второго параметра следует принять $\sigma = \Delta_{\overline{ЗП}} / 2 \approx 0{,}3046$, т.е. половину величины $\Delta_{\overline{ЗП}}$, определяющей размер доверительного интервала. При этом саму функцию принадлежности (4) для показателя-концепта $\overline{ЗП}$ можно представить в виде

$$\mu(\overline{ЗП}; 8{,}4; 0{,}3046) = \exp\left[-\frac{1}{2}\left(\frac{\overline{ЗП} - 8{,}4}{0{,}3046} \right)^2 \right]. \qquad (4а)$$

Аналогично в качестве параметров *c* и *σ* функции принадлежности Гауссова типа (4) для нечеткого показателя-концепта $x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{\max}$ (при $ЗП_{max}=10$) следует принять

$$c = \overline{ЗП} / ЗП_{max} = 8{,}4/10 = 0{,}84, \quad \sigma = \Delta_{\bar{x}_{ЗП}} / 2 = \Delta_{\overline{ЗП}} / 20 \approx 0{,}03046,$$

а саму эту функцию принадлежности (4) для показателя-концепта $x_{\overline{ЗП}} = \overline{ЗП} / ЗП_{max}$ можно представить в виде $\mu(x_{\overline{ЗП}}; 0{,}84; 0{,}03046) = \exp\left[-\frac{1}{2}\left(\frac{x_{\overline{ЗП}} - 0{,}84}{0{,}03046} \right)^2 \right]$.

В данном пункте 3.4 приведен пример определения параметров *c* и σ функции принадлежности в виде формулы (4) по данным, предоставленным экспертами для показателя-концепта *ЗПi(i= 1, 2, ..., n)*. При обработке предоставленных экспертами результатов оценки показателей-концептов *ВРi* и *ДКУi (i= 1, 2, ..., n)* следует действовать аналогично.

4. Применение теоретических основ метрологии при определении параметров функции принадлежности Гауссова типа для нечеткого числа «Приоритетное число возможности улучшения» (ПЧВУ). Воспользуемся рекомендациями теоретических основ метрологии, применяемыми при вычислении погрешностей косвенных измерений при использовании зависимостей в виде произведения переменных. Применение экспертных методов при подготовке принятия управленческих решений в соответствии с рекомендациями FMEA-методологии [7–11] или IOMEA-методологии [7–9] предполагает обработку предоставленных экспертами данных с использованием формул в виде произведения средних значений трех показателей-концептов. В случае использования так называемой IOMEA-методологии [7–9], рассмотренной во втором разделе данной статьи, вычисление результирующего значения показателя $\overline{ПЧВУ}$ (при обработке предоставленных экспертами данных) не вызывает затруднений. При этом в качестве показателя $c_{\overline{ПЧВУ}}$ ФП Гауссова типа принимают значение показателя $\overline{ПЧВУ}$, определяемое по формуле

$$c_{\overline{ПЧВУ}} = \overline{\text{ПЧВУ}} = \overline{\text{ВР}} \cdot \overline{\text{ЗП}} \cdot \overline{\text{ДКУ}}. \quad (21)$$

Смысл и порядок определения показателей-концептов, входящих в формулу (21), были подробно рассмотрены во втором разделе данной статьи. Несколько сложнее обстоит дело с определением показателя $\sigma_{\overline{ПЧВУ}}$, определяющего «спред» ФП Гауссова типа.

4.1. Применение методов оценки погрешностей косвенных измерений [15–17] в качестве основы при определении доверительного интервала для среднего значения нечеткого числа «Приоритетное число возможности улучшения» (ПЧВУ). Рассмотрим задачу об определении так называемого «спреда» для ФП нечеткого показателя-концепта $\overline{\text{ПЧВУ}}$ и соответствующей нечеткой относительной величины $x_{\overline{ПЧВУ}} = \overline{ПЧВУ} / ПЧВУ_{\max}$.

Исходные данные: Экспертами определены средние значения показателей-концептов $\overline{ВР}$, $\overline{ЗП}$, $\overline{ДКУ}$. величины доверительных интервалов $\Delta_{\overline{ВР}}$, $\Delta_{\overline{ЗП}}$, $\Delta_{\overline{ДКУ}}$ для этих показателей-концептов и параметры $c_{\overline{ВР}}, \sigma_{\overline{ВР}}, c_{\overline{ЗП}}, \sigma_{\overline{ЗП}}$, $c_{\overline{ДКУ}}, \sigma_{\overline{ДКУ}}$ соответствующих функций принадлежности в виде соотношений (4).

Требуется: Найти среднее значение показателя концепта $\overline{\text{ПЧВУ}}$, величину доверительного интервала $\Delta_{\overline{ПЧВУ}}$ и соответствующие значения параметров $c_{\overline{ПЧВУ}}$ и $\sigma_{\overline{ПЧВУ}}$ функции принадлежности в виде формулы (4).

Решение: Среднее значение показателя-концепта $\overline{\text{ПЧВУ}}$ легко вычисляется непосредственно по формуле (21), причем в качестве параметра $c_{\overline{ПЧВУ}}$ принимается $c_{\overline{ПЧВУ}} = \overline{\text{ПЧВУ}}$.

Вопрос об определении величины доверительного интервала, в котором находится найденное среднее значение показателя-концепта $\overline{\text{ПЧВУ}}$, решается несколько сложнее с применением методов, разработанных для оценки погрешностей косвенных измерений[15–17].

Рекомендации теоретических основ метрологии для вычисления погрешностей косвенных измерений при решении рассматриваемой задачи можно использовать следующим образом.

1. Прологарифмируем левую и правую части зависимости (21)

$$\ln\overline{\text{ПЧВУ}} = \ln\left(\overline{\text{ВР}} \cdot \overline{\text{ЗП}} \cdot \overline{\text{ДКУ}}\right) = \ln\overline{ВР} + \ln\overline{ЗП} + \ln\overline{ДКУ}.$$

2. Найдем дифференциалы правой и левой частей

$$d\ln\overline{\text{ПЧВУ}} = d\ln\left(\overline{\text{ВР}} \cdot \overline{\text{ЗП}} \cdot \overline{\text{ДКУ}}\right) = d\ln\overline{ВР} + d\ln\overline{ЗП} + d\ln\overline{ДКУ}.$$

3. Учитывая, что дифференциал от логарифма переменной величины x находится по формуле [15–17] $d(\ln x) = \frac{d\ln x}{dx}dx = \frac{dx}{x}$, получаем

$$\frac{d\overline{\text{ПЧВУ}}}{\overline{\text{ПЧВУ}}} = \frac{d\overline{\text{ВР}}}{\overline{\text{ВР}}} + \frac{d\overline{\text{ЗП}}}{\overline{\text{ЗП}}} + \frac{d\overline{\text{ДКУ}}}{\overline{\text{ДКУ}}}.$$

4. Произведем широко используемую в теории погрешностей замену дифференциалов малыми абсолютными погрешностями (при условии, что абсолютные погрешности достаточно малы) [15–17]:

$$d\overline{\text{ПЧВУ}} \approx \Delta\overline{\text{ПЧВУ}},\ d\overline{\text{ВР}} \approx \Delta\overline{\text{ВР}},\ d\overline{\text{ЗП}} \approx \Delta\overline{\text{ЗП}},\ d\overline{\text{ДКУ}} \approx \Delta\overline{\text{ДКУ}}.$$

Тогда $\frac{\Delta\overline{\text{ПЧВУ}}}{\overline{\text{ПЧВУ}}} = \frac{\Delta\overline{\text{ВР}}}{\overline{\text{ВР}}} + \frac{\Delta\overline{\text{ЗП}}}{\overline{\text{ЗП}}} + \frac{\Delta\overline{\text{ДКУ}}}{\overline{\text{ДКУ}}}$.

5. Учитывая, что знаки погрешностей $\Delta\overline{\text{ВР}}$, $\Delta\overline{\text{ЗП}}$, $\Delta\overline{\text{ДКУ}}$ заранее неизвестны, для получения гарантированной (*предельной*) оценки относительной погрешности косвенного измерения в последней формуле (в общем случае в ней могут присутствовать и знаки "–") все знаки "–" заменяем на знаки "+" [15–17] и в нашем случае получаем такую же формулу

$$\left(\frac{\Delta\overline{\text{ПЧВУ}}}{\overline{\text{ПЧВУ}}}\right)_{\text{пр}} = \frac{\Delta\overline{\text{ВР}}}{\overline{\text{ВР}}} + \frac{\Delta\overline{\text{ЗП}}}{\overline{\text{ЗП}}} + \frac{\Delta\overline{\text{ДКУ}}}{\overline{\text{ДКУ}}}, \quad (22)$$

которую можно представить в виде

$$\delta\overline{\text{ПЧВУ}}_{\text{пр}} = \delta\overline{\text{ВР}} + \delta\overline{\text{ЗП}} + \delta\overline{\text{ДКУ}}, \quad (22а)$$

где $\delta\overline{\text{ПЧВУ}}_{\text{пр}} = \left(\frac{\Delta\overline{\text{ПЧВУ}}}{\overline{\text{ПЧВУ}}}\right)_{\text{пр}}$, $\delta\overline{\text{ВР}} = \frac{\Delta\overline{\text{ВР}}}{\overline{\text{ВР}}}, \delta\overline{\text{ЗП}} = \frac{\Delta\overline{\text{ЗП}}}{\overline{\text{ЗП}}}$, $\delta\overline{\text{ДКУ}} = \frac{\Delta\overline{\text{ДКУ}}}{\overline{\text{ДКУ}}}$ – обозначения относительных погрешностей определения соответствующих нечетких показателей-концептов.

6. Предельную оценку абсолютной погрешности косвенного измерения можно находить по формуле

$$\Delta\overline{\text{ПЧВУ}}_{\text{пр}} = \delta\overline{\text{ПЧВУ}}_{\text{пр}} \cdot \overline{\text{ПЧВУ}}.$$

Величина предельной погрешности во многих случаях бывает завышенной, поэтому часто на практике применяют так называемую «среднеквадратическую оценку погрешности». Для получения среднеквадратической оценки погрешности поступают следующим образом. В формулах (22) и (22а) суммы, стоящие в правых частях этих формул, заменяют корнями квадратными из суммы квадратов соответствующих переменных [15–17].

7. Воспользовавшись этими рекомендациями, запишем формулы для вычисления среднеквадратических оценок относительной $\delta\overline{\text{ПЧВУ}}_{\text{ск}}$ и абсолютной $\Delta\overline{\text{ПЧВУ}}_{\text{ск}}$ погрешностей косвенного определения показателя-концепта $\overline{\text{ПЧВУ}}_{\text{ск}}$, которые имеют вид:

$$\delta\overline{\text{ПЧВУ}}_{\text{ск}} = \sqrt{\left(\frac{\Delta\overline{\text{ВР}}}{\overline{\text{ВР}}}\right)^2 + \left(\frac{\Delta\overline{\text{ЗП}}}{\overline{\text{ЗП}}}\right)^2 + \left(\frac{\Delta\overline{ДКУ}}{\overline{ДКУ}}\right)^2} = \sqrt{\left(\delta\overline{\text{ВР}}\right)^2 + \left(\delta\overline{\text{ЗП}}\right)^2 + \left(\delta\overline{\text{ДКУ}}\right)^2} \quad (23)$$

$$\Delta\overline{\text{ПЧВУ}}_{\text{ск}} = \sqrt{\left(\frac{\Delta\overline{\text{ВР}}}{\overline{\text{ВР}}}\right)^2 + \left(\frac{\Delta\overline{\text{ЗП}}}{\overline{\text{ЗП}}}\right)^2 + \left(\frac{\Delta\overline{\text{ДКУ}}}{\overline{\text{ДКУ}}}\right)^2} \cdot \overline{\text{ПЧВУ}} = \quad (23а)$$

$$= \sqrt{\left(\delta\overline{\text{ВР}}\right)^2 + \left(\delta\overline{\text{ЗП}}\right)^2 + \left(\delta\overline{\text{ДКУ}}\right)^2} \cdot \overline{\text{ПЧВУ}} = \delta\overline{\text{ПЧВУ}}_{\text{ск}} \cdot \overline{\text{ПЧВУ}}.$$

Следуя вышеизложенным рекомендациям, по формулам (21) и (23а) получают значения параметров $\overline{\text{ПЧВУ}}$ и $\Delta\overline{\text{ПЧВУ}}_{\text{ск}}$, определяющие величину доверительного интервала при доверительной вероятности $\alpha = 0{,}95$ и позволяющие записать полученный результат в виде $Вер(\overline{\text{ПЧВУ}} - \Delta\overline{\text{ПЧВУ}}_{\text{ск}} \le ПЧВУ_0 \le \overline{\text{ПЧВУ}} + \Delta\overline{\text{ПЧВУ}}_{\text{ск}}) = 0{,}95$, т.е. вероятность того, что истинное значение $ПЧВУ_0$ показателя-концепта $ПЧВУ$ находится в интервале $(\overline{\text{ПЧВУ}} - \Delta\overline{\text{ПЧВУ}}_{\text{ск}}, \overline{\text{ПЧВУ}} + \Delta\overline{\text{ПЧВУ}}_{\text{ск}})$, равна $\alpha = 0{,}95$.

4.2. Определение параметров функции принадлежности Гауссова типа для среднего значения нечеткого показателя-концепта $\overline{\text{ПЧВУ}}$ после обработки результатов работы экспертной группы. С учетом изложенного выше в п. 4.1 для показателя-концепта $\overline{\text{ПЧВУ}}$ следует рекомендовать следующий порядок вычисления параметров ФП Гауссова типа, задаваемой в виде формулы (4):

а) в качестве параметра $c_{\overline{ПЧВУ}}$, определяющего значение абсциссы показателя-концепта $\overline{\text{ПЧВУ}}$, соответствующее максимальному значению ФП (4), принимают значение $c_{\overline{ПЧВУ}} = \overline{\text{ПЧВУ}} = \overline{\text{ВР}} \cdot \overline{\text{ЗП}} \cdot \overline{\text{ДКУ}}$, рассчитанное по формуле (21);

б) в качестве параметра $\sigma_{\overline{ПЧВУ}}$, определяющего «спред» ФП (4), следует принять

$$\sigma_{\overline{ПЧВУ}} = \Delta\overline{\text{ПЧВУ}}_{\text{ск}} / 2, \quad (24)$$

т.е. половину значения $\Delta\overline{\text{ПЧВУ}}_{\text{ск}}$, определяющего величину доверительного интервала $(\overline{\text{ПЧВУ}} - \Delta\overline{\text{ПЧВУ}}_{\text{ск}}, \overline{\text{ПЧВУ}} + \Delta\overline{\text{ПЧВУ}}_{\text{ск}})$;

в) в итоге ФП в виде формулу (4) для переменной величины $\overline{\text{ПЧВУ}}$, следует записать в виде

$$\mu(\overline{\text{ПЧВУ}}; c_{\overline{ПЧВУ}}, \sigma_{\overline{ПЧВУ}}) = \exp\left[-\frac{1}{2}\left(\frac{\overline{\text{ПЧВУ}} - c_{\overline{ПЧВУ}}}{\sigma_{\overline{ПЧВУ}}}\right)^2\right]. \quad (25)$$

4.3. Определение параметров функции принадлежности Гауссова типа для нечеткого показателя концепта $x_{\overline{ПЧВУ}} = \overline{ПЧВУ}_{ск} / ПЧВУ_{\max}$ после обработки

результатов работы экспертной группы. При поддержке процесса принятия решения менеджером (ЛПР) испытательной лаборатории целесообразно использовать графики функций принадлежности, имеющие сопоставимые размеры. Например, на каждом графике (рис. 2а, б, в, г) под аргументами $x_{вр}$, $x_{зп}$,$x_{дку}$ и $x_{пчву}$ понимаются безразмерные величины $x_{вр} = \overline{ВР} / ВР_{max}$, $x_{зп} = \overline{ЗП} / ЗП_{max}$, $x_{дку} = \overline{ДКУ} / ДКУ_{max}$и $x_{пчву} = \overline{ПЧВУ} / ПЧВУ_{max}$, где $ВР_{max} = ЗП_{max} = ДКУ_{max} = 10$, а значение $ПЧВУ_{max} = 1000$, так как в соответствии с [7] $ПЧВУ_{max} = ВР_{max} \cdot ЗП_{max} \cdot ДКУ_{max}$.

Действуя по аналогии с вышеизложенным, получаем следующие результаты:

а) для нечеткого показателя-концепта $x_{\overline{ПЧВУ}} = \overline{ПЧВУ} / ПЧВУ_{\max}$ (при $ПЧВУ_{max} = 1000$) в качестве первого параметра ФП, в виде зависимости (4), следует принять

$$c_{x_{\overline{ПЧВУ}}} = \overline{ПЧВУ} / ПЧВУ_{\max}, \quad (26)$$

б) в качестве второго параметра ФП, в виде зависимости (4), следует принять

$$\sigma_{x_{\overline{ПЧВУ}}} = \Delta_{x_{\overline{ПЧВУ}}} / 2 = \Delta\overline{ПЧВУ}_{ск} / (2 \cdot ПЧВУ_{\max}), \quad (27)$$

где $\Delta_{x_{\overline{ПЧВУ}}} = \Delta\overline{ПЧВУ}_{ск} / ПЧВУ_{\max}$ – величина, определяющая размер доверительного интервала $(x_{\overline{ПЧВУ}} - \Delta_{x_{\overline{ПЧВУ}}}, x_{\overline{ПЧВУ}} + \Delta_{x_{\overline{ПЧВУ}}})$ для нечеткого показателя-концепта $x_{\overline{ПЧВУ}} = \overline{ПЧВУ} / ПЧВУ_{\max}$;

в) соответственно ФП в виде формулы (4) для нечеткого показателя-концепта $x_{\overline{ПЧВУ}} = \overline{ПЧВУ / ПЧВУ}_{\max}$ следует записать в виде

$$\mu(x_{\overline{ПЧВУ}}; c_{x_{\overline{ПЧВУ}}}, \sigma_{x_{\overline{ПЧВУ}}}) = \exp\left[-\frac{1}{2}\left(\frac{x_{\overline{ПЧВУ}} - c_{x_{\overline{ПЧВУ}}}}{\sigma_{x_{\overline{ПЧВУ}}}} \right)^2 \right]. \quad (4б)$$

5. Процедурная модель обработки предоставленных экспертами результатов оценки показателей «Вероятность реализации» (ВР), «Значимость последствий» (ЗП), «Доступность контроля и управления» (ДКУ) и «Приоритетное число возможности улучшения» (ПЧВУ) при поддержке процесса принятия решения. Итоги выполненных исследований, изложенные выше в данной статьи, были положены в основу разработанной процедурной модели (рис. 3) обработки результатов оценки значений показателей $ВР_i(i= 1, 2, ..., m_{вр})$, $ЗП_i(i= 1, 2, ..., m_{зп})$ и $ДКУ_i(i= 1, 2, ..., m_{дку})$, предоставленных экспертной группой (по десятибалльным квалиметрическим шкалам), чаще всего включающей в свой состав m = 3, …,7 человек. В общем случае: 1) количество предоставленных экспертами сведений о значениях показателей-концептов может быть различным, например, $m_{вр}$,$m_{зп}$ и$m_{дку}$; 2) наряду с десятибалльными шкалами (используемыми в данной статье) могут быть применены четырехбалльные, семибалльные и другие виды квалиметрических шкал. Поэтому во втором блоке на рисунке 3 предусмотрен ввод не только предоставленных экспертами значений $ВР_i(i= 1, 2, ..., m_{вр})$, $ЗП_i(i= 1, 2, ..., m_{зп})$ и $ДКУ_i(i= 1, 2, ..., m_{дку})$, но и величин $ВР_{max}$, $ЗП_{max}$, $ДКУ_{max}$, а также табличных значений критерия ζ_1 и коэффициента Стьюдента ζ_2 при доверительной вероятности $\alpha = 0{,}95$.

Третий, четвертый и пятый блоки на рисунке 3 предназначены (по рекомендациям п. 3.2 данной статьи) для выявления возможных грубых ошибок (промахов) среди значений показателей $ВР_i(i= 1, 2, ..., m_{вр})$, предоставленных экспертами. Аналогичные задачи решаются блоками 6–8 для выявления возможных промахов среди значений $ЗП_i(i= 1, 2, ..., m_{зп})$, а также блоками 9–11 по отношению к возможным грубым ошибкам (промахам) среди значений $ДКУ_i(i= 1, 2, ..., m_{дку})$, предоставленных экспертами.

Двенадцатый блок на рисунке 3 рассматриваемой процедурной модели предусматривает вычисление значений параметров функций принадлежности, а именно: $c_{x_{\overline{ВР}}}$, $c_{x_{\overline{ЗП}}}$, $c_{x_{\overline{ДКУ}}}$ и $c_{x_{\overline{ПЧВУ}}}$, а также $\sigma_{x_{\overline{ВР}}}$, $\sigma_{x_{\overline{ЗП}}}$, $\sigma_{x_{\overline{ДКУ}}}$ и $\sigma_{x_{\overline{ПЧВУ}}}$. Используемые для вычисления этих параметров формулы представлены в 12 блоке на рисунке 3.

Тринадцатый блок на рисунке 3 предусматривает построение графиков функций принадлежности в виде зависимости (4) для показателей-концептов $x_{\overline{ВР}}, x_{\overline{ЗП}}, x_{\overline{ДКУ}}, x_{\overline{ПЧВУ}}$ и предоставление этих графиков (рис. 4) руководителю испытательной лаборатории (лицу, принимающему решение (ЛПР)) в рамках процесса поддержки процесса принятия управленческого решения.

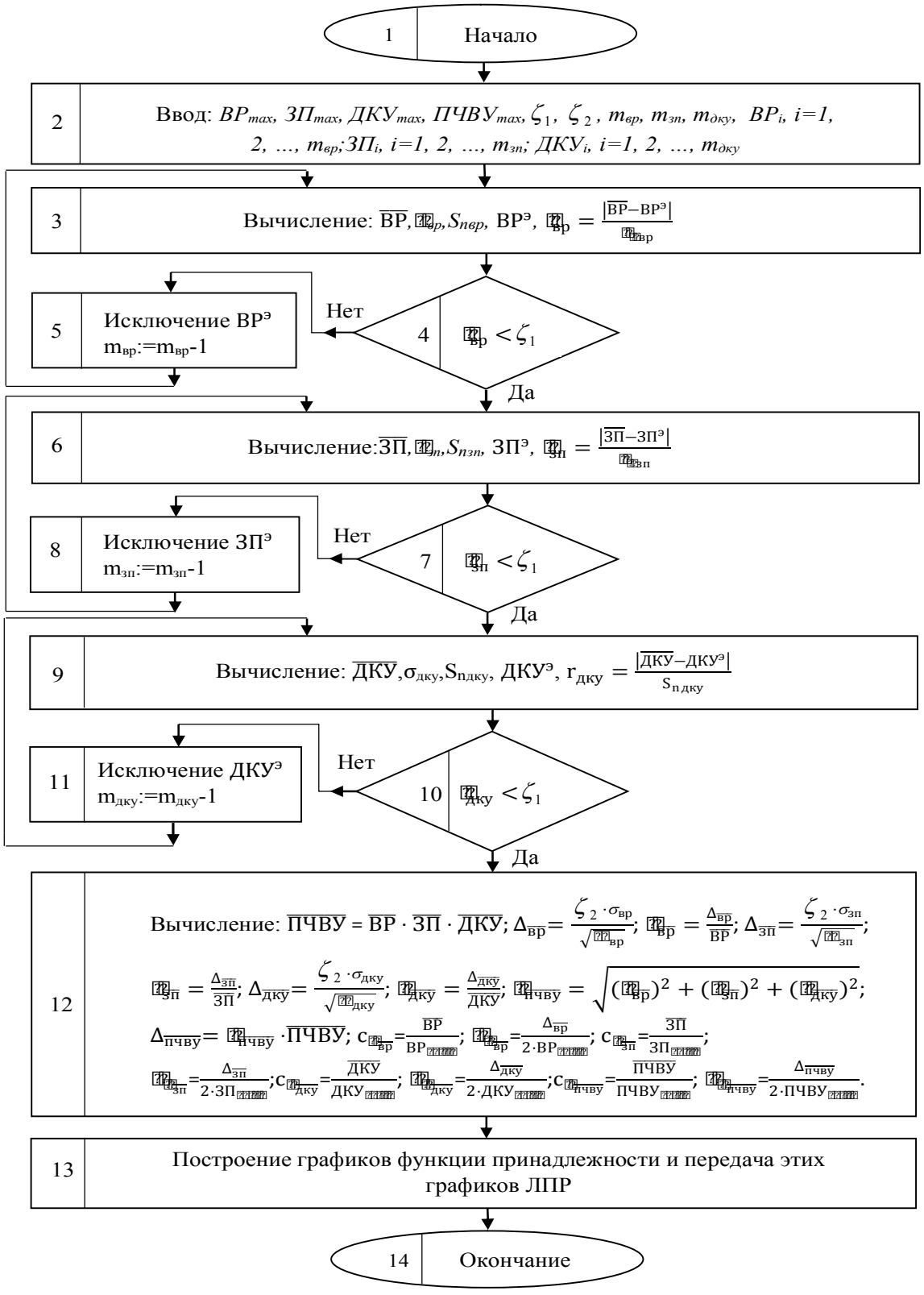


Рисунок 3 – Процедурная модель определения параметров и построения графиков функций принадлежностей в виде зависимости (4) для показателей-концептов $x_{\overline{ВР}}, x_{\overline{ЗП}}, x_{\overline{ДКУ}}, x_{\overline{ПЧВУ}}$

5.1. Пример применения разработанной процедурной модели при обработке результатов работы экспертной группы. Результаты применения вышеизложенных результатов приведены в таблице 4. Представленные в этой таблице и на рисунке 4 результаты были рассчитаны при экспертных оценках, которые достаточно близки к тем, которые ранее были использованы в статье [9] и проиллюстрированы графически на рисунке 2.

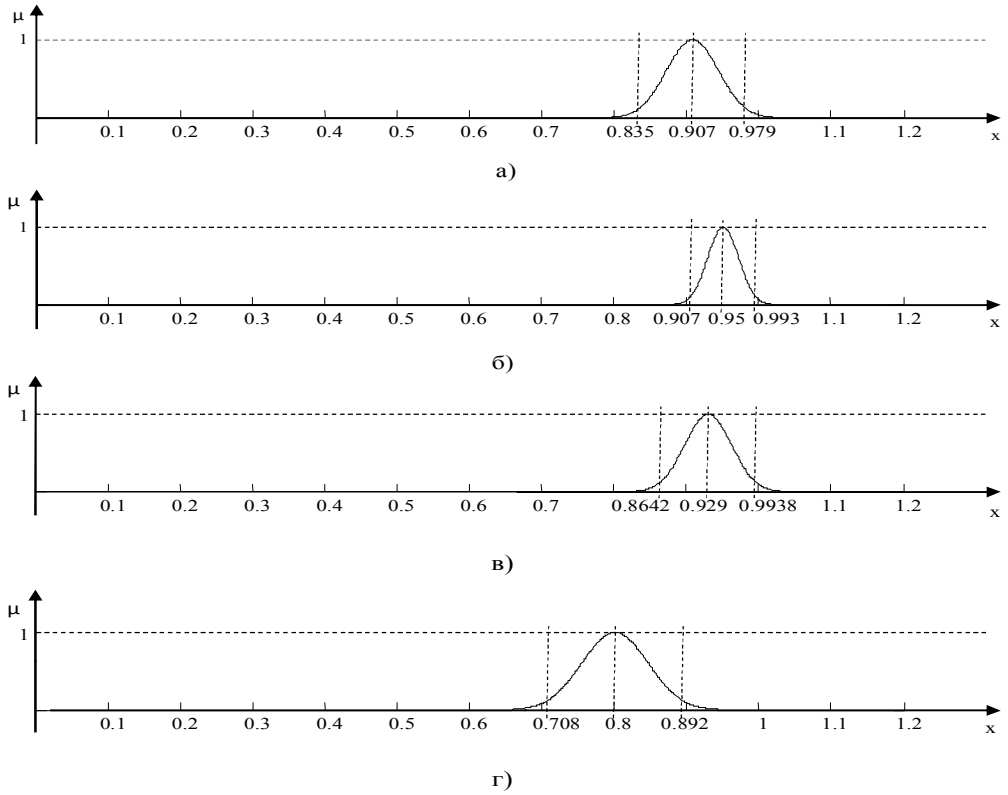


Рисунок 4 – Графики функций принадлежности Гауссова типа, используемые для представления результатов формализации вербальных оценок экспертов для показателей-концептов: а – для $x_{\overline{ВР}}$, б – для $x_{\overline{ЗП}}$, в – для $x_{\overline{ДКУ}}$, г – для $x_{\overline{ПЧВУ}}$

Таблица 4 – Результаты обработки оценок $ВР_i$, $ЗП_i$ и $ДКУ_i$ $(i = 1,...,7)$, предоставленных экспертами при выработке рекомендаций по осуществлению проекта улучшения деятельности в испытательной лаборатории

	Номер эксперта							$c = \bar{x}$	σ_x	$\sigma_{\bar{x}}$	$\Delta_{\bar{x}} = \zeta_2 \cdot \sigma_{\bar{x}}$	$\delta_{\bar{x}} = \frac{\Delta_{\bar{x}}}{\bar{x}}$	σ
	1	**2**	**3**	**4**	**5**	**6**	**7**						
$x_{вр}$	0,8	1,0	0,9	0,9	1,0	0,95	0,8	0,907	0,0776	0,0293	0,0719	0,0792	0,0360
$x_{зп}$	0,9	1,0	0,9	0,9	1,0	0,95	1,0	0,950	0,0463	0,0175	0,0429	0,0451	0,0215
$x_{доу}$	0,8	0,9	0,9	0,9	1,0	1,0	1,0	0,929	0,0699	0,0265	0,0648	0,0698	0,0324
$x_{\overline{ПЧВУ}}$								0,800			0,0919	0,1149	0,046

По аналогии с формулой (21) было определено значение $x_{\overline{ПЧВУ}}$=0,907·0,95·0,929=0,800. Далее вычислили относительную погрешность определения $\delta_{\overline{ПЧВУ}} = \sqrt{(\delta_{\overline{вр}})^2 + (\delta_{\overline{зп}})^2 + (\delta_{\overline{дку}})^2}$ $=\sqrt{(0{,}0792)^2 + (0{,}0451)^2 + (0{,}0698)^2}$ = 0,1149, а затем рассчитали значения параметров

$\Delta_{\overline{\text{пчву}}} = \delta_{\overline{\text{пчву}}} \cdot x_{\overline{ПЧВУ}} = 0{,}1149 \cdot 0{,}800 = 0{,}0919$ и $\sigma_{x_{\overline{\text{пчву}}}} = \frac{\Delta_{\overline{\text{пчву}}}}{2 \cdot \text{ПЧВУ}_{max}} = 0{,}0919/2 = 0{,}0460$, приведенные в нижней строке таблицы 2. По данным таблицы 4 были построены графики ФП, представленные на рисунке 4.

На рисунке 4 вертикальными штрихпунктирными линиями показаны середины, а также нижние и верхние границы доверительных интервалов, построенных по данным таблицы 2. На осях абсцисс графиков (рис. 4а, б, в, г) приведены числовые значения, соответствующие серединам и границам этих доверительных интервалов.

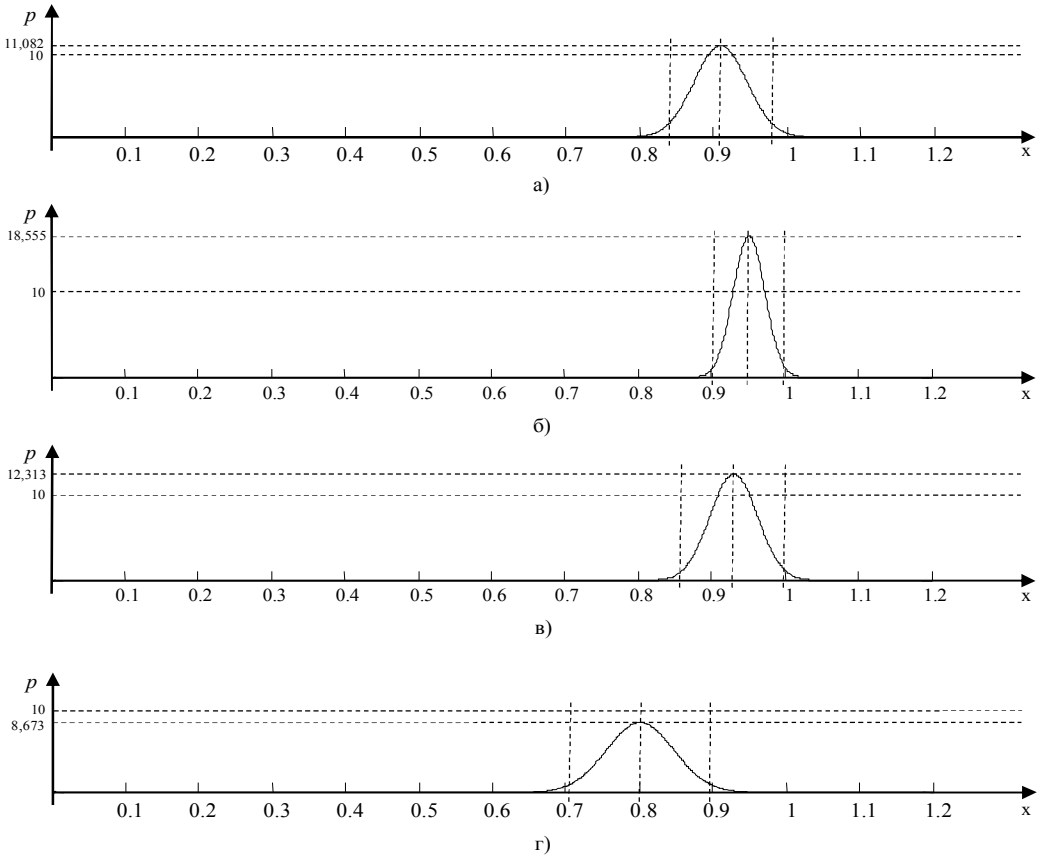


Рисунок 5 – Графики функций $p(x)$ нормальных законов распределения Гаусса, используемые для представления результатов формализации вербальных оценок экспертов для показателей-концептов: а – для $x_{\overline{ВР}}$, б – для $x_{\overline{ЗП}}$, в – для $x_{\overline{ДКУ}}$, *г* – для $x_{\overline{ПЧВУ}}$.

Следует отметить, что для сотрудников испытательных лабораторий характерно традиционное использование методов метрологии, базирующееся на применении нормального закона распределения Гаусса

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{1}{2}\left(\frac{x-c}{\sigma} \right)^2 \right]. \qquad (28)$$

Для сравнения на рисунке 5 приведены графики функций нормальных законов распределения Гаусса (28) соответственно: а – для $x_{\overline{ВР}}$, б – для $x_{\overline{ЗП}}$, в – для $x_{\overline{ДКУ}}$, г – для $x_{\overline{ПЧВУ}}$.

По аналогии с рисунком 4, на графиках (приведенных на рис. 5 а, б, в, г), вертикальными штрихпунктирными линиями показаны положения соответствующих середин и границ доверительных интервалов, численно совпадающие с приведенными выше на рисунке 4. При этом по вертикальным осям ординат на графиках (рис. 5а, б, в, г) показаны максимальные значения функций (28) в середине доверительного интервала. При сравнении данных, приведенных на рисунках 4 и 5, можно сделать вывод, что при использовании графиков в виде функций нормальных

законов распределения (28) у лица, принимающего решение (ЛПР), появляется дополнительная информация о максимальных значениях функций (28) в серединах доверительных интервалов.

Заключение. Применение вышеизложенных математических методов, рекомендуемых теоретической метрологией [15–17], позволяет достаточно просто и точно определить значения параметров $c_{x_{\overline{ВР}}}, c_{x_{\overline{ЗП}}}, c_{x_{\overline{ДКУ}}}$ и $c_{x_{\overline{ПЧВУ}}}$, а также $\sigma_{x_{\overline{ВР}}}, \sigma_{x_{\overline{ЗП}}}, \sigma_{x_{\overline{ДКУ}}}$ и $\sigma_{x_{\overline{ПЧВУ}}}$, необходимые для построения графиков функций принадлежности в виде зависимостей (1), (4), (4а) и (4б).

При сравнении графиков, представленных на рисунках 2 и 4, которые были построены при близких друг к другу результатах экспертных оценок, видно следующее:

1) графики функций принадлежности Гауссова типа в виде колоколообразных кривых (представленные на рисунке 4) значительно более привычны для сотрудников испытательных лабораторий по сравнению с графиками треугольных функций принадлежности, представленными на рисунке 2;

2) величины «спредов» для показателей-концептов $x_{\overline{ВР}}, x_{\overline{ЗП}}, x_{\overline{ДКУ}}, x_{\overline{ПЧВУ}}$, представленных на рисунке 4, оказались существенно меньше по сравнению со «спредами» для аналогичных показателей, показанных на рисунке 2; это объясняется тем, что на рисунке 2 представлены так называемые предельные оценки [15–17] «спредов» (обычно сильно завышающие реальный разброс предоставленных экспертами данных), а при построении графиков на рисунке 4 использованы среднеквадратичные оценки «спредов», которые (с точки зрения теории вероятностей и математической статистики) обычно наиболее близки к реальным оценкам разброса экспертных данных;

3) в связи с этим есть основания для того, чтобы рекомендовать сотрудникам испытательных лабораторий (при поддержке процессов принятия управленческих решений) шире применять рассмотренную в статье процедуру определения параметров $c_{x_{\overline{ПЧВУ}}}$ и $\sigma_{x_{\overline{ПЧВУ}}}$, используемых при представлении функций принадлежности Гауссова типа в виде колоколообразных кривых на основе формулы (4б).

При сравнении рисунков 4 и 5 можно сделать вывод, что приведенные на них данные очень похожи. Если руководитель испытательной лаборатории (ЛПР) предпочитает использовать графики функций принадлежности (рис. 4) в виде зависимостей (1), (4), (4а) и (4б), то в таком виде надо ему предоставлять результаты работы экспертной группы при поддержке процесса принятия решения. Если же ЛПР отдает предпочтение данным (рис. 5) в виде графиков функций нормального закона распределения (28), то при поддержке процесса принятия управленческого решения результаты работы экспертов надо предоставлять ему именно в таком виде.

Библиографический список

1. ГОСТ ISO/IEC 17025-2019. Общие требования к компетентности испытательных и калибровочных лабораторий. – Москва : Стандартинформ, 2019. – 32 с

2. ГОСТ Р 51814.2–2001. Системы качества в автомобилестроении. Метод анализа видов и последствий потенциальных дефектов. – Москва : ИПК Издательство стандартов, 2001. – 17 с.

3. Горюнова С. М. Использование анализа видов и последствий потенциальных дефектов (FMEA) для разработки системы предупреждающих мероприятий испытательной лаборатории / С. М. Горюнова, А. Ф. Дресвянников, Н. Г. Николаева, Н. М. Урманчеева // Заводская лаборатория. Диагностика материалов. – 2006. – Т. 72, № 8. – С. 58–63.

4. Горюнова С. М. Применение методологии FMEA в практике испытательной лаборатории / С. М. Горюнова, А. Ф. Дресвянников, Н. Г. Николаева, А. Ф. Сахаутдинова // Методы оценки соответствия. – 2007. – № 4. – С. 24–29.

5. Солодков Е. И. Применение FMEA-анализа для улучшения процесса градуировки электронных весов / Е. И. Солодков, С. В. Пономарев и др. // Методы менеджмента качества. – 2004. – № 8. – С. 47–49.

6. Пономарев С. В. Управление качеством продукции. Инструменты и методы менеджмента качества : учебное пособие / С. В. Пономарев, С. В. Мищенко, В. Я. Белобрагин и др. – Москва : РИА «Стандарты и качество», 2005. – 248 с.

7. Пономарев С. В. Применение балльных квалиметрических шкал для оценки индикатора «возможности» улучшения в СМК / С. В. Пономарев, С. С. С. Аль-Бусаиди // Методы менеджмента качества. – 2016. – № 11. – С. 14–18.

8. Аль-Бусаиди С. С. С. Применение показателей исполнения деятельности при планировании и принятии управленческого решения об улучшении входного контроля сырья / С. С. С. Аль-Бусаиди, Т. И. Шакирова, С. В. Пономарев // Вестник ТГТУ. – 2018. – Т. 24, № 2. – С. 258–270.

9. Аль-Бусаиди С. С. С. К вопросу о формализации вербальных оценок, полученных экспертными методами, при подготовке к принятию решений в системе управления испытательной лабораторией / С.С.С. Аль-Бусаиди, С.В. Пономарев // Прикаспийский журнал: управление и высокие технологии. – 2018. – № 3 (43). – С. 59 – 69.

10. Ажмухамедов А. И. Модели и методы информационной поддержки управления социальной подсистемой организации на основе нечеткого когнитивного подхода : дис. … канд. техн. наук / А. И. Ажмухамедов. – Тамбов, 2017. – 159 с.

11. Cheng-Jian Lin. A Pseudo-Gaussian-Based Compensatory Neural System / Cheng-Jian Lin, Wen-Hao Ho // The IEEE International Conference on Fuzzy Systems. – 2003. – P. 214–219.

12. Samingun Handoyo. Generating of Fuzzy Rule Dases with Gaussian Parameters Optimized via Fuzzy C-Mean and Ordinary Least Square / Samingun Handoyo, Achmad Efendi // International Journal of Technology Measurement. – November 2019. – P. 1–8.

13. Kuo R. J. An Intuitionistic Fuzzy Neural Network with Gaussian Membership Function / R. J. Kuo, W. C. Cheng // Journal of Intelligent and Fuzzy Systems. – 2019. – № 36. – P. 6731–6741.

14. Dongrui Wu. Twelve Considerations in Choosing between Gaussian and Trapezoidal Membership Functions in Interval Type-2 Fuzzy Logic Controllers / Wu Dongrui // WCCI 2012 IEEE World Congress on Computational Intelligence. June, 10–15, 2012, Brisbane, Australia.

15. Зайдель А. Н. Ошибки измерений физических величин / А. Н. Зайдель. – Санкт-Петербург : Лань, 2009. – 112 с.

16. Кассандрова О. Н. Обработка результатов наблюдений / О. Н. Кассандрова, В. В. Лебедев. – Москва : Наука, 1970. – 104 с.

17. Мищенко С. В. История метрологии, стандартизации, сертификации и управления качеством : учебное пособие / С. В. Мищенко, С. В. Пономарев и др. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2004. – 112 с.

18. Byung-InChoi. IntervalType-2 Fuzzy MembershipFunctionGenerationMethodsfor Pattern Recognition / Byung-InChoi, FrankChung-HoonRhee // Information Sciences. – 2009. – № 179. – P. 2102–2122.

19. Swarup Medasani. An Overview of Membership Function Generation Techniques for Pattern Recognition / Swarup Medasani, Jaeseok Kim, Raghu Krishnapuram // International Journal of Approximate Reasoning. – 1998. – № 19. – P. 391–417.

20. Beliakov Gleb. Fuzzy Sets and Membership Functions Based on Probabilities / Gleb Beliakov // Information Sciences. – 1996. – № 91. – P. 95–111.

21. M. Reha Civanlar. Constructing Membership Function Using Statistical Data / M. Reha Civanlar, H. Joel Trussell // Fuzzy Sets and Systems. – 1986. – № 18. – P. 1–13.

22. Ping-Zong Lin. Robust Self-Organizing Fuzzy-Neural Control Using Asymmetric Gaussian Membership Function / Ping-Zong Lin, Tsu-Tian Lee // International Journal of Fuzzy Systems. – June 1978. – Vol. 9, № 2. – P. 77–86.

23. Andres L. Medaglia. An Efficient and Flexible Mechanism for Construction of Membership Functions / Andres L. Medaglia, Shu-Cherng Fang, Henry L.W. Nuttle, James R. Wilson // European Journal of Operational Research. – 2002. – № 139. – P. 84–95.

24. Вентцель Е. С. Теория вероятностей / Е. С. Вентцель. – Москва : Наука, 1969. – 576 с.

References

1. *GOST ISO/IEC 17025-2019. Obshchie trebovaniya k kompetentnosti ispytatelnykh i kalibrovochnykh laboratoriy* [General requirements for the competence of testing and calibration laboratories]. Moscow, Standartinform Publ. 2019. 32 p.

2. *GOST R 51814.2–2001 Sistemy kachestva v avtomobilestroenii. Metod analiza vidov i posledstviy potentsialnykh defektov* [Quality systems in the automotive industry. Method for analyzing the types and consequences of potential defects]. Moscow, IPK Izdatelstvo standartov Publ., 2001. 17 p.

3. Goryunova S. M., Dresvyannikov A. F., Nikolaeva N. G., Urmancheeva N. M. Ispolzovanie analiza vidov i posledstviy potentsialnykh defektov (FMEA) dlya razrabotki sistemy preduprezhdayushhikh meropriyatiy ispytatelnoy laboratorii [Using Potential Defect Type and Effect Analysis (FMEA) to develop a preventive system for a testing laboratory]. *Zavodskaya laboratoriya. Diagnostika materialov* [Factory laboratory. Diagnostics of materials], 2006, vol. 72, no. 8, pp. 58–63.

4. Goryunova S. M., Dresvyannikov A. F, Nikolaeva N. G., Sakhautdinova A. F. Primenenie metodologii FMEA v praktike ispytatelnoy laboratorii [Application of the FMEA methodology in the practice of a testing laboratory]. *Metody otsenki sootvetstviya* [Conformity assessment methods], 2007, no. 4, pp. 24–29.

5. Solodkov E. I., Ponomarev S. V. etc. Primenenie FMEA-analiza dlya uluchsheniya protsessa graduirovki elektronnykh vesov [Application of FMEA Analysis to Improve the Calibration Process for Electronic Balances]. *Metody menedzhmenta kachestva* [Quality management methods], 2004, no. 8, pp. 47–49.

6. Ponomarev S. V., Mishchenko S. V., Belobragin V. Ya. et al. *Upravlenie kachestvom produktsii. Instrumenty i metody menedzhmenta kachestva: uchebnoe posobie* [Product quality management. Quality Management Tools and Techniques: A Study Guide]. Moscow, RIA «Standarty i kachestvo» Publ., 2005. 248 p.

7. Ponomarev S. V., Al-Busaidi S. S. S. Primenenie ballnykh kvalimetricheskikh shkal dlya otsenki indikatora «vozmozhnosti» uluchsheniya v SMK [The use of point qualimetric scales to assess the indicator of "opportunities" for improvement in the QMS]. *Metody menedzhmenta kachestva* [Quality management methods], 2016, no. 11, pp. 14–18.

8. Al-Busaidi S. S. S., Shakirova T. I., Ponomarev S. V. Primenenie pokazateley ispolneniya deyatelnosti pri planirovanii i prinyatii upravlencheskogo resheniya ob uluchshenii vkhodnogo kontrolya syrya [Application of performance indicators in planning and making management decisions to improve incoming control of raw materials].

Vestnik Tambovskogo gosudarstvennogo universiteta [Transactions of the Tambov State Technical University], 2018, vol. 24, no. 2, pp. 258–270.

9. Al-Busaidi S. S. S., Ponomarev S. V. K voprosu o formalizatsii verbalnykh otsenok, poluchennykh ekspertnymi metodami, pri podgotovke k prinyatiyu resheniy v sisteme upravleniya ispytatelnoy laboratoriey [On the issue of formalizing verbal assessments obtained by expert methods in preparation for decision-making in the testing laboratory management system]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2018, no. 3 (43), pp. 59–69.

10. Azhmukhamedov A. I. *Modeli i metody informatsionnoy podderzhki upravleniya sotsialnoy podsistemoy organizatsii na osnove nechetkogo kognitivnogo podkhoda* [Models and methods of information support for managing the social subsystem of an organization based on a fuzzy cognitive approach]. Tambov, 2017. 159 p.

11. Cheng-Jian Lin, Wen-Hao Ho. A Pseudo-Gaussian-Based Compensatory Neural System. *The IEEE International Conference on Fuzzy Systems*, 2003, pp. 214–219.

12. Samingun Handoyo, Achmad Efendi. Generating of Fuzzy Rule Dases with Gaussian Parameters Optimized via Fuzzy C-Mean and Ordinary Least Square. *International Journal of Technology Measurement*, November 2019, pp. 1–8.

13. Kuo R. J., Cheng W. C. An Intuitionistic Fuzzy Neural Network with Gaussian Membership Function, *Journal of Intelligent and Fuzzy Systems*, 2019, no. 36, pp. 6731–6741.

14. Dongrui Wu. Twelve Considerations in Choosing between Gaussian and Trapezoidal Membership Functions in Interval Type-2 Fuzzy Logic Controllers. *WCCI 2012 IEEE World Congress on Computational Intelligence June, 10–15, 2012, Brisbane, Australia.*

15. Zaydel A. N. *Oshibki izmereniy fizicheskikh velichin* [Measurement errors of physical quantities]. Saint Petersburg, Lan Publ., 2009. 112 p.

16. Kassandrova O. N., Lebedev V. V. *Obrabotka rezultatov nablyudeniy* [Processing of observation results]. Moscow, Nauka Publ., 1970. 104 p.

17. Mishchenko S. V., Ponomarev S. V. etc. *Istoriya metrologii, standartizatsii, sertifikatsii i upravleniya kachestvom : uchebnoe posobie* [A History of Metrology, Standardization, Certification and Quality Management: A Study Guide]. Tambov, Publishing House of Tambov State Technical Universityty], 2004. 112 p.

18. Byung-In Choi, Frank Chung-Hoon Rhee. Interval Type-2 Fuzzy Membership Function Generation Methods for Pattern Recognition. *Information Sciences*, 2009, no. 179, pp. 2102–2122.

19. Swarup Medasani, Jaeseok Kim, Raghu Krishnapuram. An Overview of Membership Function Generation Techniques for Pattern Recognition. *International Journal of Approximate Reasoning*, 1998, no. 19, pp. 391–417.

20. Beliakov Gleb. Fuzzy Sets and Membership Functions Based on Probabilities. *Information Sciences*, 1996, no. 91, pp. 95–111.

21. M. Reha Civanlar, H. Joel Trussell. Constructing Membership Function Using Statistical Data. *Fuzzy Sets and Systems*, 1986, no. 18, pp. 1–13.

22. Ping-Zong Lin and Tsu-Tian Lee. Robust Self-Organizing Fuzzy-Neural Control Using Asymmetric Gaussian Membership Function. *International Journal of Fuzzy Systems*, June 1978, vol. 9, no. 2, pp. 77–86.

23. Andres L. Medaglia, Shu-Cherng Fang, Henry L. W. Nuttle, James R. Wilson. An Efficient and Flexible Mechanism for Construction of Membership Functions. *European Journal of Operational Research*, 2002, no. 139, pp. 84–95.

24. Ventsel E. S. *Teoriya veroyatnostey* [Probability theory]. Moscow, Nauka Publ., 1969. 576 p.

УДК 004.931

АНАЛИЗ МЕТОДОВ КЛАССИФИКАЦИИ ДЕЙСТВИЙ ЧЕЛОВЕКА НА ВИДЕОИЗОБРАЖЕНИИ

Статья поступила в редакцию 21.01.2021, в окончательном варианте – 20.02.2021.

Марьенков Александр Николаевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат технических наук, доцент, ORCID: 0000-0003-1378-3553, e-mail: marenkovan17@gmail.com
Приходько Александр Александрович, Астраханский государственный университет, 414052, Российская Федерация, г. Астрахань, ул. Камышинская, 2,
магистрант, e-mail: alexsandr_498@mail.ru

В работе обоснованы актуальность и практическая значимость разработки новых методов анализа видеоизображения с целью классификации действий человека для дальнейшего выявления потенциально опасных инцидентов на объекте информатизации. Рассмотрены классификаторы на основе модели нейронной сети 3D ResNet, а также подходы, использующие векторную модель тела с применением библиотеки OpenPose. Первый эксперимент проведен с использованием модели нейронной сети 3D ResNet. Для обучения был использован датасет от Kinetic, включающий порядка 400 действий, среди которых присутствовали движения из единоборств. В тестовом наборе были использованы примеры из хоккейных драк и боевых приемов из фильмов. Следующий эксперимент заключался в классификации действия на базе анализа векторной модели тела человека. Kinect предоставляет данные о движении в виде иерархии основных узлов скелета человека, где вращение одних суставов относительно других представлено в виде кватернионов. Итоговое обучение модели происходило с применением датасета RGBU-D с 432 аннотированными действиями. В заключительном эксперименте для представления формализованного движения был выбран формат BVH. Переобучение модели проводилось на RGBU-D датасете, в связи с чем описание всех кадров пришлось изменить с 20 ключевых точек стандарта OpenPose до 17 из стандарта BVH, которые использовались в последующей работе с моделью. За основу конечного модуля по классификации действий, имеющихся на экране, была взята структура нейронной сети с LSTM-слоем с изменением входных данных – вместо набора фреймов из видео стал подаваться набор векторов тел людей в кадре. Обучение данной нейронной сети было проведено с использованием датасета в 2000 видеофайлов (1000 опасных ситуаций [в основном драки] и 1000 обычных действий в жизнедеятельности человека, не представляющие угрозы). Были проанализированы полученные результаты, сделаны выводы о применимости рассмотренных подходов для задачи распознавания действия человека на видеоизображении.

Ключевые слова: распознавание, глубокое обучение, нейронные сети, распознавание и классификация действий человека, выявление инцидентов, анализ видеоизображения

ANALYSIS OF METHODS FOR CLASSIFYING HUMAN ACTIONS ON A VIDEO IMAGE

The article was received by the editorial board on 21.01.2021, in the final version – 20.02.2021.

Marienkov Alexander N., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Engineering), ORCID: 0000-0003-1378-3553, e-mail: marenkovan17@gmail.com
Prikhodko Alexander A., Astrakhan State University, 2 Kamyshinskaya St., 414052, Astrakhan, Russian Federation,
undergraduate student, e-mail: alexsandr_498@mail.ru

The work justifies the relevance and practical significance of developing new methods for analyzing video images with the aim of classifying human actions for further identification of potentially dangerous incidents at the informatization facility. Classifiers based on model of neural network 3D ResNet, as well as approaches using vector model of body with application of library OpenPose are considered. The first experiment is made with use of model of neural network 3D ResNet. Dataset from Kinetic was used for training. That dataset is including about 400 actions, among which there were movements from martial arts. Examples from hockey fights and combat techniques from films were used in the testing set. The next experiment was to classify the action based on an analysis of a vector model of a human body. Kinect provides motion data in the form of a hierarchy of the main nodes of the human skeleton, where the rotation of some joints relative to others is represented in the form of quaternions. The final training of the model occurred using the RGBU-D dataset with 432 annotated actions. The BVH format was chosen to represent the formalized movement in the final experiment. Model retraining was carried out on the RGBU-D dataset, and therefore the description of all frames had to be changed from 20 key points of the standard OpenPose to 17 from the BVH standard, which were used in subsequent work with the model. The structure of the neural network with the LSTM layer with a change in input data was taken as the basis of the final module for classifying the actions available on the screen – instead of a set of frames, a set of vectors of people's bodies in the frame began to be supplied

from the video. Training of this neural network was carried out using a dataset in 2000 video files (1000 dangerous situations [mainly fights] and 1000 ordinary actions in human life that are not a threat). The results were analyzed as well as conclusions were made about the applicability of the approaches considered for the task of recognizing the action of a person on a video image.

Keywords: recognition, deep learning, neural networks, recognition and classification of human actions, incident detection, video image analysis

Graphical annotation (Графическая аннотация)

Введение. Системы видеонаблюдения являются одним из основных средств обеспечения безопасности на объекте информатизации. Видеонаблюдение позволяет организовать круглосуточный контроль за объектом с записью видеоархива для последующего анализа произошедших инцидентов. Однако конечный анализ происходящего на контролируемой территории проводит сотрудник службы безопасности, непосредственно наблюдающий за происходящим на экране монитора. В условиях большого количества видеокамер на сотрудника службы безопасности ложится трудновыполнимая задача анализа огромного потока видеоданных, непрерывно поступающих с объекта наблюдения [1].

В связи с этим становится актуальной задача автоматизации процесса анализа видеопотока с целью выявления инцидентов, возникающих на контролируемом объекте. В настоящее время уже существует множество разработок, направленных на предварительный анализ происходящего на видеоизображении: забытые предметы, оружие, проход людей в запретную зону (например, выход на железнодорожные пути), драки и т.п.

Несмотря на то, что проблемой анализа видеоряда занимается большое количество исследователей, данное направление все еще остается перспективным для совершенствования методик и разработки новых функциональных возможностей по анализу происходящего на экране монитора системы видеонаблюдения [8]. В рамках этой задачи основной проблемой является распознавание движений человека и их классификация. При этом стоит отметить, что на качество распознавания и классификацию движений влияют факторы, изменяющие походку человека (одежда, скрывающая человека; переносимые предметы: сумки, рюкзаки; неудобная обувь) или входные параметры изображения (ракурс, освещение, разрешение камеры, расстояние от человека до камеры) [3].

Цель данной работы – изучить и сравнить эффективность методов распознавания движений человека с применением различных нейросетевых технологий. Были рассмотрены классификаторы на основе модели нейронной сети 3D ResNet, а также подходы, использующие векторную модель тела с применением библиотеки OpenPose.

Проведение экспериментальных исследований, часть 1. Первый эксперимент был проведен с использованием модели нейронной сети 3D ResNet. Идентификация совершаемого действия человека в кадре основывается на анализе всего кадра [9].

Для обучения модели был использован датасет от Kinetic с большим количеством действий. Действия в датасете уже размечены и включают в себя порядка 400 наименований, среди которых также есть действия из единоборств. Наличие примеров с единоборствами стало причиной отбора данного датасета для обучения модели (так как является уникальным фактором относительно других подобных публичных датасетов для распознаваний действий) на поиск потенциально опасных инцидентов на контролируемом объекте. Для тестирования обученной модели была использована выборка, включающая хоккейные драки и боевые приёмы из фильмов.

После окончания обучения модели на 10 эпохе и проверки кроссвалидации на выборке из «живых ситуаций», были получены неудовлетворительные результаты, а именно, было выявлено, что данная модель не может верным способом стабильно определять предполагаемые опасные действия человека на видеоизображении.

Итоговые результаты по первичному эксперименту с определением действий человека представлены в таблице ниже (табл. 1), а динамика во времени представлена на изображении ниже (рис. 1).

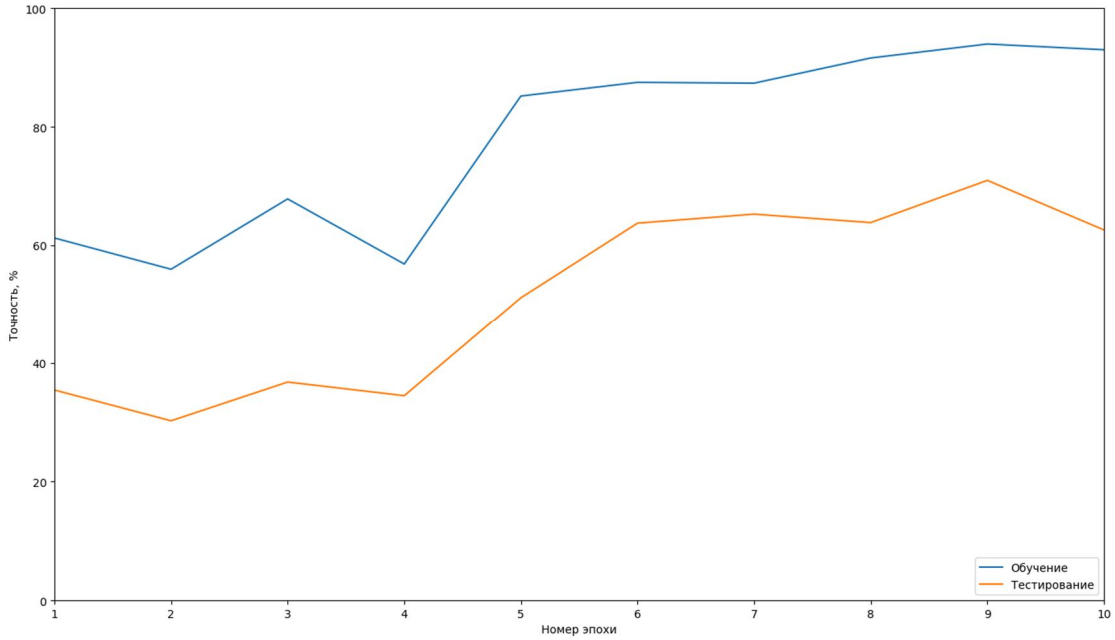


Рисунок 1 – Изменение точности во время обучения

Таблица 1 – Результаты обучения модели на основе нейронной сети 3D ResNet

Количество эпох	Фаза обучения		Фаза валидации	
	Ошибки	Точность	Ошибки	Точность
10	0,2920	0,9059	0,1703	0,5633

Проведенный анализ эксперимента показал, что причиной некорректного выявления действия на конечной выборке являлся тот фактор, что в кадре присутствовало несколько людей, выполняющих разные действия, а также для первой модели важную роль играло окружение, что в случае решения задачи не является опорным пунктом выполнения предсказания об обстановке на объекте информатизации, так как обстановка там по большей части будет неизменной.

Проведение экспериментальных исследований, часть 2. Второй эксперимент заключался в классификации действия на базе анализа векторной модели тела человека.

Векторная модель тела человека есть формализованное представление движения человека, где в виде векторов представлены кости человеческого скелета, а углам между ними соответствуют углы поворота основных узлов человеческого тела друг относительно друга.

Kinect предоставляет данные о движении в виде иерархии основных узлов скелета человека, где вращение одних суставов относительно других представлено в виде кватернионов (роль вращающихся векторов выполняют кости скелета), а смещение представлено в виде трехмерных векторов в локальной для каждого узла системе координат.

С целью улучшения результатов и ухода от прошлых ошибок последующий эксперимент проходил в направлении получения векторной модели тела человека и его анализа для классификации действия по вектору. Пример практической реализации данного подхода представлен на рисунке ниже (рис. 2) [8].

Рисунок 2 – Работа библиотеки OpenPose

Данный подход основан на предположении, что данные о позе человека, извлеченные из видеороликов, содержат достаточную информацию для обучения классификатора, способного распознавать отдельные действия и получать представления для оценки всего состояния в целом [4].

Таким образом, сперва необходимо получить вектор, описывающий текущее движение человека на видеоизображении. Дальнейшим шагом является сопоставление векторов по методу ближайшего соседа для выявления дескриптора движения и классификации действия объекта. Сама классификация действия происходит за счёт использования метода ближайшего соседа на эталонных векторах положения суставов для конкретных действий и вектора, полученного с изображения. При нахождении наименьшего сдвига с эталоном выбирается итоговое действие в классификаторе, пример эталонных векторов для бега представлен на рисунке ниже (рис. 3) [10].

Рисунок 3 – Временно-пространственное представление вектора тела

Итоговое обучение модели происходило с применением датасета RGBU-D с 432 аннотированными действиями. Процесс обучения проходил вплоть до 10 эпох с итоговой точностью 47,32 %, динамика которого представлена на рисунке ниже (рис. 4), а результаты представлены в таблице ниже (табл. 2).

Полученный результат показал, что переход к пространственно-временной модели классификации действий благоприятно повлиял на накопительную часть в обучении, но, к сожалению, не дал ожидаемых результатов, как и описанный ранее эксперимент.

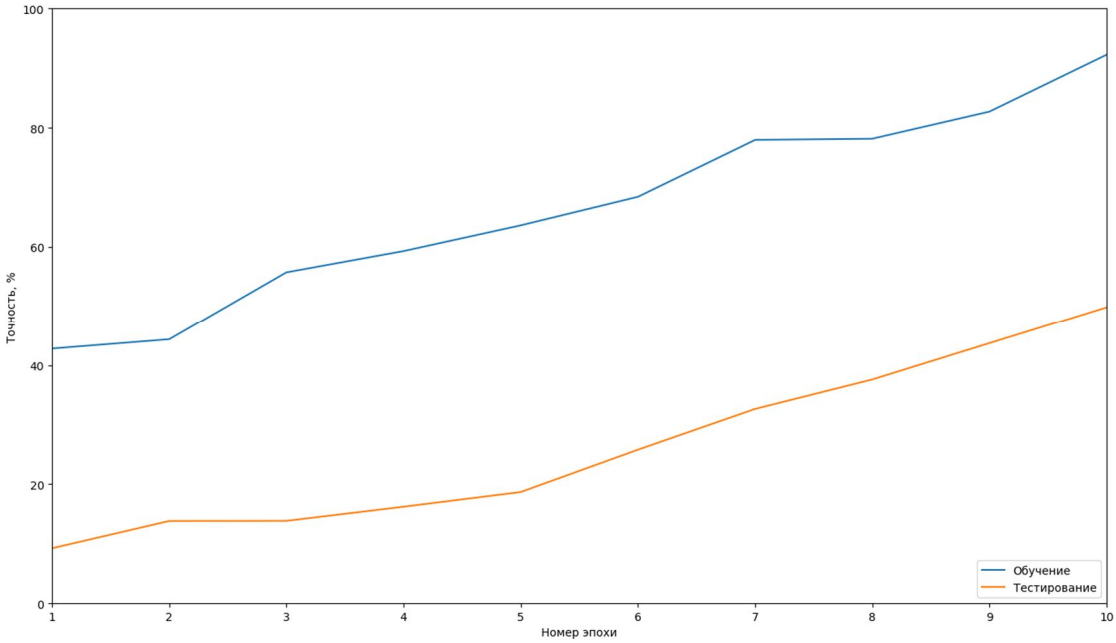


Рисунок 4 – Изменение точности во время обучения

Таблица 2 – Результаты по ошибкам первого и второго рода на обучающей выборке

	Верная гипотеза	
	H_0 Действие есть	H_1 Действия нет
Количество принятых решений	Действие распознано верно / 50 раз	Распознано несуществующее действие / 7 раз
	Действие не распознано / 0 раз	Не найдено несуществующих действий / 43 раза

Проведение экспериментальных исследований, часть 3. В третьем эксперименте для представления формализованного движения был выбран формат BVH, как наиболее распространенный и наиболее полно описывающий структуру человеческого тела. BVH обозначает данные Bio Vision Hierarchical. Этот формат предоставляет возможность представления информации об иерархии каркаса тела человека в добавление к данным о движении. Каждый элемент скелета, визуализация которого представлена на рисунке ниже (рис. 5), содержит в себе информацию о смещении и вращении относительно родительского элемента. Вращение представляется в углах Эйлера.

Переобучение модели проводилось на RGBU-D датасете [5], в связи с чем описание всех кадров пришлось изменить с 20 ключевых точек стандарта OpenPose до 17 из стандарта BVH, которые использовались в последующей работе с моделью.

За основу конечного модуля по классификации действий, имеющихся на экране, была взята структура нейронной сети с LSTM-слоем с изменением входных данных – вместо набора фреймов из видео стал подаваться набор векторов тел людей в кадре.

Рисунок 5 – Построение векторной модели тела человека

Подобный подход призван ускорить скорость обработки, а следовательно, и обучения в целом, а также уменьшить требуемое потребление ресурсов во время обучения и использования модели в программном продукте конечным пользователем.

Обучение данной нейронной сети был проведено с использованием датасета в 2000 видеофайлов (1000 опасных ситуаций [в основном драки] и 1000 обычных действий в жизнедеятельности человека, не представляющие угрозы). Отличием данного датасета от предыдущих является включение данных, полученных в рамках исследования Kinect-датчиков, совместно с видеофрагментами драк из фильмов и спортивных матчей, также постановочных драк и видео с публичных камер наружного видеонаблюдения [7].

Для поиска человека в кадре была использована предобученная модель YOLOv3 на датасете COCO, которая уже способна выявлять человека на кадре «из коробки» [2]. Поиск человека в кадре обоснован уменьшением математических вычислений для случаев, когда людей в кадре нет.

На последующем шаге понадобилось обучить модель LightTrack [6], визуализация обучения которой представлена на рисунке ниже (рис. 6), для плавного связывания объектов при переходе между кадрами. Бонусным эффектом было получено присуждение уже имеющегося номера объектам, которые возвращались в кадр из того же положения, с которого они пропали.

Обучение модели LightTrack было закончено на 23 эпохе. Суммарное время обучения заняло 4 часа. Конечная точность модели остановилась на 96,32 %.

Затем потребовалось переобучить модель по построению векторной модели структуры человека, что заняло ещё 22 часа на 15 эпох, но для дальнейшей работы использовалась резервная копия от результата 14 эпохи как наиболее стабильной.

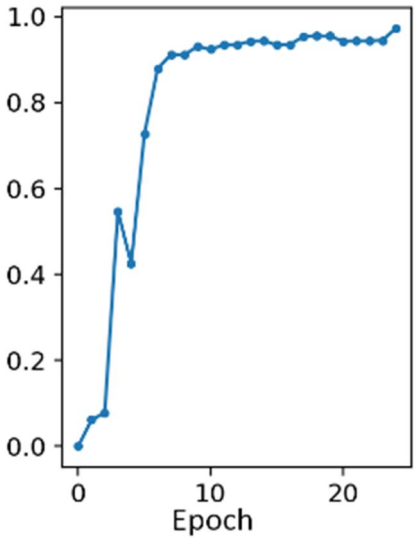


Рисунок 6 – Изменение точности во время обучения

Заключительный этап заключался в обучении модели для классификации векторных моделей людей с целью определения выявления инцидента (например, драки) на видеоизображении. Обучение данной модели заняло 18 часов, визуализация которого представлена на рисунке ниже (рис. 7), со стабильным потреблением 4 Гб оперативной памяти и 2 Гб видеопамяти на всё время обучения на площадке Google Colaboratory. Дальнейшее обучение с целью повышения точности возможно, но является трудоёмким процессом по причине имеющихся ограничений со стороны площадки.

В конечном итоге точность выявления инцидентов на видеоизображении составила 77,56 % на 15 эпохе обучения.

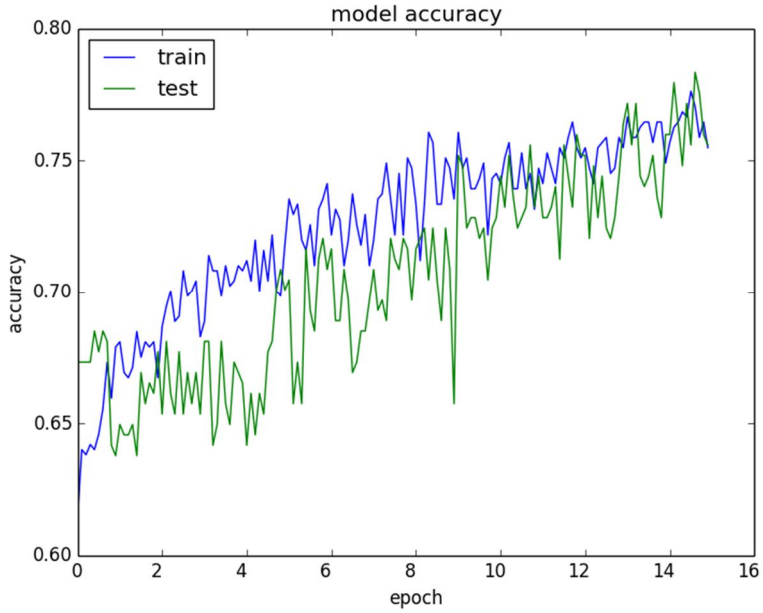


Рисунок 7 – Изменение точности модели во время обучения

Заключение. В работе был проведен обзор методов распознавания движений человека на видеоизображении. Представлены результаты экспериментов, демонстрирующих возможности данных методов:

- распознавание действий с помощью сети 3D ResNet (итоговая точность 56,33 %);
- распознавание действий человека с помощью анализа векторной модели человека (итоговая точность 47,32 %);
- распознавание действий нейронной сетью с LSTM-слоем с изменением входных данных – вместо набора фреймов из видео стал подаваться набор векторов тел людей в кадре (итоговая точность 77,56 %).

В результате проведенных экспериментов были выявлены возможности представленных в работе подходов по распознаванию и классификации действий человека в кадре. На основании полученных результатов был сделан выбор в пользу нейронной сети с LSTM-слоем, получающей на вход вектора людей для распознавания действий.

Дополнительно стоит отметить, что во всех экспериментах использовались различные датасеты, что также повлияло на итоговую точность. Однако полученные результаты позволяют интерпретировать общую эффективность методов и позволяют сделать выводы о возможностях рассмотренных методов распознавания и классификации движений человека при анализе видеоизображения.

Библиографический список

1. Дуленко В. А. Анализ подходов к обеспечению безопасности на городских территориальных объектах в рамках реализации Концепции «Безопасный город» / В. А. Дуленко, В. А. Пестриков // Вестник ВЭГУ. – 2011. – № 4 (54). – С. 22–27.

2. Белясников С. А. Методы обнаружения движущихся объектов в видеопотоке / С. А. Белясников, Р. С. Дорофеев // Молодежный вестник ИрГТУ. – 2016. – № 2. – С. 4.

3. Бокова О. И. К вопросу о внедрении механизмов интеллектуального анализа в информационную среду АПК «Безопасный город» / О. И. Бокова, В. С. Дунин, Н. С. Хохлов // Моделирование, оптимизация и информационные технологии. – 2015. – № 4. – С. 18.

4. Буйко А. Ю. Выявление действий на видео с помощью рекуррентных нейронных сетей / А. Ю. Буйко, А. Н. Виноградов // Программные системы: теория и приложения. – 2017. – Т. 8, № 4 (35). – С. 327–345.

5. RGBU-D Датасет. – Режим доступа: https://rgbd-dataset.cs.washington.edu/, свободный. – Заглавие с экрана. – Яз. англ.

6. CMU-Perceptual-Computing-Lab. – Режим доступа: https://github.com/CMU-Perceptual-Computing-Lab/openpose, свободный. – Заглавие с экрана. – Яз. англ.

7. Li Y. Online human action detection using joint classification-regression recurrent neural networks / Y. Li, C. Lan, J. Xing, W. Zeng, C. Yuan, J. Liu. – 2016. – Режим доступа: https://arxiv.org/abs/1604.05633v2, свободный. – Заглавие с экрана. – Яз. англ.

8. Francois Chollet. Deep Learning with Python / Francois Chollet. – MANNING Shelter Island, 2018. – С. 361.

9. Ормонейт Д. Циклическое обучение и отслеживание человеческого движения / Д. Ормонейт, Х. Сиденбладш, М. Блэк, Т. Хасти // Достижения в области обработки информации нейронными системами. – 2011. – № 13. – С. 894–900.

10. Тройже Н. Декомпозиция биологического движения: Фреймворк анализа и синтеза человеческой походки / Н. Тройже // Журнал зрения, нейронауки и психологии систем визуализации. – 2002. – № 5. – С. 371–387.

References

1. Dulenko V. A., Pestrikov V. A. Analiz podkhodov k obespecheniyu bezopasnosti na gorodskikh territorialnykh obektakh v ramkakh realizatsii Koncepcii «Bezopasnyy gorod» [Analysis of approaches to ensuring security at urban territorial sites in the framework of the implementation of the Safe City Concept]. *Vestnik VEGU* [VEGU Bulletin], 2011, no. 4 (54), pp. 22–27.

2. Belyasnikov S. A., Dorofeev R. S. Metody obnaruzheniya dvizhushchikhsya obektov v videopotoke [Methods of detecting moving objects in a video stream]. *Molodezhnyy vestnik IrGTU* [ISTU Bulletin of Youth], 2016, vol. 2, p. 4.

3. Bokova O. I., Dunin V. S., Khokhlov N. S. K voprosu o vnedrenii mekhanizmov intellectual nogo analiza v informatsionnuyu sredu APK "Bezopasnyy gorod" [On the introduction of mechanisms of intellectual analysis in the information environment of the agro-industrial complex "Safe City"]. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii* [Modeling, optimization and information technologies], 2015, vol. 4, p. 18.

4. Buyko A. Yu., Vinogradov A. N. Vyyavlenie deystviy na video s pomoshchyu rekurrentnykh neyronnykh setey [Identification of actions on video using recurrent neural networks]. *Programmnye sistemy: teoriya i prilozheniya* [Software systems: theory and applications], 2017, vol. 8, no. 4, pp. 327–345.

5. *RGBU-D Dataset*. Available at: https://rgbd-dataset.cs.washington.edu/

6. *CMU-Perceptual-Computing-Lab*. Available at: https://github.com/CMU-Perceptual-Computing-Lab/openpose.

7. Li Y., Lan C., Xing J., Zeng W., Yuan C., Liu J. *Online human action detection using joint classification-regression recurrent neural networks*, 2016. Available at: https://arxiv.org/abs/1604.05633v2.

8. Francois Chollet. *Deep Learning with Python*. MANNING Shelter Island, 2018, p. 361.

9. Ormoneit D., Sidenbladh H., black M., Hastie, T. Vyyavlenie deystviy na video s pomoshchyu rekurrentnykh neyronnykh setey [Cyclic training and tracking human motion]. *Programmnye sistemy: teoriya i prilozheniya* [Advances in information processing by neural systems], 2011, vol. 13, pp. 894–900.

10. Troige N. Dekompozitsiya biologicheskogo dvizheniya: Freymvork analiza i sinteza chelovecheskoy pokhodki [Decomposition of biological movement: A framework for analyzing and synthesizing human gait]. *Zhurnal zreniya, neyronauki i psikhologii sistem vizualizatsii* [Journal of Vision, Neuroscience and Psychology of Visualization Systems], 2002, vol. 5, pp. 371–387.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

УДК 519.8, 004.942

ФУНКЦИЯ КОББА – ДУГЛАСА ДЛЯ ПРОГНОЗИРОВАНИЯ СОСТОЯНИЯ МНОГОМЕРНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ

Статья поступила в редакцию 09.11.2020, в окончательном варианте – 18.01.2021.

Масаев Сергей Николаевич, Сибирский федеральный университет, Российская Федерация, 660041, г. Красноярск, пр. Свободный, 82,
кандидат технических наук, ORCID: 0000-0002-5825-2708, e-mail: faberi@list.ru

Высокая скорость прогнозирования состояния объекта исследования двухфакторными математическими моделями делает их сегодня востребованными. В статье точность прогнозирования достигнута за счет выполнения задачи идентификации объекта исследования. Рассмотрена двухфакторная модель Кобба – Дугласа для прогнозирования состояния производственной системы. Обзор работ применения двухфакторной модели Кобба – Дугласа показал, что она востребована и распространена. В современных условиях изменение характера взаимодействия факторов производства под воздействием новых факторов снижает точность прогноза. Рост количества факторов производства и влияние внешней среды затрудняет применение функции Кобба – Дугласа. Изменения взаимосвязи факторов производства образуют новые локальные функции. Установлено, что в сложных динамических объектах важность локальных функций меняется. Изменение взаимодействия факторов производства зависит от влияния внешней среды и определяет динамику развития системы. Предложен алгоритм КОББА расчета двухфакторной модели производственной системы. В авторских методе и программе реализован алгоритм и получены значения производственной функции Кобба – Дугласа. Для оценки взаимодействия факторов производства в работе рассмотрена динамическая система, которая состоит из восьми предприятий. Выполнен классический расчет двухфакторной модели как динамической системы через регрессионное уравнение. Также выполнен расчет трех локальных функций, которые можно использовать в функции Кобба – Дугласа для прогноза. Регрессионное уравнение использовано для оперативного (быстрого) прогнозирования динамической системой с учетом изменения его размерности и влияния параметров внешней среды. Достигнута заданная точность прогноза.

Ключевые слова: теория управления, динамическая система, функция Кобба – Дугласа, двухфакторная модель, производственная система, факторы производства, локальная функция, идентификация

THE FORECASTING OF STATE MULTI-DIMENSIONAL DYNAMIC SYSTEM BY COBB – DOUGLAS FUNCTION

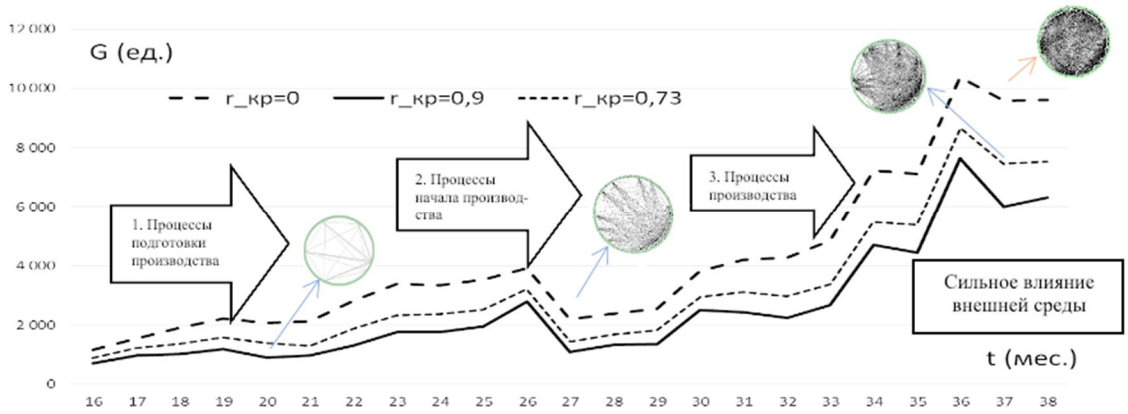
The article was received by the editorial board on 09.11.2020, in the final version – 18.01.2021.

Masaev Sergey N., Siberian Federal University, 79, Svobodnyy Ave., Krasnoyarsk, 660041, Russian Federation,
Cand. Sci. (Engineering), ORCID: 0000-0002-5825-2708, e-mail: faberi@list.ru

The high speed of predicting the state of the research object by two factor mathematical models makes them in demand today. In the article, the forecasting accuracy is achieved by performing the task of identifying the research object. A two-factor Cobb – Douglas model for predicting the state of the production system is considered. A review of researches on the application of the two factorial Cobb – Douglas model showed that it is well known and widespread. In modern conditions, the change in the nature of the interaction of production factors under the influence of new factors reduces the accuracy of the forecast. The growth in the number of factors of production and the influence of the external environment make it difficult to use the Cobb – Douglas function. Changes in the relationship of factors of production form new local functions. It was found that in complex dynamic objects the importance of local functions changes. A change in the interaction of production factors depends on the influence of the external environment and determines the dynamics of the development of the system. An algorithm COBBA for calculating a two factor model of a production system is proposed. In the author's method and program, an algorithm is implemented and the values of the Cobb – Douglas production function are obtained. To assess the interaction of production factors in the research, a dynamic system is considered, which consists of eight enterprises. The classical calculation of the two factor model as a dynamic system through the regression equation is performed. Also we calculated three local functions that can be used in the Cobb – Douglas function for forecasting. The regression equation is used for operational (fast) forecasting by a dynamic system, taking into account changes in its dimension and the influence of environmental parameters. The specified forecast accuracy has been achieved.

Keywords: control theory, dynamical system, Cobb – Douglas function, two factor model, production system, factors of production, local function, identification

Graphical annotation (Графическая аннотация)



Введение. В начале XX века соединение факторов производства труда и капитала давало наибольший прирост производства. В 1928 г. была предложена статистическая проверка взаимодействия этих факторов [1]. Такая статистическая проверка, двухфакторная модель, получила имя ее создателей производственная функция Кобба – Дугласа [1]. Главное достоинство двухфакторных моделей – это простая методология и быстрота расчета.

Двухфакторными моделями и подобными вопросами занимались Р. Солоу, К. Эрроу, В. В. Леонтьев, С. А. Айвазян, И. В. Елохова, Г. Б. Клейнер, Л. В. Канторович, А. Г. Гранберг, А. Г. Аганбегян, В. Ф. Кротов, В. С. Немчинов и другие [2–11].

В начале XXI века на взаимодействие труда и капитала в математической двухфакторной модели влияет очень много параметров. Например, фактор труд меняет свою структуру из-за механизации, автоматизации и цифровизации (промышленная революция). Капитал приобрел различные формы выражения: криптовалюты, различные виды ценных бумаг, паи и т. д. Кроме того, на взаимодействие труда и капитала одного объекта действует внешняя среда в виде взаимодействий труда и капитала других объектов. Все эти изменения снижают точность прогноза с помощью двухфакторных моделей, в том числе и прогноза функцией Кобба – Дугласа. Несмотря на эти трудности, и они нарастают, стремление человека получить преимущества в прогнозе доступными и быстрыми способами сохраняет функцию Кобба – Дугласа востребованной вот уже около ста лет. С первого взгляда функция Кобба – Дугласа проста, но включает в себя фундаментальные проблемы идентификации параметров объекта исследования, определения его размерности в точках наблюдения.

С учетом сложившихся обстоятельств актуально рассмотреть двухфакторную модель Кобба – Дугласа для прогноза состояния современной производственной системы при влиянии внешних условий.

Цель статьи – рассмотреть двухфакторную модель Кобба – Дугласа в процессе прогнозирования состояния производственной системой.

Для достижения цели необходимо выполнить задачи:

- объединить параметры производственных систем в многомерную динамическую систему;
- рассчитать локальные функции динамической системы на основе взаимосвязанности факторов производства, их формирующих;
- использовать функцию Кобба – Дугласа в ее классическом представлении;
- использовать функцию Кобба – Дугласа с рассчитанными локальными функциями;
- в динамической системе оценить возможность оперативного управления модернизированной функцией Кобба – Дугласа.

Для анализа динамической системы перейдем к формализации используемого подхода.

Используемый метод. Взаимодействие факторов производственной системы описывается следующим образом:

$$y = f(x_1, x_2 \ldots x_n). \quad (1)$$

Взаимодействие двух факторов в производственной системе представляется как

$$f(x_1, x_2) = const. \quad (2)$$

В 1872 г. В. Джевенс доказал математическое соотношение (2) и им обосновывал доходы производства. В 1930 г. продемонстрирована без доказательств производственная функция математиком Ч. Коббом и экономистом П. Дугласом:

$$y = b_0 + b_1 x_1 + b_2 x_2$$

или

$$Y = A \cdot L^{\alpha} \cdot K^{\beta}, \quad (3)$$

где Y – результат работы объекта; A – технология производства; x_L^{α}, L^{α} – связь Y от ресурсов, направленных на работу элементов объекта исполнителей L; x_K^{β} K^{β} – зависимость Y от ресурсов, направленных на совершенствование работы элементов объекта K; α, β – коэффициенты эластичности Y по L, K соответственно. Формула (3) и ее интерпретация выполнена под неизвестный объект. С классической интерпретацией (1)–(6) можно ознакомиться в отдельной работе [1, 5].

Для решения преобразуем модель в линейную форму

$$Ln(Y) = Ln(A \cdot L^{\alpha} \cdot K^{\beta}); \quad (4)$$

$$Ln(Y) = Ln(A) + \alpha Ln(L\ ) + \beta Ln(K\ ),$$

$$Ln(Y) = y,\ Ln(A) = b_0,\ \alpha = b_1,\ Ln(L) = x_1,\ Ln(K) = x_2; \quad (5)$$

$$y = b_0 + b_1 x_1 + b_2 x_2. \quad (6)$$

Для того чтобы выбрать для расчета значения L, K, необходимо найти наиболее важные элементы в объекте исследования через расчет взаимной корреляции наблюдаемых элементов объекта с учетом изменения его размерности и влияния параметров внешней среды в каждом периоде. Тогда представим объект исследования как динамическую систему

$$y(t) = A(t)x(t) + B(t)u(t) + v(t), \quad (7)$$

где $C = \{c_1, ..., c_n\}$ – список факторов производства; n – размерность; $T = \{t : t = 1, ..., T_{\max}\}$ – момент наблюдения; $x(t) = [x_1(t), x_2(t), ..., x_n(t)]^T$ – n – количество факторов производства, где $x_n(t)$ – значение факторов t пространства X в момент t. В виде фактора производства рассматривает имя бизнес-процесса, выполняемой работы на производстве. Пространство X_i формируется из $x_n^i(t)$. Классическое представление $X = [X_1, X_2, ..., X_i]^T$ дано В.Ф. у Кротова [11];

$u(t) = [u_1(t), u_2(t), ..., u_m(t)]^T$ – m – параметры управления факторами $x_n(t)$, где $u_m(t)$ – управление на фактор $x_n(t)$ в t;

$y(t) = [y_1(t), y_2(t), ..., y_z(t)]^T$ – z – наблюдаемые итоговые факторы производства, где $y_z(t)$ – наблюдаемые итоговые факторы производства отчета в момент t;

$v(t) = [v_1(t), v_2(t), ..., v_z(t)]^T$ – помеха, действующая на $x_n(t)$;

$A = \left[a_{ij} \right] - n \times n$ – матрица структуры и технологии производственного объекта, задаваемая через a_{ij} степень влияния факторов производства x_i и x_j;

$B = \left[b_{ij} \right] - n \times m$ – матрица структуры управления, через $u_m(t)$, где b_{ij} – ожидаемое взаимодействие между факторами производства x_i и x_j;

$H = \left[h_{ij} \right] - z \times n$ – матрица наблюдений объекта, позволяющая получить оценку $y_j(t)$ по фактическому уровню $x_j(t)$.

Тогда производственную систему можно рассмотреть как динамическую систему $S = \{T, X\}$ через матрицу $X_k(t)$

$$X_k(t) = \begin{bmatrix} x_1(t-1) & x_1(t-2) & \cdots & x_1(t-k) \\ x_2(t-1) & x_2(t-2) & \cdots & x_2(t-k) \\ \cdots & \cdots & \cdots & \cdots \\ x_n(t-1) & x_n(t-2) & \cdots & x_n(t-k) \end{bmatrix}, \quad (8)$$

где k – определяет количество моментов наблюдения, входящих в интервал анализа.

В отдельной работе динамическая система $S = \{T, X\}$ (производственной система) идентифицирована как цифровая копия предприятия [12]. Управление предприятием на основе цифровой копии предприятия рассмотрено в отдельных работах по методике управления менеджмента каче-

ства [13] и методике проектного управления [14]. В работе [15] динамическая система представлена как цифровой двойник образовательной организации.

Изменяя величину k, можно находить краткосрочное и долгосрочное влияние параметров внешней среды. Исследование величины k для разных параметров внешней среды подробно раскрыто в отдельной работе [16].

Далее для определения взаимного влияния факторов производства (1), (7) друг на друга используем метод интегральных показателей [12]. Взаимное влияние факторов производства для их объединения в локальные функции для подстановки в параметр L определяется корреляционной матрицей $R_k(t)$:

$$R_k(t) = \frac{1}{k-1} \overset{o}{X}{}_k^T(t) \overset{o}{X}_k(t) = \left\| r_{ij}(t) \right\|, \tag{9}$$

$$r_{ij}(t) = \frac{1}{k-1} \sum_{l=1}^{k} \overset{o}{x}_i(t-l) \overset{o}{x}_j(t-l) \quad , \; i, j = 1,...,n, \tag{10}$$

где t – моменты наблюдения; $r_{ij}(t)$ – коэффициенты взаимосвязи факторов динамической системы (коэффициенты корреляции) $x_i(t)$ и $x_j(t)$ в t.

Состояние динамической системы характеризует интегральный показатель на основе корреляционного графа $G_i(t)$:

$$G_i(t) = \sum_{j=1}^{n} \left| r_{ij}(t) \right|. \tag{11}$$

Состояние динамической системы за весь период наблюдения рассчитывается как:

$$G = \sum_{t=1}^{T=\max} \sum_{i=1}^{n} G_i(t). \tag{12}$$

Использование интегрального показателя (11) для управления цифровой копией предприятия рассмотрено в отдельной работе [12].

Реализацию предложенного метода представим в виде алгоритма.

Алгоритм эксперимента КОББА. Алгоритм анализа динамической системы выполняется по шагам:

1 шаг. Значения факторов производственной системы $x_n(t)$ отождествляются с выполняемыми работами, бизнес-процессами, формируем управление, параметры внешней среды и получаем динамическую систему (7). Вычисляем $G_i(t)$ по всем t. Из анализа взаимосвязи факторов (12) находим факторы с наибольшим корреляционным весом или объединяем их в локальную функцию по одному выбранному признаку и используем их вместо параметра L для прогнозного значения Y (3). Переходим к шагу 2.

2 шаг. Рассчитываем уравнение регрессии по параметрам K, L. По факторам производства можно выполнить оптимальное управление, которое будет влиять на прогноз Y [17]. Если уравнения регрессии рассчитаны, то переходим к шагу 3, иначе возвращаемся к идентификации значений факторов $x_n(t)$ в шаге 1.

3 шаг. Проверяем полученный набор прогнозных значений Y на соответствие нашим требованиям. Если выбранные факторы производства в L влияют неудовлетворительно на прогноз Y для пользователя алгоритма, то возвращаемся на шаг 1, иначе конец алгоритма.

Инструменты выполнения алгоритма КОББА. Идентификация факторов производства как динамической системы и выбор метода управления ей выполнены по запатентованному способу «Идентификация объекта как системы» (RU 2741138 C1). Решение о выдаче патента ФИПСом от 15.12.2020 по заявке 2019143313 от 23.12.2019.

Расчет шагов алгоритма выполняется в программах. Каждый шаг в алгоритме соответствует номеру программы по порядку:

1. Свидетельство ФИПС на ЭВМ № 2013614410. В программе моделируется объект как система. Задается структура взаимодействия переменных, вырабатывается управляющий сигнал, структура управляющего сигнала, параметры внешней среды.

2. Свидетельство ФИПС на ЭВМ № 2017616973. В программе объединяется выбранный метод контроля режимов работы системы и контур управления ей. Позволяет выбрать удобную форму интерпретации данных по методики управления.

3. Свидетельство ФИПС на ЭВМ № 2008610295. В программе оценивается оптимальность управленческого решения методом Р. Беллмана [17].

Задача реализована по способу и рассчитана в данном комплексе программ.

Практическая задача. Требуется выполнить прогноз Y (3) по сформированным локальным функциям (11) подставив их в параметр L. Предъявляемая точность к отклонению фактических данных от прогнозных значений не более 15 %.

Характеристики объекта исследования. Выполняем первый шаг алгоритма КОББА. Даны параметры: размерность производственной системы n = 9,6 млн факторов производства в 8 предприятиях i = 8, T = 5 лет, t = месяц. Пространство $X = [X_1, X_i, ..., X_8]^T$ состоит из двух предприятий деревообработки [18], двух производств изготовления сухих смесей для детей, одного строительного производства, одного нефтехимического производства и двух производств радиотехнических изделий. Каждое предприятие характеризуется основными процессами этапов своего развития за 5 лет: первый и второй год – это инвестиционные процессы формирования производства, третий и четвертый год – это запуск, работа и увеличение объемов производств, пятый год – это работа в одном темпе производства. Данные этапы определяют характер взаимосвязи и производственных функций $x_n(t)$. Подробное описание такого взаимодействия в реальном объекте можно посмотреть в работе [18].

Параметры управления в момент *t* заданы: u_1 – штраф за превышение привлеченного ресурса над потраченным ресурсом 20 %; u_2 – штраф 30 % на расходуемые ресурсы для выполняемых неавтоматизированных процедур; u_3 – штраф 2 % на расходуемые ресурсы для выполняемых автоматизированных процедур; u_4 – дополнительные ресурсы на 1 кВт/ч. энергии 3,2 усл. ед.; u_5 – 700 усл. ед. за доставку 1 куб. м.; u_6 – штраф за использование территории 200 000 усл. ед. за гектар.

Влияние внешней среды задано через параметры: v_1 – ежегодное + 4 % штрафа за ресурс; v_2 – рост штрафа за неавтоматизированные функции (в моделировании + 4 % ежегодно); v_3 – поступление ресурсов от собственника объекта; v_4 – технологические новинки; v_5 – движение материальных потоков; v_6 – мероприятия по улучшению логистики перемещения ресурсов; v_7 – трудовые ресурсы; v_8 – штрафы за технологию; v_9 – инфляция (в модели 4 % ежегодно); v_{10} – штраф за привлечение более востребованных ресурсов (в модели принято 1 усл. ед. за 70 усл. ед.). Вопросы ограниченного режима работы из других случайных факторов, например Covid-19, рассмотрены в работе [12, с. 5].

Результаты расчёта. Выполняем второй шаг алгоритма КОББА. Моделировалось состояние динамической системы из восьми производств общей размерностью 9,6 млн факторов производства на примере структуры факторов производства [18]. Прогнозные значения Y рассчитаны на основе параметров, объединенных в локальные функции производственных факторов и подставленных в значения L (табл. 1).

Таблица 1 – Прогноз состояния динамической системы в зависимости от параметра *L* (млрд усл. ед.)

Год	*Y*	*L*	*K*	Наблюдаемые параметры прогноза				Факт
				у_расход ресурса на неавтоматизированные работы	у_общие расходы ресурса	у_расход ресурса на восстановление инструментов выполнения процессов	у_перерабатываемый ресурс	у_факт
1	45,6	23,2	22,7	47,1	42,1	45,6	41,3	45,6
2	25,3	21,4	0,0	35,0	30,2	36,2	30,5	25,3
3	53,3	36,4	0,3	46,3	52,3	57,8	55,1	53,3
4	52,5	34,5	0,0	38,0	41,6	37,1	41,0	52,5
5	54,6	50,1	0,1	60,3	63,3	49,7	61,2	54,6

На основе расчитанных данных для факторов производства построены уравнения: (y_расход ресурса на неавтоматизированные работы) – $Y = 30035 \cdot L^{0,36} \cdot K^{0,02}$; (y_общие расходы ресурса) – $Y = 187,5 \cdot L^{0,67} \cdot K^{0,02}$; (y_расход ресурса на восстановление инструментов выполнения процессов) – $Y = 0,00003 \cdot L^{2,23} \cdot K^{0,04}$; (y_перерабатываемый ресурс) – $Y = 18962 \cdot L^{0,45} \cdot K^{0,04}$. Динамика прогноза по уравнениям представлена ниже (рис. 1).

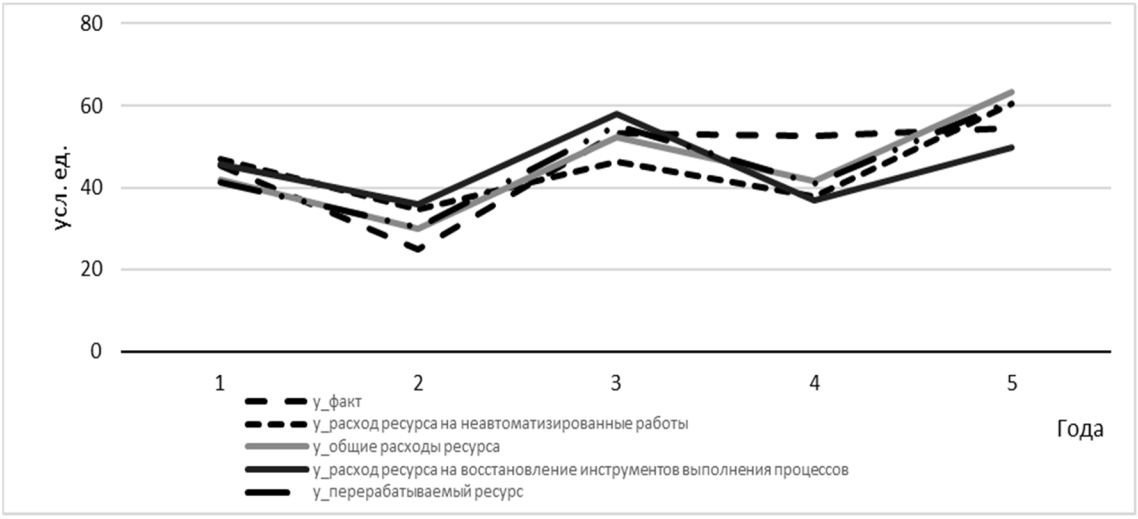


Рисунок 1 – Траектории прогнозных значений по уравнениям регрессии (6)

Выполняем третий шаг алгоритма КОББА. Рассчитанные уравнения проверяем на статистическую значимость (табл. 2).

Таблица 2 – Производственная функция (3)

L	**Уравнение**	$F_{табл}$	$F_{расч}$	**Множественный R**	**Коэффициент детерминации**	**Сумма отклонений**
Общие расходы ресурса	$Y = 187,5 \cdot L^{0,67} \cdot K^{0,02}$	7,71	0,13	0,77	0,59	5 %
Перерабатываемый ресурс	$Y = 18962 \cdot L^{0,45} \cdot K^{0,04}$	7,71	0,50	0,40	0,16	5 %
Расход ресурса на восстановление инструментов выполнения процессов	$Y = 0,00003 \cdot L^{2,23} \cdot K^{0,04}$	7,71	0,91	0,07	0,01	14 %
Расход ресурса на неавтоматизированные работы	$Y = 30035 \cdot L^{0,36} \cdot K^{0,02}$	7,71	0,44	0,45	0,20	12 %

Как видно (рис. 1), уравнения имеют похожую динамику и характеризуют линейное упорядоченное отношение параметров в динамической системе, где факторы производства, формирующие доминирующие локальные линейные функции, ограниченные структурой системы, при влиянии параметров внешней среды. При объединении объектов в динамическую систему доминирующие локальные функции уменьшают прогностические способности функции Кобба – Дугласа для управления динамической системой, так как реакция на влияние параметров внешней среды у них разная. Это подтверждается проверкой уравнений критерием Фишера. Ни одно уравнение с вероятностью 95 % статистически незначимо. Данный факт требует дополнительного обсуждения.

Обсуждение результатов. Однако видим (рис. 1), что уравнения (табл. 1) не отклоняются от фактического состояния исследуемого пространства X. Данное совпадение позволяет утверждать, что есть одинаковая реакция 8 предприятий под влиянием одних и тех же параметров внешней среды. Тогда рассматриваемая динамическая система ограниченна взаимоотношением этих 8 предприятий между собой под влиянием факторов внешней среды. Управление задается через выбор значимой локальной функции на основе факторов производства $x_n(t)$ как параметр L

(табл. 2), которые больше всего имеют взаимосвязь с остальными локальными функциями (факторами производства) в системе. К параметру K расходу ресурса на перенастройку системы и получение новых свойств системы подбирается параметр L в зависимости от типа деятельности динамической системы (табл. 1) и в силу динамичности процесса зависит от взаимосвязанности локальных функций относительно друг друга в момент времени *t*.

Если предположить, что все предприятия – это однотипные производственные системы, которые имеют высокую степень добавочной стоимости только физических ресурсов и материалов, тогда значение статистической значимости уравнений (3) станет 95 % и даже 99 %. На практике подобные динамические системы (7) состоят из разных производств, поэтому необходимо определять в каждом периоде важность G (11) локальных функций из взаимодействия факторов производства. Например, для производства высокоточных приборов значимое уравнение будет включать L из факторов производства локальной функции «расход ресурса на неавтоматизированные работы». Предприятие, производящее сухие смеси детского питания, адекватно характеризуется уравнением по параметрам локальной функции факторов производства «общие расходы ресурса».

Структура взаимодействия параметров динамической системы так устроена, что не зависит от коэффициента значимости $r_{\text{кр}}$, который рассчитывается по таблице значимости. Это легко проверить. Локальные функции факторов производства сохраняют взаимосвязь относительно друг друга при изменении коэффициента значимости $r_{\text{кр}}$ (определяется по таблице критических значений коэффициентов Пирсона для k = 6 при $\alpha = 0{,}95$, $r_{кр}$ =0,73). Формула (11) будет иметь вид $G_i(t) = \sum_{j=1}^{n} \left| r_{ij}(t) \right|$ при $\left| r_{ij}(t) \right| \geq r_{кр}$. Расчет для $r_{\text{кр}}$ =0, $r_{\text{кр}}$ =0,1 или $r_{\text{кр}}$ =0,9 (рис. 2) показывает, что рассматриваемая динамическая система имеет структуру, определяющую отношения факторов производства, и что их деятельность упорядочена с 1 по 23 период. Тогда можно добиваться различной точности прогноза при выполнении алгоритма эксперимента.

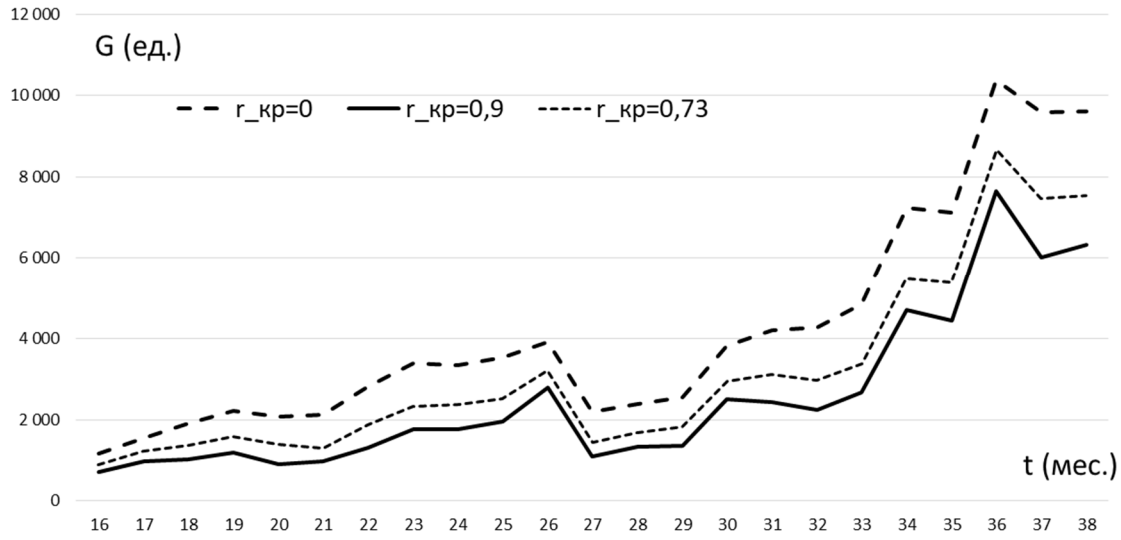


Рисунок 2 – Значение интегрального показателя (11) в зависимости от критического значения $r_{\text{кр}}$

Г.Б. Клейнер отмечал: «…производственная функция – это грубое, приближенное описание». Из этого он полагал, что нет возможности перейти к анализу конкретных комбинаций производственных факторов для их детального анализа при разумных затратах времени. Действительно, для ручного перебора 9,6 млн параметров одним человеком потребовалось бы около 30 тысяч лет. Традиционно это мнение поддерживалось. Однако в нашей работе мы показали, что утверждение Г.Б. Клейнер теряет свою актуальность. Через формулу (10) и формулу (11) возможно установить и анализировать конкретное влияние факторов производства друг на друга.

Прогнозирование состояния динамической системы в будущие моменты времени лучше использовать для укрупненного прогноза – для контура управления на верхнем уровне, где есть ограничение по времени час-два. Оперативное прогнозирование по 9,6 млн факторам производства системы – трудоемкая задача, но с сегодняшним развитием ЭВМ – выполнимая. Достаточно

перейти к оперативному управлению динамической системой по уравнению (1). Следовательно, рационально использовать комбинированное прогнозирование: для укрупненных (стратегических) и быстрых прогнозов функцию Кобба – Дугласа, так как обеспечивается требование по отклонению фактических данных от прогнозных значений не более 15 %. В комбинированном прогнозе уравнение (1) целесообразно использовать для оперативного управления, а уравнение (7) – для более долгого прогнозирования с подробным анализом взаимосвязей производственных факторов.

Статья выполнена в цикле работ по анализу динамических систем в условиях их применения в особых экономических зонах, задач идентификации взаимодействия человеко-машинных систем, децентрализованного управления, гибкого контура управления с выбором методики управления, оценок образовательных организаций и методов, санкций.

Заключение. Задачи, поставленные в начале работы, выполнены:

- объединены параметры производственных систем в динамическую систему $S = \{T, X\}$;
- определены локальные функции динамической системы на основе взаимосвязанности факторов производства, их формирующих;
- использована функция Кобба – Дугласа в ее классическом представлении: $Y = 30035 \cdot L^{0,36} \cdot K^{0,02}$;
- использована функция Кобба – Дугласа с вычисленными локальными функциями, подставленными в параметр L для трех случаев: $Y = 187,5 \cdot L^{0,67} \cdot K^{0,02}$; $Y = 0,00003 \cdot L^{2,23} \cdot K^{0,04}$; $Y = 18962 \cdot L^{0,45} \cdot K^{0,04}$;
- в динамической системе оценена возможность оперативного управления модернизированной функцией Кобба – Дугласа.

Стоит отдельно отметить, что получено комбинированное прогнозирование, в котором уравнение (1) целесообразно использовать для оперативного управления, а уравнение (7) – для более долго прогнозирования с подробным анализом взаимосвязей производственных факторов.

Выполнена практическая задача исследования через алгоритм КОББА с отклонением прогноза от фактических данных в диапазоне 5–14 %.

Цель, поставленная в начале работы, рассмотреть двухфакторную модель Кобба – Дугласа в процессе прогнозирования состояния современной производственной системы достигнута.

Библиографический список

1. Cobb C. W. A Theory of Production / C. W. Cobb, P. H. Douglas // American Economic Review. – December, 1928. – P. 139–165.

2. Golestani M. Robust Finite-Time Stabiliza-tion of Uncertain Nononlinear Systems Based on Partial Stability / M. Golestani, I. Mohammadzaman, M. J. Yazdanpanah // Nonlinear Dynamics. – 2016. – Vol. 85, no. 1. – P. 87–96.

3. Haddad W. M. Finite-Time Partial Stability and Stabilization, and Optimal Feedback Control / W. M. Haddad, A. L'Afflitto // Journal of the Franklin Institute. – 2015. – Vol. 352, no. 6. – P. 2329–2357.

4. Leontief W. W. The Structure of American Economy, 1919–1939 / W. W. Leontief. – Cambridge : Harvard University Press, 1941.

5. Клейнер Г. Б. Производственные функции: теория, методы, применение / Г. Б. Клейнер. – Москва : Финансы и статистика, 1986. – 239 с.

6. Немчинов В. С. Потребительная стоимость и потребительные оценки / В. С. Немчинов // Экономико-математические методы. – Москва : Изд-во АН СССР, 1963. – Вып. 1.

7. Аганбегяна А. Г. Экономика России на распутье… Выбор посткризисного пространства / А. Г. Аганбегяна. – Москва : АСТ, Астрель ; Владимир : ВКТ, 2010. – 185 с.

8. Гранберг А. Г. Василий Леонтьев в мировой и отечественной экономической науке / А. Г. Гранберг // Экономический журнал ВШЭ. – 2006. – № 3. – С. 471–491.

9. Гранберг А. Г. Основы региональной экономики / А. Г. Гранберг. – 4-е изд. – Москва : Изд. дом ГУ ВШЭ, 2004. 495 с.

10. Канторович Л. В. Математико-экономические работы / Л. В. Канторович. – Новосибирск : Наука, 2011. – 760 с.

11. Кротов В. Ф. Основы оптимального управления / В. Ф. Кротов. – Москва : Высшая школа, 1990. – 430 с.

12. Masaev S. N. Assessment various control methods a digital copy of enterprise by integral indicator / S. N. Masaev // Journal of Physics : Conference Series / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. – Krasnoyarsk, 2020. – P. 32011. DOI:10.1088/1742-6596/1679/3/032011.

13. Бережнова А. В. Управление процессами комплексной стандартизации деятельности предприятия : магистерская диссертация : 38.04.01 / А. В. Бережнова. – Красноярск : СФУ, 2016. – Режим доступа : http://elib.sfu-kras.ru/handle/2311/28693, свободный. – Заглавие с экрана. – Яз. рус.

14. Евдокименко Е. А. Оценка финансовой деятельности предприятия на основе эффективности бизнес-процессов : магистерская диссертация : 38.04.01 / Е. А. Евдокименко. – Красноярск : СФУ, 2018.

15. Dorrer M. G., The prototype of the organizational maturity model's digital twin of an educational institution / M. G. Dorrer // Journal of Physics : Conference Series, 1st International Scientific Conference «ASEDU-2020: Advances in Science, Engineering and Digital Education». – Krasnoyarsk, 2020. – Vol. 1691. – P. 012121. DOI: 10.1088/1742-6596/1691/1/012121.

16. Masaev S. Depth of Planning the State of a Dynamic Discrete System by Autocorrelation Function / S. Masaev // 2020 International Russian Automation Conference (RusAutoCon). – Sochi, Russia, 2020. – P. 989–993. DOI: 10.1109/RusAutoCon49822.2020.9208187.

17. Bellman R. Dynamic programming / R. Bellman. – New Jersey : Princeton University Press, 1957.

18. Masaev S. N. Acceptable area of optimal control for a multidimensional system / S. N. Masaev, G. A. Dorrer, V. V. Cyganov // Journal of Physics : Conference Series / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. – Krasnoyarsk, 2020. – P. 22091. DOI: 10.1088/1742-6596/1679/2/022091.

References

1. Cobb C. W., Douglas P. H. A Theory of Production. *American Economic Review*. – December, 1928, pp. 139–165.

2. Golestani M., Mohammadzaman I., Yazdanpanah M. J. Robust Finite-Time Stabiliza-tion of Uncertain Nononlinear Systems Based on Partial Stability. *Nonlinear Dynamics*, 2016, vol. 85, no. 1, pp. 87–96.

3. Haddad W. M., L'Afflitto A. Finite-Time Partial Stability and Stabilization, and Optimal Feedback Control. *Journal of the Franklin Institute*, 2015, vol. 352, no. 6, pp. 2329–2357.

4. Leontief W. W. *The Structure of American Economy 1919–1939*. Cambridge, Harvard University Press, 1941.

5. Kleiner G. B. *Proizvodstvennye funktsii: teoriya, metody, primenenie* [Production functions: Theory, methods, application]. Moscow, Finansy i statistika Publ., 1986, p. 239.

6. Nemchinov V. S. Potrebitelnaya stoimost i potrebitelnye otsenki [Use value and use ratings]. *Ekonomiko-matematicheskie metody* [Economic and mathematical methods]. Moscow, Publishing House of the Academy of Sciences of the USSR, 1963, vol. 1.

7. Aganbegyana A. G. *Ekonomika Rossii na raspute… Vybor postkrizisnogo prostranstva* [The Russian economy at a crossroads ... The choice of post-crisis space]. Moscow, AST Publ., Astrel Publ., Vladimir, VKT Publ., 2010, p. 185.

8. Granberg A. G. Vasily Leontiev in world and domestic economic science [Vasiliy Leontev v mirovoy i otechestvennoy ekonomicheskoy nauke] *Ekonomicheskiy zhurnal VSHE* [HSE Economic Journal], 2006, no. 3, pp. 471–491.

9. Granberg A. G. *Osnovy regionalnoy ekonomiki* [Fundamentals of Regional Economics]. 4th ed. Moscow, Publishing House of the Higher School of Economics], 2004, p. 495.

10. Kantorovich L. V. *Matematiko-ekonomicheskie raboty* [Mathematical and economic works]. Novosibirsk, Nauka Publ., 2011, p. 760.

11. Krotov V. F. *Osnovy optimalnogo upravleniya* [The Basics of Optimal Management]. Moscow, Vysshaya shkola Publ., 1990, p. 430.

12. Masaev S. N. Assessment various control methods a digital copy of enterprise by integral indicator. *Journal of Physics : Conference Series*. Krasnoyarsk, 2020, p. 32011. DOI:10.1088/1742-6596/1679/3/032011.

13. Berezhnova A. V. *Upravlenie protsessami kompleksnoy standartizatsii deyatelnosti predpriyatiya* [Management of the processes of integrated standardization of the enterprise]. Krasnoyarsk, Siberian Federal University, 2016.

14. Evdokimenko E. A. *Otsenka finansovoy deyatelnosti predpriyatiya na osnove effektivnosti biznes-protsessov* [Assessment of the financial activities of the enterprise based on the effectiveness of business processes]. Krasnoyarsk, Siberian Federal University, 2018.

15. Dorrer M. G., The prototype of the organizational maturity model's digital twin of an educational institution. *Journal of Physics: Conference Series, Volume 1691, 1st International Scientific Conference «ASEDU-2020: Advances in Science, Engineering and Digital Education»*. Krasnoyarsk, Russian Federation, 2020, p. 012121. DOI:10.1088/1742-6596/1691/1/012121.

16. Masaev S. Depth of Planning the State of a Dynamic Discrete System by Autocorrelation Function. *2020 International Russian Automation Conference (RusAutoCon)*. Sochi, Russia, 2020, pp. 989–993, DOI: 10.1109/RusAutoCon49822.2020.9208187.

17. Bellman R. *Dynamic programming*. New Jersey, Princeton University Press, 1957.

18. Masaev S. N., Dorrer G. A., Cyganov V. V. Acceptable area of optimal control for a multidimensional system. *Journal of Physics : Conference Series*. Krasnoyarsk, Russian Federation, 2020, p. 22091. DOI: 10.1088/1742-6596/1679/2/022091.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
И ЗАЩИТА ИНФОРМАЦИИ

DOI 10.21672/2074-1707.2021.53.1.063-074
УДК 004.051

ИССЛЕДОВАНИЕ ВОПРОСОВ СОВЕРШЕНСТВОВАНИЯ СИСТЕМ ЗАЩИТЫ ОТ DDOS-АТАК НА ОСНОВЕ КОМПЛЕКСНОГО АНАЛИЗА СОВРЕМЕННЫХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ

Статья поступила в редакцию 25.01.2021, в окончательном варианте – 30.01.2021.

Бачманов Дмитрий Андреевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID:0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Очередько Андрей Романович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

В статье представлены результаты анализа роста развития ботнет-сетей и новых киберугроз при их использовании злоумышленниками. Проведен обзор и сравнение моделей реализации ботнет-сетей, в результате которого основными являются два их вида. Выделены и классифицированы основные виды атак, реализуемых при помощи использования инфраструктуры распределенных компьютерных сетей, сформированных в 7 основных группах с учетом актуальности, распространенности и величины нанесенного ущерба. По результатам анализа было определено, что наиболее распространенной и актуальной является тип атаки «Отказ в Обслуживании». Представлена классификация сервисов, предоставляющих услуги обеспечения защиты сетевых ресурсов от распределенных атак по типу «Отказ в обслуживании», по типу развертывания, уровню защищённости и видам предоставляемых сервисов. Приведены критерии сравнения с учетом их инфраструктуры, наличия технической поддержки и тестового периода, доступных типов защиты, возможностей, дополнительных опций, оповещения и отчетности, а также лицензирования. Практически реализован и показан способ интеграции сервиса DDoS-Guard Protection с дополнительным модулем на уровне приложения, который позволил расширить методы защиты от DDoS-атак. Различные модификации совместного применения модуля и модифицируемой системы позволяют повысить ожидаемый уровень выявления и предотвращения кибератак.

Ключевые слова: кибербезопасность, защита информации, ботнет, DDoS, распределенные компьютерные сети, отказ в обслуживании, киберугрозы, модель OSI

RESEARCH OF THE ISSUES OF IMPROVEMENT OF PROTECTION SYSTEMS AGAINST DDOS-ATTACKS BASED ON THE COMPREHENSIVE ANALYSIS OF MODERN INTERACTION MECHANISMS

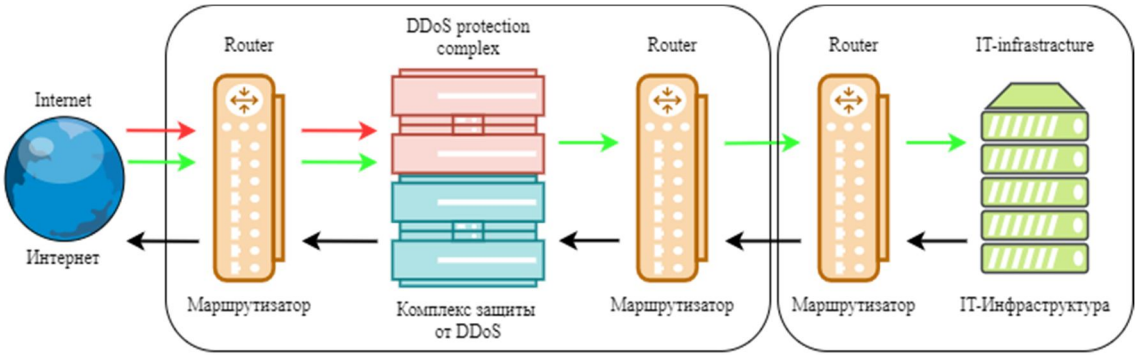
The article was received by the editorial board on 25.01.2021, in the final version – 30.01.2021.

Bachmanov Dmitriy A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
postgraduate, ORCID: 0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Ocheredko Andrey R., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
postgraduate, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

The article presents the results of an analysis of the growth in the development of botnet networks and new cyber threats when they are used by cybercriminals. A review and comparison of the models for the implementation of botnet networks is carried out, as a result of which there are two main types. The main types of attacks carried out using the infrastructure of distributed computer networks are identified and classified, formed into 7 main groups, taking into account the relevance, prevalence and amount of damage. Based on the results of the analysis, it was determined that the most widespread and relevant type of attack is “Denial of Service”. The article presents a classification of services that provide services to ensure the protection of network resources from distributed attacks by the "Denial of Service" type, by the type of deployment, the level of security and the types of services provided. The comparison criteria are given taking into account their infrastructure, availability of technical support and a test period, available types of protection, capabilities, additional options, notification and reporting, as well as licensing. Practically implemented and shown a way to integrate the DDoS-Guard Protection service with an additional module at the application level, which made it possible to expand the methods of protection against DDoS attacks. Various modifications of the combined use of the module and the modified system make it possible to increase the expected level of detection and prevention of cyber-attacks.

Keywords: cybersecurity, information security, botnet, DDoS, distributed computer networks, denial of service, cyber threats, OSI model

Graphical annotation (Графическая аннотация)



Введение. Современные возможности связи из любой точки планеты при помощи интернета и подключенных к ней устройств не только значительно расширили наши возможности, но и открыли неограниченное число реализаций для таких угроз, как вирусы, спам, кибератаки и многие другие варианты атак для киберпреступников. В отчетах по количеству атак типа «Отказ в обслуживании» (DDoS) при помощи распределенных компьютерных сетей аналитики склоняются к выводу, что угроза, которая зародилась в 1999 г., до сих пор является одной из самых актуальных, и количество подобных инцидентов стремительно растет [1, 2, 3, 4, 5]. К примеру, за 2-й и 3-й кварталы 2020 года общее количество DDoS-атак на киберпространства, по сравнению с аналогичным периодом прошлого года, увеличилось в полтора раза [6]. Опасность и распространённость использования распределенных сетей ботнет в качестве основного средства совершения кибератак отмечается в исследованиях и прогнозах ведущих аналитиков [7]. Кроме того, об этом говорит и анализ областей, которые подвергаются данным атакам (рис. 1).

Исследователи «Лаборатории Касперского» в своих отчетах отмечают, что, помимо приведенных отраслей, большое количество атак также приходилось на сетевые ресурсы силовых, образовательных и административных ведомств [8, 9]. По оценке специалистов McAfee и Центра стратегических и международных исследований, общая сумма денежных потерь в 2020 году из-за атак киберпреступников превысила 1 000 000 млн долларов, что составляет 1 % от мирового ВВП [10]. В рамках современных исследований в области кибербезопасности [11] защита от таких видов атак на киберпространство занимает одно из важнейших мест в структуре адаптивных распределенных интеллектуальных систем защиты информации [12].

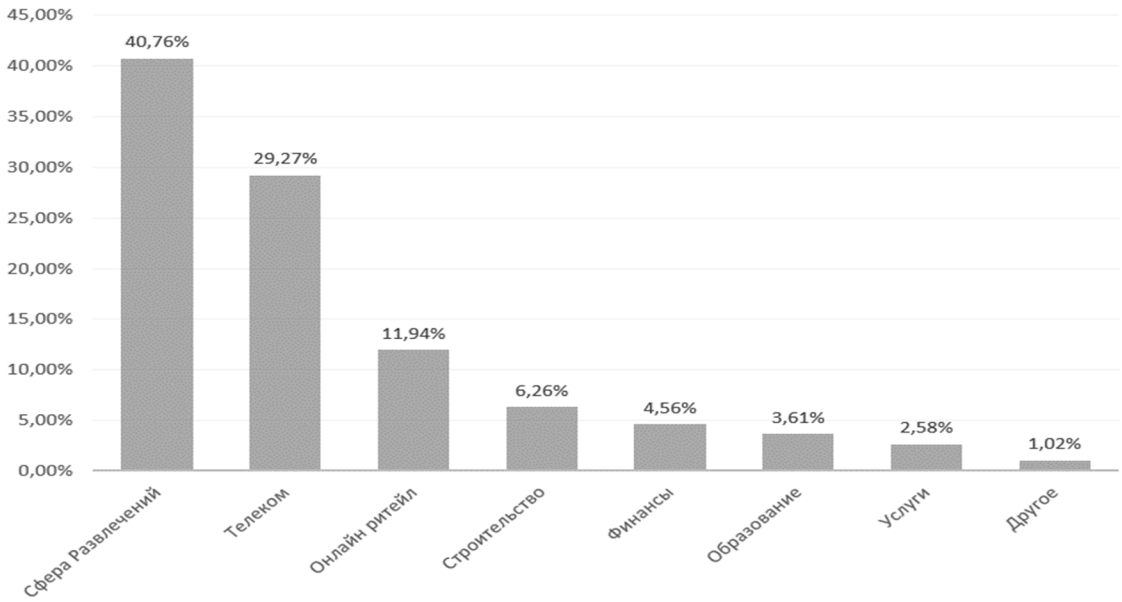


Рисунок 1 – Разделение областей, которые подвергаются атакам типа «Отказ в обслуживании» с применением распределенных компьютерных сетей

Характеристика ботнетов. Существует 2 модели реализации ботнетов (рис. 2). Реализация любой из них начинается с загрузки особого программного обеспечения со встроенным вредоносным кодом. После загрузки и установки устройство подключается к удаленному серверу, который был настроен как система управления сети (ботмастер). Используя систему управления, злоумышленник может периодически внедрять новый вредоносный код в установленную на устройство ботнета программу.

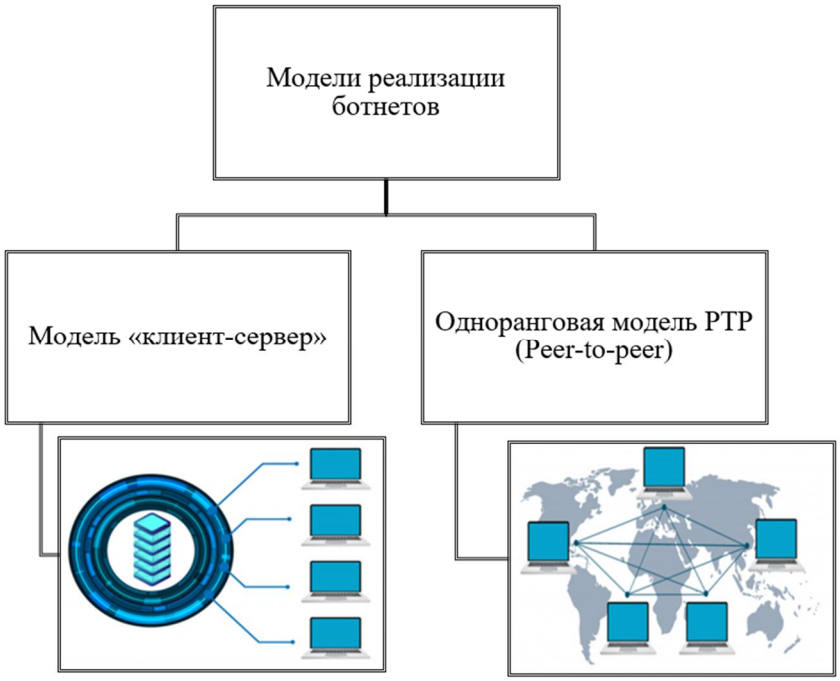


Рисунок 2 – Модели реализации ботнетов

Проведем сравнение моделей реализации ботнетов для выяснения их достоинств и недостатков (табл. 1).

Таблица 1 – Сравнение моделей реализации ботнетов

Название	Краткое описание	Достоинства	Недостатки
Модель «клиент – сервер»	Базовая сеть, в которой один сервер выступает в роли ботмастера, который посылает команды клиентам	Простота реализации и сохранение постоянного контроля над клиентскими устройствами	Легкость обнаружения и наличие одной контрольной точки, в отсутствии которой вся сеть перестает функционировать
Одноранговая модель PTP (peer-to-peer, P2P)	Каждое подключенное устройство работает независимо и как клиент, и как сервер. Координация и передача информации происходит между собой	Отсутствие централизованного управления и, вытекающая из этого, сложность детектирования	Не обнаружено

После построения ботнет-сети киберпреступник переходит к планированию, организации и реализации атак. Проведем сравнение основных типов ботнет-атак (табл. 2).

Таблица 2 – Сравнение основных типов ботнет-атак

Название атаки	Краткое описание	Сложность реализации	Уровень угрозы
Распределенные атаки типа «Отказ в обслуживании» (DDoS)	Лавинная посылка пакетов на целевую систему с целью исчерпания ресурсов и превышения полосы пропускания каналов связи	Низкая	Высокий
Применение шпионских программ и вредоносного ПО	Автоматическая установка программного обеспечения на устройствах входящих в распределенную компьютерную сеть	Высокая	Средний
Хищение персональной информации	Хищение персональной информации с зараженных устройств входящих в состав ботнета	Высокая	Высокий
Применение средств навязывания рекламы	Вредоносный код на зараженном компьютере может автоматически загружать, устанавливать и отображать всплывающие окна с рекламой или регулярно открывать в браузере определенные web-сайты	Средняя	Низкий
Рассылка спама	Отправка нежелательных сообщений по электронной почте	Средняя	Низкий
«Накручивание» кликов	Накрутка рекламной сети с оплатой за каждый клик с целью заставить платить определенного рекламодателя	Средняя	Средний
Фишинг	Поиск уязвимых серверов для размещения фишинговых сайтов с целью хищения персональных данных	Высокая	Высокий

В результате сравнения можно сделать вывод, что распределенные одноранговые P2P ботнет-модели являются сложно детектируемым средством совершения киберпреступлений с высоким уровнем угрозы реализуемых атак. Наиболее распространенной и требующей особого внимания являются распределенные атаки типа «Отказ в обслуживании» (DDoS), так как имеют относительно небольшую сложность реализации и высокую степень наносимого ущерба.

Классификация DDoS-атак. Обобщенная структура реализации такого вида атаки может быть представлена в виде структурированных объединенных групп-участников продолжительного по времени процесса (рис. 3).

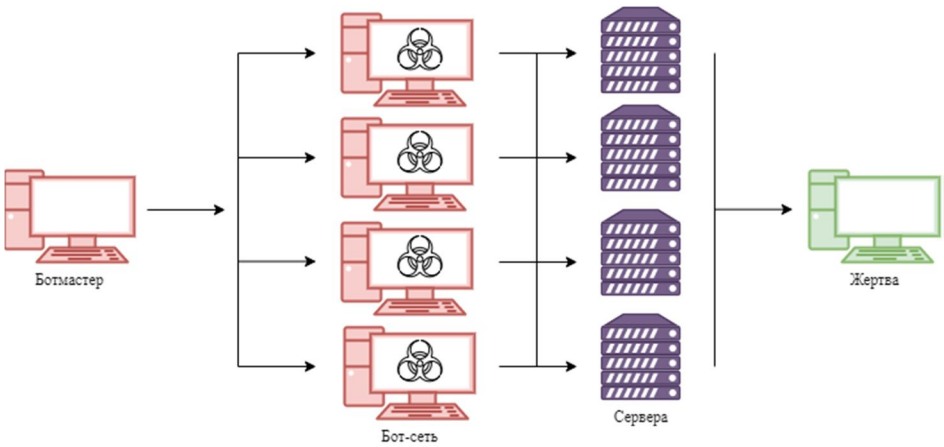


Рисунок 3 – Схема базовой DDoS-атаки

Опираясь на анализ способов реализации DDoS-атак, можно выделить основные виды (рис. 4) [13].

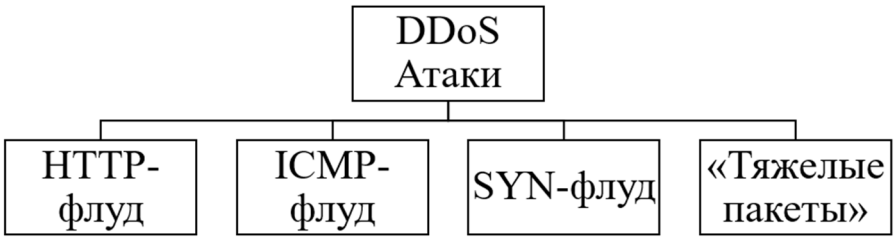


Рисунок 4 – Виды DDoS-атак

HTTP-флуд. Является самым распространённым типом DDoS-атаки. В специально сформированном запросе к серверу злоумышленник заменяет свой IP-адрес на сетевой идентификатор устройства внутри сети-жертвы, ожидая, что сервер на него ответит гораздо более емким ответом.

ICMP-флуд. Целью этого типа является перегрузка сетевого канала. Заключается в отправке ICMP-пакета усиливающей сети, либо через отправку UDP-пакетов. IP-адрес атакующего заменяется целевым, и на атакуемый сервер приходит ответ на команду, увеличенный во столько раз, сколько устройств подключено к усиливающей сети.

SYN-флуд. Так как компьютерам для совершения обмена информацией необходима установка соединения, при этом на само соединение выделяются компьютерные ресурсы – именно на их исчерпание направлена данная атака, отправляя ложные запросы на открытие соединений, которые не могут быть завершены до истечения тайм-аута.

«Тяжелые пакеты». Для реализации этого метода атаки злоумышленник с помощью ботнета отправляет серверу трудные для обработки пакеты данных, которые не переполняют канал связи, но отнимают ресурсы процессора, что может привести к его перегреву или перегрузке.

Из-за различия типов возникает проблема корректной и своевременной идентификации данных инцидентов информационной безопасности. Защита от слабых DDoS-атак организуется обобщенными процедурами настройки лимита подключений к серверу, ограничениями UDP-запросов и правильно настроенного Web application firewall (WAF). При более серьезных организованных многоэтапных атаках этими средствами уже не защититься, так как сам канал связи перестанет корректно функционировать. В этих случаях могут помочь только специальные средства защиты. Проведем сравнение и анализ современных средств защиты.

Средства защиты от DDoS-атак. В связи с высокой актуальностью данной проблемы на рынке представлено множество решений, позволяющих защищаться от распределенных атак типа «Отказ в обслуживании».

Существующие решения можно классифицировать по типу решения (рис. 5).

Рисунок 5 – Виды средств защиты от DDoS-атак по типу развёртывания

Достоинства локально развертываемых средств защиты заключаются в минимальной задержке, гибкой встраиваемости и самостоятельной настройке. При этом недостатки в виде высокой стоимости, необходимости нанимать и обучать персонал сопровождения, ограниченности функционала фильтрации и низкой пропускной способности явились причиной появления облачных и гибридных решений.

Облачные решения лишены недостатков высокой стоимости и необходимости содержать персонал сопровождения. Кроме того, они обладают высокой емкостью фильтрации и скоростью

подключения, имеют возможности получения экспертизы по эффективной нейтрализации атак и фильтрации атак на уровне веб-приложений. Из минусов можно выделить только увеличение задержки и необходимость пропуска конфиденциальных данных через облако.

Гибридные, в свою очередь, объединяют в себе как все хорошее от локальных и облачных типов, так и все плохое, нивелируя некоторые минусы друг друга.

Как правило, DDoS-атаки используют уязвимости и особенности сетевого и транспортного уровней модели взаимосвязи открытых систем (Open Systems Interconnection, OSI) [14], либо работают на уровне приложений и программных сервисов. В связи с этим появляется необходимость строить комплексную защиту, обеспечивающую высокий уровень детектирования и предотвращения подобных инцидентов. Определив требования, можно выделить следующие типы по уровню реализуемой защищенности, которую они осуществляют (рис. 6).

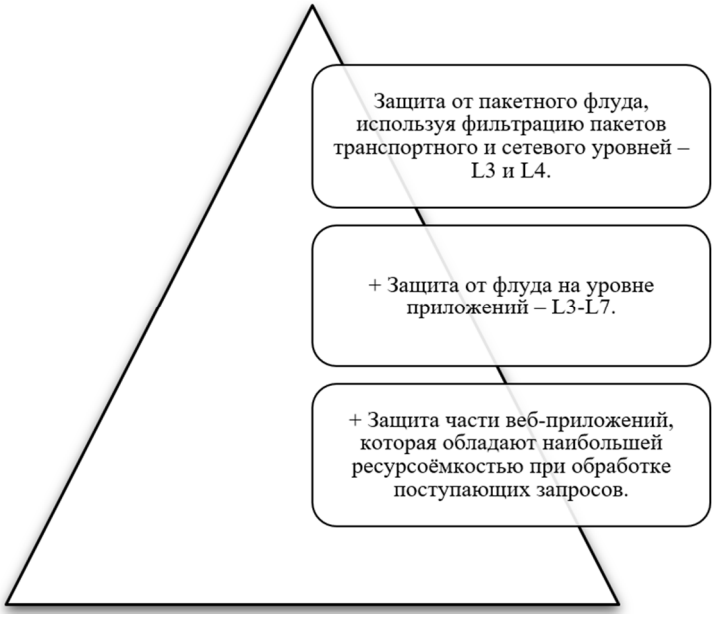


Рисунок 6 – Типы средств защиты от DDoS-атак по уровню защищенности

Включим в наше сравнение только те решения, которые обеспечивают минимум 2-й уровень защищенности и не являются индивидуальными решениями отдельных компаний. После анализа существующих решений сформировался список: Kaspersky DDoS Prevention, StormWall, Qrator, Ростелеком Anti-DDOS, DDoS-Guard Protection, CloudFlare DDoS Protection, Incapsula by Imperva.

Для сравнения будем использовать критерии комплексной оценки, которые были сформированы исходя из анализа мнений экспертов и подходящие для этого класса систем [15, 16, 17]:

1. Техническая поддержка – 7 %.
1.1. Дежурная смена реагирования на атаки 24 х 7.
1.2. Наличие русскоязычной технической поддержки.
2. Тестовый период – 3 %.
2.1. Наличие тестового периода.
2.2. Ограничения по функционалу во время тестового периода.
3. Инфраструктура – 10 %.
3.1. Наличие собственного/арендованного оборудования в ЦОД.
3.2. Используемое оборудование и ПО для очистки трафика.
4. Доступные типы подключаемой защиты – 25 %.
4.1. Защита сайта (смена А-записи DNS).
4.2. Защита сети (пула IP-адресов).
4.3. Защита автономной системы (ASN).
4.4. Услуги защищённого от DDoS ЦОД.
5. Возможности сервисов – 25 %.
5.1. Максимальная заявляемая мощность отражения атак в режиме statefull.
5.2. Фильтрация HTTPS без раскрытия ключей.
5.3. Возможность выделения нескольких IP для back-end.
5.4. Возможность балансировки между несколькими IP для back-end.

5.5. Заявленное время реакции на DDoS-атаку.

5.6. Заявленный процент ложных срабатываний под атакой (от легитимного трафика).

5.7. Возможность самостоятельно управлять фильтрацией трафика (включение/отключение/изменение параметров митигации).

5.8. Коридор гарантируемой доступности, в зависимости от тарифа (SLA), %.

5.9. Защита от ботов.

6. Дополнительные опции – 10 %.

6.1. Межсетевой экран уровня веб-приложений (WAF) (собственный, партнёрский).

6.2. Выделенные каналы MPLS VPN L2.

7. Система оповещения и отчетность – 5 %.

7.1. Экспорт отчётов.

7.2. Аналитика по трафику в личном кабинете.

8. Лицензирование – 15 %.

8.1. Ценовая политика (стоимость среднего тарифа).

Проведем сравнительный анализ выбранных систем (табл. 3).

Таблица 3 – Сравнение сервисов по полученным критериям

№ п/п	Наименование критерия	Kaspersky DDoS Prevention	Storm Wall	Qrator	Ростелеком Anti-DDOS	DDoS-Guard Protection	Incapsula by Imperva
1.1	Дежурная смена реагирования на атаки 24x7	0,07	0,07	0,07	0,07	0,07	0,07
1.2	Наличие русскоязычной технической поддержки	0	0,07	0	0	0,07	0
2.1	Наличие тестового периода	0,03	0,03	0,03	0,03	0,03	0,03
2.2	Ограничения по функционалу	0,03	0,03	0,03	0,03	0,03	0,03
3.1	Наличие собственного (арендованного) оборудования в ЦОД	0,1	0,1	0,1	0,1	0,1	0,1
3.2	Используемое оборудование и ПО для очистки трафика	0,1	0,1	0,1	0,05	0,1	0,1
4.1	Защита сайта (смена A-записи DNS)	0,25	0,25	0,25	0,25	0,25	0,25
4.2	Защита сети (пула IP-адресов)	0,25	0,25	0,25	0,25	0,25	0,25
4.3	Защита автономной системы (ASN)	0,25	0,25	0,25	0,25	0,25	0
4.4	Услуги защищённого от DDoS ЦОД	0	0,125	0,25	0,25	0,25	0
5.1	Максимальная заявляемая мощность отражения атак в режиме stateful	0,005	0,015	0,05	0,05	0,0125	0,05
5.2	Фильтрация HTTPS без раскрытия ключей	0,25	0,2	0,25	0,25	0,25	0,2
5.3	Возможность выделения нескольких IP для back-end	0,25	0,25	0,25	0,25	0,25	0,25
5.4	Возможность балансировки между несколькими IP для back-end	0,25	0,25	0,25	0,25	0,25	0,25
5.5	Заявленное время реакции на DDoS-атаку	0,15	0,15	0,2125	0,15	0,25	0,2375
5.6	Заявленный процент ложных срабатываний под атакой (от легитимного трафика)	0,2	0,2375	0,2375	0,25	0,245	0,25
5.7	Возможность самостоятельно управлять фильтрацией трафика (включение/отключение/изменение параметров митигации)	0	0,25	0	0,25	0,25	0,25
5.8	Коридор гарантируемой доступности, в зависимости от тарифа (SLA)	0,23	0,21	0,21	0,24	0,23	0,24
5.9	Защита от ботов	0,25	0,25	0,25	0,25	0	0,25
6.1	Межсетевой экран уровня веб-приложений (WAF) (собственный, партнёрский)	0,05	0,1	0,1	0,1	0,1	0,1
6.2	Выделенные каналы MPLS VPN L2	0,1	0,1	0,1	0,1	0,1	0
7.1	Экспорт отчётов	0,05	0,05	0,05	0,05	0,05	0,05
7.2	Аналитика по трафику в личном кабинете	0,05	0,05	0,05	0,05	0,05	0,05
8.1	Ценовая политика (стоимость среднего тарифа)	0,0135	0,054	0,0225	0,0405	0,15	0,0015
Итого:		2,93	3,44	3,36	3,56	3,59	3,01

Анализ результатов показывает, что сервисы DDoS-Guard Protection и StromWall являются самыми оптимальными. Решения от других компаний хоть и выигрывают по некоторым показателям, но в остальных либо проигрывают, либо предоставляют услуги, аналогичные с конкурентами за значительно большую стоимость. Так как система DDoS-Guard Protection предоставляет качество услуг на уровне с решением StromWall, но за меньшую стоимость, остановимся на ней и представим практическую реализацию дополнительных средств защиты на примере этой системы.

Практическая реализация. Функционал системы DDoS-Guard Protection покрывает практически все критерии эффективности, кроме пункта 5.9 – Защита от ботов. В рамках данной статьи мы рассмотрим способ интеграции данного решения с возможностью удовлетворять этому критерию, благодаря дополнительному модулю testcookie для NGINX, написанному на языке C.

Данный модуль позволит отсеять запросы ботов, которые используют HTTP-флуд и не имеют механизмов HTTP cookie и редиректа (рис. 7). В случае, если бот содержит данные механизмы, происходит проверка наличия в нем полноценного JavaScript Core (рис. 8). Если какое-либо условие является истиной, происходит отсеивание запросов от бота во время распределенной DDoS-атаки на уровень L7, некоторые из которых может пропустить DDoS-Guard Protection.

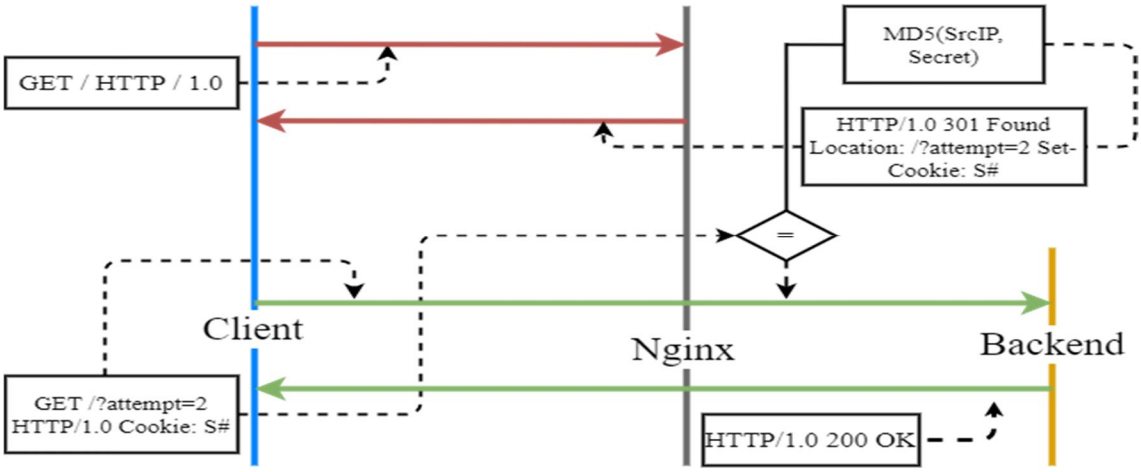


Рисунок 7 – Алгоритм работы модуля при отсутствии в боте механизмов редиректа и cookies

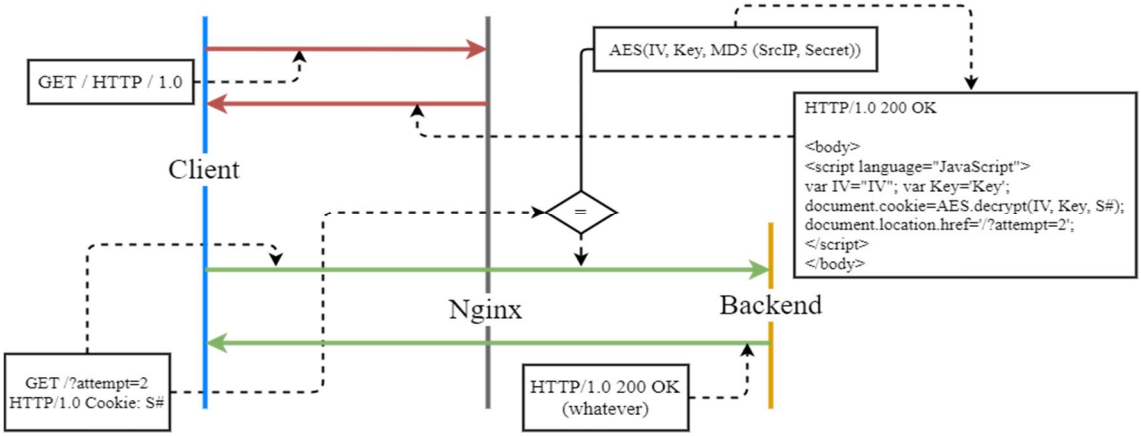


Рисунок 8 – Алгоритм работы модуля с механизмами редиректа и cookies в боте, но без JavaScript Core.

Модуль обладает широким функционалом (рис. 9).

Для установки данного модуля в NGINX-сервере последовательно выполняем команды на linux-сервере:

yum install gcc gcc-c++ kernel-devel
yum groupinstall 'Development Tools'
wget 'http://nginx.org/download/nginx-1.8.0.tar.gz'
tar -xzvf nginx-1.8.0.tar.gz
rpm -Uhv http://rpms.southbridge.ru/southbridge-rhel7-stable.rpm
yum install nginx nginx-module-testcookie

--add-module=/root/testcookie-nginx-module
make
make install
service nginx restart

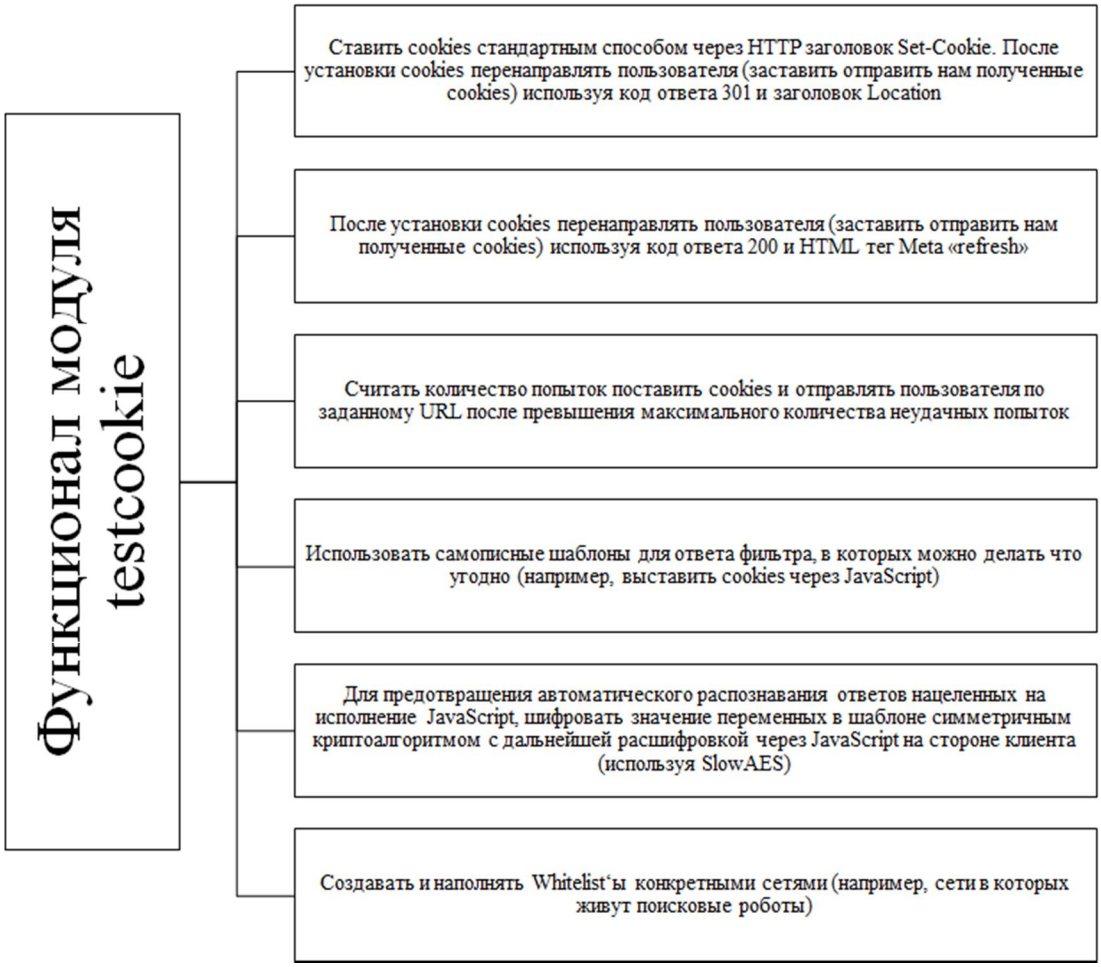


Рисунок 9 – Функционал модуля testcookie-nginx

После установки данного модуля и получения его в результате команды *nginx –V* должна появиться строка *--add-module=/root/testcookie-nginx-module*, можно приступать к формированию и настройке файлов конфигурации модуля.

Далее все зависит от сценария, который мы хотим применять:

1. Боты принимают редиректы и cookies, тот вариант, который будет использоваться в нашей конфигурации системы:

```
server {
    listen 80;
    server_name domain.com;

    testcookie off;
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
    testcookie_redirect_via_refresh on;
```

```
        testcookie_refresh_template
'<html><body><script>document.cookie="BPC=$testcookie_set";document.location.href="$testcookie_
nexturl";</script></body></html>';

        location = /cookies.html {
          root /var/www/public_html;
        }
        location / {
          testcookie on;
          proxy_set_header Host $host;
          proxy_set_header X-Real-IP $remote_addr;
          proxy_pass http://127.0.0.1:8080;
        }
    }
```

2. Конфигурация сценария, где боты не понимают редиректы и cookies будет отличаться тем, что параметр *testcookie_refresh_template* указываться не будет.

Дополнение сервиса DDoS-Guard Protection, обеспечивающего эффективную защиту от DDoS-атак, тонко настроенным модулем testcookie-nginx-module позволило с большей вероятностью отсеивать трафик от ботов, благодаря этому эффективность защиты от большинства распределенных атак типа «Отказ в обслуживании» значительно возросла.

Заключение. В результате проведенного обзора, были обозначены темпы развития ботнетов и оценены риски атак, которые совершаются с помощью них. Обозначена важность и распространённость атаки типа «Отказ в обслуживании» (DDoS) с использованием распределенных сетей.

Были выделены основные классификации средств защиты по типу развертывания и по уровню защищенности. Анализ существующих реализаций позволил сформировать критерии сравнения систем, обеспечивающих безопасность сетевых ресурсов от распределенных DDoS-атак. Исходя из анализа этих критериев, были выбраны наиболее эффективные системы, такие как: Kaspersky DDoS Prevention, StormWall, Qrator, Ростелеком Anti-DDOS, DDoS-Guard Protection, CloudFlare DDoS Protection, Incapsula by Imperva. Анализ результатов показывает, что сервисы DDoS-Guard Protection и StromWall являются самыми оптимальными.

Модификация функциональных возможностей DDoS-Guard Protection, обеспечивающих эффективную защиту от DDoS-атак, тонко настроенным модулем testcookie-nginx-module позволила с большей вероятностью отсеивать трафик от ботов, благодаря этому эффективность защиты от большинства распределенных атаки типа «Отказ в обслуживании» значительно возросла.

Проведенные исследования формируют среду для дальнейшего изучения и совершенствования подходов, связанных с алгоритмическим, математическим и методическим обеспечением процесса защиты от DDoS-атак.

Библиографический список

1. Осторожно: DDoS // comnews.ru. – 2020. – Режим доступа: https://www.comnews.ru/content/211360/2020-11-02/2020-w45/ostorozhno-ddos, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

2. Что такое ботнет Mirai, и как я могу защитить свои устройства? // habr.com. – 2019. – Режим доступа: https://habr.com/ru/post/444436/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 30.12.2020).

3. Число DDoS-атак за год выросло на 241% // ixbt.com. – 2019. – Режим доступа: https://www.ixbt.com/news/2019/11/19/chislo-ddosatak-za-god-vyroslo-na-241.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

4. Ростелеком: объем DDoS-атак в Рунете вырос в 5 раз // xakep. – 2020. – Режим доступа: https://xakep.ru/2020/07/03/runet-ddos/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

5. Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»). ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения. – 2017.

6. DDoS-атаки в III квартале 2020 года // securelist. – 2020. – Режим доступа: https:// securelist.ru/ddos-attacks-in-q3-2020/99091/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

7. Бабаш А. В. Актуальные вопросы защиты информации / А. В. Бабаш, Е. К. Баранова. – Москва, 2017. – С. 53–60.

8. Купереев О. DDoS-атаки в первом квартале 2020 года / О. Купереев, Е. Бадовская, А. Гутников // securelist by kaspersky. – 2020. – Режим доступа: https://securelist.ru/ddos-attacks-in-q1-2020/95949/, свободный. – Заглавие с экрана. – Яз. рус.

9. Отчеты о DDoS-атаках // securelist. – 2020. – Режим доступа: https://securelist.ru/category/ddos-reports/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

10. Ущерб от хакерских атак в мире превысил триллион долларов // dw. – 2020. – Режим доступа: https://www.dw.com/ru/ushherb-ot-hakerskih-atak-v-mire-prevysil-trillion-dollarov/a-55858266, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

11. Путято М. М. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 94–102.

12. Путято М. М. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М. М. Путято, А. С. Макарян, А. Н. Черкасов, И. Г. Горин // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 4. – С. 75–84.

13. DDoS-атаки (Distributed Denial of Service) // anti-malware. – 2020. – Режим доступа: https://www.anti-malware.ru/threats/ddos-attack, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

14. Московский научно-исследовательский центр (МНИЦ) Государственный Комитет Российской Федерации по связи и информатизации. ГОСТ Р ИСО/МЭК 7498-1-99 Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель // gostrf. – 2006. – Режим доступа: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf, свободный. – Заглавие с экрана. – Яз. рус (дата обращения: 14.01.2021).

15. Жуков Р. Сравнение сервисов по защите от DDoS-атак / Р. Жуков // anti-malware. – 2019. – Режим доступа: https://www.anti-malware.ru/compare/DDoS-attack-protection-services, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.01.2021).

16. Подборка: 12 сервисов для защиты от DDoS-атак // Habr. – 2018. – Режим доступа: https://habr.com/ru/post/350384/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 15.01.2021).

17. Путято М.М. Исследование применения технологии deception для предотвращения угроз кибербезопасности / М. М. Путято, А. С. Макарян, Ш. М. Чич, В. К. Маркова // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 85–98.

References

1. Ostorozhno: DDoS [Caution: DDoS]. *comnews.ru*, 2020. Available at: https://www.comnews.ru/content /211360/2020-11-02/2020-w45/ostorozhno-ddos (accessed 12.01.2021).

2. Chto takoe botnet Mirai, i kak ya mogu zashchiti' svoi ustroystva? [What is the Mirai botnet, and how can I protect my devices?]. *habr.com*, 2019. Available at: https://habr.com/ru/post/444436/ (accessed 30.12.2020).

3. Chislo DDoS-atak za god vyroslo na 241% [The number of DDoS attacks for the year increased by 241%]. *ixbt.com*, 2019. Available at: https://www.ixbt.com/news/2019/11/19/chislo-ddosatak-za-god-vyroslo-na-241.html (accessed 12.01.2021).

4. Rostelekom: obem DDoS-atak v Runete vyros v 5 raz [The number of DDoS attacks for the year increased by 241%]. *xakep*, 2020. Available at: https://xakep.ru/2020/07/03/runet-ddos/ (accessed 12.01.2021).

5. *Gosudarstvennyy nauchno-issledovatelskiy ispytatelnyy institut problem tekhnicheskoy zashchity informatsii Federalnoy sluzhby po tekhnicheskomu i eksportnomu kontrolyu (FAU "GNIII PTZI FSTEK Rossii"). GOST R 56938-2016 Zashchita informatsii. Zashchita informatsii pri ispolzovanii tekhnologiy virtualizatsii. Obshchie polozheniya* [State Research and Testing Institute for Problems of Technical Protection of Information of the Federal Service for Technical and Export Control (FAA "GNII PTZI FSTEC of Russia"). GOST R 56938-2016 Information security. Information protection when using virtualization technologies. General provisions], 2017.

6. *DDoS-ataki v III kvartale 2020 goda* [DDoS attacks in the third quarter of 2020]. *securelist*, 2020. Available at: https://securelist.ru/ddos-attacks-in-q3-2020/99091/ (accessed 12.01.2021).

7. Babash A. V., Baranova E. K. *Aktualnye voprosy zashchity informatsii* [Current issues of information security]. Moscow, 2017, pp. 53–60.

8. Kupereev O., Badovskaya E., Gutnikov A. *DDoS-ataki v pervom kvartale 2020 goda* [DDoS attacks in the first quarter of 2020]. *securelist by Kaspersky*, 2020. Available at: https://securelist.ru/ddos-attacks-in-q1-2020/95949/

9. Otchety o DDoS-atakakh [DDoS Attack Reports]. *securelist*, 2020. Available at: https://securelist.ru/category/ddos-reports/ (accessed 12.01.2021).

10. Ushcherb ot khakerskikh atak v mire prevysil trillion dollarov [The damage from hacker attacks in the world exceeded a trillion dollars]. *dw*, 2020. Available at: https://www.dw.com/ru/ushherb-ot-hakerskih-atak-v-mire-prevysil-trillion-dollarov/a-55858266 (accessed 12.01.2021).

11. Putyato M. M., Makaryan A. S. Kiberbezopasnost kak neotemlemyy atribut mnogourovnevogo zashchishchennogo kiberprostranstva [Cyber Security as an Essential Attribute of Multilevel Protected Cyber Space]. *Prikaspiskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 94–102.

12. Putyato M. M., Makaryan A. S., Cherkasov A. N., Gorin I. G. Adaptivnaya sistema kompleksnogo obespecheniya bezopasnosti kak element infrastruktury situatsionnogo tsentra [Adaptive Integrated Security Assurance System as an Element of the Infrastructure of the Situation Center]. *Prikaspiskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 75–84.

13. DDoS-ataki (Distributed Denial of Service) [DDoS Attacks (Distributed Denial of Service)]. *anti-malware*, 2020. Available at: https://www.anti-malware.ru/threats/ddos-attack (accessed 12.01.2021).

14. Moskovskiy nauchno-issledovatelskiy tsentr (MNIC) Gosudarstvennyy Komitet Rossiyskoy Federatsii po svyazi i informatizatsii. GOST R ISO/MEK 7498-1-99 Informatsionnaya tekhnologiya (IT). Vzaimosvyaz otkrytykh

sistem. Bazovaya etalonnaya model. Chast 1. Bazovaya model [Moscow Research Center (MSIC) State Committee of the Russian Federation for Communications and Informatization. GOST R ISO/IEC 7498-1-99 Information technology. Open Systems Interconnection. Basic Reference Model. Part 1. The Basic Model]. *gostrf*, 2006. Available at: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf (accessed 14.01.2021).

15. Zhukov R. Sravnenie servisov po zashchite ot DDoS-atak [Comparison of DDoS protection services]. *anti-malware*, 2019. Available at: https://www.anti-malware.ru/compare/DDoS-attack-protection-services (accessed 15.01.2021).

16. Podborka: 12 servisov dlya zashchity ot DDoS-atak [Selection: 12 services to protect against DDoS attacks]. *Habr*, 2018. Available at: https://habr.com/ru/post/350384/ (accessed 15.01.2021).

17. Putyato M. M., Makaryan A. S., Chich Sh. M., Markova V. K. Issledovanie primeneniya tekhnologii deception dlya predotvrashcheniya ugroz kiberbezopasnosti [Research On the Use of Deception Technology to Prevent Cybersecurity Threats]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, pp. 85–98.

DOI 10.21672/2074-1707.2021.53.1.074-082
УДК 004.051

ИССЛЕДОВАНИЕ IRP-СИСТЕМ НА ОСНОВЕ АНАЛИЗА МЕХАНИЗМОВ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья поступила в редакцию 15.01.2021, в окончательном варианте – 17.02.2021.

Очередько Андрей Романович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru

Бачманов Дмитрий Андреевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
аспирант, ORCID:0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com

Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com

Макарян Александр Самвелович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

В статье рассматриваются особенности и функции систем реагирования на инциденты информационной безопасности. Представлен анализ современных решений IRP и описан процесс реагирования на типовые инциденты в системах этого класса. На основании экспертных мнений сформирован перечень критериев, которые были распределены в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем. Произведена оценка основных и дополнительных характеристик IRP-систем с использованием сформированных критериальных групп. Анализ результатов сравнения показал, что наиболее перспективными решениями являются R-Vision IRP, IBM Resilient IRP и open-source решение – The Hive. Разработан и представлен алгоритм модуля предотвращения фишинговых атак, программная реализация которого произведена с использованием языка Python. В рамках интеграционных возможностей системы The Hive реализована пользовательская функция реагирования, которая не только потенциально улучшила работу системы при предотвращении фишинговых атак, но и увеличила осведомленность сотрудников об этой угрозе. Результатом является IRP-система с персональной гибкой настройкой отдельных элементов и является основой при формировании Центра обеспечения безопасности (SOC), который позволит вывести информационную безопасность организаций на новый уровень.

Ключевые слова: кибербезопасность, IRP-системы, инцидент информационной безопасности, кибератака, механизмы реагирования на инциденты, фишинговые атаки

RESEARCH OF IRP SYSTEMS BASED ON THE ANALYSIS OF MECHANISMS OF RESPONSE TO INFORMATION SECURITY INCIDENTS

The article was received by the editorial board on 15.01.2021, in the final version – 17.02.2021.

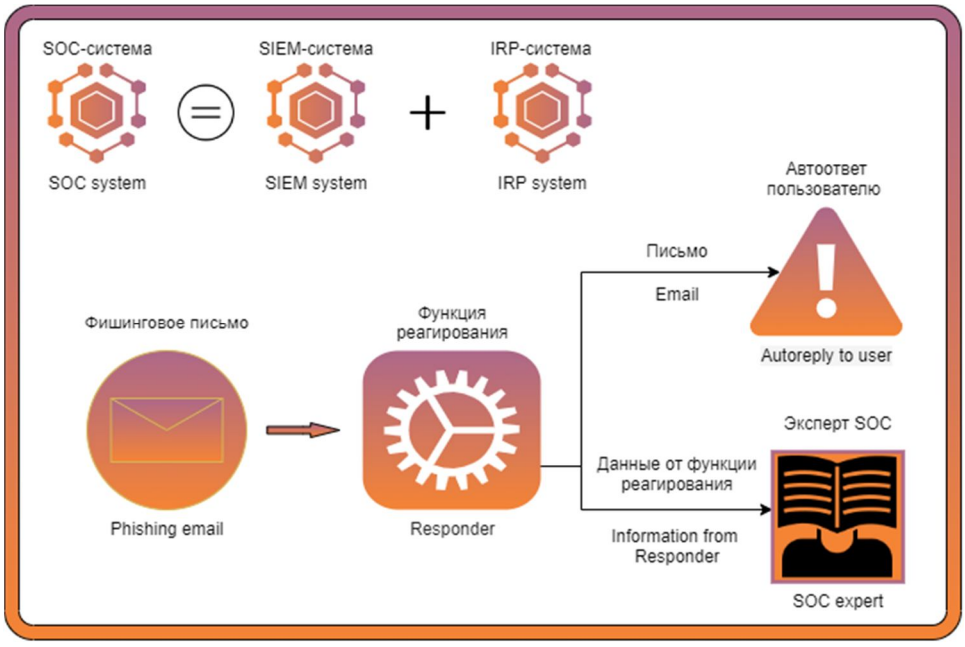
Ocheredko Andrey R., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0002-1451-995X, e-mail: andrewlisten@mail.ru

Bachmanov Dmitriy A., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
graduate student, ORCID: 0000-0003-3474-6831, e-mail: bachmanov.dm@gmail.com
Putyato Michael M., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0001-9974-7144, e-mail: putyato.m@gmail.com
Makaryan Alexander S., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci (Engineering), Associate Professor, ORCID: 0000-0002-1801-6137, e-mail: msanya@yandex.ru

The article discusses the features and functions of information security incident response systems. The analysis of modern IRP solutions is presented and the process of responding to typical incidents in systems of this class is described. Based on expert opinions, a list of criteria was formed, which were divided into groups by areas of functional responsibility for further comparison of the work of IRP systems. The assessment of the main and additional characteristics of IRP-systems was carried out using the formed criterion groups. The analysis of the comparison results showed that the most promising solutions are R-Vision IRP, IBM Resilient IRP and open-source solution - The Hive. The algorithm of the module for preventing phishing attacks was developed and presented, the software implementation of which was made using the Python language. As part of the integration capabilities of The Hive, a custom response function was implemented that not only potentially improved the system's performance in preventing phishing attacks, but also increased employee awareness of this threat. The result is an IRP system with personal flexible customization of individual elements and is the basis for the formation of the Security Center (SOC), which will bring the information security of organizations to a new level.

Keywords: cybersecurity, IRP systems, information security incident, cyber attack, incident response mechanisms, phishing attacks

Graphical annotation (Графическая аннотация)



Введение. В настоящее время информационные системы быстро развиваются, становятся обширнее и объединяют в себе множество подсистем для выполнения широкого спектра задач. С ростом количества и качества информационных систем развиваются и способы защиты информации от кибератак. Поиск решений, позволяющих минимизировать вред от нарушения информационной безопасности (ИБ), является актуальной задачей [1]. В этой работе мы рассмотрим совокупность возможных систем, средств и способов достижения приемлемого уровня защиты информационных активов современных организаций. Когда инфраструктура организации настолько сложна, что невозможно уследить за общей картиной происходящего, на помощь приходит Центр обеспечения безопасности (SOC, Security Operations Center) – это широко специализированный ситуационный центр мониторинга информационной безопасности, представляющий собой

совокупность программно-аппаратных средств, персонала и процессов [2]. Данный тип систем предназначен для централизованного сбора и анализа информации о событиях и инцидентах информационной безопасности (ИБ), поступающих из различных источников ИТ-инфраструктуры. Существует множество конкретных решений, но без ряда базовых средств мониторинга и защиты информации сложно себе представить даже внутренний SOC в средней компании («in-source»), не говоря уже о коммерческом центре. К таким средствам принято относить системы различного класса, где каждый элемент выполняет свою функциональную роль (рис. 1).

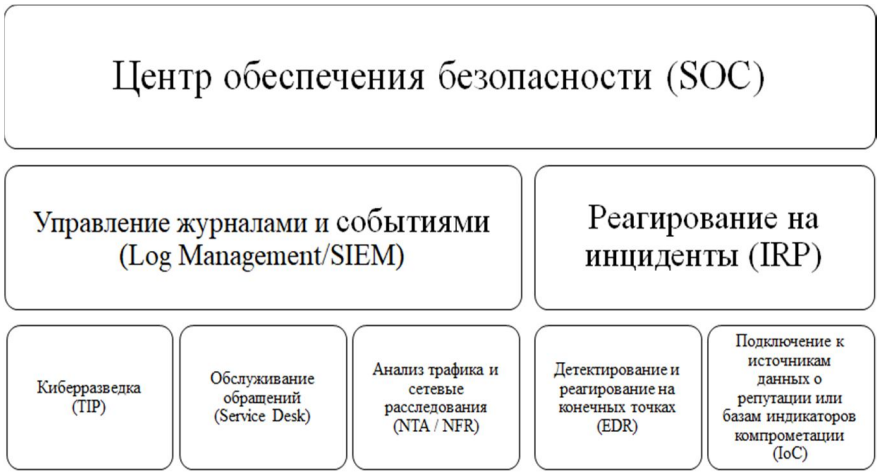


Рисунок 1 – Структура SOC

Особенности IRP систем. В предыдущих исследованиях был представлен анализ механизмов SIEM-систем и выбор лучшего решения с последующей его доработкой [3]. В данной статье мы остановимся на системе реагирования на инциденты (Incident Response Platforms, IRP) – отдельной системы для выстраивания процессов управления инцидентами, которая предназначена для автоматизации процессов мониторинга, учета и реагирования на инциденты информационной безопасности (ИБ) [4], а также решения типовых проблем управления ИБ (рис. 2) [5].

Рисунок 2 – Типы проблем управления ИБ

Поэтому применение IRP позволяет обеспечивать своевременные ответные действия группы реагирования на инциденты информационной безопасности, предоставляя при этом аналитическую информацию и контекст отслеживаемого события. Для эффективной работы IRP должна выполнять определенный перечень функций [6]:

- автоматизация процесса управления инцидентами ИБ;
- ведение единой базы знаний инцидентов;
- интеграция с существующими в компании средствами;
- совместная работа между группами реагирования на инциденты;
- автоматизация реагирования на инциденты;
- адаптивность работы;
- отчетность о проделанной работе;
- интеграция с внешними источниками.

Автоматизация процесса управления инцидентами ИБ является основной задачей IRP и предназначена для снижения нагрузки на персонал компании, связанный с обеспечением ИБ.

Ведение единой базы знаний инцидентов. Содержание в базе информации о зафиксированных инцидентах ИБ позволяет обеспечить регистрацию фактов выявления инцидентов в едином месте и повысить эффективность деятельности группы реагирования на инциденты.

Интеграция с существующими в компании средствами защиты посредством механизмов взаимодействия с целью объединения информации об инцидентах ИБ.

Совместная работа между группами реагирования на инциденты, а именно обеспечение механизмов коммуникации, оповещения о вновь появившихся инцидентах, хранения полученных материалов и его совместного анализа.

Автоматизация реагирования на инциденты. Вследствие того, что в некоторых случаях промежуток времени между обнаружением и реакцией на инцидент ИБ должен быть как можно меньше, необходимо как можно больше автоматизировать процесс реагирования на инциденты. Данные процедуры, как правило, включают готовые сценарии реагирования, совокупность технических мероприятий по обработке инцидента.

Адаптивность работы. Различие используемой инфраструктуры, средств защиты, процессов управления ИБ в различных компаниях порождает обеспечение адаптивности под группы реагирования на инциденты без участия поставщиков платформы.

Отчетность о проделанной работе. В связи с тем, что вопросы инцидентов ИБ рассматриваются руководством компании, регуляторами и контрагентами, существует необходимость визуализации полученной информации в виде диаграмм, наглядных графиков и карт, а также реализации отчета, включающего всю информацию, затрагивающую инциденты ИБ.

Интеграция с внешними источниками. Основной задачей является взаимодействие с другими участниками отрасли, экспертами и внешними организациями, а также центром реагирования на компьютерные инциденты (CERT) с целью получения оперативной и актуальной информации для своевременного принятия защитных мер.

Представим функциональную схему работы IRP-системы при осуществлении процесса реагирования на инциденты информационной безопасности (рис. 3).

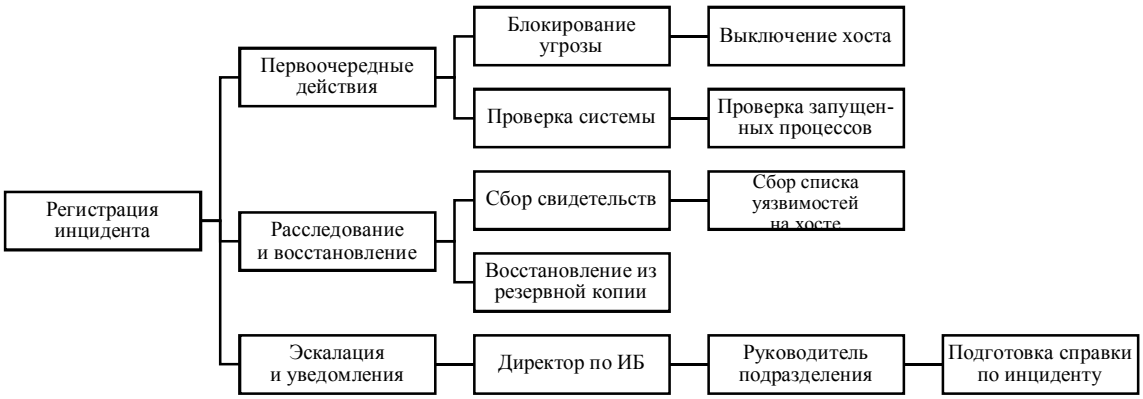


Рисунок 3 – Функциональная схема работы IRP в процессе реагирования на типовые инциденты ИБ

На данной схеме представлены основные этапы функционального взаимодействия в рамках работы с событием информационной безопасности. Эффективность работы системы в целом зависит от того, насколько точно, быстро и правильно отработает каждый блок. Так как производители являются прямыми конкурентами, каждый из них старается использовать инновационные решения при построении каркаса функционирования своей системы. Целесообразно использовать характеристики этих блоков при сравнении и анализе систем между собой.

Сравнение IRP-систем. Ведущими производителями представлено достаточно много решений в области IRP-систем, как коммерческих, так и свободного распространения:

- Jet Signal [7];
- R-Vision IRP [8];
- Security Vision IRP [9];
- IBM Resilient IRP [10];
- The Hive [11].

Проведем анализ использования программных решений IRP в SOC-системах. Для сравнения будем использовать перечень критериев, сформированный на основе исследований экспертного сообщества [12]. Объединим критерии в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем:

1. Управление инцидентами – 30 %.
1.1. Карточка инцидентов.
1.2. Планирование и обработка инцидентов.
1.3. Автоматическое реагирование.
2. Управление уязвимостями – 30 %.
2.1. Настройка собственной модели определения критичных уязвимостей.
2.2. Авторегистрация уязвимостей.
2.3. Сортировка уязвимостей по критериям.
2.4. Возможность выделения ложных срабатываний.
3. Управление рисками – 25 %.
3.1. Карточка риска.
3.2. Оценка степени реализации угрозы и тяжести последствий.
3.3. Произвольные формулы расчета риска.
4. Интеграционные возможности системы – 15 %.
4.1. Интеграция с SIEM.
4.2. Интеграция со сканерами уязвимостей.
4.3. Интеграция с IPS.
4.4. Интеграция с DLP.

Каждая из групп имеет свою степень влияния, выраженную в процентном соотношении к общему объему возможностей системы. Произведем оценку характеристик IRP-систем, используя вышеописанные критериальные группы (табл.).

Таблица – Сравнение IRP-систем

№ п/п	Наименование критерия	Jet Signal	R-Vision IRP	Security Vision IRP	IBM Resilient IRP	The Hive
1.1	Карточка инцидентов	0,3	0,3	0,3	0,3	0,3
1.2	Планирование и обработка инцидентов	0,2	0,3	0,2	0,3	0,2
1.3	Автоматическое реагирование	0,3	0,3	0,3	0,3	0,3
2.1	Настройка собственной модели определения критичных уязвимостей	0,3	0,3	0,3	0,3	0,3
2.2	Настройка собственной модели определения критичных уязвимостей	0,3	0,3	0,3	0,3	0,3
2.3	Авторегистрация уязвимостей	0,3	0,3	0,3	0,3	0,3
2.4	Сортировка уязвимостей по критериям	0,2	0,1	0,1	0,1	0,3
3.1	Возможность выделения ложных срабатываний	0,2	0,3	0,3	0,3	0,3
3.2	Карточка риска	0,2	0,2	0,2	0,2	0,2
3.3	Оценка степени реализации угрозы и тяжести последствий	0,2	0,2	0,1	0,2	0,3
4.1	Произвольные формулы расчета риска	0,2	0,2	0,2	0,2	0,2
4.2	Интеграция со сканерами уязвимостей (vulnerability scanner)	0,2	0,2	0,2	0,2	0,2
4.3	Интеграция с IPS	0,2	0,2	0,2	0,2	0,2
4.4	Интеграция с DLP	0,2	0,2	0,2	0,2	0,1
Итог		3,3	3,4	3,2	3,4	3,5

Сравнение продуктов показывает, что наиболее подходящими при реализации дополнительных систем защиты от фишинговых атак являются приложения R-Vision IRP, IBM Resilient IRP и open-source-решение – The Hive.

Реализация защиты от фишинговых атак. Для реализации защиты выберем систему The Hive. Встроенный механизм пользовательских функций реагирования (Responder) может быть использован для помощи в программе повышения осведомленности пользователей путем создания автоматических ответов на случаи, связанные с фишингом.

Разработчики системы предоставили руководство для создания функций реагирования, которые подходят для реализации возможных способов решения задач защиты. В системе есть встроенная виртуальная машина, которая используется для написания собственных функций реагирования, она позволяет протестировать и настроить все, что является необходимым для собственной функции [13].

В рамках рассматриваемого примера необходимо упомянуть об особенностях фишинга в электронной почте. Фишинг – массовая рассылка электронных писем или сообщений для того, чтобы заманить пользователя на web-сайты, которые внешне очень похожи на обычные web-сайты различных фирм и банков, но контролируются мошенниками. В результате заранее продуманных действий электронные мошенники вынуждают пользователя оставлять на таком web-сайте нужные им конфиденциальные сведения о паролях, номерах кредитных карт, банковских счетов и прочее [14, 15]. В прогнозах на 2021 от компании Group-IB фишинг упоминается как серьезная проблема, злоумышленники используют гибридные фишинговые атаки с использованием социальной инженерии [16, 17]. В такой ситуации очень важно постоянно повышать осведомленность сотрудников, чтобы новые разновидности фишинга не смогли ввести в заблуждение работников организации [18].

Решением задачи является создание модифицированных функций реагирования на фишинговые атаки при помощи совокупности скриптов на языке Python и конфигурационных элементов, которые позволяют системе интерпретировать получаемые данные из внешних источников [19].

В нашем данном случае рассмотрим проявление фишинга в виде сообщений в корпоративной электронной почте организации. Такое проявление фишинга в корпоративной среде представляет собой тщательно продуманную и реализованную таргетированную атаку. Благодаря функции реагирования система сможет моментально получить определенные параметры, которые будут необходимы эксперту для создания полной картины инцидента [20]:

- почтовый адрес, от имени которого пришло письмо;
- SMTP-сервер, использованный для отправки письма;
- порт SMTP-сервера;
- пользователь SMTP-сервера;
- пароль от SMTP-сервера.

Для того чтобы создать и запустить функцию реагирования, необходимо подготовить 2 файла: конфигурационный файл JSON и Python-файл с кодом, в котором будет описана логика-функция.

Необходимые для заполнения параметры в JSON-файле конфигурации:

- DataTypeList – это поле указывает, применим ли ответчик к рабочему случаю (use case), оповещению (alert) или просто подозрительному случаю. Разница заключается во входных данных, которые передаются системы к ответчику. Скрипт будет получать структуру JSON, представляющую случай, предупреждение или подозрительный момент. В этом примере будет сделан ответчик, применимый к рабочим случаям (use case);
- Command – это путь к скрипту относительно папки Responders, в нашем примере кода: Phishing/phishing.py;
- Config – это поле позволяет определять разные «разновидности» одних и тех же ответчиков: в системе может быть один сценарий, который предоставляет несколько различных выводов, которые будут отображаться как разные ответчики;
- ConfigurationItems – данное поле является параметром типа DataSet или набор данных, оно определяет все параметры, которые должны быть установлены пользователями через графический интерфейс системы.

В файл с логикой работы функции мы будем закладывать те же параметры, которые использовали в конфигурационном файле в интерпретации языка Python. Построим блок-схему алгоритма (рис. 5).

Настройка пользовательских функций реагирования на новые классы инцидентов потенциально улучшает не только работу системы, но и повышает качество и развитость работы функциональных блоков при предотвращении фишинговых атак. Также при помощи функции были заданы автоматические ответы сотрудникам, которые дополнительно сообщили о подозрительных письмах, тем самым повысив осведомленность персонала об опасности фишинговых писем.

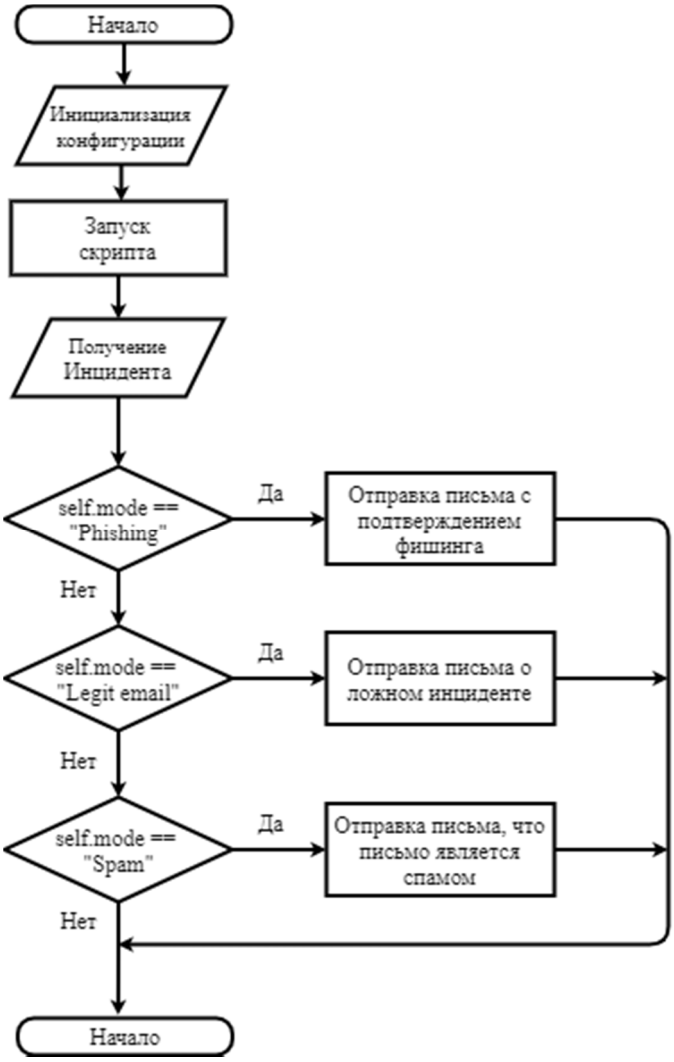


Рисунок 5 – Алгоритм работы Python-скрипта

Заключение. В результате проведенного исследования были выделены особенности и функции IRP-систем. Анализ современных решений IRP и мнений экспертов в области информационной безопасности позволил сформировать перечень критериев, которые были распределены в группы по зонам функциональной ответственности для дальнейшего сравнения работы IRP-систем. Произведена оценка характеристик IRP-систем с использованием сформированных критериальных групп. Анализ результатов сравнения показал, что наиболее перспективными решениями являются R-Vision IRP, IBM Resilient IRP и open-source-решение – The Hive. Приведен пример реализации пользовательской функции реагирования, которая не только потенциально улучшила работу системы при предотвращении фишинговых атак, но и позволила увеличить осведомленность сотрудников об этой угрозе. IRP-системы позволяют провести персональную настройку практически в любой ситуации и, как и SIEM-системы, являются основой при формировании Центра обеспечения безопасности (SOC) организации. Необходимо продолжать постоянное расширение и модернизацию функций IRP-систем для поддержания высокого уровня безопасности в условиях роста количества киберугроз. Благодаря политике свободного доступа к алгоритмам The Hive, мы будем продолжать исследования как в области модернизации существующих решений учета и реагирования инцидентов, так и в построении Центра обеспечения безопасности в целом.

Библиографический список

1. Путято М. М. Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М. М. Путято, А. С. Макарян // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3. – С. 94–102.

2. Путято М. М. Адаптивная система комплексного обеспечения безопасности как элемент инфраструктуры ситуационного центра / М. М. Путято, А. С. Макарян, А. Н. Черкасов, И. В. Горин // Прикаспийский журнал: управление и высокие технологиию. – 2020. – № 4. – С. 75–84.

3. Очередько А. Р. Исследование SIEM-систем на основе анализа механизмов выявления кибератак / А. Р. Очередько, В. С. Герасименко, М. М. Путято, А. С. Макарян // Вестник АГУ. Серия 4: Естественно-математические и технические науки. – 2020. – № 2. – С. 25–31.

4. Сравнение систем SGRC (Security Governance, Risk, Compliance). – 2017. – Режим доступа: https://www.anti-malware.ru/compare/russian_sgrc_2017, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 04.01.2021).

5. Обзор рынка платформ реагирования на инциденты (IRP) в России. – 2018. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.01.2021).

6. Бесплатная IRP-система своими силами: опыт использования платформы с открытым кодом The Hive. – 2019. – Режим доступа: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

7. Система управления инцидентами информационной безопасности Jet Signal. – Режим доступа: https://jet.su/services/software-development/products/jet-signal/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

8. Платформа для создания Центра реагирования на инциденты ИБ. – Режим доступа: https://rvision.pro/irp/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

9. Системы класса Incident Response Platform: применение и основные функции. – Режим доступа: https://www.securityvision.ru/products/irp/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

10. Платформа координации и автоматизации процессов реагирования на инциденты. – Режим доступа: https://www.ibm.com/ru-ru/products/resilient-soar-platform, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

11. Security incident response for the masses. – Режим доступа: https://thehive-project.org/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

12. Системы реагирования и управления инцидентами информационной безопасности (IRP). – 2019. – Режим доступа: https://www.anti-malware.ru/security/irp, свободный.– Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

13. The Hive-Project. – 2020. – Режим доступа: https://github.com/TheHive-Project/TheHive, свободный. – Заглавие с экрана. – Яз.англ. (дата обращения: 05.01.2021).

14. Примеры фишинга через электронную почту: как распознать фишинговое письмо. – 2020. – Режим доступа: http://www.itsec.ru/articles/primery-fishinga-cherez-elektronnuyu-pochtu-kak-raspoznat-fishingovoe-pismo/, свободный. – Заглавие с экрана. – Яз.рус. (дата обращения: 05.01.2021).

15. Email Security Predictions 2021: 6 Ways Hackers Will Target Businesses. – 2020. – Режим доступа: https://www.vadesecure.com/en/blog/email-security-predictions-6-ways-hackers-will-target-businesses/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 05.01.2021).

16. Group-IB. Прогнозы по киберугрозам, с которыми мир столкнется в новом году. – 2020. – Режим доступа: https://www.group-ib.ru/media/gib-report-2020/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 12.01.2021).

17. Прогнозы по продвинутым угрозам на 2021 год. – 2020. – Режим доступа: https://securelist.ru/apt-predictions-for-2021/99366/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 07.01.2021).

18. Создание культуры безопасности. – 2019. – Режим доступа: https://www.osp.ru/winitpro /2019/05/13055004/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 05.01.2021).

19. The Hive Docs. – 2020. – Режим доступа: https://github.com/TheHive-Project/TheHiveDocs, свободный. – Заглавие с экрана. – Яз.англ. (дата обращения: 05.01.2021).

20. Примеры фишинговых писем. Типы фишинговых атак и способы их идентификации. – 2019. – Режим доступа: https://bar812.ru/primery-fishingovyh-pisem-tipy-fishingovyh-atak-i-sposoby-ih.html/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 11.01.2021).

References

1. Putyato M. M., Makaryan A. S. Kiberbezopasnost kak neotemlimny atribut mnogourovnevogo zashchishchennogo kiberprostranstva [Cybersecurity as an integral attribute of a multi-layered secure cyberspace]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 3, pp. 94–102.

2. Putyato M. M., Makaryan A. S., Cherkasov A. N., Gorin I. V. Adaptivnaya sistema kompleksnogo obespecheniya bezopasnosti kak element infrastrukturi situacionnogo centra [An adaptive integrated security system as an element of the situation center infrastructure]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 4, pp. 75–84.

3. Ocheredko A. R., Gerasimenko V. S., Putyato M. M., Makaryan A. S. Issledovaniye SIEM-sistem na osnove analiza mekhanizmov vyyavleniya kiberatak [Investigation of SIEM-systems based on the analysis of cyberattack detection mechanisms]. *Vestnik Adygeyskogo gosudarstvennogo universiteta. Seriya 4: Yestestvenno-*

matematicheskiye i tekhnicheskiye nauki [Bulletin of the Adygea State University. Series 4: Natural-mathematical and technical sciences"], 2020, no. 2, pp. 25–31

4. *Sravnenie system SGRC (Security Governance, Risk, Compliance)* [Comparison of SGRC systems (Security Governance, Risk, Compliance)], 2017. Available at: https://www.anti-malware.ru/compare/russian_sgrc_2017 (accessed 01.04.2021).

5. *Obzor rynka platform reagirovaniya na intsidenty (IRP) v Rossii* [Market overview of incident response platforms (IRP) in Russia], 2018. Available at: https://www.anti-malware.ru/analytics/Market_Analysis/incident-response-platforms-irp-in-russia (accessed 01.11.2021).

6. *Besplatnaya IRP-sistema svoimi silami: opit ispolzovaniya platformi s otkritim kodom The Hive* [Free IRP system in-house: experience of using the open source platform The Hive], 2019. Available at: https://www.anti-malware.ru/practice/solutions/free-IRP-on-your-own (accessed 01.12.2021).

7. *Sistema upravleniya intsidentami informatsionnoy bezopasnosti Jet Signal* [Information security incident management system Jet Signal]. Available at: https://jet.su/services/software-development/products/jet-signal/ (accessed 01.12.2021).

8. *Platforma dlya sozdaniya Tsentra reagirovaniya na intsidenty IB* [Platform for creating an Information Security Incident Response Center], Available at: https://rvision.pro/irp/ (accessed 01.12.2021).

9. *Sistemy klassa Incident Response Platform: primeneniye i osnovnyye funktsii* [Incident Response Platform class systems: application and main functions], Available at: https://www.securityvision.ru/products/irp/ (accessed 01.12.2021).

10. *Platforma koordinatsii i avtomatizatsii protsessov reagirovaniya na intsidenty* [Platform for coordination and automation of incident response processes]. Available at: https://www.ibm.com/ru-ru/products/resilient-soar-platform (accessed 01.12.2021).

11. *Security incident response for the masses.* Available at: https://thehive-project.org/ (accessed 01.12.2021).

12. *Sistemy reagirovaniya i upravleniya intsidentami informatsionnoy bezopasnosti (IRP)* [Information Security Incident Response and Management Systems (IRP)], 2019. Available at: https://www.anti-malware.ru/security/irp (accessed 01.12.2021).

13. *The Hive-Project*, 2020. Available at: https://github.com/TheHive-Project/TheHive (accessed 01.05.2021).

14. *Primery fishinga cherez elektronnuyu pochtu: kak raspoznat fishingovoe pismo* [Examples of phishing via email: how to recognize a phishing email], 2020. Available at: http://www.itsec.ru/articles/primery-fishinga-cherez-elektronnuyu-pochtu-kak-raspoznat-fishingovoe-pismo (accessed 01.05.2021).

15. *Email Security Predictions 2021: 6 Ways Hackers Will Target Businesses*, 2020. Available at: https://www.vadesecure.com/en/blog/email-security-predictions-6-ways-hackers-will-target-businesses/ (accessed 01.05.2021).

16. *Group-IB. Prognozi po kiberugrozam, s kotorimi mir stolknetsya v novom godu* [Cyber Threats Predictions the World Will Face in the New Year], 2020. Available at: https://www.group-ib.ru/media/gib-report-2020/ (accessed 01.12.2021).

17. *Prognozy po prodvinutym ugrozam na 2021 god* [Predictions for advanced threats for 2021], 2020. Available at: https://securelist.ru/apt-predictions-for-2021/99366/ (accessed 01.07.2021).

18. *Sozdanie kultury bezopasnosti* [Building a safety culture], 2019. Available at: https://www.osp.ru/winitpro/2019/05/13055004/ (accessed 01.05.2021).

19. *The Hive Docs*, 2020. Available at: https://github.com/TheHive-Project/TheHiveDocs (accessed 01.05.2021).

20. *Primery fishingovikh pisem. Tipi fishingovikh atak i sposoby ikh identifikatsii* [Examples of phishing emails. Types of phishing attacks and how they are identified.], 2019. Available at: https://bar812.ru/primery-fishingovyh-pisem-tipy-fishingovyh-atak-i-sposoby-ih.html/ (accessed 01.11.2021).

DOI 10.21672/2074-1707.2021.53.1.083-090
УДК 004.89

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ ЛИЦ В СИСТЕМАХ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Статья поступила в редакцию 15.12.2020, в окончательном варианте – 17.01.2021.

Марьенков Александр Николаевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

кандидат технических наук, заведующий кафедрой информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0003-1378-3553, e-mail: marenkovan17@gmail.com

Кузнецова Валентина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

ассистент кафедры информационной безопасности и цифровых технологий, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

Гелагаев Тимур Магомедович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

студент, e-mail: tgelagaev@yandex.ru

В статье показана актуальность повсеместного использования технологии компьютерного зрения на примере распознавания лиц в рамках системы контроля и управления доступа. Рассмотрены основные методы, которые применяются при реализации классических систем контроля и управления доступом. Описана схема реализации пропускного режима с технологией распознавания лиц. Применение данной технологии позволяет повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы от нелегитимного проникновения на защищаемую территорию через СКУД с помощью пропусков легальных пользователей.

Ключевые слова: система контроля и управления доступом, распознавание лиц, нейронные сети, безопасность, пропускной режим

APPLICATION OF FACE RECOGNITION TECHNOLOGIES IN CONTROL AND ACCESS CONTROL SYSTEMS

The article was received by the editorial board on 15.01.2021, in the final version – 17.02.2021.

Marenkov Alexander N., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

Cand. Sci. (Engineering), Head of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0003-1378-3553, e-mail: marenkovan17@gmail.com

Kuznetsova Valentina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

assistant of the Department of Information Security and Digital Technologies, ORCID https://orcid.org/0000-0002-6954-5020, e-mail: arhelia@bk.ru

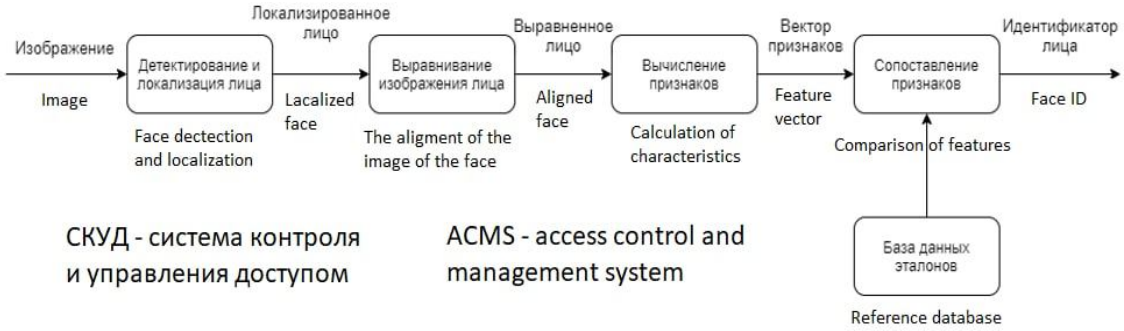
Gelagaev Timur M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

student, e-mail: tgelagaev@yandex.ru

The article shows the relevance of the widespread use of computer vision technology on the example of face recognition as part of the access control and management system. The main methods that are used in the implementation of classical control systems and access control are considered. The scheme for the implementation of the access control with face recognition technology is described. The use of this technology makes it possible to increase the level of information security of enterprises and, as a result, reduce the possible financial damage from the implementation of attacks on their assets from illegitimate penetration into the protected area through the access control system using the passes of legal users.

Keywords: access control and management system, face recognition, neural networks, security, access control

Graphical annotation (Графическая аннотация)



Введение. Использование компьютерного зрения в области обеспечения безопасности даёт огромный толчок к совершенствованию систем контроля и управления доступом (СКУД). Представители среднего и крупного бизнеса, использующие СКУД на своих объектах, приводят информацию о том, что каждый пятидесятый проход через турникет осуществляется с нарушением требований безопасности – для проникновения на территорию с ограниченным доступом используются карты легальных пользователей или поддельные карты доступа. Технологии распознавания лиц планомерно внедряются во многие технологические процессы, в том числе и в системы обеспечения безопасности. СКУД с использованием технологии распознавания лиц способствует детектированию ситуаций, когда для прохода злоумышленник применяет карту легального пользователя путем сравнения лица владельца карты из базы данных организации с портретом того, кто пытается проникнуть на охраняемую территорию. Усовершенствование СКУД таким образом позволит повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы. Кроме того, бесконтактная идентификация пользователей путем распознавания их лиц актуальна в условиях неблагоприятной эпидемиологической обстановки.

Принцип работы классической СКУД. Система контроля и управления доступом – одна из наиболее популярных и эффективных систем защиты территории с ограниченным доступом. СКУД ограничивает проход на охраняемую территорию, при этом никаким образом не вмешиваясь в бизнес-процессы организации. Кроме того, система обеспечивает отслеживание перемещений сотрудников внутри организации и учёт их отработанного времени, что способствует нарушению трудового распорядка.

Основные функции:

- ограничение доступа к помещениям охраняемого объекта;
- ведение табельного учета рабочего времени для каждого сотрудника;
- фиксирование времени прихода и ухода посетителей;
- персональный и временной контроль за открытием внутренних помещений;
- контроль за перемещениями сотрудников по объекту;
- регистрация и уведомление о случаях попыток проникновения в охраняемые помещения;
- интеграция и взаимодействие между системами видеоконтроля и охранно-пожарной сигнализации.

Классический принцип работы СКУД заключается в следующем: она представляет собой пропускную систему на основе ключ-карт с RFID-метками.

Аббревиатура RFID образована от термина Radio Frequency Identification, что в переводе на русский означает «радиочастотная идентификация». RFID-метка состоит из трёх компонентов:

- чип, который хранит идентификационную информацию и отвечает за связь со считывателем;
- антенна, позволяющая передать информацию между меткой и считывателем;
- оболочка или корпус.

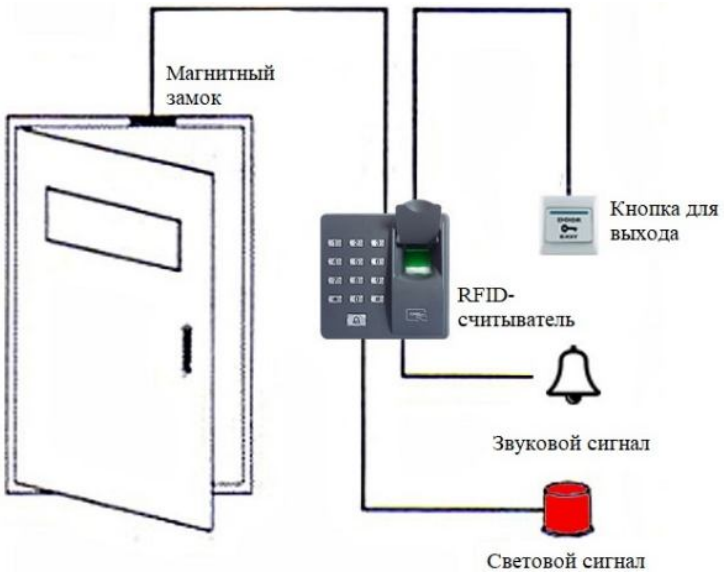


Рисунок 1 – Классическая схема СКУД на предприятии

В настоящее время системы RFID можно встретить абсолютно везде, начиная с общественного транспорта (оплата проезда посредством карты, привязанной к счёту пользователя), проживания в отеле (смарт-карта является ключом для входа в номер) заканчивая заграничным паспортом (нового поколения), который можно получить с электронным бесконтактным RFID-чипом [3].

Практика показывает, что такой вид контроля управления доступом имеет ряд недостатков, которые могут провоцировать уязвимости, связанные с несанкционированным доступом к информационным ресурсам охраняемого объекта. Наиболее ярким примером такого недостатка является использование чужих карт для прохода на охраняемую территорию, например, такое возможно, если сотрудник забыл карту дома и попросил своего коллегу «одолжить» ему карту для прохода, либо, что хуже, потерянную или выкраденную карту использовал для прохода злоумышленник.

Также существенной проблемой для СКУД является распространившееся клонирование ключей и карт доступа. В прессе и на сайтах объявлений часто можно увидеть информацию об услугах по клонированию ключей доступа для любого желающего, например, за такой услугой часто обращаются пользователи домофонов. Однако использование таких ключей в СКУД значительно снижает эффективность при обеспечении безопасности в организации. Многие СКУД не препятствуют одновременному использованию нескольких одинаковых ключей или карт доступа. Клонированный ключ позволяет не только пройти на предприятие, но также открывает все внутренние двери, которые были разрешены для аутентичного ключа.

Чаще всего данную проблему решают с помощью установки биометрических сканеров (отпечатки пальцев, сетчатки глаза и пр.), однако в условиях неблагоприятной эпидемиологической ситуации данные системы становятся все менее востребованными. При этом бесконтактные системы считывания отпечатков пальцев показывают низкую результативность. Согласно отчету американского национального института стандартов и технологий (NIST), точность бесконтактных устройств при распознавании одного пальца была относительно низкой – всего 60–70 %.

Распознавание лиц в целях обеспечения безопасности. Распознавание лиц – это одни из наиболее перспективных методов биометрической бесконтактной идентификации человека по лицу. Согласно прогнозам аналитиков Future Market Insights, мировой рынок бесконтактных биометрических технологий в период с 2020 по 2030 годы будет расти среднегодовыми темпами на уровне 17,4 % и к 2030 году достигнет $70 млрд. Ожидается, что бесконтактная технология будет более востребована из-за пандемии коронавируса в мире и проблем гигиены поверхностей, таких как контактные сканеры отпечатков пальцев [4].

Распознавание лица представляет собой процесс сопоставления изображений лиц людей, попавших в объектив камеры с фотографиями из базы данных ранее сохраненных изображений лиц эталонов, например сотрудников организации. По структурной реализации системы распознавания лиц выделяют 3 схемы:

1. Анализ видеопотока на сервере: IP-камера направляет весь видеопоток на сервер для обработки и анализа. На сервере специализированное программное обеспечение выполняет поиск лица в видеоряде и сравнивает полученные из видеопотока изображения лиц с базой лиц эталонов (рис. 2).

Рисунок 2 – Схема анализа видеопотока на сервере

Недостатками такой схемы будут высокая нагрузка на сеть, высокая стоимость сервера, даже к самому мощному серверу можно подключить ограниченное количество IP-камер, т.е. чем больше система, тем больше серверов. Преимуществом является возможность использовать существующую систему видеонаблюдения.

2. Анализ видеопотока на IP-камере: изображения будут производиться на самой камере, а на сервер будут передаваться обработанные метаданные (рис. 3).

Рисунок 3 – Схема анализа видеопотока на камере

Недостатки – нужны специальные камеры, выбор которых в данный момент крайне мал, стоимость камер выше, чем у обычных. Также в системах разных производителей будет по-разному решаться вопрос хранения и размера базы данных распознанных лиц эталонов, а также вопросов взаимодействия софта на камере и софта на сервере.

Преимущества – подключение практически неограниченного количества камер к одному серверу.

3. Анализ видеопотока на устройстве контроля доступа – камера встроена в устройство контроля доступа, которое кроме распознавания лица, происходящего на устройстве, выполняет функции управления доступом, как правило, через турникет или электрозамок, установленный на дверь (рис. 4). База данных лиц эталонов хранится на устройстве, и уже не в виде фотоизображений.

Рисунок 4 – Анализ видеопотока на устройстве контроля доступа

Недостатки – как правило, все такие устройства выпускаются для использования в помещениях. Преимущества – низкая стоимость систем по сравнению с системами видеонаблюдения, используемыми для распознавания лиц.

Как правило, все предлагаемые методы распознавания лиц реализуются преимущественно с помощью 2D-изображений, так как, несмотря на развитие трехмерных моделей, база таких эталонов еще достаточно скудная, а оборудование для организации такого рода распознавания является дорогостоящим.

Анализ подходов распознавания лиц. Несмотря на разнообразие существующих подходов, можно определить общий алгоритм распознавания лиц, представленный на рисунке 5.

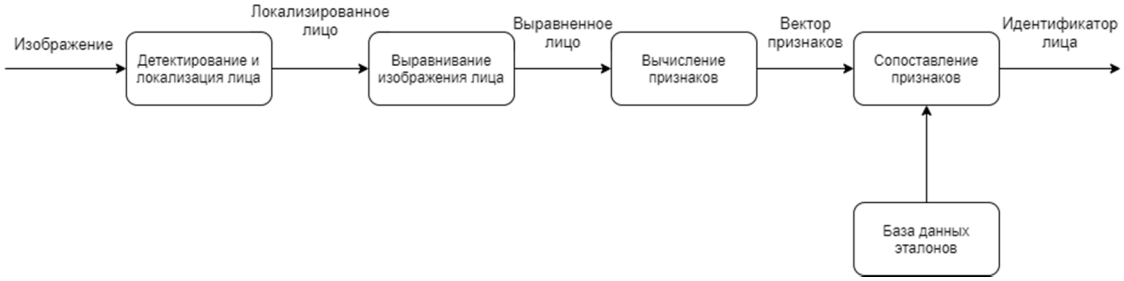


Рисунок 5 – Общая схема алгоритма распознавания лиц

Основным этапом описываемого процесса является само распознавание лица, которое обеспечивается за счет вычисления признаков и выявления схожести или несхожести фотографий. Рассмотрим несколько методов, которые могут быть применены в алгоритме распознавания лиц.

Метод гибкого сравнения на графах. Суть этого метода сводится к сопоставлению графов. Лица представляются в виде графов со взвешенными вершинами и ребрами. На этапе распознавания один из графов – эталонный – остается неизменным, в то время как другой изменяется с целью наилучшей подгонки к первому. В подобных системах распознавания графы могут представлять собой как прямоугольную решетку, так и структуру, образованную характерными (антропометрическими) точками лица. Различие (расстояние) между двумя графами вычисляется при помощи некоторой ценовой функции деформации, учитывающей как различие между значениями признаков, вычисленными в вершинах, так и степень деформации ребер графа.

Нейронные сети. В настоящее время существует около десятка разновидности нейронных сетей (НС). Обучаются нейронные сети на наборе обучающих примеров. Суть обучения сводится к настройке весов межнейронных связей в процессе решения оптимизационной задачи методом градиентного спуска. В процессе обучения НС происходит автоматическое извлечение ключевых признаков, определение их важности и построение взаимосвязей между ними. Предполагается, что обученная НС сможет применить опыт, полученный в процессе обучения, на неизвестные образы за счет обобщающих способностей. Наилучшие результаты в области распознавания лиц (по результатам анализа публикаций) показала сверточная нейронная сеть.

Скрытые Марковские модели. Одним из статистических методов распознавания лиц являются скрытые Марковские модели (СММ) с дискретным временем. СММ используют статистические свойства сигналов и учитывают непосредственно их пространственные характеристики. Элементами модели являются: множество скрытых состояний, множество наблюдаемых состояний, матрица переходных вероятностей, начальная вероятность состояний. Каждому соответствует своя Марковская модель. При распознавании объекта проверяются сгенерированные для заданной базы объектов Марковские модели и ищется максимальная из наблюдаемых вероятность того, что последовательность наблюдений для данного объекта сгенерирована соответствующей моделью.

Разработка прототипа. В разрабатываемом прототипе предлагается использовать нейронную сеть, обучение которой будет проходить с учителем. Нейросеть будет обучаться на двух изображениях, где результатом сравнения будет true или false (человек на фотографиях один и тот же человек или нет).

Учитель создает набор данных, в котором должно находиться не менее двух фотографий одного человека из многих других.

Причины выбора данного подхода:

- нейросеть переобучаема;
- нейросеть можно «дообучить», добавив новые наборы данных;
- обученная нейросеть даёт быстрые ответы (в рамках решаемой задачи «похож/не похож»);
- всегда можно повысить или убавить порог сходства.

Предлагается следующая структура прототипа СКУД с технологией распознавания лиц:

- Arduino Mega для управления считывателями RFID и турникетами;
- считыватели RFID;
- IP камеры для захвата изображений;
- компьютер с установленным приложением СКУД;
- сервер с базой данных.

Arduino Mega. Электронные устройства Arduino давно зарекомендовали себя на рынке программируемой электротехники как качественный, многофункциональный и недорогой продукт. Поэтому в данном проекте будет использоваться данное электронное устройство модели Mega, которая в свою очередь имеет в своём арсенале 256 КБ флэш-памяти и 8 КБ оперативной памяти.

Считыватель RFID. Данные считыватели нужны для чтения UID (User identifier) со смарт-карт.

IP камера. Для более качественной работы системы понадобятся IP камеры с определёнными характеристиками:

1. Наличие WDR (Wide Dynamic Range) – этот параметр, который влияет на освещённость.
2. Количество кадров в секунду – чем больше кадров в секунду будет снимать камера, тем выше вероятность что камера сделает нужный снимок. В данной задаче потребуется минимум 20 кадров в секунду.
3. Разрешение камеры видеонаблюдения – при большем разрешении будет выше детализация. Высокое разрешение положительно скажется на процессе выявления нейросетью маркеров на полученном снимке.
4. Вариофокальный объектив – объектив, где есть возможность изменить фокусное расстояние.

Компьютер. Минимальные требования для нормальной работы приложения СКУД:

- процессор 2 ядра, частота 1,1 ГГц;
- Windows 7 и новее;
- ОЗУ 2 Гб;
- установленный .NET Framework 4.8;
- 150 МБ свободного места.

Сервер с БД. На сервере должна быть установлена SQL Server Management Studio от компании Microsoft.

Концептуальная модель работы СКУД представлена на рисунке 6.

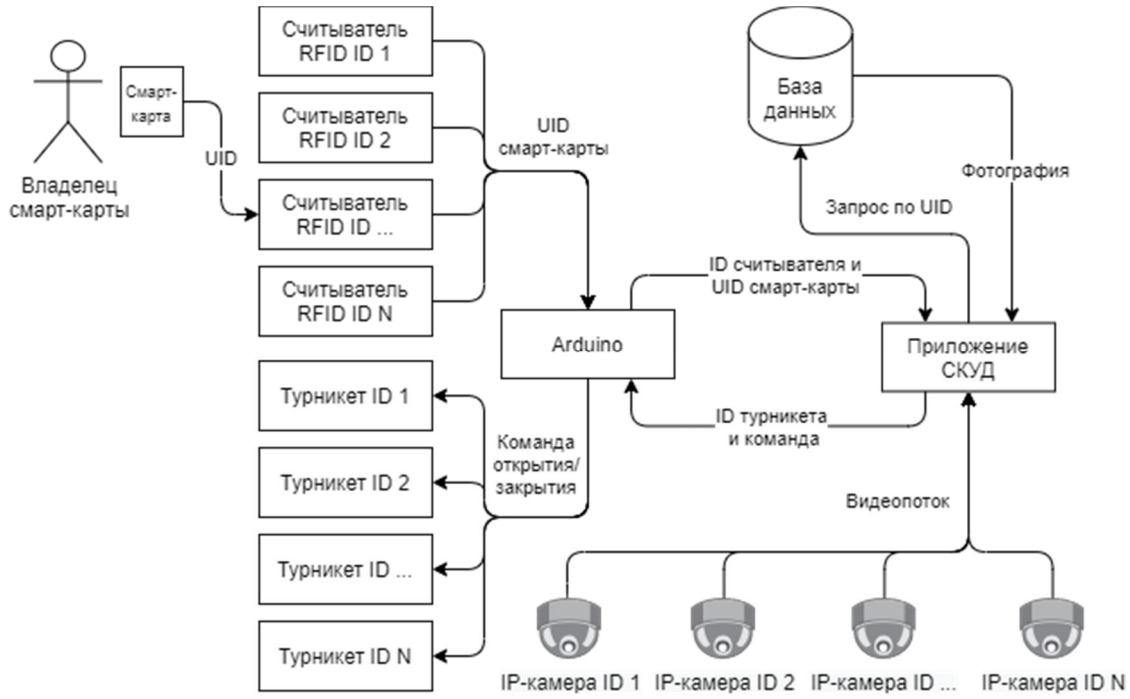


Рисунок 6 – Концептуальная схема работы СКУД

Сценарий использования СКУД с технологией распознавания лиц. Владелец смарт-карты должен поднести смарт-карту к считывателю. Считыватель получает UID поднесённой карты и отправляет его (UID смарт-карты) электронному устройству Arduino. Arduino в свою очередь отправляет на компьютер (с установленным приложением СКУД) по COM-порту UID считанной смарт-карты и ID считывателя, с которого был получен UID. На компьютере приложение СКУД отправляет запрос к базе данных с целью проверки наличия данной смарт-карты в базе, если UID смарт-карты не существует, то перед нами злоумышленник. При обнаружении карты из базы данных выгружается изображение, привязанное к UID считанной смарт-карты. Приложение СКУД проводит анализ на совпадение изображения лица, полученного из базы данных с изображением, полученным с IP-камеры. Если вероятность совпадения ниже некоторого заданного порога, значит, что перед нами злоумышленник и система запретит ему доступ. Если вероятность совпадения изображений выше порогового значения, приложение СКУД отправит на электронное устройство Arduino ID турникета и команду «открыть», а Arduino в свою очередь передаст нужному турникету команду «Открыть».

Блок-схема предложенного решения представлена на рисунке 7.

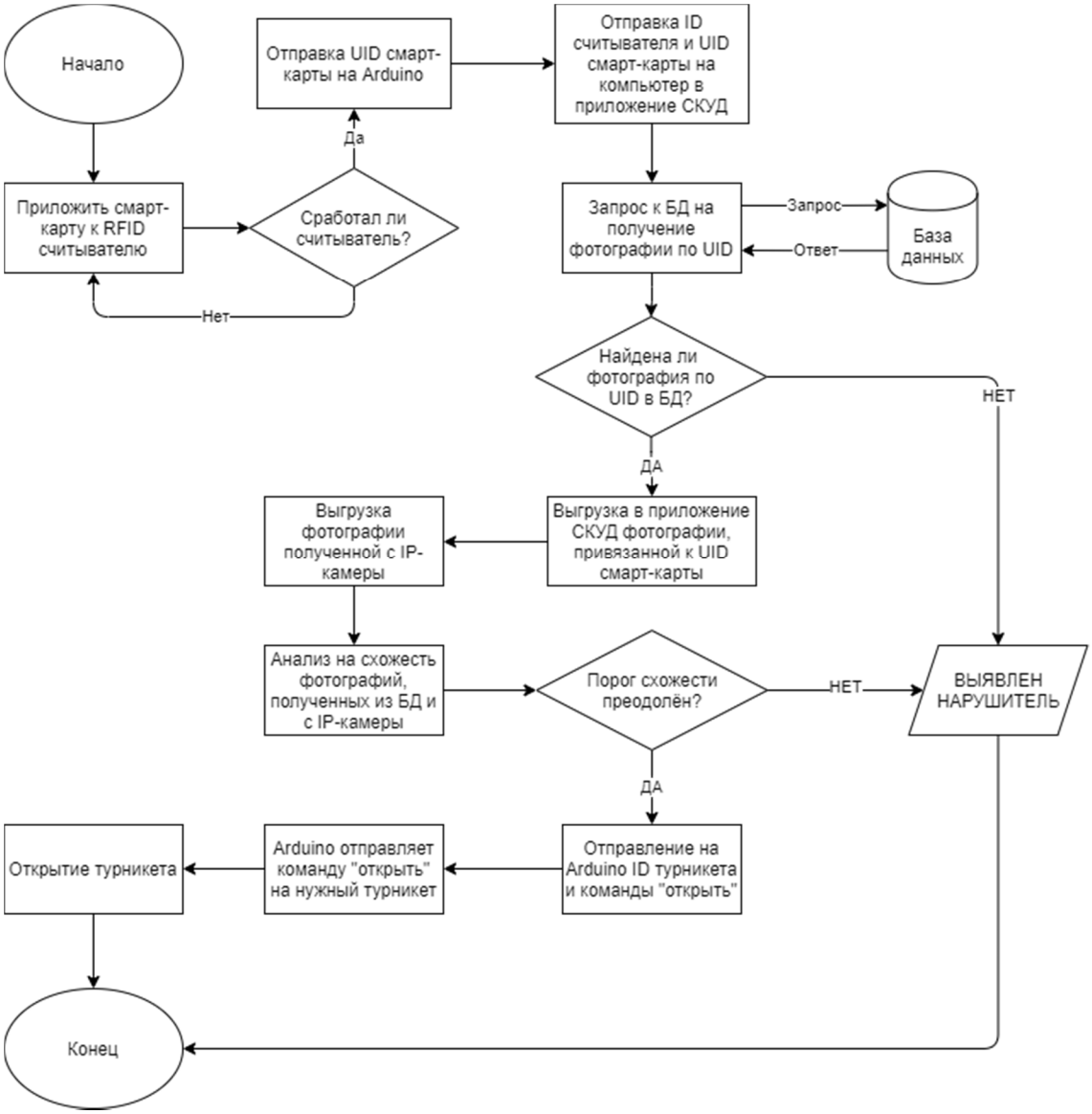


Рисунок 7 – Блок-схема процесса

Заключение.

1. Технологии распознавания лиц планомерно внедряются во многие технологические процессы, в том числе и в системы обеспечения безопасности. СКУД с использованием технологии распознавания лиц способствует детектированию ситуаций, когда для прохода злоумышленник применяет карту легального пользователя путем сравнения лица владельца карты из базы данных организации с изображением лица, пытающегося проникнуть на охраняемую территорию.
2. В работе предложена общая схема процесса контроля и управления доступом с использованием технологии распознавания лиц и продемонстрирована концептуальная схема предложенного аппаратного решения.
3. Усовершенствование СКУД позволит повысить уровень информационной безопасности предприятий и, как следствие, снизить возможный финансовый ущерб от реализации атак на их активы.
4. Бесконтактная идентификация пользователей путем распознавания их лиц актуальна в условиях неблагоприятной эпидемиологической обстановки.

Потенциальными пользователями данной системы могут являться как государственные, так и коммерческие организации, заинтересованные в обеспечении режима конфиденциальности на собственной территории.

Библиографический список

1. Ворожейкин М. Р. Общие сведения о системе распознавания лиц / М. Р. Ворожейкин, С. В. Чернова // Актуальные вопросы науки. – 2019. – № 47. – С. 35–37.
2. Рудинская Е. А. Разработка алгоритма детектирования лиц с использованием комбинаций каскадов Хаара / Е. А. Рудинская, Р. А. Парингер // Сборник трудов ИТНТ-2019. – 2019. – С. 6–12.
3. RFID метки – ультимативный гид по выбору. – Режим доступа: https://securityrussia.com/blog/rfid-metki.html, свободный. – Заглавие с экрана. – Яз. рус.
4. Сайт новостного сервиса «Киосксофт». – Режим доступа: https://kiosksoft.ru/news/2020/05/28/tochnost-beskontaktnoj-identifikacii-otpechatkov-palcev-poka-ostaetsya-nizkoj-71797, свободный. – Заглавие с экрана. – Яз. рус.
5. Власенко А. В. Обзор инструментов машинного обучения и их применения в области кибербезопасности / А. В. Власенко, П. И. Дзьобан, Р. В. Жук // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 1. – С. 144–155.
6. Сиротин Д. В. Перспективы внедрения мобильной идентификации СКУД в корпоративные IT-системы // Алгоритм безопасности. – 2019. – № 2. –С. 38–39.
7. Марьенков А. Н. Система выявления агрессивного поведения людей на основе анализа видеоматериалов с применением рекуррентной сверточной нейронной сети / А. Н. Марьенков, Е. О. Кузнецова, А. А. Приходько // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики : материалы XIX Международной научно-практической конференции. – Ростов : Ростовский государственный экономический университет, 2019. – С. 207–210.
8. Дёмин К. С. Методы распознавания движений человека с применением технологий нейронных сетей / К. С. Дёмин, А. Н. Марьенков // Математические методы в технике и технологиях ММТТ. – 2020. – Т. 8. – С. 135–138.

References

1. Vorozheykin M. R., Chernova S. V. Obshchiye svedeniya o sisteme raspoznavaniya lits [General information about the face recognition system]. Aktualnye voprosy nauki [Actual Issues of Science], 2019, no. 47, pp. 35–37.
2. Rudinskaya E. A., Paringer R. A. Razrabotka algoritma detektirovaniya lits s ispolzovaniyem kombinatsiy kaskadov Khaara [Development of a face detection algorithm using combinations of Haar cascades]. *Sbornik trudov ITNT-2019* [Proceedings of ITNT-2019], 2019, pp. 6–12.
3. *RFID metki – ultimativnyy gid po vyboru* [RFID tags – the ultimate guide to choose]. Available at: https://securityrussia.com/blog/rfid-metki.html
4. *Sayt novostnogo servisa "Kiosksoft"* [Site of the news service "Kiosksoft"]. Available at: https://kiosksoft.ru/news/2020/05/28/tochnost-beskontaktnoj-identifikacii-otpechatkov-palcev-poka-ostaetsya-nizkoj-71797
5. Vlasenko A. V., Dzoban P. I., Zhuk R. V. Obzor instrumentov mashinnogo obucheniya i ikh primeneniya v oblasti kiberbezopasnosti [Overview of machine learning tools and their use in the field of cyber security]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 1, pp. 144–155.
6. Sirotin D. V. Perspektivy vnedreniya mobilnoy identifikatsii SKUD v korporativnye IT-sistemy [Prospects for the introduction of mobile identification of access control systems in corporate IT systems]. *Algoritm bezopasnosti* [Security Algorithm], 2019, no. 2, pp. 38–39.
7. Marenkov A. N., Prikhodko A. A., Kuznetsova E. O. Sistema vyyavleniya agressivnogo povedeniya lyudey na osnove analiza videomaterialov s primeneniem rekurrentnoy svyortochnoy neyronnoy seti [A system for detecting aggressive behavior in people based on analysis of video materials using a recurrent conventional neural network]. *Problemy proyektirovaniya, primeneniya i bezopasnosti informatsionnykh sistem v usloviyakh tsifrovoy ekonomiki* [Problems of design, application and security of information systems in the conditions of the digital economy], 2019, pp. 207–210.
8. Marenkov A. N., Demin K. S. Metody raspoznavaniya dvizheniy cheloveka s primeneniyem tekhnologiy neyronnykh setey [Methods for recognizing human movements using technologies of neural networks]. *Matematicheskiye metody v tekhnike i tekhnologiyakh* [Mathematical methods in engineering and technology – MMTT], 2020, pp. 135–138.

DOI 10.21672/2074-1707.2021.53.1.091-097
УДК 004.85:004.056

АВТОМАТИЗИРОВАННЫЙ ПОИСК УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЯ НА ОСНОВЕ МАШИННОГО ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ

Статья поступила в редакцию 12.12.2020, в окончательном варианте – 15.01.2021.

Выборнова Ольга Николаевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат технических наук, ORCID: 0001-9458-1093, e-mail: olga.vyb.90@gmail.com
Рыжиков Александр Николаевич, Национальный исследовательский ядерный университет МИФИ, 115409, Российская Федерация, г. Москва, Каширское ш., 31,
магистрант, e-mail: alexander.ryzhikov.work@gmail.com

Проанализирована актуальность задачи создания более эффективного (по сравнению с аналогами) средства автоматизированного поиска уязвимостей на основе современных технологий. Показана схожесть процесса выявлений уязвимостей с марковским процессом принятия решения и обоснована целесообразность применения технологии машинного обучения с подкреплением для решения данной задачи. Поскольку анализ безопасности веб-приложений является в настоящее время наиболее приоритетным и востребованным, в рамках данной работы рассматривается приложение математического аппарата машинного обучения с подкреплением именно к этой предметной области. Представлена математическая модель, описана специфика процесса обучения и тестирования для задачи автоматизированного поиска уязвимостей веб-приложений. На основе анализа руководства по тестированию OWASP определено пространство действий и множество состояний среды. Описаны характеристики программной реализации предложенной модели: Q-обучение реализовано на языке программирования Python, для реализации политики обучения с помощью библиотеки tensorflow была создана нейронная сеть. Продемонстрированы результаты работы агента обучения с подкреплением на реальном веб-приложении, а также их сравнительный анализ с отчетом сканера уязвимостей Acunetix. Полученные данные свидетельствуют о перспективности предложенного решения.

Ключевые слова: уязвимость, автоматизированный поиск уязвимостей, пентестинг, обучение с подкреплением, Q-обучение

AUTOMATED VULNERABILITY SEARCH IN A WEB APPLICATION BASED ON REINFORCEMENT LEARNING

The article was received by the editorial board on 12.12.2020, in the final version – 15.01.2021.

Vybornova Olga N., Astrakhan State University, 20a Tatischev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Engineering), ORCID: 0001-9458-1093, e-mail: olga.vyb.90@gmail.com
Ryzhikov Aleksander N., National Research Nuclear University MEPHI, 31 Kashirskoe shosse, Moscow, 115409, Russian Federation,
undergraduate student, e-mail: alexander.ryzhikov.work@gmail.com

We analyzed the urgency of the task of creating a more efficient (compared to analogues) means of automated vulnerability search based on modern technologies. We have shown the similarity of the vulnerabilities identifying process with the Markov decision-making process and justified the feasibility of using reinforcement learning technology for solving this problem. Since the analysis of the web application security is currently the highest priority and in demand, within the framework of this work, the application of the mathematical apparatus of reinforcement learning with to this subject area is considered. The mathematical model is presented, the specifics of the training and testing processes for the problem of automated vulnerability search in web applications are described. Based on an analysis of the OWASP Testing Guide, an action space and a set of environment states are identified. The characteristics of the software implementation of the proposed model are described: Q-learning is implemented in the Python programming language; a neural network was created to implement the learning policy using the tensorflow library. We demonstrated the results of the Reinforcement Learning agent on a real web application, as well as their comparison with the report of the Acunetix Vulnerability Scanner. The findings indicate that the proposed solution is promising.

Keywords: vulnerability, automated vulnerability search, pentesting, reinforcement learning, Q-learning

Graphical annotation (Графическая аннотация)

Введение. Одним из важнейших этапов процесса обеспечения информационной безопасности информационной системы является выявление уязвимостей, или пентестинг (от англ. Penetration Testing). Поиск уязвимостей позволяет получить объективную оценку того, насколько легко осуществить несанкционированный доступ к информационной системе, а также взглянуть на нее с точки зрения злоумышленника, а именно – понять, каким образом можно скомпрометировать данную систему и какие вредоносные действия совершить [6].

Задача обнаружения уязвимостей является трудоемкой, поэтому идея ее автоматизации не нова. Существует большое количество систем автоматизированного поиска уязвимостей. Они применяются в различных средах: обнаруживают уязвимости локальной сети (Nessus, OpenVAS и др.) [1], исследуют безопасность веб-ресурсов (SQL-map, what-web и др.), анализируют бреши в коде программного обеспечения (например, Kaspersky антивирус) и т. д. [2]. При этом в общем случае процесс автоматизированного поиска уязвимостей сводится к полному перебору уязвимостей, содержащихся в базе данных используемого инструмента. Поэтому задача создания более эффективного средства автоматизированного поиска уязвимостей на основе современных технологий является актуальной.

В последнее время наблюдается прорыв в области машинного обучения и искусственного интеллекта. Благодаря приложению глубокого обучения и сложных искусственных нейронных сетей на математический аппарат принятия решений, были достигнуты большие результаты в областях робототехники, эконометрики, компьютерного зрения и т.д. Искусственный интеллект все лучше и лучше справляется с не тривиальными задачами и способен действовать подобно человеку.

В связи с этим целью данной работы является автоматизация процесса поиска уязвимостей на основе применения технологий машинного обучения.

Процесс поиска уязвимостей. Прежде всего необходимо проанализировать классический процесс поиска уязвимостей, производимый человеком вручную. Существует множество методик аудита автоматизированных систем на предмет наличия уязвимостей. Например, общепринятой методикой для тестирования веб-ресурсов на проникновение считается методика OWASP [8]. Данное направление (анализ безопасности веб приложений) является в настоящее время наиболее приоритетным и востребованным [4], поэтому в рамках данной работы целесообразно рассматривать именно эту предметную область.

Анализ методики OWASP показал, что поиск уязвимостей представляет собой итеративный процесс. Целью каждого этапа является сбор дополнительных сведений об исследуемом объекте, которые помогут в дальнейшем анализе. Выбор инструментальных средств для осуществления поиска и эксплуатации уязвимостей при этом зависит от имеющегося набора сведений об исследуемой информационной системе.

Схематически процесс тестирования на проникновение представлен на рисунке 1.

Анализ процесса поиска уязвимостей позволяет сделать вывод о его схожести с Марковским процессом принятия решений (МППР). При этом текущий перечень сведений о системе определяется как состояние системы, а применение той или иной утилиты – как действие [2].

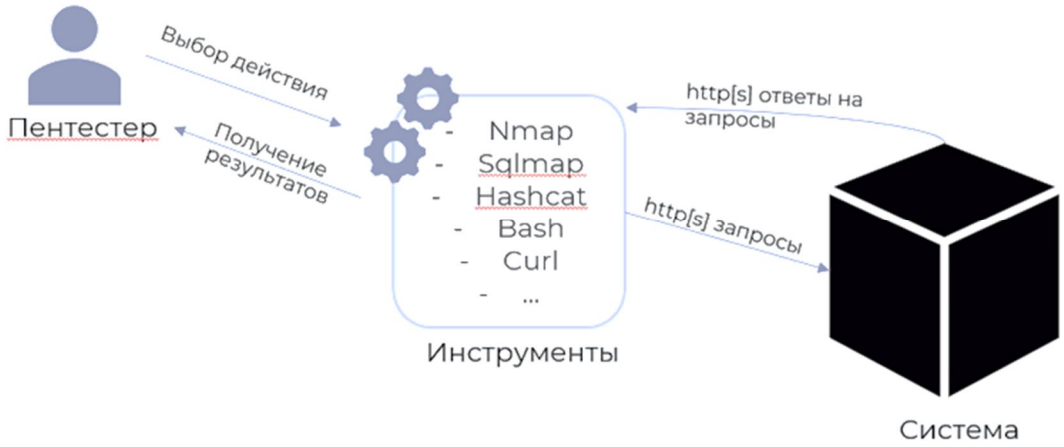


Рисунок 1 – Схема тестирования на проникновение

Построение математической модели. Задаче автоматизированного поиска уязвимостей присущи разнородность входных и выходных данных, отсутствие правильных пар «приложение – уязвимость», взаимодействие модели с объектом анализа, а также схожесть процесса поиска с МППР. В связи с этим при разработке интеллектуальной системы поиска уязвимостей целесообразно применять модель машинного обучения с подкреплением.

Обучение с подкреплением – это обучение машины отображать ситуации в действия, чтобы максимизировать некоторый сигнал поощрения (вознаграждения), принимающий числовые значения. Основная цель обучения с подкреплением – зафиксировать наиболее важные аспекты реальной задачи, имея в виду организацию взаимодействия агента со средой для достижения некоторой цели. Такого рода агент должен иметь возможность в какой-то мере воспринимать состояния окружающей среды, а также – предпринимать действия, которые могут повлиять на состояние среды [7].

В контексте задачи автоматизированного поиска уязвимостей, средой является некий объект исследования: информационная система, сетевой или веб ресурс, программное обеспечение. В произвольный момент времени t агент характеризуется состоянием среды $s_t \in S$ и множеством возможных действий $A(s_t)$. Состоянием является перечень сведений, известных об исследуемом объекте в момент времени t. Выбирая действие $a \in A(s_t)$, агент получает от среды новые сведения, переходит в состояние s_{t+1} и получает выигрыш r_t. При этом если найдены новые уязвимости или хотя бы новые сведения о приложении, выигрыш будет положительным. Отсутствие новых сведений говорит о бесполезности применения действия, следовательно, выигрыш в этом случае будет отрицательным. Основываясь на таком взаимодействии с окружающей средой, агент, обучающийся с подкреплением, должен выработать стратегию P: $S \rightarrow A$, которая максимизирует величину вознаграждения $R = r_0 + r_1 + \ldots + r_n$ в случае МППР, имеющего терминальное состояние, или, в случае МППР без терминальных состояний, величину, рассчитываемую по формуле (1):

$$R = \sum_t \gamma^t r_t \,, \tag{1}$$

где γ – дисконтирующий множитель для «предстоящего выигрыша» ($0 \le \gamma \le 1$) [2].

Действиями в задаче пентестинга являются блоки программного кода, которые взаимодействуют с объектом исследования посредством запросов. В случае веб-приложения используются http и https запросы. Для определения пространства действий целесообразно обратиться к руководству по тестированию OWASP. Согласно данной методике, пространство действий включает в себя:

- сбор первичной информации;
- тестирование конфигурации;
- тестирование идентификации, аутентификации и авторизации;
- тестирование валидации введенных данных;
- тестирование уязвимостей на стороне клиента [8].

Чтобы определить множество состояний среды, было проанализировано, какие данные способны возвращать функции и методы, составляющие пространство действий. Все типы возвращаемых данных можно условно разделить на 3 группы, представленные в таблице 1.

Таблица 1 – Типы возвращаемых значений

Тип	Описание	Примеры
Бинарный	Принимает значений «истина» и «ложь». «Истина» означает, что сетевой узел содержит данную уязвимость или ему присущ данный атрибут	- работает ли данный веб-ресурс по протоколу https; - возвращает ли веб-ресурс, зарегистрированный на данном сетевом узле, cookies
Множественный	Принимают значения из определенного множества, могут быть одинаковыми у нескольких сетевых узлов	- версия веб-сервера Apache может принимать значения из множества {1.0, 1.1, 1.2.1, …}; - адрес панели администратора часто принимает значения из множества {admin, administrator, administrative}
Уникальный	Может принимать как строковые, так и числовые значения. У разных сетевых узлов они не повторяются	- пароль администратора; - уязвимый параметр в get http запросе для слепой sql инъекции

Обозначенные группы данных необходимо привести к формату, пригодному для дальнейшего обучения системы – сделать все параметры бинарными. В случае «уникальных» параметров: если значение параметра существует, то при переводе к бинарному виду он принимает значение «истина», в обратном случае – «ложь».

Обучение и программная реализация модели. Существуют разные методы обучения с подкреплением. Самым известным является Q-обучение, которое целесообразно использовать в поставленной задаче. Суть алгоритма Q-обучения в следующем: агент на основе получаемого от среды вознаграждения формирует функцию полезности Q, что впоследствии дает ему возможность выбирать стратегию поведения не случайно, а учитывать опыт предыдущего взаимодействия со средой. Одно из преимуществ Q-обучения – то, что оно в состоянии сравнить ожидаемую полезность доступных действий, не формируя модели окружающей среды [5, 7].

Таким образом, алгоритм – это функция качества от состояния и действия: $Q{:}S\times A\rightarrow R$.

Перед обучением Q инициализируется случайными значениями. Далее в каждый момент времени t агент выбирает действие a_t, получает награду r_t, переходит в новое состояние s_{t+1}, которое может зависеть от предыдущего состояния s_t и выбранного действия, и обновляет функцию Q. Обновление функции использует взвешенное среднее между старым и новым значениями:

$$Q(s_t, a_t) = (1-\alpha)Q(s_t, a_t) + \alpha \cdot (r_t + \gamma \cdot \max_a Q(s_{t+1}, a)), \quad (2)$$

где r_t – это награда, полученная при переходе из состояния s_t в состояние s_{t+1}, и α – это скорость обучения ($0 < \alpha \leq 1$). Алгоритм завершает работу, когда агент переходит в терминальное состояние s_{t+1} [5].

Блок-схема алгоритма обучения с подкреплением для задачи автоматизированного поиска уязвимостей, а также пример его работы для одного веб приложения были опубликованы ранее в [2].

Для доказательства эффективности предлагаемого подхода была программно реализована упрощенная модель системы автоматизированного поиска уязвимостей веб-ресурсов. Алгоритм Q-обучения был реализован на языке программирования Python [10]. Для реализации политики обучения с помощью библиотеки tensorflow была создана нейронная сеть [3]. Она имеет следующие характеристики:

1. Входной слой – вектор бинарных значений, описывающих состояние среды. Количество входных нейронов соответствует количеству элементов в векторе состояния среды.
2. Скрытый слой. Количество нейронов скрытого слоя соответствует количеству нейронов на входном слое. Функция активации – функция сигмоиды.
3. Выходной слой – вектор вещественных значений, определяющий предпочтительность применения каждого действия. Количество нейронов выходного слоя соответствует количеству функций в пространстве действий.
4. Оптимизатор – метод обновления весов – «adam» – улучшенный алгоритм стохастического градиентного спуска, обеспечивающий более высокую сходимость.
5. Функция потерь – среднеквадратичная ошибка.

Пространство действий соответствует действиям, представленным в методике OWASP, и содержит в том числе функции таких программных средств анализа уязвимостей, как nmap, SQLmap, WhatWeb, XSScrapy. При реализации пространства действий использовались библиотеки с открытым исходным кодом [9, 11, 13]. Вектор бинарных значений, описывающий текущие сведения о веб ресурсе, состоит из 256 элементов, которые описывают веб сервер, версию веб сервера, субдомены, открытые директории, SQL-инъекции, XSS уязвимости и другие характеристики системы. Были подготовлены тестовый и обучающий набор данных – характеристик различных веб-ресурсов.

Экспериментально были получены значения гиперпараметров модели γ и α. Каждая эпоха обучения представляет собой t итераций, в которых, s_t – состояние на t-й итерации, a_t – действие, которое следует применить на t-й итерации. Награда $r(t)$ равна +1, если найдены новые сведения, и –1 – в противном случае. В качестве оптимального действия на t-м шаге выбирается действие с максимальным значением функции качества. Разработанной модели на вход подавались адреса реальных веб-приложений, на которых модель обучалась в течение более 100 эпох.

Анализ полученных результатов. Классическим подходом для определения качества модели обучения с подкреплением является исследование суммарной награды. Для этого во время обучения для каждого объекта исследования, то есть для каждого веб-приложения, накапливается суммарная награда, затем берется усредненное значение для всех веб-приложений. Таким образом, после нескольких эпох обучения можно построить график зависимости суммарной награды R, полученный за эпоху обучения, от числа эпох e (рис. 2). На графике видно, что на первых эпохах суммарная награда отрицательна. Однако с ростом числа эпох обучения растет и суммарная награда, что говорит об эффективности модели.

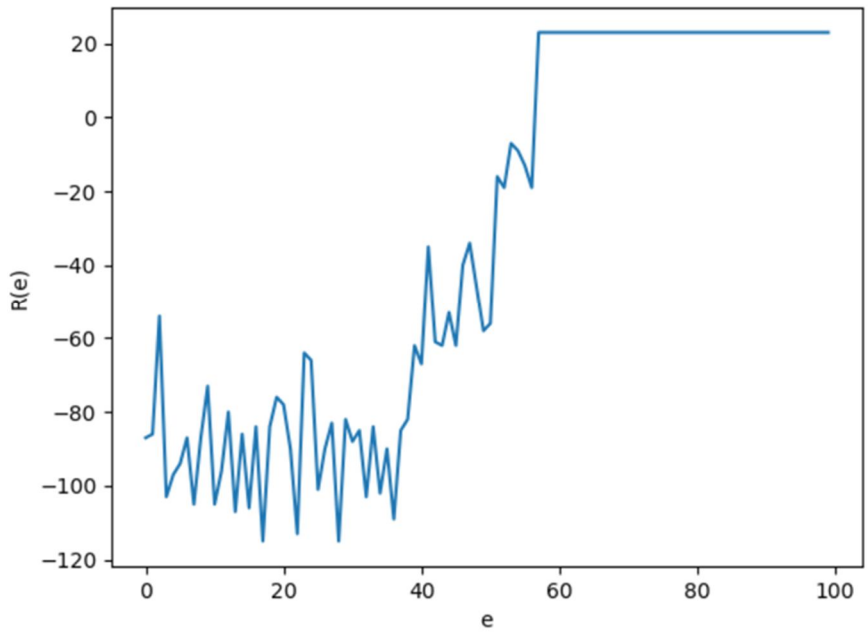


Рисунок 2 – График зависимости суммарного выигрыша от эпохи обучения

Кроме того, с целью проверки работоспособности и эффективности предложенной модели было проведено тестирование реального веб-приложения и сравнение результатов с результатами известного сканера уязвимостей.

Для анализа был выбран веб сайт testphp.vulnweb.com, который предоставляется компанией Acunetix для тестирования работоспособности одноименного сканера уязвимостей [12]. С помощью разработанного приложения был произведен его анализ и получены следующие результаты:

1. Был корректно определен веб-сервер – nginx.
2. Была корректно определена уязвимость integer overflow – у сервера nginx.
3. Была найдена отраженная XSS-уязвимость в POST параметре страницы /guestbook.
4. Была найдена SQL-инъекция в GET-параметрах страницы /search.php.
5. Была корректно определена СУБД – MySQL.
6. SQL-инъекция была эксплуатирована, в результате чего были определены названия всех таблиц и сделан дамп самих таблиц.
7. Был определен пользователь базы данных – acuart.
8. Был проанализирован дамп таблицы users, в котором был найден логин – test и пароль в открытом виде – test.
9. Был успешно произведен вход с использованием обнаруженных логина и пароля.
10. На странице пользователя, доступной после входа, была найдена еще одна XSS-уязвимость – в параметре name пользователя. Уязвимость хранимая, а значит, более опасная.

Это же веб-приложение было проанализировано с помощью сканера уязвимостей Acunetix. Так как данный веб-сайт разрабатывался специально для демонстрации работы этой программы,

очевидно, что сканер тоже показал хорошие результаты. В количественном отношении сканер нашел более 50 уязвимостей, однако большинство из них повторяются или являются ложными срабатываниями. Так, сканер нашел более 20 SQL-инъекций в одних и тех же post-запросах на разных страницах. С другой стороны, он обнаружил уязвимость Directory Traversal, в одном из GET-параметров страницы getimage.php. Действительно, если отправить запрос со значением параметра типа «/../../../../../etc/passwd», сервер вернет ответ со статусом 200. Однако в качестве ответа вернется информация об ошибке, в которой говорится о запрете на доступ в данную директорию. Следовательно, веб-приложение защищено от атак через уязвимость Directory Traversal.

Таким образом, в результате детального сравнительного анализа двух программ была сформирована таблица 2.

Таблица 2 – Сравнение разработанной модели с аналогом

Уязвимость	**Acunetix Vulnerability Scanner**	**Разработанный сканер на основе обучения с подкреплением**	**Потенциальные угрозы**
Integer Overflow	+	+	Отказ в обслуживании веб сервера
SQL-инъекция типа Union	+	+	Утечка данных из базы данных (БД)
SQL-инъекция типа Blind	+	+	Утечка данных из БД
Отраженная XSS-уязвимость	+	+	Перехват атрибутов доступа пользователя путем заманивания его на страницу
Хранимая XSS-уязвимость	-	+	Перехват атрибутов пользователя
Directory Traversal	+	-	Угрозы отсутствуют

Таким образом, агент обучения с подкреплением справился с поставленной задачей лучше. Он не только обнаружил SQL-инъекцию, но и предпринял действия для ее эксплуатации, собрав при этом дополнительные данные, которые пригодились для более глубокого тестирования. Модель автоматически определила страницу аутентификации и с помощью полученных заранее данных смогла войти в систему и обнаружить, благодаря этому, новую, более опасную уязвимость. Следует отметить, что сканер уязвимостей Acunetix нашел гораздо больше уязвимостей ввиду того, что обладает большой базой знаний для проведения автоматических тестов. При этом сканер не способен эксплуатировать уязвимости в реальном времени, что делает его потенциально менее эффективным, чем предложенная модель.

Заключение. Проведенное исследование показывает целесообразность применения математической модели машинного обучения с подкреплением для задачи поиска уязвимостей веб ресурсов. Разработанный сканер уязвимостей является прототипом, однако анализ результатов его работы свидетельствует о перспективности предложенного решения. Расширение базы знаний и пространства действий обеспечит большую эффективность и позволит применять данную модель и разработанное программное средство для реальных задач тестирования веб приложений на проникновение.

Библиографический список

1. Ажмухамедов И. М. Выявление аномалий в вычислительных сетях общего пользования на основе прогнозирования объема сетевого трафика / И. М. Ажмухамедов, А. Н. Марьенков // Проблемы информационной безопасности. Компьютерные системы. – 2012. – № 3. – С. 35–39.

2. Выборнова О. Н. Применение машинного обучения с подкреплением для автоматизированного поиска уязвимостей информационных систем / О. Н. Выборнова, А. Н. Рыжиков // Математические методы в технике и технологиях. – ММТТ. – 2020 – Т. 4. – С. 110–113.

3. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow / О. Жерон. – Москва : Вильямс, 2018. – 688 с.

4. Итоги внешних пентестов 2020. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/external-pentests-2020/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 28.12.2020).

5. Обучение с подкреплением. – Режим доступа: http://neerc.ifmo.ru/wiki/index.php?title=Обучение_с_подкреплением (дата обращения 28.12.2020), свободный. – Заглавие с экрана. – Яз. рус.

6. Плешков А. С. Тестирование на проникновение как анализ защищенности компьютерных систем / А. С. Плешков, Д. Д. Рудер // Известия Алтайского государственного университета. – 2015. – № 1 (85). – С. 174–181.

7. Саттон Р. С. Обучение с подкреплением / Р. С. Саттон, Э. Г. Барто. – Москва : БИНОМ. Лаборатория знаний, 2017. – 380 с.

8. Meucci M. Owasp Testing Guide / M. Meucci, A. Muller. – OWASP Foundation, v4.0, 2014. – 384 p.

9. PwnXss: Vulnerability (XSS) scanner exploit. – Режим доступа: https://github.com/pwn0sec/PwnXSS, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.12.2020).

10. Reinforcement learning tutorial using Python and Keras. – Режим доступа: https://adventuresinmachinelearning.com/reinforcement-learning-tutorial-python-keras/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.12.2020).

11. Sqlmap. – Режим доступа: https://github.com/sqlmapproject/sqlmap свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.12.2020).

12. Test and Demonstration site for Acunetix Web Vulnerability Scanner. – Режим доступа: http://testphp.vulnweb.com/ свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 28.12.2020).

13. WAD – Web Application Detector. – Режим доступа: https://github.com/CERN-CERT/WAD (дата обращения: 28.12.2020), свободный. – Заглавие с экрана. – Яз. англ.

References

1. Azhmukhamedov I. M., Marenkov A. N. Vyyavlenie anomaliy v vychislitelnykh setyakh obshchego polzovaniya na osnove prognozirovaniya obema setevogo trafika [Anomaly detection in public computer networks on the basis of forecasting volume of network traffic]. *Problemy informatsionnoy bezopasnosti. Kompyuternye sistemy* [Information Security Problems. Computer Systems], 2012, no. 3, pp. 35–39.

2. Vybornova O. N., Ryzhikov A. N. Primenenie mashinnogo obucheniya s podkrepleniem dlya avtomatizirovannogo poiska uyazvimostey informatsionnykh sistem [Reinforcement learning for automated vulnerability search]. *Matematicheskie metody v tehnike i tekhnologiyakh – MMTT* [Mathematical Methods in Technics and Technologies – MMTT], 2020, vol. 4, p. 110-113.

3. Geron A. *Prikladnoe mashinnoe obuchenie s pomoshhyu Scikit-Learn i TensorFlow* [Hands-On Machine Learning with Scikit-Learn and TensorFlow]. Moscow, Williams Publ., 2018. 688 p.

4. *Itogi vneshnikh pentestov 2020* [Results of external pentests 2020]. Available at: https://www.ptsecurity.com/ru-ru/research/analytics/external-pentests-2020/ (accessed 28.12.2020).

5. *Obuchenie s podkrepleniem* [Reinforcement learning]. Available at: http://neerc.ifmo.ru/wiki/index.php?title=Обучение_ с_подкреплением (accessed 28.12.2020).

6. Pleshkov A. S., Ruder D. D. Testirovanie na proniknovenie kak analiz zashchishhennosti kompyuternykh sistem [Penetration testing as a security analysis of computer system]. *Izvestiya Altayskogo gosudarstvennogo universiteta* [Izvestiya of Altai State University], 2015, no. 1 (85), pp. 174–181.

7. Sutton R. S., Barto A. G. *Obuchenie s podkrepleniem* [Reinforcement learning]. Moscow, BINOM Publ., 2017. 380 p.

8. Meucci M., Muller A. *Owasp Testing Guide*. OWASP Foundation, v4.0, 2014. 384 p.

9. *PwnXss: Vulnerability (XSS) scanner exploit.* Available at: https://github.com/pwn0sec/PwnXSS (accessed 28.12.2020).

10. *Reinforcement learning tutorial using Python and Keras.* Available at: https://adventuresinmachinelearning.com/reinforcement-learning-tutorial-python-keras/ (accessed 28.12.2020).

11. *Sqlmap.* Available at: https://github.com/sqlmapproject/sqlmap (accessed 28.12.2020).

12. *Test and Demonstration site for Acunetix Web Vulnerability Scanner.* Available at: http://testphp.vulnweb.com/ (accessed 28.12.2020).

13. *WAD – Web Application Detector.* Available at: https://github.com/CERN-CERT/WAD (accessed 28.12.2020).

УДК 004.056; 34.05

ЮРИДИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ СОЗДАНИЮ И РАСПРОСТРАНЕНИЮ «ФЕЙКОВОГО» КОНТЕНТА

Статья поступила в редакцию 12.02.2021, в окончательном варианте – 20.02.2021.

Крайнюкова Ляйсян Маратовна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
ассистент кафедры международного права, e-mail: 5leska5@mail.ru
Станишевская Алина Владимировна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
ассистент кафедры информационной безопасности и цифровых технологий, e-mail: a.stanishevskaia@gmail.com
Ажмухамедов Искандар Маратович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
декан факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности и цифровых технологий, ORCID: 0000-00019058-123X, e-mail: iskander_agm@mail.ru

Авторами была проанализирована юридическая сторона вопроса обеспечения информационной безопасности в рамках противодействия деструктивной, в том числе так называемой «фейковой» информации. Отмечено, что нормативно-правовое регулирование в данной сфере имеет ряд пробелов, наличие которых создает процессуальные затруднения при выявлении такого контента и назначении наказания за его распространение. При этом отмечено, что данная проблема актуальна как для российского законотворчества, так и для зарубежного и международного права. В статье указано, что требуется междисциплинарное изучение феномена дезинформации и «фейковой информации», включая технологический, юридический, журналистский аспект с целью понимания сущности данного явления, нормативного закрепления унифицированного категориального аппарата в обозначенной сфере. Также отмечено, что существует необходимость привлечения всех заинтересованных сторон с учетом принципа «мультистейкхолдернизма» и саморегулирования глобального пространства интернет, с привлечением представителей гражданского общества, бизнес-структур, частного сектора, представителей IT-индустрии, а также правительств государств. В ходе исследования была обнаружена необходимость межгосударственного взаимодействия с целью разработки и принятия международного механизма сотрудничества в сфере противодействия дезинформации. Это позволит создать унифицированный комплексный механизм, включающий международные стандарты правового и технологического характера.

Ключевые слова: дезинформация, фейковая информация, стейкхолдер, медийные технологии

LEGAL ASPECTS OF COUNTERING THE CREATION AND DISTRIBUTION OF FAKE CONTENT

The article was received by the editorial board on 12.02.2021, in the final version – 20.02.2021.

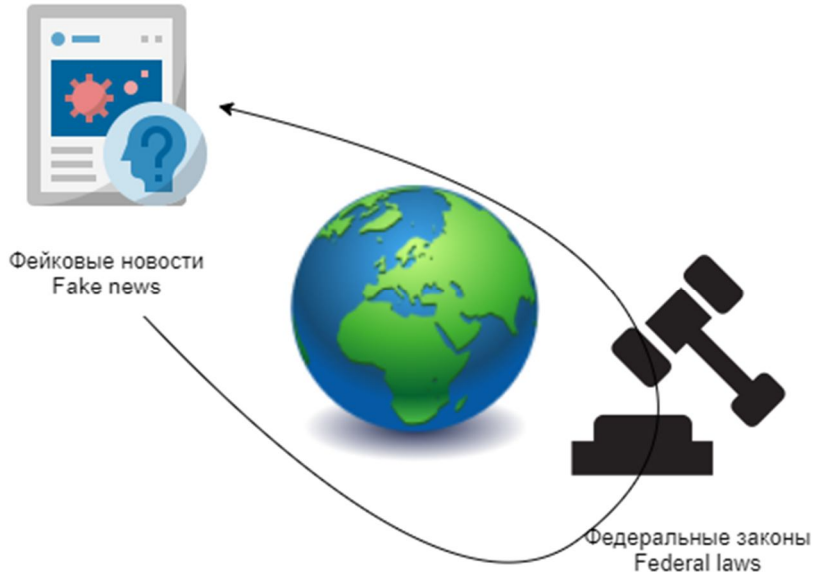
Krainyukova Lyaysyan M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
assistant of the Department of International Law, e-mail: 5leska5@mail.ru
Stanishevskaya Alina V., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
assistant of the Department of Information Security and Digital Technologies, e-mail: a.stanishevskaia@gmail.com
Azhmukhamedov Iskandar M., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Dean of the Faculty of Digital Technologies and Cybersecurity, Professor of the Department of Information Security and Digital Technologies, ORCID: 0000-00019058-123X, e-mail: iskander_agm@mail.ru

The authors analyzed the legal side of the issue of ensuring information security within the framework of countering destructive, including the so-called “fake” information. It is noted that the legal regulation in this area has a number of gaps, the presence of which creates procedural difficulties in identifying such content and imposing penalties for its distribution. At the same time, it was noted that this problem is relevant both for Russian lawmaking and for foreign and international law. The article indicates that an interdisciplinary study of the phenomenon of disinformation and "fake information" is required, including the technological, legal, and journalistic aspects in order

to understand the essence of this phenomenon, normative consolidation of a unified categorical apparatus in the designated area. It was also noted that there is a need to involve all stakeholders, taking into account the principle of "multistakeholderism" and self-regulation of the global Internet space, with the involvement of representatives of civil society, business structures, the private sector, representatives of the IT industry, as well as state governments. The study revealed the need for interstate cooperation in order to develop and adopt an international mechanism for cooperation in countering disinformation. This will make it possible to create a unified comprehensive mechanism that includes international legal and technological standards.

Keywords: disinformation, fake information, stakeholder, media technologies

Graphical annotation (Графическая аннотация)



Введение. Обмен информацией и возможность ее распространения можно рассматривать в качестве основы существования и функционирования любого сообщества. С середины XX века человечество вступило в новый, постиндустриальный или информационный этап развития, для которого характерно трансграничное распространение информационных потоков, значительное их расширение, обусловленное быстрыми темпами прогресса в сфере цифровых технологий. Информационный обмен как базовая детерминанта функционирования современного общества вышел на совершенно новый уровень как по объему циркулирующей информации, так и по скорости ее распространения. При этом отмечается резкое увеличение уровня информационного воздействия на социальную, экономическую, политическую, духовную и другие сферы общественного развития.

Все эти процессы приводят к необходимости структурных трансформаций в общественном устройстве – фактического перевода базовых сфер общественной жизнедеятельности, в первую очередь сфер экономики, государственного управления, образования, финансового сектора, здравоохранения, предпринимательства на цифровые платформы. Задача масштабной цифровизации – обеспечение максимально быстрого и удобного доступа пользователей к общественно-полезной и ценной информации, предоставление возможности публичного обсуждения значимых общественных проблем посредством коллективного взаимодействия, повышение эффективности процессов обмена информацией и знаниями как ценным ресурсом. Между тем масштабный переход к массовому применению цифровых технологий имеет как положительные, так и отрицательные последствия. Одним из негативных проявлений трансформирующейся информационной среды можно считать проблему широкомасштабного и систематического распространения так называемой «фейковой» (недостоверной, ложной) информации. Ее распространение не только подрывает доверие к циркулирующему в сети контенту, но и оказывает деструктивное воздействие и создает угрозы функционированию демократических институтов, неприкосновенности частной жизни, вплоть до угроз общественно-политическому устройству и государственной безопасности.

Ряд экспертов отмечают также наметившиеся тенденции обострения международного информационного противоборства, которое ведется уже в виде так называемых «информационных войн». Их характерной особенностью является «согласованная планомерная деятельность, направленная на использование информации в качестве оружия для разрушающего воздействия

на противника в экономической, политической, социальной и духовной сферах. При этом ошибочно полагать, что объектом информационного противоборства являются исключительно информационные системы. Информационное оружие – это средство воздействия на сознание людей, их поведение и психологическое здоровье с целью распространения паники, дезориентации и «зомбирования» населения» [8].

Все это свидетельствует о повышенной степени общественной опасности феномена создания и распространения «фейковой информации». То, что зарождалось как «непроверенная информация» и до широкого распространения интернета, называлось «газетными утками» и на сегодняшний момент приобрело характер глобальной угрозы, катастрофической по своим разрушающим последствиям.

Таким образом, исследование сущности данного явления, характерных критериев, форм, методов распространения фейковой информации в интернете становится весьма актуальной задачей, которая в последние годы обращает на себя внимание различных исследователей.

В частности, рассмотрению данной проблемы посвящены работы Н.А. Марковой [5, 6], А.С. Курганової [6], Д. Бебич [1], М. Воларевич [1], С.В. Полищук [8], М.О. Зыряновой [2, 3] и др.

В данных работах сделан вывод о том, что эффективное противодействие данной угрозе может быть реализовано только посредством комплексного подхода, включающего в себя в том числе и разработку соответствующего правового инструментария.

Исходя из этого, **целью** данной работы стало рассмотрение основных юридических аспектов борьбы с данным явлением как на уровне суверенных государств, так и на международном уровне.

Юридический аспект исследования данной проблемы должен включать сравнительно-правовой анализ существующих подходов к определению и нормативному закреплению категории «фейковая» информация», выделению сущностных характеристик данного явления, критериев отнесения той или иной информации к разряду «фейковой», криминализации деяний по созданию и распространению «фейковых новостей» в медиапространстве на примере внутреннего законодательства различных государств, а также обзор имеющихся международных инициатив в данной сфере, предпринимаемых на уровне региональных международных организаций (на примере ЕС), и мер универсального характера (инициативы ООН). Это позволит в дальнейшем сформулировать предложения по совершенствованию и гармонизации законодательства.

Запрос правоприменительной практики сводится к необходимости криминализации деяний по созданию и распространению «фейковой» информации с целью установления ответственности за так называемую «дезинформацию», которая может повлечь серьезные последствия, в числе которых «реальная опасность жизни и здоровью граждан, массовые беспорядки, угроза государственной, общественной или экологической безопасности» [10]. Многие государства на сегодняшний день выступают с рядом законодательных инициатив, направленных на создание механизма противодействия распространению «фейковой» информации, ее запрещению и криминализацию обозначенных деяний. Так, в Российской Федерации в марте 2019 г. был внесен ряд законодательных поправок.

Обзор российского законодательства. Федеральный закон от 18.03.2019 г. № 31-ФЗ «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации» дополнил перечень видов информации, распространяемой с нарушением закона, тем самым закрепив на законодательном уровне категорию «фейковая информация», под которой следует понимать «недостоверную общественно значимую информацию, распространяемую под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи».

Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее – Закон № 27-ФЗ) установил ответственность за размещение в информационно-телекоммуникационных сетях и средствах массовой информации заведомо недостоверной общественно значимой информации под видом достоверных сообщений. Административная ответственность за распространение фейковой (недостоверной) информации предусматривается пунктами 9, 10, 10.1 и 10.2 статьи 13.15 КоАП РФ. При этом разграничение составов указанных административных правонарушений осуществляется по вышеобозначенным пунктам ст. 13.15 КоАП РФ в зависимости от характера наступивших общественно-опасных последствий и категорий субъектов, совершивших данные действия. Так, пункты 9, 10 ст. 13.15 КоАП РФ предусматривают административную ответственность для граждан, должностных лиц и юридических лиц, в то время как пункты 10.1 и 10.2 ст. 13.15 КоАП РФ предусматривают административную ответственность только для юридических лиц.

Согласно п. 9 ст. 13.15 КоАП РФ, распространяемая недостоверная информация должна «создавать угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи». Пункт 10 запрещает те же деяния при условии, если они повлекли «создание помех функционированию объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, но при этом не содержат состава уголовно наказуемого деяния».

Далее стоит отметить апрельские поправки, внесенные в УК РФ в 2020 г. в ст. 207.1, 207.2, криминализующие, по сути, аналогичные деяния, что и пп. 10.1, 10.2 ст. 13.15 КоАП РФ, а именно «публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств» (ст. 207.1), а также «публичное распространение под видом достоверных сообщений заведомо ложной общественно значимой информации, повлекшее по неосторожности причинение вреда здоровью человека (ч.1 ст. 207.2), по неосторожности смерть человека или иные тяжкие последствия (ч. 2 ст. 207.2)». Необходимо отметить, что разграничение административной ответственности, предусмотренной ст. 13.15 КоАП РФ и уголовной ответственности, предусмотренной ст. 207.1, 207.2 УК РФ проводится, исходя из критерия субъектного состава, поскольку административная ответственность за правонарушения, предусмотренные пунктами 10.1 и 10.2 ст. 13.15 КоАП РФ, установлена для юридических лиц, а граждане, должностные лица и руководители юридических лиц могут быть привлечены к уголовной ответственности, предусмотренной ст. 207.1 УК РФ и ст. 207.2 УК РФ.

Таким образом, упомянутые поправки в российское законодательство можно расценивать как свидетельство повышенного уровня общественной опасности проблемы распространения «фейковой информации», актуальности разработки и принятия эффективного и достаточного правового механизма противодействия данной угрозе. Стоит отметить, что российский законодатель пошел по пути нормативного закрепления конкретного юридического определения категории «фейковой информации» (Федеральный закон от 18.03.2019 № 31-ФЗ «О внесении изменений в статью 15-3 Федерального закона «Об информации, информационных технологиях и о защите информации»). Нормы о криминализации рассмотренных составов преступлений и административных правонарушений достаточно обширно охватывают признаки и состав данных деяний, при этом существует определенная сложность с разграничением видов ответственности (уголовной и административной), обусловленная неким дублированием составов деяний. Кроме того, представляется, что законодательные конструкции не в полной мере учитывают технологические и технические аспекты данного рода деятельности, что затрудняет выделение четких критериев отнесения той или иной информации к категории «фейковой», а также криминализации и привлечения к ответственности за совершение тех или иных действий по созданию такого информационного продукта.

Обзор европейского законодательства. Рассмотрим законодательные меры противодействия «фейковой информации» на примере других государств. Так, власти Германии в 2017 г. приняли Закон «Net Enforcement Act (NetzDG)» (дословный перевод Закон «О правовом регулировании Сети»), направленный на установление ответственности для владельцев социальной сети в интернете за нарушение правил своевременного удаления незаконного контента. Фактически закон направлен на борьбу с различными проявлениями деструктивной, негативной, враждебной, общественно-опасной информации в сети, в частности распространением фейковых новостей. Стоит отметить, что закон охватывает большой перечень видов запрещенного контента, который включает порядка 20 составов преступлений по УК Германии и в зависимости от объекта преступного посягательства выделяет информацию, распространение которой подрывает основы государственного устройства и стабильности, посягает на общественный порядок или влечет нарушение прав граждан.

При этом закон не содержит четкого определения понятия «фейковой информации», а содержащиеся в нем критерии определения данного контента как «ложной информации» представляются весьма обобщенными.

Таким образом, закон не определяет новые термины незаконного контента, а носит процессуальный характер, устанавливая порядок применения существующих норм Уголовного кодекса к новому виду преступной деятельности [12].

Законодательство Франции устанавливает запрет на распространение «неточных или лживых утверждений и обвинений, которые имеют целью изменить подлинные результаты голосования». Кроме того, законом установлена возможность блокировки на территории страны вещания

«иностранного телеканала или другого СМИ иностранного государства, осуществляющего целенаправленную дезинформацию». Представляет интерес законодательное закрепление обязанности социальных сетей в случае, если они размещают проплаченную политическую рекламу, указывать, что информация оплачена одним из коммерческих клиентов, размещать ссылку на ее заказчика и публиковать сумму финансовых начислений [13]. Обращает на себя внимание тот факт, что отмеченные законодательные инициативы французских властей главным образом направлены на ограничение распространения так называемой «ложной информации» преимущественно в условиях предвыборной агитации, в частности направлены на ограничение деятельности иностранных СМИ, что можно охарактеризовать в качестве некого злоупотребления законодательной властью и попыток ограничить свободу слова [11].

Вопрос о законодательном закреплении юридической категории «фейковая информация» весьма детально и показательно проработан в Малайзии. В 2018 г. был принят специализированный законодательный акт «Anti-fake news Act», в котором было закреплено понятие «фейковая информация» – «любые новости, информация, сведения и отчеты, которые являются или полностью, или частично ложными, в формате журнальной или газетной статьи, или телевизионной программы, видео- или аудиозаписи, или же в любом ином формате, способном передавать слова и мысли». Закреплены различные категории «фейковой информации» в зависимости от формы их создания и передачи:

а) любая письменная публикация, а равно любая иная публикация, обладающая аналогичными с письменной публикацией свойствами, а также любое копирование, полное или частичное воспроизведение такой публикации;

б) любая публикация, изготовленная цифровым, электронным, магнитным или механическим способом, а равно полное или частичное копирование таких публикаций.

Закон устанавливает уголовную ответственность для лиц, которые любыми способами, действуя злонамеренно, создают, предлагают, издают, печатают, поставляют, передают или распространяют любые «фейковые новости» или публикации, содержащие такие новости. Уголовная ответственность по Anti-fake news Act Малайзии предусмотрена и для лиц, которые прямо или косвенно финансируют распространение «Fake news» [13].

Это лишь некоторые примеры подобных законодательных инициатив. Аналогичные законы были приняты на протяжении последних 5 лет во многих странах, в частности в Египте, Бразилии, Вьетнаме, Катаре, Китае, Кыргызстане, США, Казахстане, Белоруссии. Анализ правовой базы внутреннего законодательства государств в сфере противодействия фейковой информации, регулирования интернет-пространства и борьбы с иными формами киберпреступности позволяет сделать вывод о значительных усилиях, предпринимаемых правительствами государств и активной реализации обозначенных законодательных инициатив.

Между тем многие национальные законы оцениваются экспертами как попытки установления жесткой цензуры и чрезмерного государственного контроля национального сегмента информационного пространства, когда под «громкими лозунгами» защиты прав человека вводятся юридические нормы, которые становятся инструментом давления на СМИ. Как отмечает официальный представитель МИД РФ Мария Захарова в своем выступлении на заседании комитета Генеральной Ассамблеи ООН по информации, «вследствие усиления политических противоречий в международных отношениях мировое информационное пространство все больше начинает превращаться в арену борьбы между отдельными государствами и группами влияния, а медийные технологии становятся орудием информационной войны. В этой ситуации существенным вызовом остается феномен дезинформации и его проявление в виде «фейковых новостей»».

Представляется, что для решения глобальной проблемы противодействия дезинформации и распространению «фейкового контента» недостаточно проведение законодательных реформ в одностороннем порядке. Необходимо объединение усилий на уровне международного сообщества, принятие базовых соглашений на площадке международных организаций в строгом соответствии с основополагающими принципами международного права, такими как свобода слова и равный доступ к информации.

В этой связи следует рассмотреть политику Европейского Союза, с 2017 г. осуществляющего комплексную планомерную работу в данной сфере. 13 ноября 2017 г. Европейская Комиссия инициировала проведение консультации с общественностью на тему «фейковых новостей» и дезинформации в интернете и создала Экспертную группу высокого уровня, в состав которой вошли представители академического сообщества, IT-компаний, СМИ и представителей гражданского общества. Всего в группу вошли порядка 40 экспертов.

Целью работы Комиссии стала разработка и последующая реализация всеобъемлющего и комплексного механизма противодействия онлайн-дезинформации в Европе, включающего

в себя различные направления деятельности: от принятия законодательных инициатив и региональных соглашений для обеспечения правовой базы (Кодекс практики в области дезинформации, Европейский план действий по активизации усилий по противодействию дезинформации в Европе и за ее пределами) до создания специализированных международных площадок (Европейская обсерватория цифровых медиа), проведения регулярных встреч в формате конференций и подготовки регулярных обзорных отчетов и докладов.

Согласно обозначенному Плану действий против дезинформации, под «дезинформацией понимается заведомо ложная или вводящая в заблуждение информация, которая создается, представляется и распространяется с целью получения экономической выгоды или преднамеренного обмана общественности и может причинить общественный вред. При этом общественный вред может включать угрозы демократическим процессам, а также общественным благам, таким как здоровье граждан Союза, окружающая среда или безопасность. Свобода выражения мнения названа основной ценностью Европейского Союза, закрепленной в Хартии основных прав Европейского Союза и в конституциях государств-членов».

Важная роль отводится объединению усилий и участию гражданского общества и частного сектора (платформы социальных сетей), представителей бизнес-структур, IT-индустрии в решении проблемы дезинформации. Такой подход представляется наиболее эффективным, поскольку согласуется с моделью «стейкхолдернизма», одной из основ построения и функционирования интернет-пространства [4], поскольку противодействие дезинформации требует согласованных действий с участием всех заинтересованных сторон. В научной доктрине понятие «Stakeholders» переводится как «заинтересованные участники» и используется в таком словосочетании или как акроним «стейкхолдеры». Кроме того, используются производные понятия и термины, например, «мультистейкхолдеризм» (Multistakeholderism), «мультистейхолдерская модель» (Multistakeholder's Model), «мультистейкхолдерский подход» (Multistakeholder's Approach); либо «многостороннее взаимодействие заинтересованных участников», «многосторонняя модель взаимодействия заинтересованных участников».

Именно поэтому работа Европейской комиссии в этом направлении на первом этапе предполагала проведение так называемых «консультаций с общественностью» (гражданами, социальными сетями, новостными организациями (вещателями, печатными СМИ, информационными агентствами, онлайн-СМИ), исследователями и государственными учреждениями, что позволило сформулировать общие подходы к пониманию того, какой комплекс мер необходимо осуществить на уровне ЕС для решения проблемы дезинформации. В Плане действий подчеркнута необходимость сотрудничества в данной сфере, в том числе на международном уровне. Скоординированный ответ на дезинформацию, представленный в этом Плане действий, основан на четырех принципах:

1) улучшение возможностей институтов Союза по обнаружению, анализу и разоблачению дезинформации;

2) усиление согласованных и совместных ответов на дезинформацию;

3) мобилизация частного сектора на борьбу с дезинформацией;

4) повышение осведомленности и повышение устойчивости общества.

Таким образом, европейский подход представляется достаточно эффективным и комплексным, поскольку вышеназванные инициативы реализуются в четком соответствии с принципами международного права, с соблюдением прав человека и основан на сотрудничестве заинтересованных участников «стейкхолдеров». Кроме того, европейский законодатель стремится к унификации нормативной базы и разработке базовых соглашений в обозначенной сфере. В то время как инициативы отдельных государств по внедрению новых законов, направленных на борьбу с дезинформацией, в частности «фейковой информацией», скорее можно расценивать как установление государственного контроля информационного пространства посредством введения императивных правил и ограничений, «расширительную» криминализацию деяний в отсутствие законодательного закрепления самого понятия «фейковой информации», а также критериев отнесения той или иной информации к разряду фейковой, квалификации соответствующих деяний.

Стоит отметить, что необходимость объединения усилий по противодействию проблеме дезинформации на уровне международного сообщества получила особую актуальность на фоне развернувшейся эпидемии коронавируса, по свои масштабам и последствиям затронувшей все сферы человеческой жизнедеятельности.

Ускоренные темпы цифровизации и глобальный перевод многих аспектов повседневной деятельности в цифровую среду спровоцировал ответный удар со стороны криминальных структур, значительный рост киберпреступности и глобальной угрозы дезинформации широких слоев населения, что в свою очередь вывело проблему «фейковых новостей» на уровень глобальной универсальной площадки Организации Объединенных Наций (ООН).

Так, на Всемирной конференции по безопасности (февраль 2020 г.) в частности обсуждалась проблема распространения недостоверных данных и новостей о коронавирусе. Представители ВОЗ обозначили новый термин «инфодемия», под которым следует понимать «распространение недостоверной информации о коронавирусе, которая способствует распространению слухов, неточных данных и фейковых новостей в период чрезвычайной ситуации в области здравоохранения на мировом уровне, что в свою очередь затрудняет принятие эффективных мер в сфере общественного здравоохранения и создает атмосферу паники и растерянности среди населения». Для противодействия обозначившейся проблеме объединенными усилиями ООН и ВОЗ была создана так называемая «Команда разрушителей мифов», объединившая представителей крупнейших интернет-провайдеров и социальных сетей, таких как Facebook, Google, Pinterest, Tencent, Twitter, TikTok, Youtube и др. Данные компании ведут активную работу по удалению фейковой информации (недостоверные медицинские сведения, рецепты, советы, диагностика, слухи, теории заговора и подобная информация, представляющая опасность для здоровья населения).

Между тем на сегодняшний момент в рамках ООН не принято универсальных соглашений, посвященных проблеме противодействия дезинформации и распространению фейковых новостей. В марте 2019 г. РФ выступила с инициативой обратиться от имени Комитета ГА ООН по информации в секретариат ООН с предложением «принятия мер, направленных на разработку механизма противодействия «фейковой информации» в мировом масштабе». Несмотря на поддержку секретариата ООН и ряда государств, инициатива не была включена в четкой формулировке в проект Резолюции ГА ООН, поскольку была заблокирована представителями США [9].

Заключение. Таким образом, проблема глобального распространения «фейковой информации» стремительными темпами приобретает трансграничный масштаб, а обеспечение эффективного противодействия данной угрозе требует объединения усилий государств и всего международного сообщества с целью разработки универсального комплексного механизма борьбы, основанного на принципах международного права, соблюдении и уважении прав человека и ценностях демократического общества. Представляется, что для решения данной проблемы недостаточно односторонних инициатив на уровне национальных законов государств. Комплексный подход предполагает объединение усилий по различным направлениям:

- необходимость междисциплинарного изучения феномена дезинформации и «фейковой информации», включая технологический, юридический, журналистский аспект с целью понимания сущности данного явления, нормативного закрепления унифицированного категориального аппарата в обозначенной сфере, в частности терминов «дезинформация», «фейковая информация», критериев определения составов деяний, которые могут подлежать криминализации, критериев отнесения той или иной информации к разряду «фейковой» и т.д.;
- необходимость привлечения всех заинтересованных сторон с учетом принципа «мультистейкхолдернизма» и саморегулирования глобального пространства Интернет, с привлечением представителей гражданского общества, бизнес-структур, частного сектора, представителей IT-индустрии, а также правительств государств (поскольку установление правил регулирования и правовых рамок в обозначенной сфере возможно только посредством публичного обсуждения и выработки единых подходов, а не путем установления императивных предписаний и жесткой регламентации информационного пространства, с нарушением общепринятых принципов международного права);
- необходимость межгосударственного взаимодействия с целью разработки и принятия международного механизма сотрудничества в сфере противодействия дезинформации, «фейковой информации», что позволит создать унифицированный комплексный механизм, включающий международные стандарты правового и технологического характера. Это в свою очередь будет способствовать преодолению фрагментарности односторонних мер, принимаемых на уровне отдельных государств и минимизации попыток превращения «медийных» технологий в орудие информационного противостояния. Безусловно, подобный механизм сотрудничества и противодействия обозначенной проблеме должен быть разработан и реализован в строгом соответствии с общепринятыми принципами и нормами международного права и стать своего рода сдерживающим фактором на пути стремления отдельных правительств к установлению цензуры и чрезмерного государственного контроля информационного пространства, ограничению прав человека и свободы СМИ под предлогом обеспечения информационной безопасности и защиты граждан от деструктивного воздействия дезинформации в сети.

Библиографический список

1. Бебич Д. Новые проблемы – старые решения? Критический взгляд на доклад экспертной группы высокого уровня европейской комиссии о фейковых новостях и онлайн дезинформации / Д. Бебич, М. Воларевич // Вестник Российского университета дружбы народов. Серия: Политология. – 2018. – № 3 (20). – С. 447–460.
2. Зырянова М. О. «Фейковые» новости как инструмент управления общественным мнением / М. О. Зырянова // Диагностика и прогнозирование социальных процессов : материалы Национальной научно-практической конференции. – 2019. – С. 21–25.
3. Зырянова М. О. Способы противодействия распространению фейковой информации / М. О. Зырянова // Общество: социология, психология, педагогика. – 2020. – № 6 (74). – С. 80–83.
4. Касенова М. Б. Проблемы правового регулирования трансграничного использования Интернета / М. Б. Касенова. – Москва : МГИМО-Университет, 2015. – С. 59–65.
5. Маркова Н. А. К вопросу об административной ответственности за распространение фейковых новостей / Н. А. Маркова // Ученые записки. – 2019. – № 2 (30). – С. 90–95.
6. Маркова Н. А. Некоторые аспекты регулирования юридической ответственности за распространение фейковой информации в интернете и средствах массовой информации: российский и зарубежный опыт / Н. А. Маркова, А. С. Курганова // Вестник Владимирского юридического института. – 2019. – № 3 (52). – С. 81–85.
7. Международный опыт борьбы с фейками. На кого равняется Россия. Об этом сообщает «Рамблер». – Режим доступа: https://news.rambler.ru/other/41616357/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).
8. Полищук Сергей Викторович. Правовые аспекты противодействия фейковым атакам / Сергей Викторович Полищук // Социально-гуманитарные знания. – 2019. – № 9. – Режим доступа: https://cyberleninka.ru/article/n/pravovye-aspekty-protivodeystviya-feykovym-atakam, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).
9. РФ призвала ООН разработать механизм борьбы с «фейковыми новостями». – Режим доступа: https://iz.ru/738621/2018-05-02/rf-prizvala-oon-razrabotat-mekhanizm-borby-s-feikovymi-novostiami, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).
10. Федеральный закон «О внесении изменений в статью 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» от 18.03.2019 № 31-ФЗ (последняя редакция).
11. Франция приняла закон против фейковых новостей. – Режим доступа: https://rg.ru/2018/11/21/francii-priniala-zakon-protiv-fejkovyh-novostej.html, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).
12. Янина Воронко. Fake news: как страны борются с недостоверными новостями / Янина Воронко. – Режим доступа: https://ilex.by/news/fake-news-kak-strany-boryutsya-s-nedostovernymi-novostyami/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).
13. Fake News как объект уголовно-правовой регуляции: опыт Малайзии // Anti-fake news Act. – 2018 (Act 803). – Режим доступа: https://news.rambler.ru/other/41616357/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.01.2021).

References

1. Bebich D., Volarevich M. Novye problemy – starye resheniya? Kriticheskiy vzglyad na doklad ekspertnoy gruppy vysokogo urovnya evropeyskoy komissii o feykovykh novostyakh i onlayn dezinformatsii [New problems – old solutions? A critical look at the European Commission's high-level expert panel report on fake news and online disinformation]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Politologiya.* [Bulletin of the Peoples' Friendship University of Russia. Series: Political Science], 2018, no. 3 (20), pp. 447–460.
2. Zyryanova M. O. "Feykovye" novosti kak instrument upravleniya obshchestvennym mneniem ["Fake" news as a tool for managing public opinion]. *Diagnostika i prognozirovanie sotsialnykh protsessov : materialy Natsionalnoy nauchno-prakticheskoy konferentsii* [Diagnostics and forecasting of social processes. Materials of the National Scientific and Practical Conference], 2019, pp. 21–25.
3. Zyryanova M. O. Sposoby protivodeystviya rasprostraneniyu feykovoy informatsii [Ways to counter the spread of fake information]. *Obshchestvo: sotsiologiya, psikhologiya, pedagogika* [Society: Sociology, Psychology, Pedagogy], 2020, no. 6 (74), pp. 80–83.
4. Kasenova M. B. *Problemy pravovogo regulirovaniya transgranichnogo ispolzovaniya Interneta* [Problems of legal regulation of cross-border use of the Internet]. Moscow, MGIMO-University, 2015, pp. 59–65.
5. Markova N.A. K voprosu ob administrativnoy otvetstvennosti za rasprostranenie feykovykh novostey [On the issue of administrative responsibility for the distribution of fake news]. *Uchenye zapiski* [Scholarly notes], 2019, no. 2 (30), pp. 90–95.
6. Markova N. A., Kurganova A. S. Nekotorye aspekty regulirovaniya yuridicheskoy otvetstvennosti za rasprostranenie feykovoy informatsii v internete i sredstvakh massovoy informatsii: rossiyskiy i zarubezhnyy opyt [Some aspects of regulating legal liability for the dissemination of fake information on the Internet and the media: Russian and foreign experience]. *Vestnik Vladimirskogo yuridicheskogo instituta* [Bulletin of the Vladimir Law Institute], 2019, no. 3 (52), pp. 81–85.

7. *Mezhdunarodnyy opyt borby s feykami. Na kogo ravnyaetsya Rossiya. Ob etom soobshchaet "Rambler"* [International experience in combating fakes. Who does Russia look up to? Reported by "Rambler"]. Available at: https://news.rambler.ru/other/41616357 (accessed 22.01.2021).

8. Polishchuk Sergej Viktorovich. Pravovye aspekty protivodeystviya feykovym atakam. Socialno-gumanitarnye znaniya [Legal aspects of countering fake attacks]. *Sotsialno-gumanitarnye znaniya* [Social and humanitarian knowledge], 2019, no. 9. Available at: https://cyberleninka.ru/article/n/pravovye-aspekty-protivodeystviya-feykovym-atakam (accessed 22.01.2021).

9. *RF prizvala OON razrabotat mekhanizm borby s «feykovymi novostyami»* [The Russian Federation called on the UN to develop a mechanism to combat "fake news"]. Available at: https://iz.ru/738621/2018-05-02/rf-prizvala-oon-razrabotat-mekhanizm-borby-s-feikovymi-novostiami (accessed 22.01.2021).

10. *Federalnyy zakon "O vnesenii izmeneniy v statyu 15.3 Federalnogo zakona "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" ot 18.03.2019 N 31-FZ (poslednyaya redaktsiya)* [Federal Law "On Amendments to Article 15.3 of the Federal Law" On Information, Information Technologies and Protection of Information" dated 18.03.2019 N 31-FZ (last edition)].

11. *Frantsiya prinyala zakon protiv feykovykh novostey* [France passed a law against fake news]. Available at: https://rg.ru/2018/11/21/franciia-priniala-zakon-protiv-fejkovyh-novostej.html (accessed 22.01.2021).

12. Yanina Voronko. *Fake news: kak strany boryutsya s nedostovernymi novostyami* [Fake news: how countries deal with fake news]. Available at: https://ilex.by/news/fake-news-kak-strany-boryutsya-s-nedostovernymi-novostyami/ (accessed 22.01.2021).

13. Fake News kak obekt ugolovno-pravovoy regulyatsii: opyt Malayzii [Fake News as an Object of Criminal Law Regulation: The Experience of Malaysia]. *Anti-fake news Act*, 2018 (Act 803). Available at: https://news.rambler.ru/other/41616357/ (accessed 22.01.2021).

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

УДК 004.93’1

СКАНИРУЮЩЕЕ УСТРОЙСТВО ДЛЯ ПОЛУЧЕНИЯ ОБЪЕМНЫХ МОДЕЛЕЙ МАЛОГАБАРИТНЫХ ОБЪЕКТОВ КУЛЬТУРНОГО НАСЛЕДИЯ

Статья поступила в редакцию 21.12.2020, в окончательном варианте – 15.02.2021.

Барсуков Никита Сергеевич, Московский государственный технический университет имени Н.Э. Баумана, 105007, Российская Федерация, г. Москва, ул. 2 Бауманская, 5.
бакалавр, ORCID: 0000-0003-3067-4340, e-mail: barsukov-nikita@inbox.ru
Лыков Артем Андреевич, Московский государственный технический университет имени Н.Э. Баумана, 105007, Российская Федерация, г. Москва, ул. 2 Бауманская, 5.
бакалавр, ORCID: 0000-0001-6119-2366, e-mail: tema.lykov@gmail.com
Воротников Сергей Анатольевич, Московский государственный технический университет имени Н.Э. Баумана, 105007, Российская Федерация, г. Москва, ул. 2 Бауманская, 5.
кандидат технических наук, доцент, ORCID: 0000-0001-6795-1132, e-mail: vorotn@bmstu.ru

Статья посвящена разработке сканирующего устройства для оперативного и точного определения формы малогабаритных объектов культурного наследия, например, обнаруженных при археологических раскопках. В состав устройства, использующего принцип структурированной подсветки, входят: сервер для обработки данных, микрокомпьютер Raspberry PI, два сервопривода, телевизионная камера и линейный лазер. На микроконтроллере формируются пакеты данных, которые отправляются на удаленный сервер по протоколу http. На сервере происходит обработка полученных пакетов данных в среде David-laserscanner и их дальнейшее совмещение в среде Meshlab. Результатом обработки является 3D-модель сканируемого объекта в формате obj. На основе аналитических расчетов определены оптимальные значения параметров сканирующего устройства, при которых достигается одновременно высокое быстродействие и допустимое качество полученной модели, с учетом его конструкции и выбранных компонентов. Разработан и изготовлен макет сканирующего устройства, позволяющего оперативно получать 3D-модели объектов габаритами до 100×100×140 мм, и приводятся результаты его экспериментального исследования.

Ключевые слова: 3D-сканер, структурированная подсветка, сервопривод, линейный лазер, объемная модель, археологические объекты, David-laserscanner

SCANNING DEVICE FOR OBTAINING VOLUMETRIC MODELS OF SMALL-SIZED OBJECTS OF CULTURAL HERITAGE

The article was received by the editorial board on 21.12.2020, in the final version – 15.02.2021.

Barsukov Nikita S., Bauman Moscow State Technical University, 5 2nd Baumanskaya St., Moscow, 105007, Russian Federation,
bachelor, ORCID: 0000-0003-3067-4340, e-mail: barsukov-nikita@inbox.ru
Lykov Artem A., Bauman Moscow State Technical University, 5 2nd Baumanskaya St., Moscow, 105007, Russian Federation,
bachelor, ORCID: 0000-0001-6119-2366, e-mail: tema.lykov@gmail.com
Vorotnikov Sergey A., Bauman Moscow State Technical University, 5 2nd Baumanskaya St., Moscow, 105007, Russian Federation,
Cand. Sci. (Engineering), ORCID: 0000-0001-6795-1132, e-mail: vorotn@bmstu.ru

The article is devoted to the development of a scanning device for prompt and accurate determination of the shape of small-sized objects of cultural heritage, for example, found during archaeological excavations. The structured lighting device includes: a data processing server, a Raspberry PI microcomputer, two servos, a television camera and a line laser. Data packets are formed on the microcontroller, which are sent to a remote server via the http protocol. The server processes the received data packets in the David-laserscanner environment and their further combination in the Meshlab environment. The result of processing is a 3D model of the scanned object in obj format.

On the basis of analytical calculations, the optimal values of the parameters of the scanning device have been determined, at which both high speed and acceptable quality of the resulting model are achieved, taking into account its design and selected components. A mock-up of a scanning device has been developed and manufactured, which makes it possible to quickly obtain 3D-models of objects with dimensions up to 100×100×140 mm, and the results of its experimental study are presented.

Keywords: 3D-scanner, structured lighting, servo drive, line laser, volumetric model, archaeological objects, David-laserscanner

Graphical annotation (Графическая аннотация)

Введение. С использованием технологии лазерного сканирования в работе археологов появились новые возможности, которые позволяют сделать исследования более точными, детализированными и оперативными [1]. Подобное оборудование сегодня используется при решении целого ряда задач, связанных с каталогизацией археологических материалов, среди которых встречаются и объекты культурного наследия, их визуализацией при создании виртуальных экспозиций [2].

Объекты культурного наследия – это предметы, возникшие в ходе исторических событий, представляющие собой ценность с точки зрения науки и искусства и являющиеся свидетельством эпох и цивилизаций, подлинными источниками информации о развитии культуры. Очевидно, что при нахождении нового такого объекта, множество специалистов разных областей стремятся получить к нему доступ с целью досконального изучения. Однако непосредственный доступ к найденному объекту может быть невозможным по разным причинам. Например, если объект находится в другой точке земного шара или в непригодных для проведения исследований условиях. Также в контексте археологии иногда важно как можно меньше физически взаимодействовать с найденным объектом, чтобы не подвергать его опасности разрушения. В этих случаях помочь может трехмерное сканирование находки непосредственно на месте. При этом с полученной моделью могут проводить исследования сразу несколько специалистов одновременно [3].

В настоящее время существует ряд объемных сканеров для археологии [3]. Наряду с достоинствами (высокой детализацией и качеством текстур) они имеют общие недостатки, связанные с немалыми габаритами и значительным временем сканирования. Если проводится масштабное исследование, то использование таких сканирующих устройств оправдано [3]. В таких исследованиях специалисты могут позволить разместить габаритную технику и проводить сканирование в течение несколько дней.

Однако нередко перед исследователями встает задача произвести оперативное сканирование большого количества малых по размеру объектов за ограниченное время [4, 5]. Примерами являются различные статуэтки, предметы культа, фрагменты посуды и пр. При этом важным оказывается не столько качество сканирования, сколько скорость. В такой ситуации описанное выше оборудование оказывается неэффективным, а все его преимущества оказываются не принципиальными. Такая ситуация может возникнуть если объект очень востребован, и специалисты не могут в настоящий момент позволить потратить на сканирование много часов. Объект может быстро разрушаться, что также делает проведение над ним долгой процедуры сканирования невозможным [6]. Кроме того, может возникнуть необходимость произвести сканирование в экспедиции, где не только нет возможности взять с собой габаритное оборудование, но и долгие остановки могут быть невозможны.

Для всех описанных выше задач требуется портативное устройство, позволяющее получать объемные модели малогабаритных объектов культурного наследия с большой скоростью и приемлемым качеством.

Структура системы управления. В соответствии с поставленной задачей предлагается двухуровневая структура системы управления сканирующим устройством (рис. 1).

Задачей исполнительного уровня является сбор данных с телекамеры и управление световым модулем, состоящим из линейного лазера, светодиода, освещающего область сканирования, и модулем позиционирования, состоящим из двух приводов, построенных на базе шаговых двигателей и соответствующих драйверов. За прием данных и управление модулями на исполнительном уровне отвечает микрокомпьютер.

На верхнем уровне решаются задачи приема данных на локальном сервере, их передачи через программу IPCamAdapter в программу David-laserscanner, в которой происходит обработка данных и вывода полученных данных в графический интерфейс среды Meshlab. Там же происходит передача управляющих команд на микрокомпьютер. Вся информация передается через шину локальной сети Wi-Fi. Всем процессом сканирования управляет оператор, который получает готовое изображение – 3D-модель объекта из среды Meshlab.

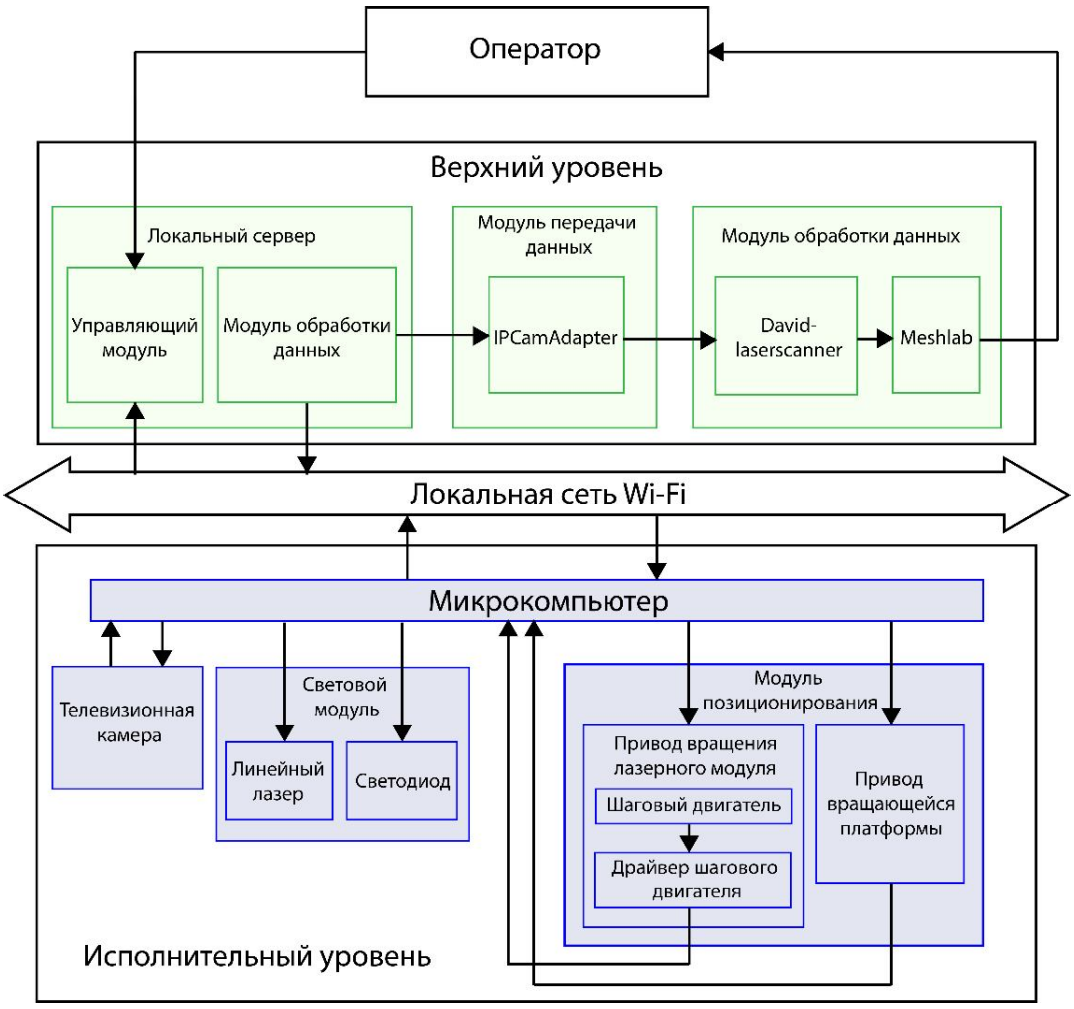


Рисунок 1 – Структура системы управления сканирующим устройством

Такое построение системы управления, в отличие от известных решений, позволит не только оперативно проводить сканирование объектов дистанционно, но и снизить требования к квалификации оператора на этапе получения исходных сканов.

Разработка конструкции устройства. На первом этапе разработки были подобраны управляющие компоненты. Для проведения всех процессов, связанных с обработкой информации, был выбран ПК с ОС Windows, для управления всеми подвижными частями – микрокомпьютер

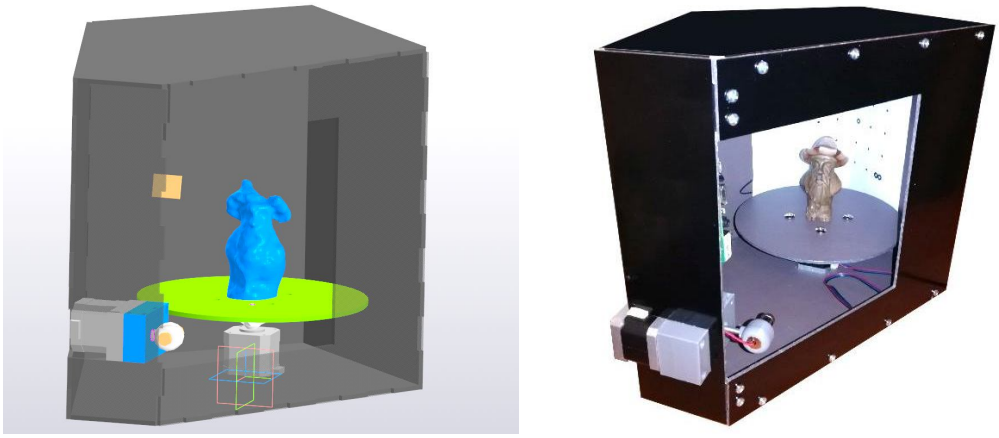
Raspberry PI 3 с операционной системой Raspberry PI OS. Разработка программ исполнительного уровня проводилась на языке Python.

Узел структурированной подсветки реализован на исполнительном уровне управления и состоит из трех элементов: светового модуля, телекамеры и модуля позиционирования.

В качестве устройства, формирующего структурированный световой поток, использовался линейный лазер RYS1230 с линзой, преломляющей свет в форме прямой горизонтальной линии. Прием отраженного от объекта светового сигнала проводился с помощью телевизионной камеры. Модуль телекамеры выбирался из условий максимальной совместимости с микрокомпьютером. Для Raspberry Pi – это 5-мегапиксельная телевизионная камера Raspberry Pi Camera Module Rev 1.3.

Для получения полноценного трехмерного изображения исследуемого объекта он должен быть сканирован со всех сторон. Эту задачу решал модуль позиционирования, предназначенный для согласованного управления линейным лазером и поворотной платформой. Управление осуществлялось с помощью двух однотипных приводов на основе шаговых двигателей NEMA 17 17HS4401 и драйверов A4988.

В соответствии с выбранными комплектующими была создана графическая модель сканирующего устройства (рис. 2*а*) и изготовлен его макетный образец (рис. 2*б*):



а *б*

Рисунок 2 – Графическая модель (а) и макет (б) сканирующего устройства

При изготовлении макета сканирующего устройства использовались алюминиевые композитные панели (АКП) толщиной 3 мм, обработка которых проводилась на фрезерном станке с числовым программным управлением. Конструктивные элементы сложной формы изготавливались из ABS-пластика на 3D-принтере.

Для получения большей контрастности изображения объекта корпус сканирующего устройства выполнялся закрытым [4].

Программное обеспечение. Важной частью сканера является его программное обеспечение, которое выполняет оцифровку, предварительную обработку изображения и склеивание его в трехмерный образ. На основе анализа известных программных решений, используемых при структурированной подсветке [7, 8], был выбран пакет David-laserscanner [9], обладающий широким функционалом и не предъявляющий к сканируемому объекту особых требований по форме.

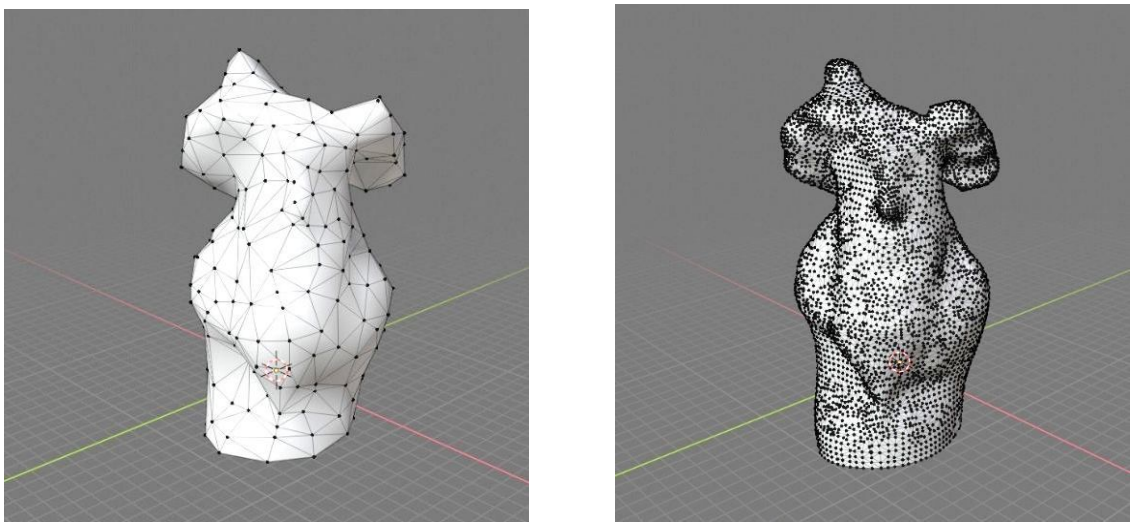
Преимуществами David-laserscanner являются [9]:

- импортирование полученных сканов в формате obj;
- возможность использования одного линейного лазера;
- возможность оперативного просмотра и редактирования полученной 3D-модели в интегрированном в программу модуле OpenGL-Viewer.

В пакет David-laserscanner поступал видеопоток с телекамеры в режиме реального времени через программу IPCamAdapter. Результатом обработки видеопотока являлись трехмерные сканы, экспортируемые в формате obj. Для объединения отдельных сканов в единую модель их было необходимо импортировать в среду Meshlab [10, 11]. С помощью встроенных алгоритмов реконструкции поверхностей и фильтров постобработки в Meshlab получается различимая 3D-модель достаточно высокого качества.

Для управления приводами двигателей были написаны управляющие скрипты на языке Python 3.7 с использованием библиотеки для работы с шаговым двигателем RpiMotorLib [12].

Качество полученных сканирующим устройством моделей тесно связано с количеством полигонов, из которых она состоит. Полигоны или ячейки полигональной сетки – это элементарные плоскости, образуемые некоторым количеством соединенных ребрами точек в пространстве модели. В разрабатываемом решении используется метод триангуляции, поэтому все полигоны имеют 3 вершины. Ниже представлены примеры моделей одного и того же тестового объекта (фигурки гнома размером 100×45×55мм), содержащие в себе 500 (рис. 3*а*) и 14000 (рис. 3*б*) полигонов.



а *б*

Рисунок 3 – Модель, составленная из 500 (а) и из 14000 полигонов (б)

Максимальное количество полигонов, которые можно получить на модели зависит от разрешающей способности телевизионной камеры, используемой при сканировании. Будем считать, что, для того чтобы вписать три вершины полигона, необходимо минимальное пиксельное пространство, размером 4×6 пикселей (рис. 3*б*). Зависимости между размерами рабочей области телевизионной камеры и габаритами сканируемого объекта имеют вид (1):

$$h_{\text{пкс}} = \frac{d \cdot h}{q}; \qquad b_{\text{пкс}} = \frac{c \cdot b}{g}, \tag{1}$$

где $h_{\text{пкс}}$, $b_{\text{пкс}}$ – высота и ширина изображения объекта в пикселях; d и c – разрешение телевизионной камеры (количество пикселей) по вертикали и горизонтали, соответственно; h и b – высота и ширина сканируемого объекта в мм; q и g – коэффициенты преобразования оптической системы телекамеры по вертикали и горизонтали, соответственно. Значения этих коэффициентов определялись эмпирическим путем при калибровке телекамеры (q = 267, g = 149).

В общем случае максимальное количество полигонов p, которые можно получить при использовании произвольной телевизионной камеры известного разрешения, определяется зависимостью (2):

$$p = \frac{n}{k \cdot \varphi} \cdot 100, \tag{2}$$

где $n = h_{\text{пкс}} \cdot b_{\text{пкс}}$ и k – количество пикселей телевизионной камеры, в которое вписывается объект и наибольший полигон, соответственно; φ – процент поверхности модели, попадающей в телевизионную камеру.

Указанные выражения позволяют определить зависимость возможного количества полигонов (т.е. визуального качества полученного 3D-изображения) от разрешения телевизионной камеры и габаритов сканируемого объекта (3):

$$p = \frac{d \cdot h \cdot c \cdot b}{k \cdot \varphi \cdot q \cdot g} \cdot 100. \tag{3}$$

В графическом представлении указанная зависимость имеет вид (рис. 4).

Рисунок 4 – Диаграмма зависимости максимально возможного количества полигонов модели от разрешения телекамеры

Так, для используемой телекамеры Raspberry Pi Camera Module Rev 1.3 с разрешением 1280×720 и φ = 45 % получим p = 14000. Такое количество полигонов обеспечивает качественную детализацию всех частей сканируемого объекта и дает наилучшее представление о его форме по сравнению с моделями этого объекта, содержащими меньшее количество полигонов.

Экспериментальные исследования. Целью экспериментов являлось определение зависимости визуального качества полученной модели от параметров вращения двигателей сканирующего устройства. Для оценки качества модели производился подсчет количества полигонов после сканирования при каждой из комбинаций параметров. Для оценки быстродействия сканирующего устройства для каждой комбинации параметров фиксировалось время, затраченное на полное сканирование.

ПО сканирующего устройства позволяет изменять два параметра:

- микрошаг m шагового двигателя линейного лазера, который влияет на количество линий, спроецированных на объект. Формула микрошага: $m = 200 \cdot 2^r$, где r – регулируемый параметр драйвера шагового двигателя от 0 до 4;
- шаг двигателя, поворачивающего платформу между этапами сканированиями объекта; от него зависит количество сканов, совмещение которых образует полную 3D-модель объекта.

В ходе экспериментального исследования было произведено сканирование телекамерой Raspberry Pi Camera Module Rev 1.3 тестового объекта с пятью разными микрошагами шагового двигателя линейного лазера (400, 800, 1600, 3200 и 6400) и с 4 различными шагами сканирования, при которых 3D-модель получалась совмещением 2, 3, 4 и 5 сканов, соответственно. В качестве сканируемого объекта была взята керамическая модель игрушки с габаритными размерами 100×55×45. Результаты экспериментального исследования представлены в виде графика (рис. 5).

Как следует из рисунка 5, при приближении количества полигонов модели к 14000 путем увеличения количества сторон сканирования и микрошага шагового двигателя, скорость роста количества полигонов уменьшается, что соответствует теоретически полученным данным. Максимальное количество полигонов, которое может быть получено при использовании телевизионной камеры Raspberry Pi Camera Module Rev 1.3, согласно теоретическим данным, равно 14000.

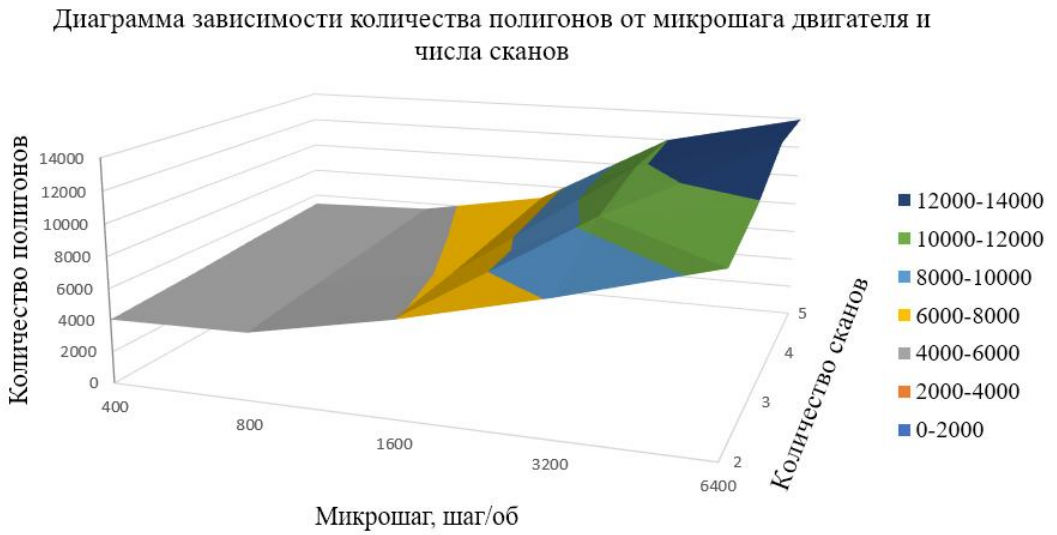


Рисунок 5 – Диаграмма зависимости количества полигонов от микрошага двигателя и числа сканов

Измерение времени полного сканирования позволило определить быстродействие сканирующего устройства при каждой из используемых комбинаций параметров. При этом учитывалось время, затраченное на сканирование и поворот платформы. Время на совмещение сканов в программе MashLab не учитывалось, так как оно зависит от мощности ПК. Результат измерений представлен в виде графика (рис. 6).

Рисунок 6 – Диаграмма зависимости времени полного сканирования от микрошага и числа сканов

На основании полученных результатов можно сделать заключение, что с увеличением микрошага и количества сканов, время полного сканирования растет равномерно, а скорость увеличения количества полигонов постепенно уменьшается. Таким образом можно определить оптимальные значения параметров сканирующего устройства с учетом его конструкции и выбранных компонентов. Это значения параметров, при которых достигается одновременно высокое быстродействие и допустимое качество полученной модели. Исходя из графиков на рисунках 5 и 6, оптимальные значения – это микрошаг 3200 и количество сканов 4. Дальнейшее увеличение параметров приводит к незначительному увеличению количества полигонов при значительном увеличении времени сканирования. Если эти значения по какой-либо причине не устраивают оператора, он может самостоятельно выбрать режим работы сканирующего устройства, используя график зависимости количества полигонов от времени сканирования (рис. 7).

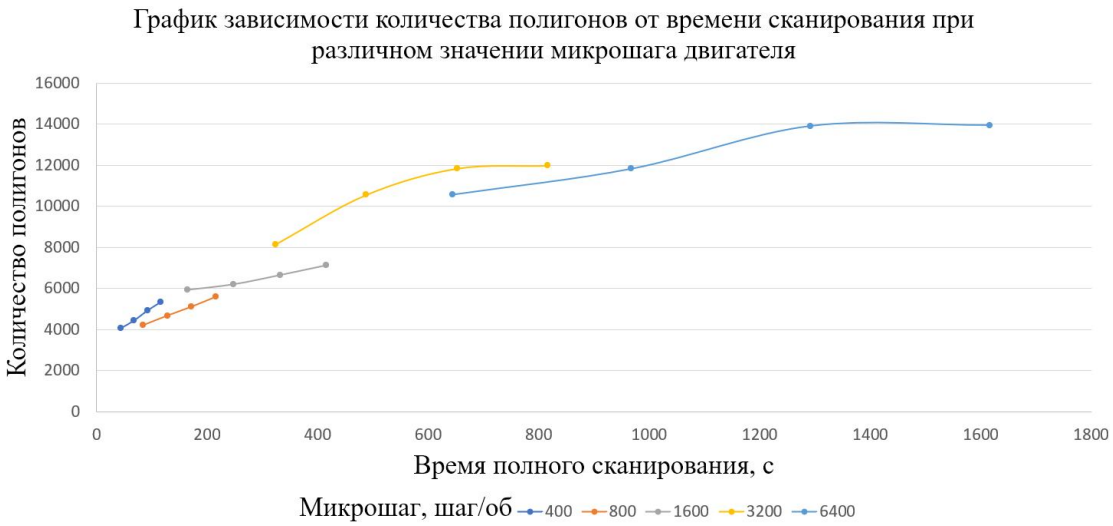


Рисунок 7 – График зависимости количества полигонов от времени сканирования при различном значении микрошага двигателя

При использовании других тестовых объектов и той же телекамеры вид графиков на рисунках 6 и 7 не изменится, хотя количество полигонов в полученной 3D-модели может быть иным.

Заключение. Предложенный подход к проектированию сканирующих устройств позволит разрабатывать малогабаритные 3D-сканеры для задач оперативного получения трехмерных моделей различных объектов. На основании аналитических расчетов и экспериментальных исследований изготовленного макета определены значения рабочих параметров устройства, при которых достигается высокое быстродействие и качество трехмерной модели сканируемого объекта. Разработанное устройство при существенно меньших габаритах обладает более высоким быстродействием по сравнению с существующими аналогами, что делает перспективным его использование в задачах оперативного получения 3D-моделей объектов, особенно в полевых условиях, например, непосредственно в местах проведения археологических раскопок.

Библиографический список

1. Чистяков П. В. 3D моделирование археологических артефактов при помощи сканеров структурированного подсвета / П. В. Чистяков, В. С. Ковалев, К. А. Колобова, А. В. Шалагина, А. И. Кривошапкин // Теория и практика археологических исследований. – 2019. – № 3 (27). – С. 102–112.

2. Wrona M. 3D reconstruction with handheld structured light scanner / M. Wrona, W. Piotrowska // 16th International Multidisciplinary Scientific GeoConference SGEM 2016. Conference Proceedings. – 2016. – P. 553–560.

3. Khalil W. New trends in archaeology and museology / W. Khalil // The New Past. – 2020. – № 2. – P. 246–253.

4. Bakirman T. Comparison of low-cost 3D structured light scanner for face modeling / T. Bakirman, M. U. Gumusay, M. O. Selbesoglu, B. Bayram, H. C. Reis, S. Yosmaoglu, M. C. Yaras, D. Z. Seker // Applied Optics. – 2017. – Vol. 56, № 4. – P. 985–992.

5. Коротковс В. И. Управление мобильным манипуляционным роботом в задаче адаптивной обработки зеленых насаждений / В. И. Коротковс, С. А. Воротников, Н. А. Выборнов // Прикаспийский журнал: управление и высокие технологии. – 2016. – № 2 (34). – С. 48–58.

6. Уваров К. А. Анализ методов 3D-сканирования и разработка 3D-сканера / К. А. Уваров, А. П. Борисов // Современный взгляд на будущее науки : сборник статей Международной научно-практической конференции : в 3 частях. – 2016. – С. 76–79.

7. Грязнов Н. А. Структурированная лазерная подсветка для технологий трехмерного зрения робототехнических средств / Н. А. Грязнов, В. В. Кириченко, Е. В. Егоров // Оптический журнал. – 2007. – Т. 74, № 8. – С. 37–43.

8. Попов С. Б. Использование структурированной подсветки в системах технического зрения / С. Б. Попов // Компьютерная оптика. – 2013. – Т. 37, № 2. – С. 233–238.

9. DAVID Vision Systems GmbH. DAVID Laserscanner. Starter Kit. Руководство по эксплуатации. – 2014.

10. Ranzuglia G. MeshLab as a complete tool for the integration of photos and color with high resolution 3D geometry data / G. Ranzuglia, M. Callieri, M. Dellepiane, P. Cignoni, R. Scopigno // CAA 2012 Conference Proceedings. – 2013. – P. 406–416.

11. Cignoni P. MeshLab: An Open-Source Mesh Processing Tool / P. Cignoni, M. Callieri, M. Corsini, M. Dellepiane, F. Ganovelli, G. Ranzuglia // Sixth Eurographics Italian Chapter Conference. – 2008. – P. 129–136.

12. Lyons G. RpiMotorLib / G. Lyons // GitHub, 2018. – Режим доступа: https://github.com /gavinlyonsrepo/RpiMotorLib/, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 05.02.2021).

References

1. Chistyakov P. V., Kovalev V. S., Kolobova K. A., Shalagina A. V., Krivoshapkin A. I. 3D modelirovaniye arkheologicheskikh artefaktov pri pomoshchi skanerov strukturi-rovannogo podsveta [3D modeling of archaeological artifacts using structured illumination scanners]. *Teoriya i praktika arkheologicheskikh issledovaniy* [Theory and practice of archaeological research], 2019, no. 3 (27), pp. 102–112.

2. Wrona M., Piotrowska W. 3D reconstruction with handheld structured light scanner. *16th International Multidisciplinary Scientific GeoConference SGEM 2016. Conference Proceedings*, 2016, pp. 553–560.

3. Khalil W. New trends in archaeology and museology. *The New Past*, 2020, no. 2, pp. 246–253.

4. Bakirman T., Gumusay M. U., Selbesoglu M. O., Bayram B., Reis H. C., Yosmaoglu S., Yaras M. C., Seker D. Z. Comparison of low-cost 3D structured light scanner for face modeling. *Applied Optics*, 2017, vol. 56, no. 4, pp. 985–992.

5. Korotkovs V. I., Vorotnikov S. A., Vybornov N. A. Upravleniye mobil'nym manipulyatsionnym robotom v zadache adaptivnoy obrabotki zelenykh nasazhdeniy [Adaptive processing of green planting with a mobile manipulator robot]. *Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii* [Caspian Journal: Control and High Technologies], 2016, no. 2 (34), pp. 48–58.

6. Uvarov K. A., Borisov A. P. Analiz metodov 3D-skanirovaniya i razrabotka 3D-skanera [Analysis of 3D scanning methods and development of a 3D scanner]. *Sovremennyy vzglyad na budushcheye nauki : sbornik statey Mezhdunarodnoy nauchno-prakticheskoy konferentsii* [A modern view of the future of science : Proceedings of the International Scientific and Practical Conference], in 3 parts, 2016, pp. 76–79.

7. Gryaznov N. A., Kirichenko V. V., Yegorov Ye. V. Strukturirovannaya lazernaya podsvetka dlya tekhnologiy trekhmernogo zreniya robototekhnicheskikh sredstv [Structured laser illumination for technologies of three-dimensional viewing of robotic facilities]. *Opticheskiy zhurnal* [Journal of Optical Technology], 2007, vol. 74, no. 8, pp. 37–43.

8. Popov S. B. Ispolzovaniye strukturirovannoy podsvetki v sistemakh tekhnicheskogo zreniya [The use of structured lighting in computer vision systems]. *Kompyuternaya optika* [Computer Optics Journal], 2013, vol. 37, no. 2, pp. 233–238.

9. *DAVID Vision Systems GmbH. DAVID Laserscanner. Starter Kit. Rukovodstvo po ekspluatatsii* [DAVID Vision Systems GmbH. DAVID Laserscanner. Starter Kit. User Manual], 2014.

10. Ranzuglia G., Callieri M., Dellepiane M., Cignoni P., Scopigno R. MeshLab as a complete tool for the integration of photos and color with high resolution 3D geometry data. *CAA 2012 Conference Proceedings*, 2013, pp. 406–416.

11. Cignoni P., Callieri M., Corsini M., Dellepiane M., Ganovelli F., Ranzuglia G. MeshLab: An Open-Source Mesh Processing Tool. *Sixth Eurographics Italian Chapter Conference*, 2008, pp. 129–136.

12. Lyons G. RpiMotorLib. *GitHub*, 2018. Available at: https://github.com/gavinlyonsrepo/RpiMotorLib/ (accessed 05.02.2021).

УДК 004.896:007.52

КОНЦЕПЦИЯ РОБОТИЗИРОВАННОГО ТЕПЛИЧНОГО КОМПЛЕКСА ДЛЯ ВЫРАЩИВАНИЯ ТОМАТОВ С ОДНИМ ОПЕРАТОРОМ

Статья поступила в редакцию 15.02.2021, в окончательном варианте – 23.02.2021.

Рыбаков Алексей Владимирович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат физико-математических наук, директор физико-математического института АГУ, e-mail: rybakov_alex@mail.ru http://orcid.org/0000-0003-1192-0913
Степанович Екатерина Юрьевна, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
кандидат физико-математических наук, доцент, доцент кафедры общей физики, e-mail: stepekyr1@mail.ru
Михайлов Иван Викторович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
студентка, e-mail: 051098anastasiya@gmail.com
Дусалиев Амит Бекторганович, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
студент, e-mail: amit19@mail.com
Астахов Федор Алексеевич, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
студент, e-mail: gsx-r600_k2@mail.ru

Авторами разработана концепция ресурсосберегающего роботизированного тепличного комплекса по выращиванию томатов под управлением одного оператора. Отдельное внимание в данной концепции уделяется вопросам использования мобильных транспортных роботов и мобильных роботов с манипуляторами для операций расстановки кассет с рассадой, формирования куста и сбора плодов. В качестве источников энергии для теплицы предлагается использовать альтернативные источники в совокупности с газовыми электрогенераторами и станциями для получения биогаза. Рассмотрены и экономические аспекты полной автоматизации тепличного комплекса.

Ключевые слова: роботизированный манипулятор, компьютерное зрение, агромехатроника, распознавание изображений, сельскохозяйственные роботы, автоматизированный сбор урожая, управление роботами

THE CONCEPT OF A ROBOTIC GREENHOUSE COMPLEX FOR GROWING TOMATOES WITH ONE OPERATOR

The article was received by the editorial board on 15.02.2021, in the final version – 23.02.2021.

Rybakov Aleksey V., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Physics and Mathematics), Director of the ASU Physical and Mathematical Institute, e-mail: rybakov_alex@mail.ru http://orcid.org/0000-0003-1192-0913
Stepanovich Ekaterina Yu., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Cand. Sci. (Physics and Mathematics), Associate Professor, Associate Professor of the Department of General Physics, e-mail: stepekyr1@mail.ru
Mikhailov Ivan V., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: 051098anastasiya@gmail.com
Dusaliev Amit B., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: amit19@mail.com
Astakhov Fedor A., Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
student, e-mail: gsx-r600_k2@mail.ru

The authors developed the concept of a resource-saving robotic greenhouse complex for growing tomatoes under the control of a single operator. Special attention in this concept is paid to the use of mobile transport robots and mobile robots with manipulators for the operations of placing cassettes with seedlings, forming a bush and collecting fruits. As energy sources for the greenhouse, it is proposed to use alternative sources in conjunction with gas-fired

electric generators and stations for the production of biogas. The economic aspects of full automation of the greenhouse complex are also considered.

Keywords: robotic manipulator, computer vision, agromechatronics, image recognition, agricultural robots, automated harvesting, robot control

Graphical annotation (Графическая аннотация)

Введение. В последнее время в связи с распространением эпидемии COVID-19 остро встал вопрос нехватки рабочей силы для выполнения сельскохозяйственных операций. Работодатели заявляют о нехватке кадров в сферах, где обычно трудились мигранты. Причиной обычно называют закрытие границ из-за пандемии. Сегодня на территории России находится на 0,6–1,4 млн (или на 10–20 %) иностранных рабочих меньше, чем было бы в обычное время [1]. Такая ситуация происходит на фоне ограничений на использование труда мигрантов и низкой мотивации трудоспособного населения нашей страны к выполнению тяжелой низкооплачиваемой работы [2]. Наблюдается ряд проблем, связанных с большой текучестью кадров и необходимостью поиска и обучения новых. Связанные с обучением прямо на рабочем месте проблемы приводят к значительным затратам со стороны сельхозпроизводителей и отрицательно влияют на качество продукции [3].

В то же время в тепличных хозяйствах остро стоит вопрос профилактики болезней растений, в том числе ограничение попадания бактерий и спор, переносимых человеком. Необходимо безоговорочное соблюдение фитосанитарных норм в процессе вегетации, снижающее количество вторичной инфекции, передающейся на рабочем инструменте, тележках, руках, одежде [4]. Более того, активно рассматриваются вопросы организации тепличных хозяйств в суровых условиях Крайнего Севера [5]. Все эти причины в совокупности со значительным снижением в последние годы стоимости электронных компонентов, распространенностью бесплатного программного обеспечения и средств разработки, увеличением вычислительных мощностей и созданием легких аккумуляторов большой емкости позволяют рассматривать альтернативой рунному труду использование сельскохозяйственных роботов.

Структурная схема роботизированной теплицы. В данной работе предлагается концепция роботизированного тепличного комплекса, структурная схема которого показана на рисунке 1.

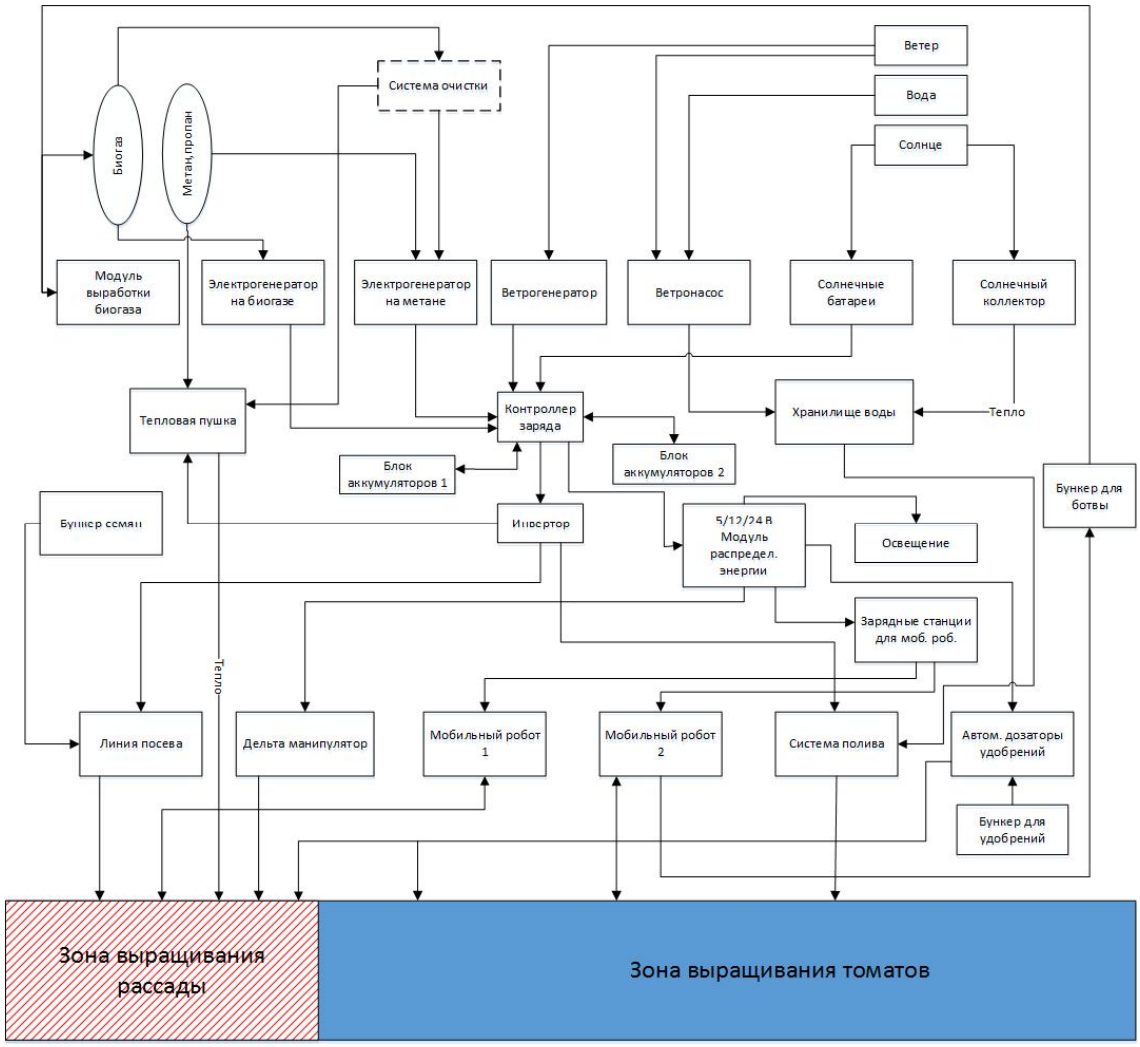


Рисунок 1 – Структурная схема роботизированной теплицы

Данная концепция предполагает разделение тепличного комплекса на зону выращивания рассады и зону выращивания плодов, в рассматриваемом случае – томатов. В зоне выращивания рассады может быть установлена автоматизированная линия посева, дополненная дельта-манипулятором и обслуживаемая мобильным роботом с манипулятором для выполнения операций с рассадой. В зоне выращивания томатов установлена автоматизированная система полива и автоматические дозаторы удобрений. Уборка томатов и ботвы осуществляется мобильными роботами с манипуляторами и транспортными роботами. Теплица обеспечивается электрической энергией и теплом за счет комбинации альтернативных и экологичных традиционных источников: ветрогенератора, солнечных батарей, электрогенераторов на биогазе и метане. Вода перекачивается не только за счет электрических насосов, но и благодаря применению ветронасосов. Подогрев воды и обеспечение микроклимата в теплице возможно осуществить при помощи солнечного коллектора и тепловой пушки, работающей на метане. Оставшаяся после сбора урожая ботва вместе с испорченными плодами собирается в бункер и расходуется на выработку биогаза. Электрическая энергия, поступающая от всех источников, распределяется контроллером на зарядку аккумуляторных батарей, от которых питаются потребители постоянного тока низкого напряжения, например станции подзарядки роботов, и потребители переменного тока через инвертор.

Основными операциями при выращивании томатов являются [6]:

1. Посев семян томатов на рассаду.
2. Уход за рассадой томатов.
2.1. Полив рассады помидоров.
2.2. Подкормка рассады помидоров.
2.3. Пикировка рассады помидоров.

3. Высаживание рассады в грунт.
4. Полив томатов в теплице.
5. Подкормка томатов.
6. Формирование томатов: пасынкование, прищипывание стебля и удаление листьев.
7. Обработка томатов.
8. Обрывание листьев.

Семена томата высевают как свежие, так и с длительностью хранения до 7 лет. Конкретные сроки посева зависят от принятой технологии подготовки рассады. Высев возможен в ящики, кассеты или горшочки с торфосмесью, заправленной удобрениями и нормализованной по кислотности. Сеют семена во влажный теплый субстрат на глубину 1–2 см, кассеты или ящики закрывают пленкой и ставят в темное место с температурой 22–25 °С. Посев проводят сухими семенами или их предварительно проращивают при температуре 22–24 °С до появления корешка [6].

Применение автоматизированных линий и стационарных роботов. Для операции автоматического посева хорошо зарекомендовали себя автоматизированные линии для посадки семян. Например, линии фирмы Urbinati (Италия). Именно их предлагается использовать в данной концепции (рис. 2).

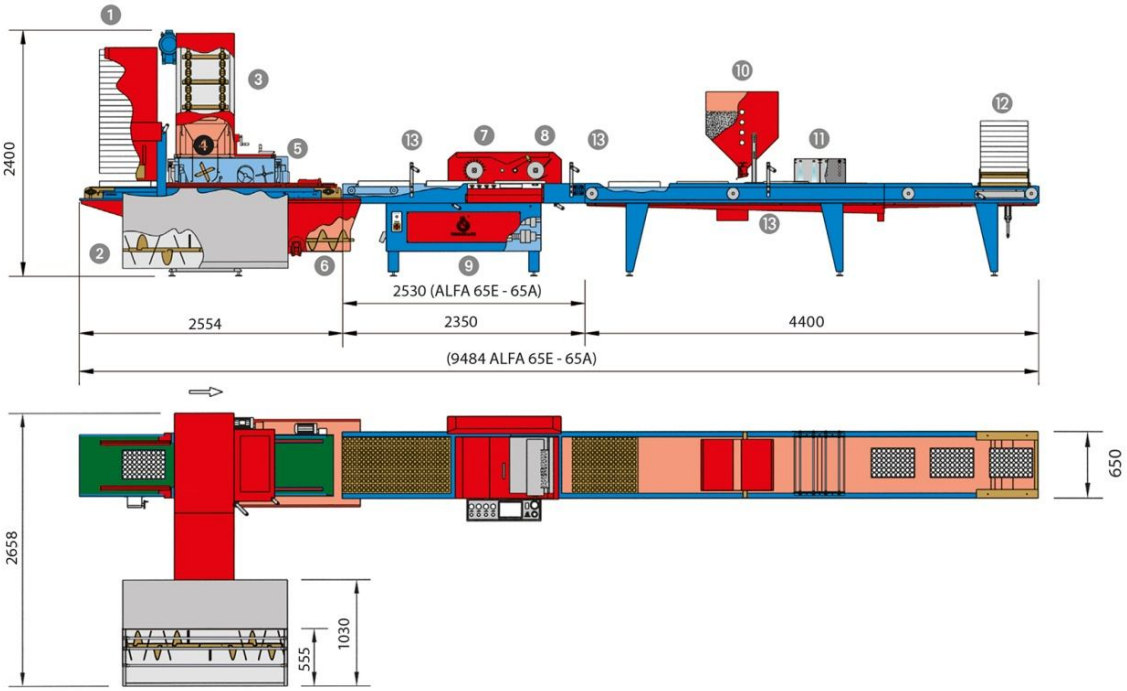


Рисунок 2 – Пример автоматизированной посадочной линии Urbinati (Италия) [7]

Автоматизированная посадочная линия состоит из следующих частей:

1. Пневматическая машина для выборки тары с двухтактным движением для поддонов из пенополистирола.
2. Ёмкость для почвы 1200 л с мешалкой.
3. Ковшевой погрузчик с двойной цепью.
4. Аппарат для заполнения поддонов с четырехлопастным линейным ротором.
5. Щетка для очистки поддонов с двойным шнеком.
6. Система рециркуляции избытков грунта.
7. Ведомый лункокопатель со щеткой для очистки.
8. Управляемый барабан диаметром 169 мм со вставками, чтобы сделать отверстия с минимальным диаметром 0,15 мм. Воздушные штанги с двойными рядами сопел и колеблющейся пластиной для посева. Молотки с регулируемой скоростью для улучшения размещения семян в центре отверстия.
9. Электрическая панель и сенсорный экран.
10. Крышка барабана для вермикулита с корректировкой скорости и дозировки емкостью 230 л.
11. Поливное устройство с 4 оросительными стержнями.
12. Автоматический балансовый штабелеукладчик.

13. Самоцентрующая система для корректировки ширины поддонов с рукоятями.
14. Рама.

Посадочный барабан автоматизированной системы высадки семян является основной ее частью и представляет собой достаточно сложную конструкцию. Однако он хорошо справляется с высокоинтенсивной посадкой семян различной формы и размеров. Семена прикрепляются на барабан с использованием специальных сопел и отверстий, присасывающих их за счет откачивания воздуха (рис. 3).

Рисунок 3 – Способ прикрепления семян на барабан [7]

Для прикрепления семян сложной формы сопла выдвигаются из отверстий (рис. 4).

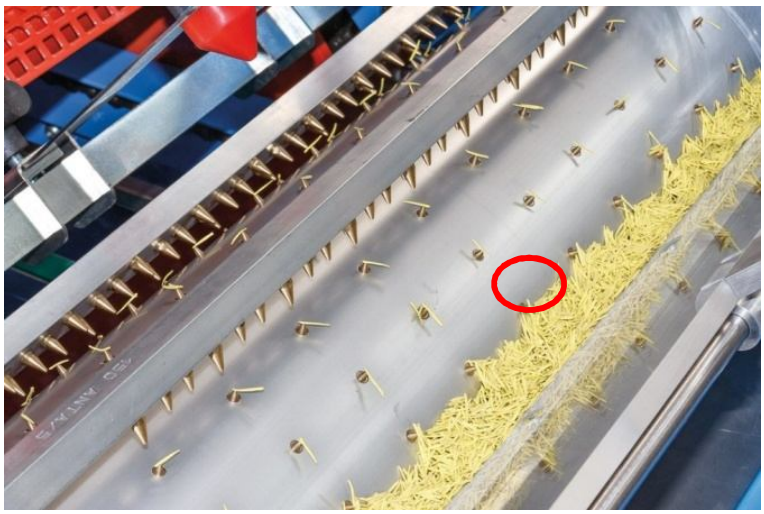


Рисунок 4 – Способ прикрепления семян сложной формы на барабан [7]

Однако при посадке с использованием таких барабанов может возникнуть ситуация пропуска ячейки в кассете при посеве, особенно легких и сравнительно небольших семян томатов или попадание нескольких семян в одну ячейку (рис. 5).

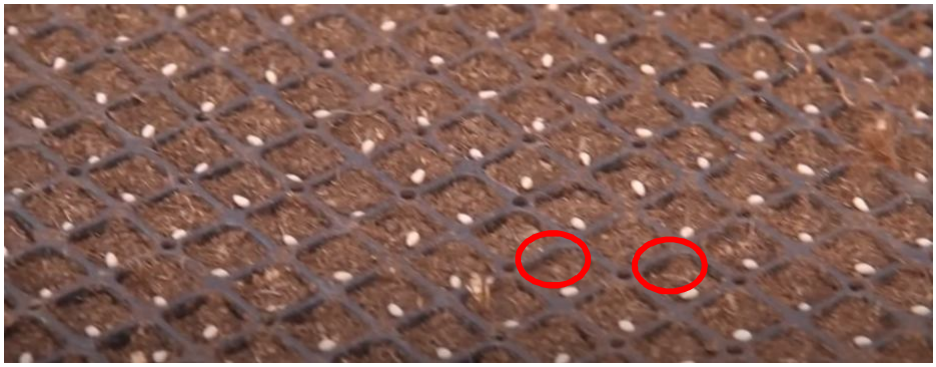


Рисунок 5 – Пропущенные ячейки в кассете [8]

Устранить такую погрешность позволит установка дополнительной секции с высокоскоростным дельта-манипулятором с пневматическим захватным устройством и системой компьютерного зрения для определения пустых или излишне заполненных ячеек. Пример такого устройства – дельта-манипулятор фирмы ABB (рис. 6).

Рисунок 6 – Дельта-робот фирмы ABB [9]

Однако он имеет сравнительно высокую стоимость и может быть заменен на более дешевые аналоги с подобной кинематикой. Модуль с данным манипулятором можно использовать как вместе с посевным барабаном, так и вместо него.

Контроль времени начала автоматизированного включения дополнительного освещения (досветки), внесения удобрений, полива, пикировки и формирования рассады может осуществляться с использованием системы компьютерного зрения, расположенной над ящиками с рассадой. Система позволит отследить момент раскрытия первых ростков (рис. 7), появления первого настоящего листа (рис. 8), появления больных, слабых, поврежденных и неразвитых растений, позволит контролировать всхожесть и отслеживать затенение растений.

Рисунок 7 – Состояние всхода, регистрируемое СТЗ для включения досветки [10]

Внешний вид взошедшей и развитой рассады и результат работы алгоритма выделения контуров ростков с использованием цветового фильтра в составе системы технического зрения показаны на рисунке 8.

Рисунок 8 – Внешний вид первых настоящих листков и результат выделения контуров [11]

Разработка моделей мобильных сельскохозяйственных роботов. Размещение посевных ящиков возможно с использованием мобильных транспортных роботов (рис. 9).

Рисунок 9 – 3D-модель транспортного робота для проведения типовых транспортировочных операций [12]

Транспортный робот основывается на платформе на базе трех всенаправленных колес. Каждое колесо имеет независимое вращение от бесколлекторного двигателя постоянного тока (БДПТ) с датчиками холла. Датчики холла необходимы для отслеживания скорости вращения колес. На грузовой платформе робота расположены три всенаправленных колеса для перемещения груза по платформе. Это необходимо в случаях, когда группе роботов необходимо построить конвейерную линию для сортировки грузов. В случае работы в режиме перевозки и складирования для поднятия груза используются три линейных актуатора. Чтобы независимо управлять скоростями всех шести БДПТ с датчиками холла, применяется шесть контроллеров двигателей, которые принимают на вход показания с датчиков холла, затем микроконтроллер производит обработку сигналов и подает на выходы обмоток мотора ШИМ сигнал, тем самым регулируя скорость вращения вала двигателя.

Контроль влажности почвы возможно производить с использованием системы датчиков влажности, размещаемых на манипуляторе мобильного робота. Мобильные роботы с манипуляторами в данной концепции роботизированной теплицы могут производить следующие операции: анализ влажности почвы и температуры в различных частях теплицы, пикирование и пасынкование рассады, прищипывание стебля, удаление листьев, сбор урожая и уборка ботвы. Нами предлагается решение в виде группы взаимодействующих роботов с одним или двумя 5-звенными манипуляторами и сменяемыми концевыми эффекторами (рис. 10).

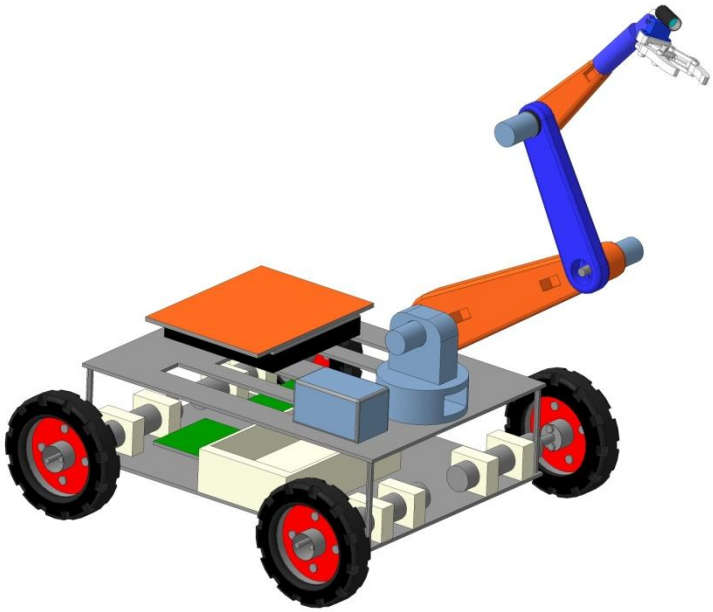


Рисунок 10 – 3D-модель мобильного робота для формирования куста томатов и единичных операций с рассадой

Анализ влажности и температуры подразумевает установку на конце манипулятора модуля с зондовым датчиком влажности почвы и датчиком температуры. Пикирование предусматривает модуль с отщипывающим инструментом, тот же модуль можно унифицировать для операций пасынкования и прищипывания стебля. Для этих задач необходимо использовать плоский захват с загнутыми и заостренными краями, так как требуется не только отделить листья, пасынки, части стебля или корня, но и не оставлять отделенные части возле куста. С помощью захвата предлагаемой формы отделенная часть может быть собрана в специальный ящик и вывезена в биореакторную установку для утилизации.

Для выполнения задач по высадке рассады в тепличный грунт могут быть использованы двухпальцевые захваты в комбинации со специальным рассадопосадочным устройством, внешний вид которого представлен на рисунке 11.

Рисунок 11 – Концевой механизм рассадопосадочного устройства [13]

Для сбора урожая требуется более сложное захватное устройство – например трехпальцевый камерный захват или захват с камерами, заполненными сыпучим материалом для распределения давления на собираемые плоды с целью исключения их повреждения. Концепцию роботизированного сбора урожая с помощью мобильных роботов, оснащенных манипуляторами, можно пояснить с использованием рисунка 12. Ранее в [14] были представлены особенности управления манипулятором такого робота.

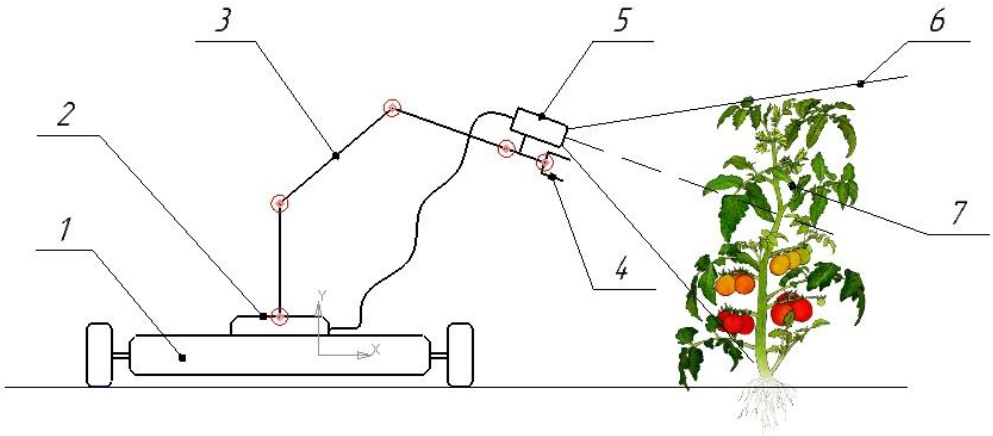


Рисунок 12 – Обобщенная схема мобильного робота для сбора урожая [14]

На рисунке 12 показана мобильная робототехническая платформа «1» с установленным на ней манипулятором «3», оснащенным специализированным схватом «4» и СТЗ «5». Последняя представляет собой видеокамеру и ультразвуковой дальномер, подключенные к блоку управления «2». Видеокамера и дальномер обладают определенным углом обзора «6» и предназначены для обеспечения точного сближения схвата с плодом, расположенным на стебле растения «7». Основными задачами в этом случае являются следующие: точное определение позиций плодов; траекторное управление перемещением схвата манипулятора; осуществление операции отделения плода от стебля.

Реальный прототип робота для сбора урожая томатов может быть построен на основе 3D-модели, показанной на рисунке 13. Четырехколесное шасси робота, выполненное по схеме Акермана, может регулироваться по высоте и ширине в зависимости от параметров теплицы и применяемых сортов томатов. Робот снабжен двумя манипуляторами, системой позиционирования, системой компьютерного зрения, состоящей из видеокамер и ультразвуковых датчиков на манипуляторах и на раме, прожекторами для подсветки, системой управления движением, рулевым электроприводом и ходовыми электродвигателями. Плоды собираются в стандартные ящики и передаются транспортным роботам, показанным ранее на рисунке 9.

Рисунок 13 – 3D-модель робота для сбора урожая

Разрабатываемая концепция подразумевает отказ от статичных конвейерных линий, в силу их трудного обслуживания и гибкости систем в целом, и заменой группами роботов, которые могут собирать конвейерные линии и производить сортировку грузов весом до ста килограммов. Подобная система позволит оборудовать любое помещение с ровной поверхностью под нужды сортировки. Пример конвейерной линии из роботов представлен на рисунке 14.

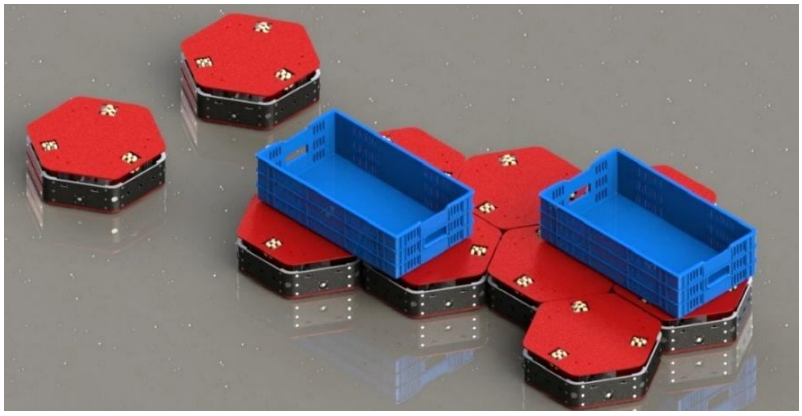


Рисунок 14 – Вариант согласованной работы нескольких транспортных роботов

Для предотвращения столкновений могут быть применены ультразвуковые (УЗ) и инфракрасные (ИК) датчики. Все показания с датчиков обрабатываются системой верхнего уровня, и в случае возникновения преграды система отправляет сигнал нижнему уровню о приостановке работы всех актуаторов. Для локальной системы позиционирования используются QR-метки и высокочастотная камера. За счет считывания информации с метки робот определяет текущую позицию в теплице. Персонал теплицы, ответственный за выполнение стандартных агротехнических операций с рассадой и созревшими плодами, таким образом, может быть заменен робототехническими комплексами и одним оператором. Такой подход востребован при определенных угрозах, с которыми сталкиваются или будут сталкиваться сельхозпроизводители.

Заключение. В работе была рассмотрена концепция роботизированной теплицы, полное управление которой может осуществлять только один оператор, спроектированы модели мобильных роботов, которые могут быть применены в рамках данной концепции. Возможность использования вышеописанных роботов, несомненно, определяется помимо технических еще и экономическими факторами и в рамках данной работы не рассматривается. Однако подробное экономическое обоснование перспектив роботизации тепличных комплексов будет выполнено в дальнейших работах, учитывая возрастающий интерес крупных предприятий к внедрению таких технологий. В дополнение к материалу настоящей работы отдельно будут подробно проанализированы и вопросы навигации мобильных роботов в теплице с использованием системы технического зрения. Представляет интерес и рассмотрение социальных аспектов роботизации сельского хозяйства.

Библиографический список

1. Жители России не готовы заместить иностранных мигрантов. – Режим доступа: https://www.vedomosti.ru/society/articles/2020/11/29/848719-zamestit-gastarbaiterov, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.12.2020).

2. Минсельхоз попросил пустить в Россию мигрантов для сезонных работ в поле. Местные жители не хотят собирать урожай даже за повышенную плату. – Режим доступа: https://www.rbc.ru/business/10/02/2021/602284149a79477561239575 , свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 10.02.2021).

3. Что произошло на рынке труда России с начала 2020 года. – Режим доступа: https://fingazeta.ru/ekonomika/rossiyskaya_ekonomika/467683, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.12.2020).

4. Обеззараживание теплиц. – Режим доступа: http://www.kaicc.ru/otrasli/sredstva-zashity/obezzarazhivanie-teplic, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.12.2020).

5. «Умные» теплицы и свет по потребностям: как развиваются аграрные технологии в Арктике. – Режим доступа: https://tass.ru/ekonomika/5446688 , свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.12.2020).

6. Выращивание томатов. Основные этапы и методы. – Режим доступа: http://ogorodogo.ru/vyrashhivanie-tomatov-osnovnye-etapy/#i-9, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 18.12.2020).

7. Линия для посева семян Alfa. – Режим доступа: http://urbinati.net/products/alfa-seeding-line/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.12.2020).

8. Линия для рассады посев семян рассады в кассеты. – Режим доступа: https://www.youtube.com/watch?reload=9&v=Jij1PW4xBaY, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 21.12.2020).

9. IRB 360 FlexPicker. – Режим доступа: https://new.abb.com/products/robotics/industrial-robots/irb-360, свободный. – Заглавие с экрана. – Яз. англ. (дата обращения: 21.12.2020).

10. Выращивание рассады томатов в домашних условиях. – Режим доступа: https://chudoclumba.ru/vyrasivanie-rassady-tomatov-v-domasnih-usloviah/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.12.2020).

11. Показываю, какую рассаду томатов мне удалось вырастить. Подробное описание всех процессов от покупки семян до результата. – Режим доступа: https://zen.yandex.ru/media/id/5d82364ce882c300ac2f74b4/pokazyvaiu-kakuiu-rassadu-tomatov-mne-udalos-vyrastit-podrobnoe-opisanie-vseh-processov-ot-pokupki-semian-do-rezultata-5e959c63aa749e6d77b8ec75, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.12.2020).

12. Степанович Е. Ю. Особенности применения складских роботов для предприятий агропромышленного комплекса / Е. Ю. Степанович, П. И. Тамков // Каспий XXI века: пути устойчивого развития : материалы Международного научного форума. – 2020. – С. 108–111.

13. Пистолет для посадки рассады Базука. – Режим доступа: https://www.blagodatmir.ru /product/rassadoposadochnoe-ustroystvo-pld0100, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 22.12.2020).

14. Рыбаков А. В. Проектирование робототехнических манипуляторов с системой компьютерного зрения для сбора томатов / А. В. Рыбаков, А. М. Лихтер, А. Б. Погожева, А. В. Михайлова, А. Б. Дусалиев // Прикаспийский журнал: управление и высокие технологии. – 2020. – № 3 (51). – С. 135–147.

References

1. *Zhiteli Rossii ne gotovy zamestit inostrannykh migrantov* [Russian residents are not ready to replace foreign migrants]. Available at: https://www.vedomosti.ru/society/articles/2020/11/29/848719-zamestit-gastarbaiterov (accessed 22.12.2020).

2. *Minselkhoz poprosil pustit v Rossiyu migrantov dlya sezonnykh rabot v pole. Mestnye zhiteli ne hotyat sobirat urozhay dazhe za povyshennuyu platu* [The Ministry of Agriculture asked to let migrants to Russia for seasonal work in the field. Local residents do not want to harvest even for an increased fee]. Available at: https://www.rbc.ru/business/10/02/2021/602284149a79477561239575 (accessed 10.02.2021).

3. *Chto proizoshlo na rynke truda Rossii s nachala 2020 goda* [What has happened in the Russian labor market since the beginning of 2020]. Available at: https://fingazeta.ru/ekonomika/rossiyskaya_ekonomika/467683 (accessed 18.12.2020).

4. *Obezzarazhivanie teplits* [Disinfection of greenhouses]. Available: http://www.kaicc.ru/otrasli/sredstva-zashity/obezzarazhivanie-teplic (accessed 18.12.2020).

5. *"Umnye" teplitsy i svet po potrebnostyam: kak razvivayutsya agrarnye tekhnologii v Arktike* ["Smart" greenhouses and light according to your needs: how agricultural technologies are developing in the Arctic]. Available at: https://tass.ru/ekonomika/5446688 (accessed 18.12.2020).

6. *Vyrashchivanie tomatov. Osnovnye etapy i metody* [Growing tomatoes. Main stages and methods]. Available at: http://ogorodogo.ru/vyrashhivanie-tomatov-osnovnye-etapy/#i-9 (accessed 18.12.2020).

7. *Liniya dlya poseva semyan Alfa* [Alfa seed sowing line]. Available at: http://urbinati.net/products/alfa-seeding-line/ (accessed 21.12.2020).

8. *Liniya dlya rassady posev semyan rassady v kassety* [The line for the planting of seedlings seeds, seedlings magazine]. Available at: https://www.youtube.com/watch?reload=9&v=Jij1PW4xBaY (accessed 21.12.2020).

9. *IRB 360 FlexPicker.* Available at: https://new.abb.com/products/robotics/industrial-robots/irb-360 (accessed 21.12.2020)

10. *Vyrashchivanie rassady tomatov v domashnikh usloviyakh* [The cultivation of seedlings of tomatoes in the home]. Available at: https://chudoclumba.ru/vyrasivanie-rassady-tomatov-v-domasnih-usloviah/ (accessed 22.12.2020).

11. *Pokazyvayu, kakuyu rassadu tomatov mne udalos vyrastit. Podrobnoe opisanie vsekh protsessov ot pokupki semyan do rezultata* [I show you what kind of tomato seedlings I managed to grow. A detailed description of all the processes from the purchase of seeds to the result]. Available at: https://zen.yandex.ru/media/id/5d82364ce882c300ac2f74b4/pokazyvaiu-kakuiu-rassadu-tomatov-mne-udalos-vyrastit-podrobnoe-opisanie-vseh-processov-ot-pokupki-semian-do-rezultata-5e959c63aa749e6d77b8ec75 (accessed 22.12.2020).

12. Stepanovich E. Yu., Tamkov P. I. Osobennosti primeneniya skladskikh robotov dlya predpriyatiy agropromyshlennogo kompleksa [Features of the use of warehouse robots for enterprises of the agro-industrial complex]. *Kaspiy XXI veka: puti ustoychivogo razvitiya* : *materialy Mezhdunarodnogo nauchnogo foruma* [The Caspian Sea of the XXI century: ways of sustainable development : Materials of International Forum], 2020, pp. 108–111.

13. *Pistolet dlya posadki rassady Bazuka* [Bazooka seedling Planting Gun]. Available at: https://www.blagodatmir.ru/product/rassadoposadochnoe-ustroystvo-pld0100 (accessed 22.12.2020).

14. RybakovA. V., Likhter A. M., Pogozheva A. B., Mikhaylova A. V., Dusaliev A. B. Proektirovanie robototekhnicheskikh manipulyatorov s sistemoy kompyuternogo zreniya dlya sbora tomato [Design of robotic manipulators with a computer vision system for picking tomatoes]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Control and High Technologies], 2020, no. 3 (51), pp. 135–147.

ПРАВИЛА ДЛЯ АВТОРОВ

1. В журнале публикуются материалы на английском и русском языках по тематике, соответствующей утвержденным для журнала отраслям наук, группам специальностей.

2. В список соавторов работ включаются только те лица, которые внесли творческий вклад в подготовку представленных материалов. Лицам, оказавшим только техническую помощь, можно выразить благодарность в конце статьи. Один человек может быть автором (соавтором) не более чем двух статей в одном номере журнала, причем единственным автором он может быть только в одной статье.

3. Объем публикаций для научных статей должен быть не менее 8 страниц, а количество источников в библиографическом списке (списке литературы) – не менее 10 позиций.

4. Содержание каждой статьи должно включать следующие элементы: УДК; название статьи; сведения об авторах, включая их место работы, должность, адрес электронной почты; аннотацию объемом от 100 до 250 слов, ключевые слова (от 9 до 13); графическую аннотацию, отражающую содержание статьи; название статьи, сведения об авторах, аннотацию и ключевые слова на английском языке (для англоязычных статей – на русском языке); введение – оно должно заканчиваться формулировкой цели работы в явной форме; собственно текст статьи – очень желательна его сегментация на разделы, имеющие содержательные заголовки; выводы или заключение (должны соответствовать формулировке цели статьи).

5. Для русскоязычных статей приводится два библиографических списка: на языке оригинала статьи; список с транслитерацией русскоязычных источников на латиницу и (дополнительно) приведением в квадратных скобках переводов названий статей и названий источников на английский язык.

В «русскоязычном» библиографическом списке (списке литературы) порядок следования источников – по алфавиту фамилий авторов (сначала русскоязычные источники, потом иноязычные). На все источники, включенные в библиографический список, должны быть даны ссылки в тексте статьи в квадратных скобках. При необходимости авторы могут указывать номера страниц в источниках, на которые даются ссылки. Приветствуются ссылки на иноязычные источники, а также на материалы, опубликованные ранее в журнале «Прикаспийский журнал: управление и высокие технологии». Однако в последнем случае количество таких ссылок не должно превышать 20 % от общего количества источников, включенных в библиографический список. Для источников, имеющих DOI, целесообразно его указывать. При ссылках на статьи, опубликованные в журнале «Прикаспийский журнал: управление и высокие технологии», целесообразно в конце библиографического описания источника в круглых скобках указывать гиперссылку, указывающую на место размещения статьи на страничке сайта Астраханского государственного университета.

Ссылки в библиографическом списке на материалы, размещенные в интернете, допускаются при соблюдении следующих условий: если у материала, на который дается ссылка, имеется автор и/или название, то они должны быть указаны для этого источника; должен быть приведен полный маршрут доступа к источнику в интернете; должна быть указана дата обращения (доступа) к источнику.

Ограничения по списку литературы: доля самоцитирований для любого из авторов статьи, а также по совокупности всех авторов статьи, не должна превышать 25 %; доля ссылок на статьи с участием одного автора, не являющегося автором (соавтором) статьи, не должна превышать 25 %.

6. Суммарная доля таблиц и иллюстраций в общем объеме представляемой статьи не должна превышать 40 %. Под иллюстрациями понимаются следующие объекты: диаграммы; графики; рисунки; эскизы; фотографии; карты и т.п.

7. Доля оригинального текста в статьях (оцениваемого через систему «Антиплагиат» на сайте www.antiplagiat.ru) должна быть не менее 80 %.

8. Указание на то, что работа финансируется по какому-либо гранту, в рамках Федеральной целевой программы, государственного заказа и пр. дается в виде постраничной сноски после заголовка (названия) работы.

9. В сведения об авторах работ помимо места работы и должности целесообразно включать ORCID автора и гиперссылку на страничку с его личными наукометрическими показателями на сайте www.elibrary.ru. По желанию можно привести также ссылки на странички с наукометрическими показателями на Scopus, в ResearchGate; на личную страничку, размещенную на сайте организации.

10. Основные технические требования к оформлению статей (материалов):

10.1. Текст должен быть расположен по ширине страницы формата А4 с учётом полей (все поля по 2,5 см), набран шрифтом Times New Roman, кегль 14, межстрочный интервал 1,0. В таблицах, подрисуночных надписях допускается уменьшенный шрифт – вплоть до 10 кегля. Альбомная ориентация страниц допускается только в порядке исключения для следующих случаев: широкоформатные таблицы с большим количеством колонок; иллюстрации большого размера, которые не умещаются на странице с книжной ориентацией.

Абзацные отступы одинаковы по всему тексту – 1,25 см. Кавычки («»), скобки ([ ], ( )), маркеры и другие знаки должны быть аналогичными на протяжении всего предоставляемого для публикации материала.

10.2. Все таблицы, рисунки, формулы должны иметь сквозную нумерацию в пределах текста статьи. Заголовки таблиц пишутся над ними и должны включать в себя номер таблицы и ее содержательное наименование.

10.3 Формулы должны иметь сквозную нумерацию в пределах текста статьи. Для формул желательно избегать «многоэтажных конструкций». Нумероваться могут только те формулы, на которые есть ссылки в статье. Размеры шрифтов для формул в MS Equation Editor: основные символы – 14 пт.; подстрочные и надстрочные индексы – 10 пт.; дополнительные индексы для подстрочных и надстрочных индексов – 8 пунктов. Константы в формулах записываются прямым шрифтом, переменные – курсивом (наклонным шрифтом); векторные и матричные величины – полужирным шрифтом. Матричные величины могут указываться в квадратных скобках, векторные величины (наборы скаляров) – в фигурных скобках.

Дополнительная информация для авторов статей

Основная тематика журнала и требования к научному уровню представляемых статей – http://hi-tech.asu.edu.ru/docs/ru-rules/ trebovaniya.pdf.

Адрес и телефоны редакционно-издательского дома – http://hi-tech.asu.edu.ru/docs/ru-rules/address.pdf.

Пример оформления текста статьи – http://hi-tech.asu.edu.ru/docs/ru-rules/primer.pdf.

Рекомендации по оформлению графических аннотаций – http://hi-tech.asu.edu.ru/docs/ru-rules/graf_ann.pdf, дополнительных материалов к статьям – http://hi-tech.asu.edu.ru/docs/ru-rules/dop_mat.pdf.

Подробные правила оформления таблиц – http://hi-tech.asu.edu.ru/docs/ru-rules/tables.pdf, оформления формул – http://hi-tech.asu.edu.ru/docs/ru-rules/formul.pdf, оформления иллюстраций – http://hi-tech.asu.edu.ru/docs/ru-rules/ilustr.pdf.

Пример оформления основного списка литературы к статье – http://hi-tech.asu.edu.ru/docs/ru-rules/spisok_liter.pdf, транслитерированного списка- – http://hi-tech.asu.edu.ru/docs/ru-rules/trasn_spisok_liter.pdf.

Дополнительные документы к статьям, представляемые авторами – http://hi-tech.asu.edu.ru/docs/ru-rules/dop_doc.pdf.

Переписка с авторами и порядок рецензирования статей – http://hi-tech.asu.edu.ru/docs/ru-rules/poryadok_recenz.pdf.

Условия и порядок оплаты статей – http://hi-tech.asu.edu.ru/docs/ru-rules/poryadok_oplaty.pdf.

RULES FOR THE AUTHORS – http://hi-tech.asu.edu.ru/docs/en-rules/rules-for-authors.pdf.

Подписка на наши издания осуществляется
по Объединённому каталогу «Пресса России»

Журнал фундаментальных и прикладных исследований ***«Гуманитарные исследования»***

Подписной индекс – 11109

В журнале публикуются статьи по широкому спектру проблем гуманитарного знания. Ведущие направления публикаций отражены в следующих рубриках: «Языкознание», «Литературоведение».

Периодичность издания – 4 раза в год.

Ориентировочная стоимость одного номера – 3762 руб.

Телефон: (8512) 24-64-95. E-mail: asupress@yandex.ru

Научно-технический журнал ***«Геология, география и глобальная энергия»***

Подписной индекс – 11173

Редколлегия журнала принимает к рассмотрению статьи по проблемам геологии, нефтегазоностности различных регионов, охватывающие важнейшие и крайне полезные для науки и производства, а также для обучения студентов естественного направления.

Периодичность издания – 4 раза в год.

Ориентировочная стоимость одного номера – 4500 руб.

Телефон: (8512) 24-64-95. E-mail: asupress@yandex.ru

Научный журнал «***Каспийский регион: политика, экономика, культура»***

Подписной индекс – 11170

Профиль журнала – анализ проблем настоящего, прошлого и будущего Каспийского региона в их взаимосвязи с современным развитием мира.

Издание имеет многоплановый, междисциплинарный характер, знакомит читателя с исследованиями и дискуссиями во всех областях социальных и гуманитарных знаний по проблемам Каспийского региона.

Периодичность издания – 4 раза в год.

Ориентировочная стоимость одного номера – 3500 руб.

Телефон: (8512) 24-64-95. E-mail: asupress@yandex.ru

Научно-технический журнал ***«Прикаспийский журнал: управление и высокие технологии»***

Подписной индекс – 73313

На страницах журнала представлены результаты исследований и новейшие разработки в области технических наук.

Ведущие направления публикаций отражены в следующих рубриках: «Управление в социальных и экономических системах», «Системный анализ, управление и обработка информации», «Математическое моделирование, численные методы и комплексы программ», «Информационная безопасность и защита информации», «Информационно-измерительные и управляющие системы».

Периодичность издания – 4 раза в год.

Ориентировочная стоимость одного номера – 9000 руб.

Телефон: (8512) 24-64-95. E-mail: asupress@yandex.ru

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2021
№ 1 (53)

Свидетельство о регистрации средства массовой информации
Федеральной службы по надзору в сфере массовых коммуникаций,
связи и охраны культурного наследия
ПИ № ФС77-31932 от 16 мая 2008 г.

Учредитель
Астраханский государственный университет
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Адрес редакции:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20

Адрес издателя:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Подписной индекс – 73313
По Объединенному каталогу «Пресса России»

Главный редактор И.М. Ажмухамедов

Редактирование,
компьютерная правка, верстка *Н.Н. Сахно*

Дата выхода в свет 16.04.2021 г.

Цена свободная
Уч.-изд. 9,5. Усл. печ. л. 13,2.
Заказ № 4284. Тираж 500 экз. (первый завод – 22 экз.)

Оттиражировано на базе Издательского дома «Астраханский университет»
414056, г. Астрахань, ул. Татищева, 20а
Тел. (8512) 24-64-95, тел./факс (8512) 24-68-37
E-mail: asupress@yandex.ru