ПРИКАСПИЙСКИЙ ЖУРНАЛ

УПРАВЛЕНИЕ И ВЫСОКИЕ ТЕХНОЛОГИИ

2024
№4 (68)

ISSN 2074-1707

16+

ISSN 2074-1707

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ В. Н. ТАТИЩЕВА

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2024
№ 4 (68)

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

Группа специальностей 1.2 «Компьютерные науки и информатика»:

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

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

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

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

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

Группа специальностей 2.3 «Информационные технологии и телекоммуникации»:

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

2.3.4 – Управление в организационных системах (технические науки);

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

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

Журнал входит в базу данных Ulrich’s Periodicals Directory.

Астрахань
Астраханский государственный университет имени В. Н. Татищева
2024

ББК 30
П75

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

ПРИКАСПИЙСКИЙ ЖУРНАЛ: управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2024
№ 4 (68)

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

ISSN 2074-1707

ASTRAKHAN TATISHCHEV STATE UNIVERSITY

PRIKASPIYSKIY ZHURNAL:
Upravlenie i Vysokie Tekhnologii

CASPIAN JOURNAL:
Control and High Technologies

A SCIENTIFIC AND TECHNICAL JOURNAL

2024
No. 4 (68)

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

Group of specialties 1.2 "Computer science and informatics":

1.2.2 – Mathematical modelling, numerical methods and complexes of programms (technical sciences).

Group of specialties 2.2 "Electronics, photonics, instrument engineering and communication":

2.2.4 – Instruments and methods of measurement (by type of measurement) (technical sciences);

2.2.11 – Information-measuring and control systems (technical sciences);

2.2.12 – Medical devices, systems and products (technical sciences).

Group of specialties 2.3 "Information technologies and telecommunications":

2.3.1 – System analysis, information control and processing (technical sciences);

2.3.4 – Management in organizational systems (technical sciences);

2.3.5 – Mathematical software and software for computing systems, complexes and computer networks (technical sciences);

2.3.6 – Information security methods and systems, information security (technical sciences).

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

Astrakhan
Astrakhan Tatishchev State University
2024

Recommended by the Editorial and Publishing Board
of Astrakhan Tatishchev State University

**CASPIAN JOURNAL:
Control and High Technologies**

A SCIENTIFIC AND TECHNICAL JOURNAL

**2024
No. 4 (68)**

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

CONTENTS

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.896

АЛГОРИТМ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ OSINT ДЛЯ ПОИСКА НАЧАЛЬНЫХ ТОЧЕК СКАНИРОВАНИЯ ЦЕЛЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Жукова Марина Николаевна, Сибирский государственный университет науки и технологий, 660037, Российская Федерация, г. Красноярск, пр. им. газ. «Красноярский рабочий», 31,
кандидат технических наук, доцент, ORCID: 0000-0003-3441-3041, e-mail: zhukova@sibsau.ru

Эффективность защитных мер, применяемых для целевой информационной системы, существенно зависит от информации, которую возможно «считать» с системы, используя открытые источники информации. Уровень представления данных может быть весьма обширен. Пользуясь этим, злоумышленник проникает в систему и находится там довольно долгое время, до своего обнаружения. Поиск точек компрометации, которые могут показать путь проникновения и дальнейших уязвимых узлов системы, – сложный процесс, основная проблема которого – обширность ИТ-инфраструктуры и невозможность одновременного сканирования всех направлений. Технологии поиска информации из открытых источников (OSINT) могут успешно решать задачу поиска компрометирующей информации. Настоящая работа содержит описание проблемы поиска индикаторов компрометации без первоначального определения точек сканирования в архитектуре информационной системы. Представлено описание применения технологии OSINT в задаче поиска начальных точек сканирования. Алгоритм, описание которого приведено в статье, подробно раскрывает основные шаги применения технологии поиска OSINT. Предложенный подход позволяет существенно сузить и приоретизировать перечень начальных точек сканирования целевой информационной системы с целью дальнейшего выявления индикаторов компрометации.

Ключевые слова: индикаторы компрометации, технология OSINT, информационная инфраструктура, целевая информационная система, точки входа в информационную систему

Финансирование: *исследование выполнено при финансовой поддержке Минцифры РФ (грант ИБ, проект № 40469-02/23-Д).*

ALGORITHM FOR USING OSINT TECHNOLOGY TO SEARCH FOR INITIAL SCANNING POINTS OF A TARGET INFORMATION SYSTEM

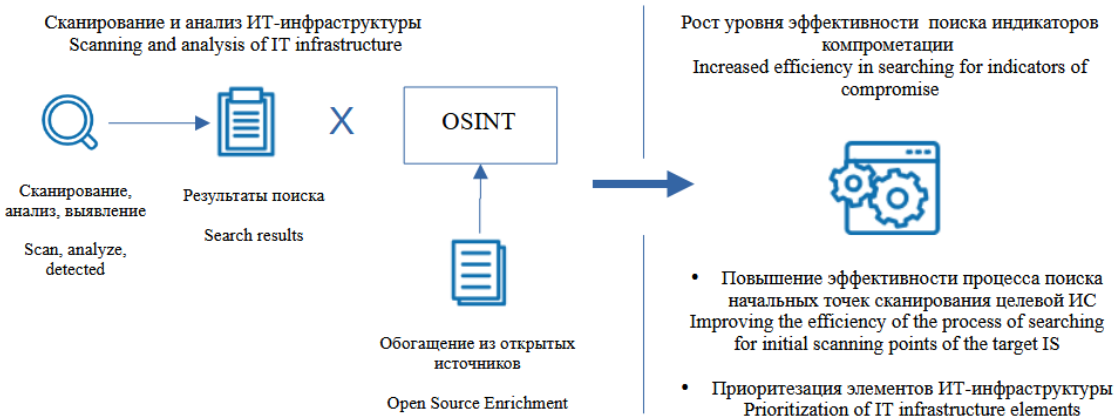
Zhukova Marina N.**,** Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-3441-3041, e-mail: zhukova@ sibsau.ru

The effectiveness of protective measures applied to the target information system significantly depends on the information that can be “read” from the system using open sources of information. The level of data presentation can be quite extensive. Using this, an intruder penetrates the system and remains there for quite a long time before being detected. Searching for points of compromise that can show the path of penetration and further vulnerable nodes of the system is a complex process. The main problem of which is the vastness of the IT infrastructure and the impossibility of simultaneous scanning of all directions. Open source intelligence (OSINT) technologies can successfully solve the problem of searching for compromising information. This paper describes the problem of searching for indicators of compromise without initially defining scanning points in the architecture of the information system. A description of the use of OSINT technology in the task of searching for initial scanning points is presented. The algorithm described in the article reveals in detail the main steps of applying OSINT search technology. The proposed approach allows you to significantly narrow and prioritize the list of initial scanning points of the target information system in order to further identify indicators of compromise.

Keywords: indicators of compromise, OSINT technology, information infrastructure, target information system, entry points into the information system

Financial support: *the work was supported by the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation (IS grant, project No. 40469-02/23-D).*

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

С развитием технологий и увеличением количества пользователей возрастает и риск угроз информационной безопасности. Одной из наиболее опасных угроз является компрометация информационных систем. Информационные ресурсы компании, доступные через сеть Интернет, составляют ее внешний периметр. Скомпрометировав внешний периметр, злоумышленник может получить доступ к конфиденциальной информации и нарушить работу критичных элементов инфраструктуры.

Для предотвращения компрометации необходимо проводить поиск и оценку индикаторов компрометации для принятия решения о необходимых мерах защиты информации и информационных ресурсов.

Индикаторы компрометации – это признаки, которые могут указывать на то, что система была скомпрометирована. Они могут быть различными: от изменений в конфигурационных файлах до подозрительной сетевой активности. Индикаторы компрометации могут включать в себя хэш-суммы файлов, их имена и расположение, IP-адреса, DNS-имена серверов в сети Интернет или конкретные URL (например, ссылки на фишинговые страницы), названия веток и ключей реестра Windows и др.

Поиск индикаторов компрометации является сложным и трудоемким процессом [1]. Для его выполнения могут использоваться различные методы: регулярный мониторинг систем на предмет подозрительной активности; анализ вредоносных артефактов; сканирование сети или определенного хоста на предмет наличия в них индикаторов компрометации; мониторинг активности APT-группировок с целью сбора индикаторов компрометации извне (Threat Intelligence); использование платформ для хранения и обработки индикаторов компрометации [2] и др. Для выполнения этих действий необходимо использовать соответствующие дорогостоящие инструменты, которые есть не у всех компаний, а также различные разработки, активно регистрируемые в последние годы [3, 4]. К таким инструментам можно отнести такие решения, как SOAR- и SIEM-, XDR- и EDR-, UBA- и UEBA-, TI-платформы.

Даже при наличии соответствующих инструментов для поиска индикаторов компрометации возникает проблема определения начальной точки для обнаружения индикаторов компрометации. Рассматривая стандартные архитектуры информационных систем, анализируя ИТ-инфраструктуры, становится необходимым анализировать и в последующем мониторить достаточно большое количество критических «точек» системы. Более того, каждый раз необходимо снова определять, с какого элемента или части ИТ-инфраструктуры начинать сканирование и последующий анализ. На первый взгляд, достаточно простая задача становится действительно непростой при практическом рассмотрении.

Целью исследования, результаты которого приведены ниже, является решение следующей задачи: предложить алгоритм и методику применения технологии поиска информации из открытых источников (OSINT) для поиска и приоритезации «начальных точек» сканирования целевой информационной системы.

Новыми результатами исследования, представленными ниже, стали:

1) алгоритм встраивания элементов поиска дополнительных сведений из результатов сканирования и анализа внешних источников информации о целевой ИС в процесс принятия решений при мониторинге информационной безопасности ИТ-инфраструктуры;

2) повышение эффективности системы мониторинга объектов и систем информатизации, находящихся под воздействием угроз безопасности.

ТЕХНОЛОГИИ ПОИСКА ИНФОРМАЦИИ ИЗ ВНЕШНИХ ОТКРЫТЫХ ИСТОЧНИКОВ

OSINT – это метод сбора информации из открытых источников. Он позволяет получить доступ к большому объему данных, которые могут быть использованы для определения возможных точек входа в информационную инфраструктуру на ее внешнем периметре. Выявленные точки входа

в информационную систему будут являться начальными точками для поиска индикаторов компрометации и глубокого анализа системы на предмет наличия индикаторов компрометации.

Cyber Threat Hunting (поиск киберугроз) – поиск угроз внутри сети организации: анализ потенциальных свидетельств атаки как известных, так и неизвестных вирусов, поиск следов деятельности киберпреступных групп, а также поиск признаков заражений, в том числе и на самом глубоком уровне, например, прошивках аппаратных устройств, а также в сообщениях от сторонних компаний (поиск признаков атак с IP-адресов защищаемой компании) [5].

Активный поиск угроз позволяет на ранней стадии выявлять новые и сложные угрозы и рассматривается как дополнение к имеющейся защите информационных систем организации, а не как ее замена. От традиционных методов защиты Threat Hunting отличает именно проактивность.

Поскольку проникновение в систему может произойти в любой момент, поиск угроз – это непрерывный процесс. Он состоит из двух шагов [6]:

1) формирование гипотезы: на этом этапе строятся предположения о местах поиска угроз. Источником информации для выдвижения гипотезы могут служить как внутренние данные компании (сведения о состоянии информационной инфраструктуры, результаты тестов на проникновение и т. д.), так и внешние (тактики и техники Mitre Att&ck, отчеты разведки киберугроз, новости безопасности и т. д.). Например, если в новом отчете приводится анализ ранее неизвестного вредоносного программного обеспечения, можно предположить, что оно могло проникнуть в инфраструктуру компании;

2) проверка гипотезы: после того как гипотеза сформулирована, производится ее тестирование. Например, производится анализ данных с конечных точек на предмет наличия индикаторов компрометации, связанных с новым вредоносным программным обеспечением.

Если гипотеза подтвердилась, компания может принять необходимые меры. Кроме того, информацию, полученную в ходе поиска угроз, можно использовать для формирования новых гипотез и улучшения защитных систем, например, для обновления правил фильтрации трафика [6].

Cyber Threat Intelligence (кибербразведка) – это поиск информации о потенциальных атакующих, в том числе о серьезных киберпреступных группах (APT-группировки от Advanced Persistent Threat (усложненная устойчивая угроза или целевая кибератака)) [5].

Информация об актуальных угрозах и группировках киберпреступников позволяет организациям изучить цели, тактику и инструменты злоумышленников и выстроить эффективную стратегию защиты от атак. Данные о киберугрозах можно условно разделить на три основных группы [7]:

1) тактические – техническая информация, например, индикаторы компрометации;

2) операционные – описание техник и процедур, которыми пользуются злоумышленники, а также их возможностей и преследуемых ими целей;

3) стратегические – данные о рисках, связанных с конкретными угрозами.

Threat Intelligence может применяться на разных этапах защиты организации. В частности, компании могут использовать эти данные для активного поиска угроз в инфраструктуре организации. Индикаторы компрометации позволяют усовершенствовать пассивные защитные инструменты, например, обновить правила межсетевого экрана. Кроме того, данные об угрозах могут применяться для атрибуции при расследовании инцидентов информационной безопасности.

Потоки данных Threat Intelligence используются в различных решениях для обеспечения информационной безопасности, таких как SIEM и EDR-платформы [7], IRP-системы, антивирусы.

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ OSINT ДЛЯ ПОИСКА НАЧАЛЬНЫХ ТОЧЕК СКАНИРОВАНИЯ ЦЕЛЕВОЙ ИС

Для обнаружения точек входа в информационную инфраструктуру применяются специализированные OSINT-инструменты, позволяющие получить данные об открытых портах на внешнем периметре информационной сети, о DNS-структуре и домене организации, о возможных уязвимостях приложений, сервисов и ресурсов информационной системы, о структуре информационной сети, используемых серверах и IP-адресах, об электронной почте и др. [8].

Обработанные результаты сканирования позволяют определить перечень начальных точек, с которых следует начать анализ целевой информационной системы. Данная информация может помочь для поиска индикаторов компрометации внутри информационной системы с целью определения элементов информационной инфраструктуры и объектов, на которые совершены воздействия злоумышленников [9].

Выявленные критичные точки на внешнем периметре информационной инфраструктуры организации сопоставляются с различными тактиками и техниками злоумышленников, которые могут быть использованы путем взаимодействия с этими точками.

Общая схема применения технологии OSINT в процессе определения начальных точек сканирования представлена на рисунке 1.

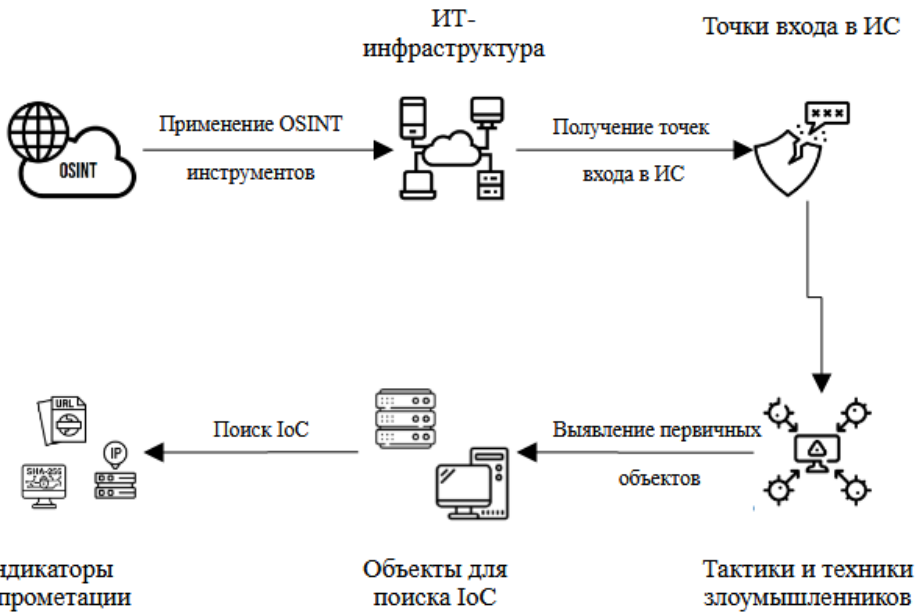


Рисунок 1 – Общая схема применения OSINT при поиске информации о начальных точках сканирования целевой ИС

Как видно из схемы, первым этапом является применение OSINT-инструментов на объекте, которые позволяют получить возможные точки входа на внешнем периметре информационной инфраструктуры [10]. Получив точки входа в информационную систему, определяются возможные уязвимости, которые могут быть использованы злоумышленником для компрометации системы.

Далее определяются тактики и техники злоумышленников, используя широко известные фреймворки (Mitre Att&k, Owasp, Capec), использующие найденные точки входа в информационную систему, которые могут быть применены для компрометации этой системы. Выбор фреймворка может быть выполнен произвольным образом или на основе дополнительных данных, которые приведены в различных исследованиях [11]. После определения тактик и техник нарушителей путем определения взаимодействующих между собой в рамках атаки элементов выявляются первичные объекты (начальные точки для сканирования) для поиска индикаторов компрометации на них (хост, сервер и т. д.). После этого возможно запускать процесс поиска индикаторов компрометации на выявленных первичных объектах, например, с помощью сканеров или специализированных программных средств, полученные индикаторы анализируются для дальнейших действий специалистами по информационной безопасности.

Таким образом, применение технологии OSINT может дать дополнительные данные, которые возможно использовать для определения начальных точек поиска индикаторов компрометации в информационной инфраструктуре объектов.

Даже небольшая по объему информационная система содержит в себе множество объектов, на которых возможно производить поиск индикаторов компрометации. В данном случае возникает проблема определения начальных точек поиска индикаторов компрометации, так как объектов для поиска в системе существует огромное количество.

АЛГОРИТМ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ OSINT ДЛЯ ПОИСКА НАЧАЛЬНЫХ ТОЧЕК СКАНИРОВАНИЯ ЦЕЛЕВОЙ ИС

Алгоритм применения технологии OSINT, в задаче поиска начальных точек сканирования целевой информационной системы для последующего поиска индикаторов компрометации, может быть реализован следующим образом:

1. Анализ информационной инфраструктуры организации.

Анализ информационной инфраструктуры выполняется со следующими целями: определение основной информации об устройстве локальной сети организации; определение категорий защищаемой информации; определение защищаемых объектов в сети организации; определение используемых средств для защиты информации и соответствующих мер; определение наиболее важных узлов в сети с точки зрения их критичности.

2. Анализ OSINT-инструментов с точки зрения их применимости к определенной инфраструктуре.

На данном этапе анализируются различные общедоступные инструменты, а также проводится тестирование этих инструментов с точки зрения определения их функционала. Анализ должен

привести к конкретному списку инструментов, которые будут использоваться для выявления возможных точек входа в информационную систему организации. Для каждой организации такой набор будет разным, так как организации ведут свою деятельность по-разному. С учетом специфики организации и применяемых для выполнения своих функций средств формируется список OSINT-инструментов, который будет актуален для данной организации. В таблице 1, как пример, представлен набор инструментов, прошедших тестирование и успешно применяемых при поиске начальных точек «входа» в целевую информационную систему.

Таблица 1 – Анализ инструментов OSINT

Инструмент	Получаемая информация
Censys	Информация о доменах, субдоменах, IP-адресах, открытых портах, сервисах на этих портах
Intelligence X	Адреса электронной почты, утекшие пароли и файлы
Whois	Основная информация о домене
Hacket Target Tools	Информация о доменах, субдоменах, IP-адресах, открытых портах, сервисах на этих портах, DNS-записях
ZoomEye	Информация о доменах, субдоменах, IP-адресах, открытых портах, сервисах на этих портах
crt.sh	Информация об используемых TLS-сертификатах
Shodan	Информация о доменах, субдоменах, IP-адресах, открытых портах, сервисах на этих портах
Qualys SSL Labs	Информация об используемых TLS-сертификатах, шифрах, возможных уязвимостях, имитация рукопожатий
DNS dumpster	Информация о доменах, субдоменах, IP-адресах, открытых портах, сервисах на этих портах, DNS-записях
Утилита Subfinder	Поиск всех доменов и субдоменов
LeakCheck	Утекшие пароли, данные об утечках
Phonebook.cz	Сбор контактов организации, адреса электронной почты
Have I been pwned	Утекшие пароли, данные об утечках

3. Применение OSINT-инструментов на объекте защиты с целью выявления возможных точек входа в информационную систему.

На данном этапе производится сбор исходных данных для определения начальных точек поиска индикаторов компрометации. Производится сбор наиболее полного объема данных, включающий в себя: основную информацию об исследуемом домене; данные об используемых TLS-сертификатах и их возможных уязвимостях; данные о DNS-структуре, которые включают в себя информацию о субдоменах организации, DNS-записях, адресации домена; сведения об открытых портах, доступных сервисах, программном обеспечении, применяемых технологиях; данные о возможных уязвимостях и экслойтах; информацию об утекших адресах электронной почты; сведения об утечках, связанных с целевой организацией.

Как можно увидеть, список собираемых данных достаточно большой, при этом такой список будет отличаться для каждой компании, но в общем случае он будет выглядеть примерно так, как показано выше.

4. Анализ полученных результатов и определение тактик и техник злоумышленников.

На данном этапе вся собранная информация анализируется с целью выявления возможных точек входа в информационную систему, а также формируется набор тактик и техник злоумышленников, которые могут быть реализованы через полученные точки входа в систему. Данный шаг необходим для того, чтобы сформировать первичный перечень точек, с которых необходимо начать поиск индикаторов компрометации.

Полученные результаты, как пример, можно свести в виде таблицы, с указанием тактик и последующих техник злоумышленников (табл. 2).

Таблица 2 – Тактики и техники злоумышленников

Сервис /порт	Вектор атаки	Описание вектора атаки	Возможный результат
Port: 22 SSH			
22/TCP (SSH)	Захват баннера	Захват баннера SSH: злоумышленник запускает сканирование и получает данные о версии сервера. Получив эти данные, злоумышленник подбирает эксплойт для компрометации сервиса	Зная версию установленного ПО, злоумышленник может подобрать эксплойт и проанализировать доступные уязвимости
22/TCP (SSH)	Brute Force учетных данных	SSH Brute Force: usernames, passwords Злоумышленник авторизуется на SSH-сервер (через Brute Force атаку) и после этого, используя команду «port», подключается к другим серверам. Может использоваться nmap и msf	Получение доступа к операционной системе устройства
22/TCP (SSH)	Brute Force слабых SSH-ключей, созданных с использованием устаревших алгоритмов шифрования	Weak Cipher Algorithms Злоумышленник путем отправки специальных команд проверяет SSH-сервис на предмет использования слабых алгоритмов создания SSH-ключей (SHA1, RSA 1024-bit) и в случае, если такие алгоритмы были использованы, может попытаться осуществить брутфорс ключей. Существуют отдельные базы (словари) SSH-ключей для брутфорса	Получение доступа к операционной системе устройства

После определения тактик и техник злоумышленников необходимо понять общий принцип атак, которые могут быть реализованы через обнаруженные точки входа в информационную систему и определить объекты, взаимодействующие между собой в рамках данных атак. Выявленные объекты и будут являться первичными точками для поиска индикаторов компрометации.

5. Выявление начальных точек поиска индикаторов компрометации (компонентов ИС).

На данном этапе выявляются конкретные объекты системы, на которых необходимо произвести поиск индикаторов компрометации. С учетом полученной в предыдущих этапах информации формируется перечень конкретных объектов системы: сервер, компьютер, сетевое оборудование и т. д.

Чтобы выявить такие объекты, необходим перечень тактик и техник злоумышленников, в котором указывается возможный результат от реализации атаки. Например, при *Brute Force* атаке злоумышленник получает доступ к учетной записи пользователя в системе. Атакуемый пользователь выполняет свою работу на конкретном рабочем месте, за которым закреплен конкретный хост. Именно этот хост и будет являться начальной точкой для поиска индикаторов компрометации.

6. Приоритезация полученных компонентов ИС с точки зрения их критичности для информационной системы.

Данный этап помогает сузить круг выявленных объектов для поиска индикаторов компрометации и расставить очередность объектов целевой информационной системы для сканирования.

7. Обнаружение индикаторов компрометации на выявленных объектах.

Данный шаг алгоритма сам по себе является практически отдельной задачей, по сложности сопоставимой с исходной. Данный этап требует отдельной проработки и применения инструментов сканирования и поиска «следов» нахождения злоумышленника в системе. Рассматриваемый в статье подход призван облегчить процесс поиска точек входа в ИТ-инфраструктуру организации, чтобы, в последующем, запускать специализированные инсрументы поиска IoC уже на конкретных элементах системы.

8. Анализ полученных индикаторов с целью принятия решения о необходимых мерах защиты и составление рекомендаций.

На данном этапе производится анализ полученных индикаторов компрометации и производится дальнейшее расследование инцидента с целью отслеживания хода выполнения атаки и выявления «пострадавших» ресурсов. Проанализировав полученные в ходе расследования данные, составляются рекомендации для принятия мер защиты.

Схему алгоритма можно представить в следующем виде (рис. 2).

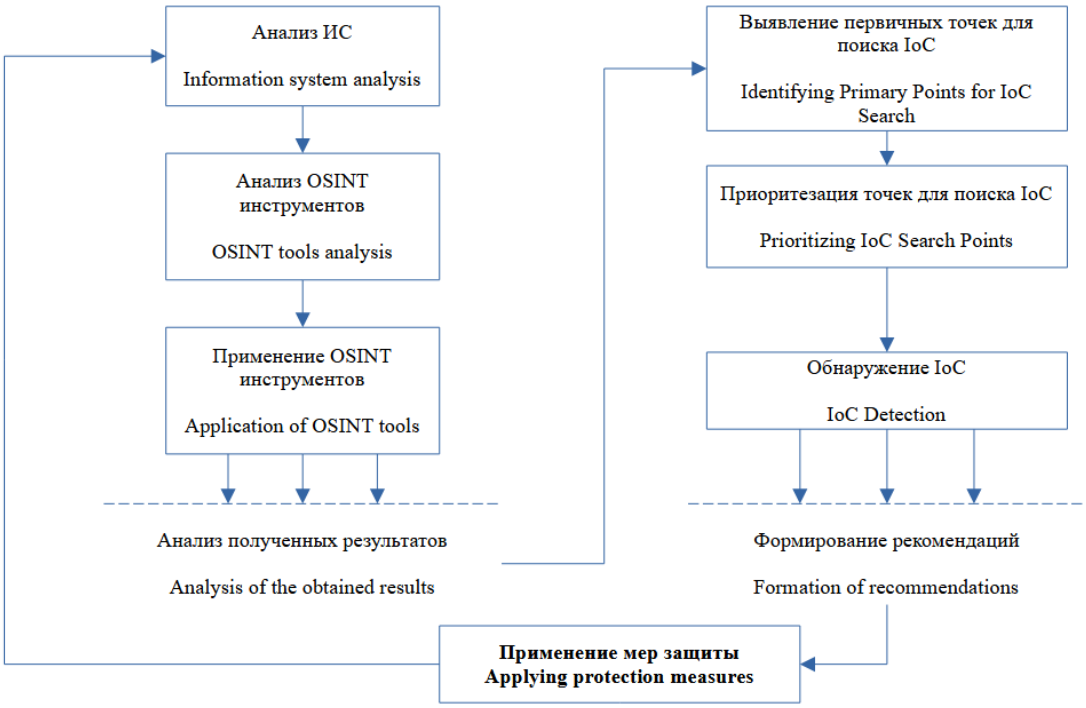


Рисунок 2 – Схема алгоритма применения технологии OSINT для поиска точек входа в целевую ИС для последующего поиска индикаторов компрометации

Представленная схема показывает только основную последовательность этапов и может быть расширена в зависимости от сложности объекта исследования.

ЭКСПЕРИМЕНТ ПО ПРИМЕНЕНИЮ АЛГОРИТМА

В рамках проводимого эксперимента рассматривалась информационная система компании, относящейся к топливно-энергетическому комплексу – субъект КИИ без значимых объектов. В ней присутствуют несколько филиалов, почтовый сервер, сервера хранения данных, DNS-сервер, DHCP-сервер, сервер контроллера домена, веб-сервера, сервера виртуальных машин, терминальные сервера приложений, менеджер паролей и сервер, на котором развернут Kaspersky Security Center. Между главным офисом организации и ее филиалами организованы VPN-туннели. Действующий веб-сайт организации расположен на хостинге, при этом существуют старые незакрытые версии веб-сайтов, которые расположены на веб-серверах внутри инфраструктуры организации.

Применение предложенного алгоритма позволило определить дополнительные факторы, полученные после запуска выбранных инструментов OSINT. По результатам применения OSINT инструментов на объекте были выявлены потенциальные точки входа в информационную инфраструктуру объекта: открытые порты с установленными на них сервисами и их версиями; скомпрометированные учетные данные.

Возможными точками входа в информационную систему могут быть подобранные под определенные приложения и сервисы уязвимости, эксплуатация которых может привести к НСД к целевой системе.

Все результаты приоритезированы в соответствием критичности их влияния на бизнес-процессы организации. Рассмотрены и определены тактики и техники злоумышленников. Полученные данные дали возможность определить и существенно сузить круг начальных точек для сканирования и поиска индикаторов компрометации.

Кроме того, на основе полученной в ходе исследования внешнего периметра информационной инфраструктуры информации сформированы рекомендации для снижения рисков информационной безопасности.

ЗАКЛЮЧЕНИЕ

Анализируя общепринятые способы поиска индикаторов компрометации, примеры индикаторов компрометации, практики поиска индикаторов компрометации от различных поставщиков услуг российского рынка информационной безопасности, стало понятно, что единой методики

обнаружения индикаторов компрометации не существует. При обнаружении индикаторов компрометации возникает проблема определения начальных точек для поиска индикаторов компрометации. Требуется дополнительная информация, которая поможет сузить поиск. При этом информация должна быть не внутренняя, а та, которая «видна» вне периметра организации. В таком случае весьма эффективным должен оказаться принцип поиска информации из открытых источников, заложенный в методологии OSINT.

Предложенное решение в виде алгоритма встраивания технологии OSINT в процесс поиска индикаторов компрометации, на этапе определения начальных точек сканирования системы, показало свою эффективность.

Список источников

1. Мещеряков, Р. В. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем / Р. В. Мещеряков, С. Ю. Исхаков // Вопросы кибербезопасности. – 2022. – № 5 (51). – С. 82–99. – DOI: 10.21681/2311-3456-2022-5-82-99.

2. Дрянных, Ю. Ю. Автоматизация сбора, проверки и загрузки индикаторов компрометации в платформу threat intelligence / Ю. Ю. Дрянных, В. Г. Жуков // Актуальные проблемы авиации и космонавтики : сборник материалов V Международной научно-практической конференции, посвященной Дню космонавтики. В 3-х томах. Красноярск, 08–12 апреля 2019 года / под общ. ред. Ю. Ю. Логинова. – Красноярск : Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», 2019. – Т. 2. – С. 225–227.

3. Патент № 2743619 C1 Российская Федерация, МПК G06F 21/56. Способ и система генерации списка индикаторов компрометации : № 2020126232 ; заявл. 06.08.2020 ; опубл. 20.02.2021 / И. С. Померанцев ; заявитель Общество с ограниченной ответственностью «Группа АйБи ТДС».

4. Свидетельство о государственной регистрации программы для ЭВМ № 2021615340 Российская Федерация. Программный интерфейс взаимодействия с базами индикаторов компрометации : № 2021614652 ; заявл. 06.04.2021 ; опубл. 06.04.2021 / А. Д. Бершадский, О. А. Суслов ; заявитель Общество с ограниченной ответственностью «Современные технологии».

5. IoCs / Индикаторы компрометации / Indicators of Compromise. – URL: https://www.securityvision.ru /blog/indikatory-komprometatsii/ (дата обращения: 02.09.2024).

6. Активный поиск угроз (охота на угрозы, threat hunting). – URL: https://encyclopedia. kaspersky.ru/glossary/threat-hunting/ (дата обращения 03.09.2024).

7. Threat intelligence (данные о киберугрозах). – URL: https://encyclopedia.kaspersky.ru/glossary /threat-intelligence/ (дата обращения: 03.09.2024).

8. Сидорова, М. Е. Разведка по открытым источникам данных и ее применение для решения задач кибербезопасности / М. Е. Сидорова, А. Р. Кузьмин // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2023. – № 1. – С. 61–74. – DOI: 10.18137/RNU.V9187.23.01.P.61.

9. Шаханова, М. В. Выявление событий информационной безопасности с помощью индикаторов компрометации / М. В. Шаханова, Е. В. Лутов, Э. С. Шаханова // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7, № 3–3 (25). – С. 59–64.

10. Мельшиян, М. А. Автоматизация процесса сбора информации с применением методов OSINT при проведении аудита информационной безопасности / М. А. Мельшиян, А. О. Брюшинин, А. В. Душкин, С. С. Кочедыков // Актуальные проблемы прикладной математики, информатики и механики : сборник трудов Международной научной конференции, Воронеж, 13–15 декабря 2021 года. – Воронеж : Общество с ограниченной ответственностью «Вэлборн», 2022. – С. 958–965.

11. Веревкин, С. А. Сравнительный анализ баз данных MITRE ATT&CK и CAPEC / С. А. Веревкин, Е. В. Федорченко // Известия Тульского государственного университета. Технические науки. – 2023. – № 4. – С. 29–39. – DOI: 10.24412/2071-6168-2023-4-29-39.

References

1. Meshcheryakov, R. V., Meshcheryakov, R. V., Iskhakov, S. Yu. Study of indicators of compromise for means of protecting information and cyber-physical systems. *Cybersecurity Issues*, 2022, no. 5 (51), pp. 82–99. DOI: 10.21681 /2311-3456-2022-5-82-99 (In Russ.).

2. Dryannykh, Yu. Yu., Zhukov, V. G. Automation of collection, verification and loading of indicators of compromise into the threat intelligence platform. *Actual problems of aviation and cosmonautics: collection of materials of the V International scientific and practical conference dedicated to Cosmonautics Day. In 3 vol. Krasnoyarsk, April 08–12, 2019. By the general editorship of Yu. Yu. Loginov.* Krasnoyarsk: Federal State Budgetary Educational Institution of Higher Education "Siberian State University of Science and Technology named after Academician M.F. Reshetnev", 2019, vol. 2, pp. 225–227 (In Russ.).

3. *Patent No. 2743619 C1 Russian Federation, IPC G06F 21/56. Method and system for generating a list of indicators of compromise* : no. 2020126232 : decl. 06.08.2020 ; publ. 20.02.2021. I. S. Pomerantsev ; applicant Limited Liability Company “IB TDS Group” (In Russ.).

4. *Certificate of state registration of a computer program no. 2021615340 Russian Federation. Software interface for interaction with indicator of compromise databases* : no. 2021614652 ; decl. 06.04.2021 ; publ. 06.04.2021. A. D. Bershadsky, O. A. Suslov ; applicant Limited Liability Company “Modern Technologies” (In Russ.).

5. *IoCs / Indicators of Compromise.* Available at: https://www.securityvision.ru/blog/indikatory-komprometatsii/ (accessed 02.09.2024) (In Russ.).

6. *Active threat hunting.* Available at: https://encyclopedia.kaspersky.ru/glossary/threat-hunting/ (accessed 03.09.2024) (In Russ.).

7. *Threat intelligence (data on cyber threats).* Available at: https://encyclopedia.kaspersky.ru/glossary/threat-intelligence/ (accessed 09.03.2024) (In Russ.).

8. Sidorova, M. E., Sidorova, M. E., Kuzmin, A. R. Intelligence from open data sources and its application to solving cybersecurity problems. *Bulletin of the Russian New University. Series: Complex systems: models, analysis and mana-gement*, 2023, no. 1, pp. 61–74. DOI: 10.18137/RNU.V9187.23.01.P.61 (In Russ.).

9. Shakhanova, M. V., Lutov, E. V., Shakhanova, E. S. Identification of information security events using indicators of compromise. *International Journal of Information Technology and Energy Efficiency*, 2022, vol. 7, no. 3–3 (25), pp. 59–64 (In Russ.).

10. Melshiyan, M. A., Bryushinin, A. O., Dushkin, A. V., Kochedykov, S. S. Automation of the information collection process using OSINT methods during an information security audit. *Actual problems of applied mathematics, computer science and mechanics: Collection of works of the International scientific conference, Voronezh, December 13–15, 2021.* Voronezh, Limited Liability Company "Velborn", 2022, pp. 958–965 (In Russ.).

11. Verevkin, S. A., Fedorchenko, E. V. Comparative analysis of MITRE ATT&CK and CAPEC databases. *Bulletin of Tula State University. Technical sciences*, 2023, no. 4, pp. 29–39. DOI: 10.24412/2071-6168-2023-4-29-39 (In Russ.).

Статья поступила в редакцию 04.09.2024; одобрена после рецензирования 23.09.2024; принята к публикации 24.09.2024.

The article was submitted 04.09.2024; approved after reviewing 23.09.2024; accepted for publication 24.09.2024.

УДК 004.056+614.2+342.9

ЗАКОНОДАТЕЛЬНЫЕ АСПЕКТЫ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ: ОСНОВНЫЕ ПОЛОЖЕНИЯ И ТРЕБОВАНИЯ ЗАЩИТЫ ДАННЫХ

Ржевская Наталья Витальевна, Северо-Кавказский Федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,

аспирант кафедры вычислительной математики и кибернетики, ORCID: 0009-0002-1285-4196, e-mail: natalia070901@gmail.com

Лапина Мария Анатольевна, Северо-Кавказский Федеральный университет, 355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1,

доцент кафедры вычислительной математики и кибернетики, ORCID: 0000-0001-8117-9142, e-mail: mlapina@ncfu.ru

Лапин Виталий Геннадьевич, Ставропольский краевой клинический консультативно-диагностический центр, 355000, Российская Федерация, г. Ставрополь, ул. Ленина, 304,

начальник отдела АСУ, ORCID: 0000-0002-0611-7002, e-mail: vitlx@yandex.ru

Современное развитие здравоохранения требует детального правового регулирования вопросов применения информационных технологий для обеспечения безопасности и качества оказания медицинских услуг. Целью данного исследования является анализ правовой регламентации электронного здравоохранения на основе российского и международного законодательства с точки зрения защиты данных. При проведении анализа были использованы следующие методы исследования: системно-структурный метод анализа нормативно-правовой базы, включая федеральное законодательство Российской Федерации, акты правительственного уровня, а также международные документы и стандарты, регулирующие цифровое взаимодействие в здравоохранении. Источники правовых актов отбирались с учетом их актуальности и признанности на международном уровне, а также значимости для регулирования электронного здравоохранения. В результате исследования будут определены основные положения и требования к правовому регулированию электронного здравоохранения, включая анализ российского и международного законодательства. Выявлены ключевые нормы и направления для обеспечения безопасности данных и эффективного оказания цифровых медицинских услуг.

Ключевые слова: электронное здравоохранение, правовое регулирование, телемедицинские технологии, нормативные акты, цифровые медицинские услуги, защита данных, безопасность данных

LEGISLATIVE ASPECTS OF E-HEALTH: BASIC PROVISIONS AND DATA PROTECTION REQUIREMENTS

Rzhevskaya Natal'ya V., North Caucasus Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

graduate student of the Department of Computational Mathematics and Cybernetics, ORCID: 0009-0002-1285-4196, e-mail: natalia070901@gmail.com

Lapina Maria A., North Caucasus Federal University, 1 Pushkin St., Stavropol, 355017, Russian Federation,

Associate Professor of the Department of Computational Mathematics and Cybernetics, ORCID: 0000-0001-8117-9142, e-mail: mlapina@ncfu.ru

Lapin Vitaly G., Stavropol Regional Clinical Consulting and Diagnostic Center, 304 Lenin St., Stavropol, 355000, Russian Federation,

Head of the Automated Control System Department, ORCID: 0000-0002-0611-7002, e-mail: vitlx@yandex.ru

The modern development of healthcare requires detailed legal regulation of the use of information technologies to ensure the safety and quality of medical services. The purpose of this study is to analyze the legal regulation of e-health based on Russian and international legislation from the point of view of data protection. The following research methods were used in the analysis: a system-structural method for analyzing the regulatory framework, including federal legislation of the Russian Federation, acts of the government level, as well as international documents and standards governing digital interaction in healthcare. The sources of legal acts were selected taking into account their relevance and recognition at the international level, as well as their importance for the regulation of e-health. As a result of the study, the main provisions and requirements for legal regulation will be determined. The key norms and directions for ensuring data security and effective provision of digital medical services have been identified.

Keywords: e-health, legal regulation, telemedicine technologies, regulations, digital medical services, data protection, data security

ВВЕДЕНИЕ

Электронное здравоохранение (далее – ЭЗ, eHealth) сегодня становится неотъемлемой частью современной медицины, обеспечивая доступность, оперативность и качество медицинской помощи благодаря использованию информационных технологий. Развитие телемедицины, электронных медицинских карт, автоматизированных систем учета и дистанционного мониторинга позволяет повысить эффективность оказания услуг и улучшить качество медицинского обслуживания. В то же время активное внедрение цифровых технологий требует точного правового регулирования для защиты персональных данных пациентов, соблюдения стандартов качества медицинской помощи и предотвращения правовых рисков.

В статье проводится анализ нормативных актов, регулирующих электронное здравоохранение, с целью выявления основных положений и требований в сфере безопасности и конфиденциальности данных. Особое внимание уделено российским и международным правовым актам, которые определяют основные принципы защиты данных и регламентацию оказания медицинской помощи с применением цифровых технологий.

РЕГУЛИРОВАНИЕ ЗАЩИТЫ ЭЛЕКТРОННОГО ЗДРАВООХРАНЕНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Согласно требованиям Свода правил 158.13330.2014 [1], анализируя пункт 7.6.11, системы телемедицины должны устанавливаться в крупных медицинских центрах и удаленных организациях в специально оборудованных помещениях, обеспечивая трансляцию и обработку видеопотоков, аудиопотока, биометрических данных и медицинской информации в реальном времени. Эти системы должны включать современные технологии для сбора, обработки, хранения и передачи данных от различных источников, обеспечивать быстрый доступ к архивам по цифровым протоколам, компиляцию изображений и возможность обмена данными с медицинской информационной системой (МИС).

Уязвимость медицинских данных должна быть учтена при создании единого информационного пространства здравоохранения. При этом должна быть составлена модель защиты прав пациента, закрепленной законодательно, а также определены полномочия при обмене информацией между субъектами этой системы. При обеспечении информационной безопасности в медицинской сфере необходимо руководствоваться тремя принципами: целостностью, доступностью и конфиденциальностью [2, 4].

Электронное здравоохранение в России регулируется рядом законов и подзаконных актов, которые определяют правовые основы и механизмы реализации телемедицинских технологий. Изучение использования телемедицинских технологий невозможно без учета анализа обеспечения конфиденциальности персональных данных пациентов. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [5] регулирует вопросы обработки и защиты персональных данных, что особенно актуально в контексте электронного здравоохранения, где часто обрабатываются конфиденциальные данные пациентов. Закон обязывает медицинские организации обеспечивать защиту таких данных, а также устанавливает требования к их обработке.

В соответствии с нормативной документацией Российской Федерации, персональная медицинская информация признается особой категорией персональных данных, что говорит о том, что ее необходимо эксплуатировать, соблюдая определенные требования. Соблюдая данные требования, такая информация должна храниться на более высоком уровне. Утечка таких данных потенциально угрожает субъектам персональных данных, а обработка вышеупомянутой информации допускается только в определенных случаях. При этом необходимо соблюдать условие, что обработкой персональных данных занимается лицо, осуществляющее медицинскую деятельность и обязанное в соответствии с законодательством Российской Федерации соблюдать медицинскую тайну [9]. Так как информация, относящаяся к врачебной тайне, является конфиденциальной и такие персональные данные (ПДн) относятся к специальной и (или) биометрической категориям ПДн, то, согласно Приказу ФСТЭК России № 21 [6], такие информационные системы персональных данных относятся не ниже чем к третьему уровню защищенности персональных данных, в зависимости от категории обработки ПДн. Для данных системы необходимо придерживаться требований к мерам защиты информации.

Таким образом, использование телемедицинских технологий приводит к росту ответственности медицинских учреждений за обработку данных [3]. Однако отсутствие специальных норм, касающихся ответственности операторов персональных данных при предоставлении телемедицинских услуг, позволяет учреждениям передавать эту задачу третьим лицам, что влечет за собой увеличение риска утечки информации.

Так как электронное здравоохранение в первую очередь обрабатывает медицинские данные, то анализ данной области невозможен без рассмотрения Федерального закона от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». Этот закон является основополагающим в сфере здравоохранения и устанавливает права и обязанности граждан, медицинских работников и организаций. В частности, он определяет право граждан на получение медицинской помощи с использованием телемедицинских технологий.

Стоит отметить, что российское законодательство в качестве отсылки к электронному здравоохранению в основном использует такие слова, как цифровизация здравоохранения, телемедицина, телемедицинские технологии и т. д. Хотя данные определения и относятся к ЭЗ, но не отражают целостности данной технологии, уделяют внимание регулированию ее отдельных компонентов.

Полагаясь на Методические рекомендации № 2003/46, утвержденные Минздравом РФ [11] на момент публикации документа (17.04.2003), в Российской Федерации отсутствовали официальные документы, регламентирующие конфиденциальность данных при применении телемедицинских технологий. В этом же документе акцентировалось внимание, что такой ход вещей частично нарушает понятие врачебной тайны. Также на сегодняшний момент нет сформулированных мер наказания за нарушения правил обработки данных именно с применением электронного здравоохранения. Оценить регулирование данного вопроса можно только косвенно на основе отсылок к смежным нормативно-правовым документам, регулирующим вопросы обработки ПДн и защиты прав граждан при обращении в медицинские организации.

В вышеупомянутой методической рекомендации впервые были определены понятия и общие требования к защите медицинской информации при телемедицинских консультациях, также были описаны основные условия защиты информации, полученной в ходе такой консультации.

В документе была представлена формула метода обеспечения ИБ в телемедицине. Авторы НПА выделяют три основные меры защиты медицинской информации при телемедицинских консультациях: организационно-методические, технические и правовые.

В качестве мер рзащиты выделяются аутентификация пользователей, управление доступом, использование электронных цифровых подписей и шифрование данных. В документе подчеркивается важность регламентации условий доступа к информации и обязанностей сотрудников, что способствует снижению рисков несанкционированного доступа и утечек данных.

Организационно-методические меры защиты данных, предложенные в рекомендации, включают в себя необходимые документы для обеспечения информационной безопасности, такие как должностные инструкции, права доступа и процедуры идентификации пользователей. Важное внимание уделяется обучению персонала, чтобы повысить уровень безопасности и снизить риски.

В разделе 3.3 документа [11] рассматриваются программно-аппаратные средства для защиты информации, включая системы аутентификации, фильтрации трафика и резервного копирования данных. Основные причины нарушения информационной безопасности при проведении телемедицинских консультаций представлены на рисунке 1.

Статья 36.2 (далее ст.) п. 5 ФЗ-323 гласит: «Применение телемедицинских технологий при оказании медицинской помощи осуществляется с соблюдением требований, установленных законодательством Российской Федерации в области персональных данных, и соблюдением врачебной тайны» [9]. Формулировка данной статьи ссылает исследователей данного вопроса на основные требования защиты персональных данных, регламентированных в ФЗ-152 и ФЗ-323.

Приказ Минздрава России от 27 декабря 2019 г. № 965н «Об утверждении порядка организации оказания медицинской помощи с использованием телемедицинских технологий» [10] детализирует порядок оказания медицинских услуг с применением телемедицинских технологий, описывает необходимые условия и требования к организации таких услуг, а также права и обязанности участников процесса.

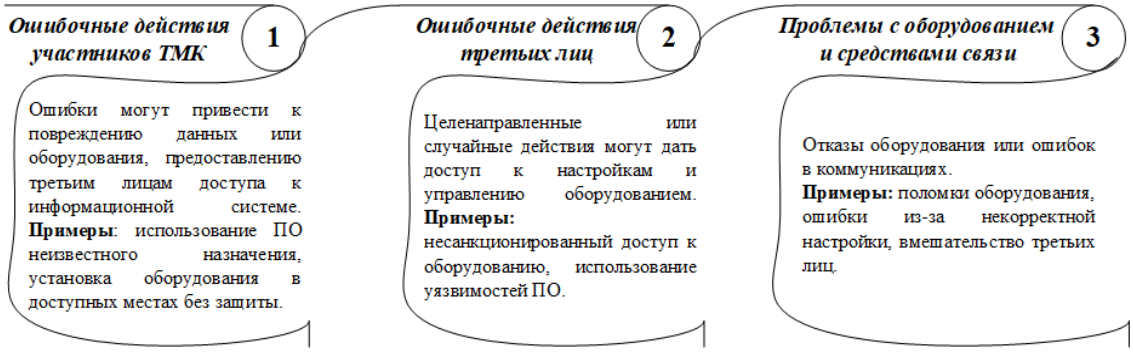


Рисунок 1 – Ключевые причины компрометации информационной безопасности в процессе ТМК

В качестве методов защиты данных, полученных в ходе телемедицинских сеансов, согласно вышеупомянутых законов, выступают единая система идентификации и аутентификации (далее – ЕСИА) (п. 6, ст. 36.2 [9], п. 7, гл. 2 [9]) и использование усиленной квалифицированной электронной подписи медицинского работника (п. 6 ст. 36.2 [9], п. 57, гл. 11 [10]).

Также в законодательстве Российской Федерации четко регламентировано, что оказание медицинской помощи с применением телемедицинских технологий могут осуществлять только медицинские работники, сведения о которых внесены в Федеральный регистр медицинских работников, а также при условии регистрации соответствующих медицинских организаций в Федеральном реестре медицинских организаций Единой государственной информационной системы в сфере здравоохранения (далее – Единая система).

Стоит отметить, что при проведении таких консультаций необходимо использовать Единую систему, а также государственные информационные системы в сфере здравоохранения субъекта Российской Федерации или медицинские информационные системы медицинской организации. В приказе [10] также разрешается использование иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг (далее – иные информационные системы).

Консультации и (или) консилиумы врачей при оказании медицинской помощи с применением телемедицинских технологий проводятся в режиме реального времени и (или) отложенных консультаций, что также необходимо учитывать в качестве потенциальной точки проникновения для злоумышленника.

В главе 8 приказа [10] описывается порядок проведения консультаций с применением телемедицинских технологий. При этом четко описаны этапы передачи данных от лечащего врача к консультанту. В п. 46 описан большой список ПДн, которые обрабатываются при телемедицинской консультации.

Стоит обратить внимание, что в этом же приказе нет четкой регламентации защиты данных при передаче. Именно поэтому руководствоваться данным приказом стоит комплексно с другими нормативными актами для предотвращения кражи или утечки ПДн.

Проводя анализ Постановления Правительства РФ № 1164 от 18.07.2023 [12], можно выделить некоторые требования к медицинским информационным системам. Так, конкретные требования к скорости соединения и разрешению видеокамеры направлены на обеспечение качества и безопасности данных при видеоконференц-связи, минимизируя риски потери или искажения информации в процессе передачи. В п. 4 гл. 2 закреплен обязательный порядок оформления согласия на обработку персональных данных, что отражает требования закона о защите данных и гарантирует безопасность персональной информации пациентов.

В данной программе (п. 20, 21) устанавливаются требования к субъектам экспериментального правового режима для телемедицины, включая наличие медицинской лицензии, использование информационных систем, соответствующих государственным стандартам, и выполнение внутреннего контроля качества. Для подтверждения соответствия необходимо представить заверенные документы, такие как копии лицензии, положения о внутреннем контроле, правила проведения консультаций с перечнем противопоказаний и данные об используемом сертифицированном программном обеспечении. В данном случае Министерство здравоохранения Российской Федерации выступает федеральным органом, ответственным за формирование государственной политики и нормативное правовое регулирование в рамках экспериментального правового режима.

Дополнением к вышеуказанным нормативно-правовым актам (НПА) выступает Письмо Минздрава России от 09.04.2018 № 18-2/0579 [13], касающееся организации телемедицинской помощи. Данное письмо не выдвигает специфических требований к ИБ в телемедицине, кроме общей привязки к использованию ЕСИА для идентификации и аутентификации участников.

Дополнительные требования к методам построения МИС и обеспечения безопасности обработки данных представлены в документах [14–17], которые также необходимо учитывать при комплексной анализе нормативно-правовой базы в области электронного здравоохранения.

Не стоит забывать и о смежных НПА, регламентирующих данное направление. Согласно Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [7], фактически все медицинские организации являются субъектами критической информационной инфраструктуры. Также в соответствии с Постановлением Правительства РФ № 127 [8] можно сказать, что организации здравоохранения относятся к категориям значимой критической информационной инфраструктуры. Полагаясь на это, согласно требованиям законодательства РФ, для реализации итогового набора мер должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности

в формах сертификации, а также данные средства должны соответствовать классу защиты. Сертифицированные СрЗИ и используемые средства вычислительной техники должны подбираться в соответствии с категорией значимости объектов КИИ.

Существует обширное законодательное поле (рис. 2), требующее, чтобы медицинские учреждения, как частные, так и государственные, обеспечивали защиту медицинской информации своих пациентов. Эти законы предписывают, что персональные данные, в том числе медицинские, должны быть защищены соответствующими мерами безопасности, такими как шифрование, контроль доступа и т. д.

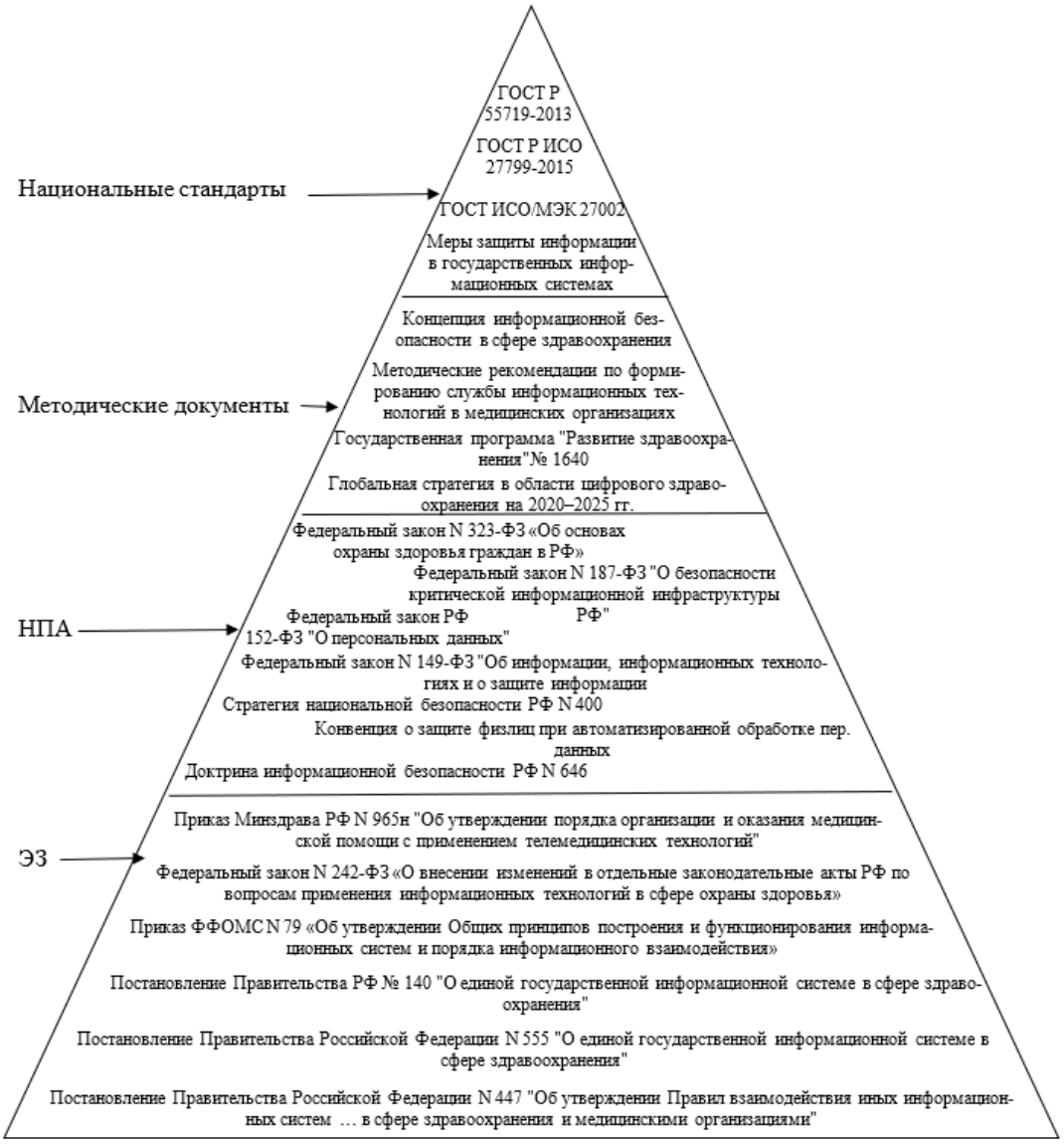


Рисунок 2 – Нормативно-правовая база (НПБ) исследуемой области

На сегодняшний момент имеется огромная нормативная база как в области обеспечения информационной безопасности, так и электронного здравоохранения в целом.

Данные нормативные документы являются базовыми в области обеспечения защиты персональных данных. Необходимо отметить, что при комплексной защите персональных данных в области здравоохранения необходимо, также учитывать другие правовые документы по данному вопросу.

МЕЖДУНАРОДНАЯ ПРАКТИКА РЕГУЛИРОВАНИЯ E-HEALTH

Всемирная организация здравоохранения отмечает, что внедрение электронной системы здравоохранения приведет к укреплению этой области. Это может способствовать реализации основных прав человека путем улучшения справедливости, солидарности, качества жизни и уровня медицинской помощи.

В отличие от российской практики, где понятие электронного здравоохранения не закреплено в документации, но подразумевается под другими определениями, такими как телемедицина и цифровизация здоровья, в англоязычных странах и других регионах термин «электронное здравоохранение» (e-health) имеет четкое определение в нормативно-правовых документах.

Зарубежный опыт телемедицины, особенно в США, демонстрирует высокие стандарты и требования к безопасности данных пациентов. Министерство здравоохранения и социальных служб США (HHS) определяет телемедицину как использование технологий для медицинской помощи и управления здравоохранением на расстоянии.

Так же как и в Российском законодательстве, ключевым моментом при обеспечении защиты данных пациентов с применением электронного здравоохранения становится защита персональных данных.

В США законодательство в области электронного здравоохранения (e-health) строится вокруг HIPAA [31] (Закон о переносимости и подотчетности медицинского страхования) и HITECH (Закон о здоровье и информационных технологиях).

Требования HIPAA обеспечивают защиту личной информации пациентов, установив национальные стандарты конфиденциальности и безопасности. Правило конфиденциальности HIPAA регулирует защиту данных пациентов, предоставляя им права на доступ, исправление и контроль использования их информации.

Правило безопасности данного закона предписывает меры для защиты электронных медицинских записей, разделяя их на три категории:

– административные меры: управление политиками безопасности, аудит и подготовка персонала;

– технические меры: шифрование данных, управление доступом и аутентификация;

– физические меры: защита оборудования и помещений.

В свою очередь, HITECH расширяет требования HIPAA для электронных записей, стимулируя внедрение электронных систем управления данными и усиливая ответственность за утечки и нарушение безопасности.

Анализируя опыт внедрения электронного здравоохранения в европейских странах, на примере опыта Эстонии и Франции также можно выделить несколько особенностей [32–33].

Так, в Эстонии создана централизованная система управления медицинскими данными, обеспечивающая безопасный обмен данными между учреждениями. В России же, несмотря на попытки внедрения единой системы, недостаточная стандартизация и согласованность данных остаются актуальной проблемой. Российская система телемедицины пока что менее интегрирована на национальном уровне, что усложняет обмен данными и делает их защиту более сложной задачей.

Кроме того, эстонская система регулирует телемедицину через четко определенные нормативные акты и стандарты ЕС, включая централизованные информационные системы и проектные решения для защиты данных пациентов.

Во Франции законодательство в этой области начало формироваться с 2009 г., когда был введен Закон № 2009-879. Статья 78 данного закона определила первое понятие электронного здравоохранения в стране.

Значимым шагом стало принятие Указа в 2010 г., который определил пять ключевых действий в телемедицине, таких как телеконсультация и теленаблюдение. В 2018 г. телемедицина получила новые возможности, обеспечивая удаленный доступ пациентов к врачам, что улучшает качество медицинской помощи и экономит ресурсы.

Однако проблема защиты информации остается актуальной и по сей день. Различные директивы ЕС конкретно очерчивают требования к защите данных в телемедицине. Однако в свете смягчений правил использования телемедицины, введенных в ковидное время, создает вызов для соблюдения GDPR и требует развития внутренних актов о защите данных пациентов.

ЗАКЛЮЧЕНИЕ

Регламентация использования электронных технологий в здравоохранении подробно отражена в российском законодательстве. Конституция Российской Федерации и Федеральный закон № 323-ФЗ [9] закрепляют основные положения о праве граждан на охрану здоровья и использовании цифровых технологий в оказании медицинской помощи. Проанализировав всю нормативно-правовую базу, можно сделать вывод о сложности и многоуровневости национальной нормативно-правовой базы в области персональных данных, охраны здоровья и критической информационной инфраструктуры, а также электронного здравоохранения в целом. Часть таких НПА представлена в таблице.

Таблица – Нормативно-правовая база Российской Федерации в области электронного здравоохранения

№	Наименование документа	Описание
Описание нормативно-правовой базы в области персональных данных		
1.	Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»	Регулирует отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами госвласти и т. д.
2.	Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Регулирует вопросы, связанные с обработкой и защитой информации, использованием информационных технологий и установлением механизмов обеспечения информационной безопасности.
3.	Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»	Устанавливает требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».
4.	Конвенция о защите физических лиц при автоматизированной обработке персональных данных	Регулирует вопросы, связанные с защитой прав и свобод физических лиц в отношении их персональных данных, которые обрабатываются с использованием автоматизированных средств.
5.	Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646	Регулирует основные принципы и подходы к обеспечению безопасности информационных систем, защите информации, предотвращению и противодействию угрозам в киберпространстве, а также определяет правовые и организационные механизмы по обеспечению информационной безопасности.
Описание нормативно-правовой базы в области охраны здоровья и критической информационной инфраструктуры		
1.	Федеральный закон от 21.11.2011 № 323-ФЗ (ред. от 24.07.2023) «Об основах охраны здоровья граждан в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2023)	Определяет механизмы и принципы обеспечения медицинской помощи, контроля за качеством медицинских услуг, защиту прав пациентов, организацию медицинских учреждений и другие аспекты, направленные на поддержание и улучшение здоровья населения
2.	Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400	Регулирует основные направления и приоритеты государственной политики национальной безопасности России.
3.	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	Регулирует вопросы обеспечения защиты критической информационной инфраструктуры от угроз и воздействий, обеспечения устойчивого функционирования, защиты прав и законных интересов граждан, охраны государственных и коммерческих секретов, а также содействия в развитии международного сотрудничества в области обеспечения информационной безопасности.
4.	ГОСТ Р 55719-2013 «Изделия медицинские электрические. Требования к содержанию и оформлению технических заданий для конкурсной документации при проведении государственных закупок высокотехнологичного медицинского оборудования»	Регулирует требования к содержанию и оформлению технических заданий для конкурсной документации при проведении государственных закупок высокотехнологичного медицинского оборудования.
5.	Приказ ФФОМС от 07.04.2011 N 79 "Об утверждении Общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования"	Регулирует основные принципы организации и использования информационных систем, а также устанавливает порядок обмена информацией в сфере обязательного медицинского страхования.

Продолжение таблицы

Описание нормативно-правовой базы в области электронного здравоохранения в целом		
1.	ГОСТ Р ИСО 27799-2015	Предназначено для медицинских организаций и других хранителей персональной медицинской информации, чтобы помочь им эффективно защитить конфиденциальность, целостность и доступность этой информации путем внедрения ИСО/МЭК 27002.
2.	Постановление Правительства РФ от 9 февраля 2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения»	Регулирует установление и функционирование централизованной информационной системы, обеспечивающей оперативную обработку и анализ медицинских данных для улучшения качества и эффективности здравоохранения.
3.	Концепция информационной безопасности в сфере здравоохранения	Определяет правила и принципы, регулирующие обработку, хранение и передачу информации в системах здравоохранения с целью обеспечения ее конфиденциальности, целостности и доступности.
4.	Глобальная стратегия в области цифрового здравоохранения на 2020–2025 гг.	Представляет цель, задачи и план действий для обеспечения развития и применения цифровых технологий в здравоохранении.
5.	Указ Президента РФ № 254 от 07.06.2019 «О Стратегии развития здравоохранения в Российской Федерации на период до 2025 года»	Регулирует основные приоритеты и меры в сфере здравоохранения в целях улучшения качества и доступности медицинских услуг для граждан России в ближайшие пять лет.
6.	Государственная программа «Развитие здравоохранения», утверждена постановлением Правительства от 26.12.2017 г. № 1640	Регулирует меры и приоритетные направления развития системы здравоохранения в стране.
7.	Методические рекомендации по формированию службы информационных технологий в медицинских организациях (утв. ФГБУ «ЦНИИОИЗ» Министерства здравоохранения РФ 4 марта 2022 г.)	Представлены методические рекомендации по формированию в медицинской организации службы информационных технологий, предназначенной для обеспечения работоспособности, развития и модернизации информационных технологий и соответствующей инфраструктуры, интегрированных с единым цифровым контуром в здравоохранении

Такая обширная и детализированная правовая база позволяет обеспечить взаимодействие различных участников и обеспечить более высокий уровень безопасности и качества медицинских услуг.

Международный опыт в защите данных в электронном здравоохранении варьируется и включает разные меры для защиты конфиденциальности пациентов. Нормативные акты, такие как HIPAA в США, регулируют безопасность данных через административные, технические и физические меры, акцентируя защиту на шифровании, контроле доступа и обучении персонала [19–21]. Финляндия успешно внедрила e-health и e-welfare, подчеркивая безопасность данных [24]. Современные технологии, включая облачные сервисы, блокчейн и ИИ, предлагают новые возможности, но также создают вызовы в кибербезопасности [28–30].

Правовое регулирование электронного здравоохранения, несмотря на значительное развитие, сталкивается с вызовами обеспечения межгосударственной интеграции, формальными требованиями к безопасности данных и технологическим особенностям предоставления цифровых медицинских услуг.

Система правового регулирования электронного здравоохранения в России основывается на федеральных актах, основополагающих стандартах международного права и нормативных документах, что обеспечивает возможность гармонизации и актуализации нормативной базы для цифровых медицинских технологий.

В большинстве стран термины, связанные с электронным здравоохранением, не закреплены законодательно, что может создать потенциальные проблемы с регулированием мер защиты данных в этой области. Именно поэтому как в Российской Федерации, так и зарубежом нет четко сформулированных нормативно-правовых актов, которые включают описание всех необходимых мер регулирования информационной безопасности и защиты персональных данных специализированно для электронного здравоохранения. Вместо этого разработаны отдельные документы, регламентирующие ИБ и ЗИ, которые косвенно можно отнести к электронному здравоохранению. Стоит отметить, что необходимость в четких определениях и правилах становится особенно актуальной в условиях роста телемедицинских услуг.

Список источников

1. Здания и помещения медицинских организаций. Правила проектирования: Свод правил СП 158.13330.2014 № 58/пр : [утв. приказом Министерства строительства и жилищно-коммунального хозяйства РФ от 18 февраля 2014 г.] // Гарант. – URL: https://base.garant.ru/70725636/ (дата обращения: 26.10.2024).

2. Kaspersky: Кибербезопасность в здравоохранении: где болезнь, где болезнь роста. – URL: https://www.kaspersky.ru/blog/healthcare-safeguarding-data/4474/.

3. Иванова, А. А. Применение Big Data в сфере здравоохранения: российский и зарубежный опыт / А. А. Иванова // Научные записки молодых исследователей. – 2020. – № 5. – URL: https://cyberleninka.ru /article/n/primenenie-big-data-v-sfere-zdravoohraneniya-rossiyskiy-i-zarubezhnyy-opyt (дата обращения: 01.11.2023).

4. Андриянова, Е. А. Проблемы формирования системы электронного здравоохранения в России / Е. А. Андриянова, Н. В. Гришечкина // Здравоохранение Российской Федерации. – 2012. – № 6. – С. 27–30.

5. Российская Федерация. Законы. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ // Справочно-правовая система «Консультант Плюс». – URL: https://www.consultant.ru/document/cons_doc _LAW_61801/.

6. Российская Федерация. Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» : зарегистрировано в Минюсте России 14.05.2013 № 28375 // Справочно-правовая система «Консультант Плюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_146520/.

7. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 № 187-ФЗ // Справочно-правовая система «Консультант Плюс». – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/.

8. Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

9. Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон РФ от 21 ноября 2011 г. № 323-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_121895 (дата обращения: 22.10.2024).

10. Порядок организации и оказания медицинской помощи с применением телемедицинских технологий: приказ М-ва здравоохранения РФ от 30 ноября 2017 г. № 965н. – URL: http://www.consultant.ru/ document/cons_doc_LAW_287515/?ysclid=l64v8tqrs7989403027 (дата обращения: 22.10.2024).

11. Методические рекомендации № 2003/46 «Конфиденциальность и защита информации при телемедицинских консультациях». – URL: https://login.consultant.ru/link/?req=doc&base=OTN&n=23958&demo=1 (дата обращения: 27.10.2024).

12. Российская Федерация. Постановление Правительства Российской Федерации от 18.07.2023 № 1164 «Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по направлению медицинской деятельности, в том числе с применением телемедицинских технологий и технологий сбора и обработки сведений о состоянии здоровья и диагнозах граждан» // Официальный интернет-портал правовой информации. Официальное опубликование. – URL: http://actual.pravo.gov.ru/content/content.html#pnum=0001202307200023.

13. О разъяснении порядка организации и оказания медицинской помощи с применением телемедицинских технологий: Письмо Министерства здравоохранения РФ от 9 апреля 2018 г. № 18-2/0579 [утв. приказом Министерства здравоохранения РФ] // Гарант. – URL: https://www.garant.ru/products/ipo /prime/doc/71842326/ (дата обращения: 26.10.2024).

14. ГОСТ 34244-2017. Межгосударственный стандарт. Системы телемедицинские. Общие требования безопасности с учетом основных функциональных характеристик к стационарным телемедицинским консультативно-диагностическим центрам // Гарант. – URL: https://base.garant.ru/71881340/ (дата обращения: 26.10.2024).

15. ГОСТ 34243-2017. Межгосударственный стандарт. Системы телемедицинские. Общие требования безопасности с учетом основных функциональных характеристик к мобильным телемедицинским лабораторно-диагностическим комплексам // Гарант. – URL: https://base.garant.ru/71881348/ (дата обращения: 26.10.2024).

16. ГОСТ Р 57092-2016. Национальный стандарт Российской Федерации. Изделия медицинские электрические. Аппаратура для телемедицинских видеоконференций. Технические требования для государственных закупок // Гарант. – URL: https://base.garant.ru/71958568/ (дата обращения: 26.10.2024).

17. Методические рекомендации по обеспечению функциональных возможностей региональных медицинских информационных систем (РМИС) (утв. Министерством здравоохранения РФ 23 июня 2016 г.) // Гарант. – URL: https://base.garant.ru/71498190/ (дата обращения: 26.10.2024).

18. Благодарева, М. С. Правовое регулирование оказания медицинской помощи с применением телемедицинских технологий нормативными актами Российской Федерации / М. С. Благодарева, И. В. Григорьев, С. В. Мартиросян // УРМЖ. – 2022. – № 5. – URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-okazaniya-meditsinskoy-pomoschi-s-primeneniem-telemeditsinskih-tehnologiy-normativnymi-aktami-rossiyskoy (дата обращения: 30.10.2024).

19. Liddick, B. L. Defining HIPAA’s Security Rule Within the COVID-19 Telehealth Era : dis. / B. L. Liddick. – Utica College, 2021.

20. Moore, W. Review of HIPAA, part 1: history, protected health information, and privacy and security rules / W. Moore, S. Frye // Journal of Nuclear Medicine Technology. – 2019. – Vol. 47, № 4. – P. 269–272.

21. A Brief History of Digital Health. – URL: https://medium.com/that-medic-network/a-brief-history-of-digital-health-b238f1f5883c (дата обращения: 01.10.2023).

22. McKeigue, P. M. Relation of incident type 1 dia-betes to recent COVID-19 infection: cohort study using e-health record linkage in Scotland / P. M. McKeigue et al. // Diabetes Care. – 2023. – Vol. 46, № 5. – P. 921–928.

23. Biancone, P. E-health for the future. Managerial perspectives using a multiple case study approach / P. Biancone et al. // Technovation. – 2023. – Vol. 120. – P. 102406.

24. Wind, T. R. The COVID-19 pandemic: The 'black swan'for mental health care and a turning point for e-health / T. R. Wind et al. // Internet interventions. – 2020. – Vol. 20.

25. Tebeje T. H. Applications of e-health to sup-port person-centered health care at the time of COVID-19 pandemic / T. H. Tebeje, J. Klein // Telemedicine and e-Health. – 2021. – Vol. 27, № 2. – P. 150–158.

26. Hossain, N. Factors influencing rural end-users' acceptance of e-health in developing countries: a study on port-able health clinic in Bangladesh / N. Hossain et al. // Telemedicine and e-Health. – 2019. – Vol. 25, № 3. – P. 221–229.

27. Alanezi, F. Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia / F. Alanezi // International Health. – 2021. – Vol. 13, № 5. – P. 456–470.

28. Tagde, P. Blockchain and artificial intelligence technology in e-Health / P. Tagde et al. // Environmental Science and Pollution Research. – 2021. – Vol. 28. – P. 52810–52831.

29. Sivan, R. Security and privacy in cloud-based e-health system / R. Sivan, Z. A. Zukarnain // Symmetry. – 2021. – Vol. 13, № 5. – P. 742

30. Scott, R. E. Global e-health policy: From concept to strategy / R. E. Scott // Telehealth in the developing world. – CRC Press, 2019. – P. 55–67.

31. Закон о переносимости и подотчетности медицинского страхования (HIPAA): Стандарты безопасности и конфиденциальности для защиты информации о здоровье пациентов : [утв. приказом Министерства здравоохранения и социальных служб США от 31 июля 1996 г.] // URL: https://www.govinfo.gov/content/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf (дата обращения: 26.10.2024).

32. Маркарян, А. Э. Защита персональных данных в телемедицине: опыт РОССИИ и США / А. Э. Маркарян // Юриспруденция 2.0: новый взгляд на право. – 2020. – С. 425–430.

33. Новиков, Б. М. Правовое регулирование телемедицины в Эстонии / Б. М. Новиков // Юриспруденция 2.0: новый взгляд на право. – 2020. – С. 431–436.

References

1. Buildings and premises of medical organizations. Design rules: Code of rules SP 158.13330.2014 No. 58/pr: [approved by the order of the Ministry of Construction and Housing and Communal Services of the Russian Federation dated February 18, 2014]. *Garant.* Available at: https://base.garant.ru/70725636/ (accessed 26.10.2024) (In Russ.).

2. *Kaspersky: Cybersecurity in Healthcare: Where is the Disease, Where are the Growing Pains*. Available at: https://www.kaspersky.ru/blog/healthcare-safeguarding-data/4474/ (In Russ.).

3. Ivanova, A. A. Application of Big Data in Healthcare: Russian and Foreign Experience. *Scientific Notes of Young Researchers,* 2020, no. 5. Available at: https://cyberleninka.ru/article/n/primenenie-big-data-v-sfere-zdravoohraneniya-rossiyskiy-i-zarubezhnyy-opyt (accessed 01.11.2023) (In Russ.).

4. Andrianova, E. A., Grishechkina, N. V. Problems of formation of the electronic health care system in Russia. *Healthcare of the Russian Federation*, 2012, no. 6, pp. 27–30 (In Russ.).

5. Russian Federation. Laws. On personal data: Federal Law of July 27, 2006 No. 152-FZ. *Reference and legal system "Consultant Plus".* Available at: https://www.consultant.ru/document/cons_doc_LAW_61801/ (In Russ.).

6. Russian Federation. Order of the FSTEC of Russia dated 18.02.2013 N 21 (as amended on 14.05.2020) "On approval of the Composition and content of organizational and technical measures to ensure the security of personal data when processing them in personal data information systems": Registered in the Ministry of Justice of Russia on 14.05.2013 No. 28375. *Reference and legal system "Consultant Plus".* Available at: https://www.consultant.ru/document/cons_doc_LAW_146520/ (In Russ.).

7. Russian Federation. Laws. On the security of the critical information infrastructure of the Russian Federation federal. Law of July 26, 2017 No. 187-FZ. *Reference and legal system "Consultant Plus".* Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ (In Russ.).

8. *Resolution of the Government of the Russian Federation of February 8, 2018 No. 127 "On approval of the Rules for categorizing critical information infrastructure facilities of the Russian Federation, as well as the list of indicators of significance criteria for critical information infrastructure facilities of the Russian Federation and their values"* (In Russ.).

9. *On the Fundamentals of Protecting the Health of Citizens in the Russian Federation: Federal Law of the Russian Federation of November 21, 2011 No. 323-FZ.* Available at: http://www.consultant.ru/document/cons_doc_LAW_121895 (accessed 22.10.2024) (In Russ.).

10. *The procedure for organizing and providing medical care using telemedicine technologies: order of the Ministry of Health of the Russian Federation dated November 30, 2017 No. 965n.* Available at: http://www.consultant.ru/document /cons_doc_LAW_287515/?ysclid=l64v8tqrs7989403027 (accessed 22.10.2024) (In Russ.).

11. *Methodological recommendations No. 2003/46 "Confidentiality and protection of information during telemedicine consultation".* Available at: https://login.consultant.ru/link/?req=doc&base=OTN&n=23958&demo=1 (accessed 27.10.2024) (In Russ.).

12. Russian Federation. Resolution of the Government of the Russian Federation of July 18, 2023 No. 1164 "On the establishment of an experimental legal regime in the field of digital innovations and approval of the Program for an experimental legal regime in the field of digital innovations in the direction of medical activity, including the use of telemedicine technologies and technologies for collecting and processing information on the health status and diagnoses of citizens". *Official Internet portal of legal information Official publication.* Available at: http://actual.pravo. gov.ru/content/content.html#pnum=0001202307200023 (In Russ.).

13. On clarification of the procedure for organizing and providing medical care using telemedicine technologies: Letter of the Ministry of Health of the Russian Federation dated April 9, 2018 No. 18-2 / 0579 [approved. by order

of the Ministry of Health of the Russian Federation]. *Garant.* Available at: https://www.garant.ru/products/ipo /prime/doc/71842326/ (accessed 26.10.2024) (In Russ.).

14. GOST 34244-2017. Interstate standard. Telemedicine systems. General safety requirements, taking into account the main functional characteristics, for stationary telemedicine consultative and diagnostic centers. *Garant.* Available at: https://base.garant.ru/71881340/ (accessed 26.10.2024) (In Russ.).

15. GOST 34243-2017. Interstate standard. Telemedicine systems. General safety requirements, taking into account the main functional characteristics, for mobile telemedicine laboratory and diagnostic complexes. *Garant.* Available at: https://base.garant.ru/71881348/ (accessed 26.10.2024) (In Russ.).

16. GOST R 57092-2016. National standard of the Russian Federation. Medical electrical products. Equipment for telemedicine videoconferencing. Technical requirements for public procurement. *Garant.* Available at: https://base.garant.ru/71958568/ (accessed 26.10.2024) (In Russ.).

17. Methodological recommendations for ensuring the functionality of regional medical information systems (RMIS) (approved by the Ministry of Health of the Russian Federation on June 23, 2016). *Garant.* Available at: https://base.garant.ru/71498190/ (accessed 26.10.2024) (In Russ.).

18. Blagodareva, M. S., Grigoriev, I. V., Martirosyan, S. V. Legal regulation of the provision of medical care using telemedicine technologies by regulatory acts of the Russian Federation. *URMZh*, 2022, no. 5. Available at: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-okazaniya-meditsinskoy-pomoschi-s-primeneniem-telemeditsinskih-tehnologiy-normativnymi-aktami-rossiyskoy (accessed 30.10.2024) (In Russ.).

19. Liddick, B. L. *Defining HIPAA's Security Rule Within the COVID-19 Telehealth Era : dis.* Utica College, 2021.

20. Moore, W., Frye, S. Review of HIPAA, part 1: history, protected health information, and privacy and security rules. *Journal of Nuclear Medicine Technology*, 2019, vol. 47, no. 4, pp. 269–272.

21. *A Brief History of Digital Health.* Available at: https://medium.com/that-medic-network/a-brief-history-of-digital-health-b238f1f5883c (accessed 01.10.2023).

22. McKeigue, P. M. et al. Relation of incident type 1 diabetes to recent COVID-19 infection: cohort study using e-health record linkage in Scotland. *Diabetes Care*, 2023, vol. 46, no. 5, pp. 921–928.

23. Biancone, P. et al. E-health for the future. Managerial perspectives using a multiple case study approach. *Technovation*, 2023, vol. 120, p. 102406.

24. Wind, T. R. et al. The COVID-19 pandemic: The 'black swan'for mental health care and a turning point for e-health. *Internet interventions*, 2020, vol. 20.

25. Tebeje, T. H., Klein, J. Applications of e-health to support person-centered health care at the time of COVID-19 pan-demic. *Telemedicine and e-Health*, 2021, vol. 27, no. 2, pp. 150–158.

26. Hossain, N. et al. Factors influencing rural end-users' acceptance of e-health in developing countries: a study on port-able health clinic in Bangladesh. *Telemedicine and e-Health*, 2019, vol. 25, no. 3, pp. 221–229.

27. Alanezi, F. Factors affecting the adoption of e-health system in the Kingdom of Saudi Arabia. *International Health*, 2021, vol. 13, no. 5, pp. 456–470.

28. Tagde, P. et al. Blockchain and artificial intelligence technology in e-Health. *Environmental Science and Pollution Research*, 2021, vol. 28, pp. 52810–52831.

29. Sivan, R., Zukarnain, Z. A. Security and privacy in cloud-based e-health system. *Symmetry*, 2021, vol. 13, no. 5, p. 742.

30. Scott, R. E. Global e-health policy: From concept to strategy. *Telehealth in the developing world*. CRC Press, 2019, pp. 55–67.

31. *Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy Standards for Protecting Patient Health Information: [approved by order of the U.S. Department of Health and Human Services dated July 31, 1996]*. URL: https://www.govinfo.gov/content/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf (accessed 26.10.2024) (In Russ.).

32. Markaryan, A. E. Protection of personal data in telemedicine: experience of RUSSIA and the USA. *Jurisprudence 2.0: a new look at the law*, 2020, pp. 425–430 (In Russ.).

33. Novikov, B. M. Legal regulation of telemedicine in Estonia. *Jurisprudence 2.0: a new look at the law*, 2020, pp. 431–436 (In Russ.).

Статья поступила в редакцию 04.12.2024; одобрена после рецензирования 08.12.2024; принята к публикации 09.12.2024.

The article was submitted 04.12.2024; approved after reviewing 08.12.2024; accepted for publication 09.12.2024.

УДК 004.056

РАСЧЕТ КОЭФФИЦИЕНТОВ, ОТРАЖАЮЩИХ СТЕПЕНЬ ВЛИЯНИЯ ВЫПОЛНЕНИЯ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ОЦЕНКИ СООТВЕТСТВИЯ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ

Жукова Марина Николаевна, Сибирский государственный университет науки и технологий, 660037, Российская Федерация, г. Красноярск, пр. им. газ. «Красноярский рабочий», 31,
кандидат технических наук, доцент, ORCID: 0000-0003-3441-3041, e-mail: zhukova@sibsau.ru
Яковлева Анастасия Олеговна, Сибирский государственный университет науки и технологий, 660037, Российская Федерация, г. Красноярск, пр. им. газ. «Красноярский рабочий», 31,
аспирант, ORCID: 0009-0008-7828-0977, e-mail: petrova754@mail.ru

В работе рассмотрена процедура проведения оценки соответствия набора базовых мер защиты информации требованиям уровня защищенности для финансовых организаций. В целях определения параметров, оказывающих влияние на оценку соответствия требованиям к защите информации по ГОСТ Р 57580.2–2018, произведен расчет коэффициентов влияния мер защиты, реализуемых для выполнения требований ГОСТ Р 57580.1–2017. Представлены расчетные формулы, позволяющие получить численное значение для каждого контура защиты информации информационной системы. Применение знаний о весовом коэффициенте для каждой меры даст специалистам возможность принять более эффективное решение в ситуации внесения изменений или доработки инфраструктуры и подготовке к предстоящей процедуре оценки. При условии реализации непрерывного мониторинга за контурами безопасности, которые подлежат оценке, полученные расчеты позволят минимизировать риск получения недостаточной оценки соответствия стандартам информационной безопасности финансовых систем. Полученные результаты предлагается в дальнейшем использовать в практических задачах повышения оценки путем оптимизированного подбора параметров в зависимости от заданных критериев и разности значений текущего и требуемого уровня оценки.

Ключевые слова: финансовая организация, контур защиты информации, расчет оценки соответствия, степень влияния, мера защиты

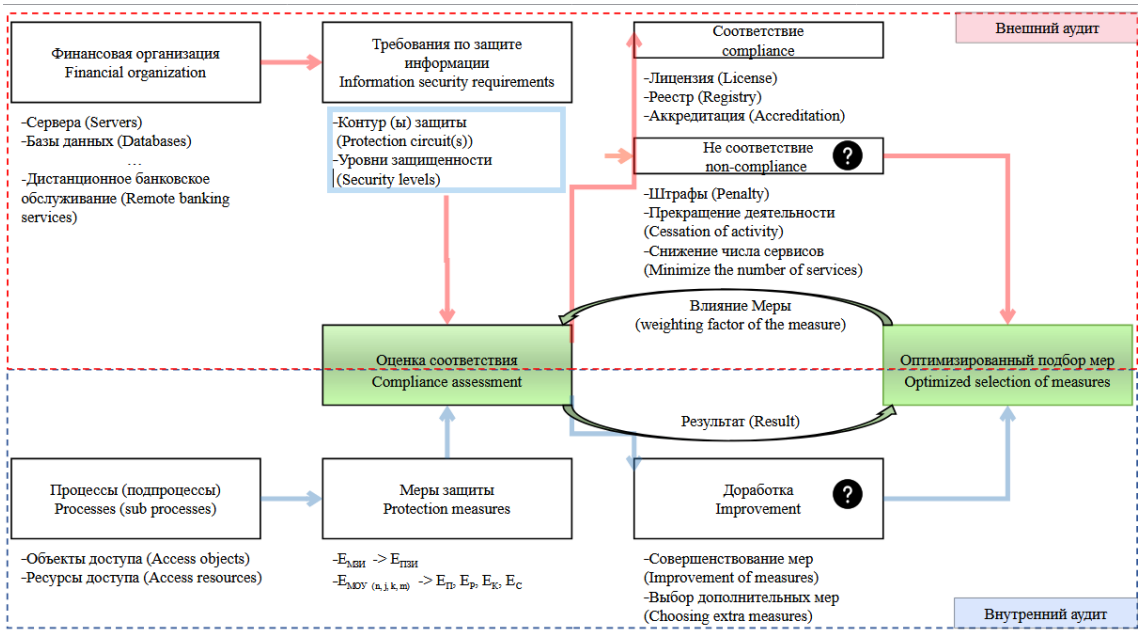
CALCULATION OF COEFFICIENTS REFLECTING THE DEGREE OF INFLUENCE OF THE IMPLEMENTATION OF INFORMATION PROTECTION MEASURES DURING COMPLIANCE ASSESSMENT FOR FINANCIAL ORGANIZATIONS

Zhukova Marina N., Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-3441-3041, e-mail: zhukova @sibsau.ru
Iakovleva Anastasia O., Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,
graduate student, ORCID: 0009-0008-7828-0977, e-mail: petrova754@mail.ru

The paper considers the procedure for assessing the compliance of a set of basic information security measures with the security level requirements for financial organizations. In order to determine the parameters that influence the assessment of compliance with the information security requirements according to GOST R 57580.2–2018, the coefficients of influence of security measures implemented to meet the requirements of GOST R 57580.1–2017 were calculated. Calculation formulas are presented that allow obtaining a numerical value for each information security contour of the information system. Using knowledge of the weighting factor for each measure will enable specialists to make a more effective decision in a situation of making changes or finalizing the infrastructure and preparing for the upcoming assessment procedure. Provided that continuous monitoring of the security contours subject to assessment is implemented, the obtained calculations will minimize the risk of receiving an insufficient assessment of compliance with the information security standards of financial systems. The obtained results are proposed to be further used in practical tasks of improving the assessment by optimized selection of parameters depending on the specified criteria and the difference in the values of the current and required assessment levels.

Keywords: financial institution, information security contour, calculation of conformity assessment, degree of influence, measure of protection

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

Серия стандартов ГОСТ Р 57580 содержит в себе требования к обеспечению информационной безопасности финансовых организаций. Банк России, являющийся основным регулятором, обязал выполнять меры защиты информации ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и проводить оценку соответствия выполнения этих мер согласно ГОСТ Р 57580.2–2018«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

Работа со стандартами вызывает сложности у специалистов: «соответствовать требованиям ГОСТ Р 57580 непросто: в стандарте приведено более 400 требований – далеко не все из них понятны, некоторые просто очень сложно выполнить», – говорят эксперты ITGLOBAL [1]. О проблемах работ со стандартами свидетельствует статистика об инцидентах информационной безопасности финансовых организаций, представленная в Отчете об атаках на финансовый сектор в 2023 г. от группы компаний Солар:

– в 2023 г. Solar JSOC зафиксировал 6,8 тыс. киберинцидентов в финансовом секторе, большая часть которых связана с эксплуатацией уязвимостей и несанкционированным доступом к системам и сервисам;

– количество фишинговых атак на банки выросло в полтора раза с начала 2023 г., этот вектор по-прежнему остается достаточно эффективным, несмотря на высокую степень защищенности отрасли;

– за 2023 г. в общий доступ попало более 161 млн строк, содержащих персональные данные клиентов;

– финансовая отрасль занимает первое место по размеру бюджетов на ИБ: в 2023 г. на эти цели организации потратили 18 млрд рублей [2].

Очевидно, что сложности связаны с определенными проблемами:

1) формальным выполнением требований, без учета ограничений (особенностей) инфраструктуры;

2) сложность (иногда и невозможность) учета мер в перечне выполненных, оценка влияния данной меры в рамках жизненного цикла автоматизированной системы;

3) степень влияния выбранных (или не выбранных) мер на общую оценку соответствия;

4) будет ли достаточным полученный набор мер и реализованных требований для соответствия показателям необходимого уровня защищенности.

Общепринятый подход, использующий моделирование и последующую оценку результатов, не дает ожидаемого эффекта [3]. Поэтому решение вышеописанных проблем возможно путем организации деятельности по аудиту и мониторингу выполнения требований внутри организации.

Данные процессы необходимо в определенной степени формализовать, чтобы иметь количественные показатели результатов [4]. Для этого предлагается разработка и применение инструмента расчета оценки (реализованного в формате «калькулятор»), разработка механизма для определения величины «веса», который имеет каждая мера в общей оценке, а также оптимизационная процедура для подбора мер в соответствии с установленными лицами, принимающими решения критериями.

Инструмент расчета, описание которого ранее представлено авторами [5], необходим для анализа ситуации в «реальном времени» относительно соответствия системы защиты информации (ЗИ) требованиям ГОСТ Р 57580.1–2017, что достигается путем расчета оценки, например, перед проведением аудита или при проектировании изменений в уже существующей инфраструктуре. Понимание веса каждой меры необходимо для того, чтобы оценить ее влияние на итоговый результат при проведении процедуры оценки соответствия, формулы для расчета которой даны в ГОСТ Р 57580.2–2018.

Целью исследования, результаты которого представлены ниже, является определение расчетного показателя для каждой меры в виде коэффициентов для учета степени ее влияния в итоговой оценке соответствия финансовых организаций. Основная сложность в том, чтобы учесть формирование параметров, которые участвуют в расчетных формулах и от выбора и реализации которых может зависеть итоговый результат.

Впоследствии полученные результаты планируется использовать для создания инструмента оптимизации при подборе мер защиты для достижения нужного уровня защищенности. Применение этого инструмента специалистами возможно для оценки требуемых ресурсов на реализацию различных вариантов стратегий повышения оценки.

МЕТОДОЛОГИЯ РАСЧЕТА ПОКАЗАТЕЛЕЙ ОЦЕНКИ

Требования к оценке соответствия выполняются по нормативным актам Банка России, для кредитных организаций – это:

– 683-П от 17.04.2019 «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»;

– 802-П от 25.07.2022 «О требованиях к защите информации в платежной системе Банка России»;

– 821-П от 17.08.2023 «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Согласно этим документам, оценка соответствия субъектов (финансовых организаций) должна проводиться не реже одного раза в 2 года независимо от реализуемого уровня защиты (УЗ) стандартного или усиленного [6–8]. При этом организации должны обеспечить уровень соответствия не ниже 4 ($E_i > 0{,}85$).

Оценка E_i, которая и определяет соответствие требованиям Банка России, вычисляется по формуле, приведенной в таблице 1.

Таблица 1 – Расчет оценки E_i

Формула расчета	Описание
$E_i = \frac{E_{ПЗИ_i} + (0{,}2E_{П_i} + 0{,}4E_{Р_i} + 0{,}25E_{К_i} + 0{,}15E_{С_i})}{2}$	Числовое значение оценки соответствия каждого процесса системы ЗИ E_i вычисляют отдельно по каждому из i-го процессов системы ЗИ как среднеарифметическое значение числовой оценки $E_{ПЗИ_i}$ и суммы числовых значений оценок $E_{П_i}$, $E_{Р_i}$, $E_{К_i}$, $E_{С_i}$ с учетом их весовых коэффициентов

В состав оценки E_i входит значение оценки $E_{ПЗИ_i}$ для каждого из 8 процессов, которая определяет выбор мер ЗИ $E_{МЗИ_j}$ и оценивается как среднее арифметическое полученных оценок в зависимости от отсутствия или наличия у проверяемой организации свидетельств выбора: 0 – мера не выбрана; 1 – мера выбрана.

ГОСТ четко определяет, что оценивается не просто теоретический выбор меры защиты, а еще и реализация ее на практике: если мера реализуется только для части систем, входящих в область оценки и контур безопасности, то такая мера оценивается «0» [8]. При этом, несмотря на то, что внутри процесса может иметься несколько подпроцессов, на итоговый расчет это не повлияет, поскольку если есть подпроцессы, то сначала считается оценка по каждому из них, а затем все равно берется их среднее арифметическое. И если сложить оценки за все меры $E_{МЗИ_j}$ сразу, не разбивая на подпроцессы, получится тот же результат.

Помимо $E_{ПЗИ_i}$, в состав оценки E_i входят значения оценок $E_{П_i}$(Планирование), $E_{Р_i}$(Реализация), $E_{К_i}$(Контроль), $E_{С_i}$(Совершенствование)для каждого из 8 процессов, которые определяют выполнение мер системы организации и управления защитой информации $E_{МОУ_{n,j,k,m}}$ на системных уровнях и оцениваются как среднее арифметическое полученных оценок:

– 0 – полностью не реализуется;
– 0,5 – реализуется не в полном объеме;
– 1,0 – реализуется в полном объеме.

Схематично компоненты, которые входят в оценку E_i, представлены на рисунке ниже (рис.).

Оценка E_i, которая и определяет соответствие требованиям Банка России, вычисляется по формуле, приведенной в таблице 1.

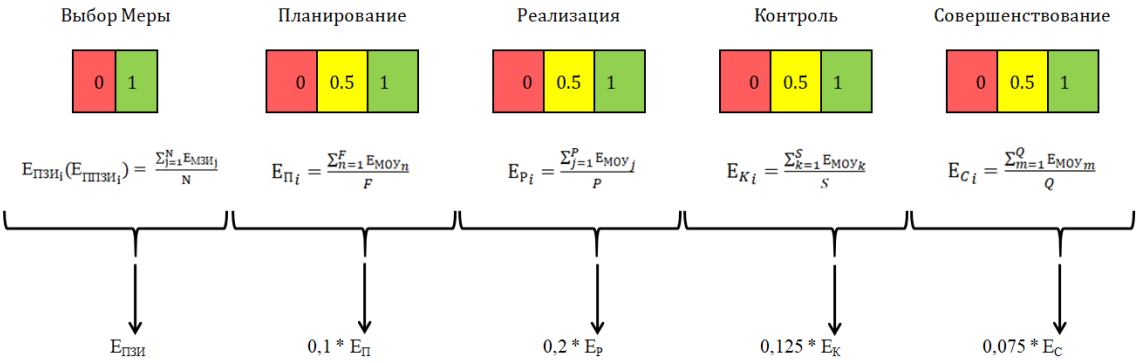


Рисунок – Компоненты, входящие в состав оценки соответствия

Поскольку в финансовой организации формируются один или несколько контуров безопасности, для которых может быть установлен разный УЗ, в случае если в область оценки соответствия ЗИ входят несколько контуров безопасности с различными УЗ, числовое значение оценки каждого процесса системы ЗИ E_i вычисляют:

– отдельно по контурам безопасности с одинаковым уровнем ЗИ;
– как сумму числовых значений оценок E_i для контура(ов) безопасности с учетом их весовых коэффициентов [9].

Формула расчета оценки соответствия при наличии несколько контуров безопасности с различными уровнями ЗИ представлена в таблице 2.

Таблица 2 – Расчет оценки E_i для нескольких контуров

Формула расчета	Описание
$E_i = 0{,}6E_{1_i} + 0{,}3E_{2_i} + 0{,}1E_{3_i}$	Расчет числового значения оценки каждого процесса системы ЗИ E_i при оценке контуров безопасности с первым, вторым и третьим уровнями ЗИ
$E_i = 0{,}7E_{1_i} + 0{,}3E_{2_i}$	Расчет числового значения оценки каждого процесса системы ЗИ E_i при оценке контуров безопасности с первым и вторым уровнями ЗИ
$E_i = 0{,}8E_{1_i} + 0{,}2E_{3_i}$	Расчет числового значения оценки каждого процесса системы ЗИ E_i при оценке контуров безопасности с первым и третьим уровнями ЗИ
$E_i = 0{,}6E_{2_i} + 0{,}4E_{3_i}$	Расчет числового значения оценки каждого процесса системы ЗИ E_i при оценке контуров безопасности со вторым и третьим уровнями

По данным формулам в дальнейшем необходимо провести расчеты, чтобы определить значения коэффициентов для оценки влияния мер защиты информации на итоговую оценку соответствия для целевой информационной системы финансовой организации.

РАСЧЕТ КОЭФФИЦИЕНТОВ ДЛЯ ОЦЕНКИ МЕР ЗАЩИТЫ

Результаты расчета коэффициентов приведены в таблицах 3 и 4, основываясь на ранее приведенных теоретических сведениях и формулах расчетов.

Таблица 3 – Коэффициенты для мер защиты при расчете оценки E_i для одного контура

Мера	Формула расчета коэффициента	Пояснения
$E_{ПЗИ_i}$	$0,5 \cdot (E_{МЗИ_j}/ N)$	N – общее число применимых мер i процесса
$E_{П_i}$	$0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	F – общее количество мер ЗИ, реализация которых оценивается в рамках направления «Планирование для соответствующего уровня ЗИ»
$E_{Р_i}$	$0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	P – общее количество мер ЗИ, реализация которых оценивается в рамках направления «Реализация для соответствующего уровня ЗИ»
$E_{К_i}$	$0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$	S – общее количество мер. реализация которых оценивается в рамках направления «Контроль для соответствующего уровня ЗИ»
$E_{С_i}$	$0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$	Q – общее количество мер ЗИ, реализация которых оценивается в рамках направления «Совершенствование для соответствующего уровня ЗИ»

Полученные результаты позволяют распространить подход на все контуры и посчитать необходимые оценки.

Таблица 4 – Коэффициенты для мер защиты при расчете E_i для нескольких контуров

Мера	Контур 1 УЗ	Контур 2 УЗ	Контур 3 УЗ
$E_i = 0,6E_{1_i} + 0,3E_{2_i} + 0,1E_{3_i}$			
$E_{ПЗИ_i}$	$0,6 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$	$0,3 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$	$0,1 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$
$E_{П_i}$	$0,6 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	$0,3 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	$0,1 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$
$E_{Р_i}$	$0,6 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	$0,3 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	$0,1 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$
$E_{К_i}$	$0,6 \cdot 0,5 \cdot (0,125^* (E_{МОУ_k}/ S))$	$0,3 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$	$0,1 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$
$E_{С_i}$	$0,6 \cdot 0,5 \cdot (0,075^* (E_{МОУ_m}/ Q))$	$0,3 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$	$0,1 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$
$E_i = 0,7E_{1_i} + 0,3E_{2_i}$			
$E_{ПЗИ_i}$	$0,7 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$	$0,3 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$	
$E_{П_i}$	$0,7 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	$0,3 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	
$E_{Р_i}$	$0,7 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	$0,3 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	
$E_{К_i}$	$0,7 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$	$0,3 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$	
$E_{С_i}$	$0,7 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$	$0,3 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$	
$E_i = 0,8E_{1_i} + 0,2E_{3_i}$			
$E_{ПЗИ_i}$	$0,8 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$		$0,2 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$
$E_{П_i}$	$0,8 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$		$0,2 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$
$E_{Р_i}$	$0,8 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$		$0,2 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$
$E_{К_i}$	$0,8 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$		$0,2 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$
$E_{С_i}$	$0,8 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$		$0,2 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$
$E_i = 0,6E_{2_i} + 0,4E_{3_i}$			
$E_{ПЗИ_i}$		$0,6 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$	$0,4 \cdot 0,5 \cdot (E_{МЗИ_j}/ N)$
$E_{П_i}$		$0,6 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$	$0,4 \cdot 0,5 \cdot (0,1 \cdot (E_{МОУ_n}/ F))$
$E_{Р_i}$		$0,6 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$	$0,4 \cdot 0,5 \cdot (0,2 \cdot (E_{МОУ_j}/ P))$
$E_{К_i}$		$0,6 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$	$0,4 \cdot 0,5 \cdot (0,125 \cdot (E_{МОУ_k}/ S))$
$E_{С_i}$		$0,6 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$	$0,4 \cdot 0,5 \cdot (0,075 \cdot (E_{МОУ_m}/ Q))$

Приведенные ранее таблицы показывают, что для расчета коэффициента, отражающего степень влияния меры на оценку, необходимо обладать знанием формул расчета из ГОСТ Р 57580.2–2018 и описанием показателей.

Однако процесс оценки имеет ряд практических сложностей, которые также влияют на коэффициенты, а именно:

1) невозможность обеспечить единую шкалу оценки, в связи с этим возникает вероятность различного вклада в итоговую оценку [10];

2) если какие-то меры процесса или подпроцесса не применяются – они не оцениваются, а делитель, отражающий общее число мер для контура, уменьшается на число исключенных мер, что дает возможность выбора для специалиста, например, в случае оценки меры, например, на 0,5 либо доработать ее до 1, либо попытаться обосновать неприменимость или описать компенсирующей.

3) важным является и тот факт, что компенсирующие меры оцениваются так же, как оценивалась бы исходная мера, что дает возможность при должном обосновании реализовать компенсирующую меру и получить за нее ту же оценку, что получили бы за изначальную, при этом сама мера может, например, работать хуже;

4) в случае, когда в области оценки несколько контуров с одинаковым уровнем защищенности – возникает неоднозначная ситуация с трактовкой требования ГОСТ – отсутствует информация по расчету общей оценки E_i.

ПРИМЕНЕНИЕ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

В рамках проводимого исследования проведены теоретические расчеты, определены расчетные формулы для определения конкретных числовых показателей при различных случаях расчета оценки соответствия. При этом расчетные формулы одинаково эффективны независимо от категории финансовой организации.

Практическое подтверждение возможно только путем применения расчетных формул на практике на примере оценки соответствия конкретной целевой информационной системы требованиям по защите информации в соответствии с требованиями ГОСТ 57580.

Очевидно, что результаты такого апробирования невозможно вынести за пределы информационной системы финансовой организации. Однако можно воспользоваться различными результатами путем обезличивания информации, и использовав практику проведения данной услуги у организации, предоставляющей ее в сфере оценки информационной безопасности.

В данном случае для оценки и подтверждения полученных результатов использованы данные компании по управлению цифровыми рисками (BI.ZONE), специалисты которой предлагают три подхода к повышению оценки, работающих с разной степенью эффективности и имеющих различную стоимость (табл. 5). Значения повышения оценки, представленные в таблице ниже, являются итоговыми для повышения оценки в сумме с применением подхода для всех 8 процессов [11].

Таблица 5 –Характеристики подходов повышения оценки (BI.ZONE «Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза» [9])

Подход	Размер бюджета*	Срок проекта	Повышение оценки
Разработка ОРД	Малый	1–2 мес.	+ 0,16
Разработка ОРД и полное внедрение процесса	Средний	3–5 мес.	+ 0,57
Подключение сервисов кибербезопасности, внедрение СЗИ	Большой	2–6 мес.	+ 0,37

Согласно приведенной таблице, можно предположить, что рассчитанные коэффициенты повышения оценок в последнем столбце получились исходя из:

1) оценки степени влияния только организационных мер защиты;
2) вычисления веса организационных мер и реализации процессного подхода;
3) применения технических мер их вклада в оценку соответствия.

Приведенные значения являются одним из вариантов расчета повышения оценки, который представлен исходя из выбора критериев конкретно компанией BI.ZONE при оказании услуг. Вполне возможно, что этот подход используется компанией для демонстрации своего спектра предоставляемых услуг или реализуемых сервисов. Нет гарантии, что выбор критериев и параметров в нем является оптимальным и универсальным.

Следовательно, анализ других сценариев достижения требуемого уровня соответствия для финансовых организаций является актуальной задачей. Реализация этой задачи возможна только при знании коэффициентов, отражающих степень влияния мер защиты на итоговый показатель оценки соответствия, расчет которых и был получен в данной работе.

ЗАКЛЮЧЕНИЕ

В работе произведен расчет коэффициентов для оценки степени влияния мер защиты на итоговый показатель оценки соответствия. Приведено описание основных расчетных недостатков, которые могут трактоваться по-разному специалистами, проводящими работу как по выбору базовых мер и их реализации, так и по оценке соответствия. По итогам проделанной работы можно сделать вывод, что итоговое влияние меры на результат оценки при ее расчете зависит от следующих параметров:

1) уровня защищенности контура, поскольку от этого показателя зависит базовое количество мер, необходимых для реализации;
2) количества контуров безопасности и разницы между их уровнями защищенности;
3) количества применяемых мер для каждой конкретной системы, поскольку меры, которые не используются в связи с отсутствием той или иной технологии, – не оцениваются;
4) относительно процессных мер – оценки за меру и корректирующего коэффициента для направления защиты.

Изученные особенности определения коэффициентов при проведении процедуры оценки соответствия и полученные расчеты в дальнейшем предлагается использовать для решения задачи автоматизации процесса оптимизированного подбора мер защиты, реализуемых в инфраструктуре финансовой организации, для достижения нужного уровня защищенности в зависимости от заданных критериев и разности значений текущего и требуемого уровня оценки.

Список источников

1. ГОСТ Р 57580: безопасность банковских операций. – URL: https://itglobal.com/ru-ru/company/blog /gost-r-57580 (дата обращения: 10.09.2024).

2. Атаки на российские финансовые организации в 2023 году. – URL: https://rt-solar.ru /analytics/reports/4077 (дата обращения: 12.09.2024).

3. Прокушева А.П., Прокушев Я.Е. Моделирование и оптимизация выбора средств программно-аппаратной защиты информации с точки зрения экономической и технической целесообразности // Информация и безопасность. – 2012. – Т. 15, № 1. – С. 55–60.

4. Ситская, А. В. Вопросы автоматизации проведения аудита в соответствии с ГОСТ р 57580.2-2018 / А. В. Ситская, В. А. Табакаева, В. В. Селифанов // Интерэкспо Гео-Сибирь. – 2021. – Т. 6. – С. 268–275. – DOI: 10.33764/2618-981X-2021-6-268-275.

5. Яковлева, А. О. Разработка программного решения для формирования адаптированного набора мер при проведении оценки соответствия по ГОСТ Р 57580.2 в зависимости от требований ГОСТ Р 57580.1 / А. О. Яковлева, М. Н. Жукова // Современные методы, средства и технологии защиты информации – 2024 : материалы XV Международной научно-практической конференции имени Олега Борисовича Макаревича. – URL: https://conf-is.tilda.ws/.

6. Положение Банка России 683-П от 17.04.2019. – URL: https://base.garant.ru/72246408/ (дата обращения: 15.09.2024).

7. Положение Банка России 802-П от 25.07.2022. – URL: https://base.garant.ru/405828183/ (дата обращения: 15.09.2024).

8. Положение Банка России 821-П от 17.08.2023. – URL: https://base.garant.ru/408182189/ (дата обращения: 15.09.2024).

9. ГОСТ Р 57580.2-2018 от 28.03.2018. – URL: https://base.garant.ru/72072356/ (дата обращения: 20.09.2024).

10. Макаренко, С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С. И. Макаренко // Системы управления, связи и безопасности. – 2018. – № 1. – URL: https://sccs.intelgr.com/20181.html (дата обращения: 10.10.2024).

11. Как повысить оценку ГОСТ 57580: быстро, эффективно, с первого раза. – URL: https://bi.zone /expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (дата обращения: 12.10.2024).

References

1. *GOST R 57580: security of banking operations.* Available at: https://itglobal.com/ru-ru/company/blog /gost-r-57580 (accessed 09.10.2024) (In Russ.).

2. *Attacks on Russian financial organizations in 2023.* Available at: https://rt-solar.ru /analytics/reports/4077 (accessed 09.12.2024) (In Russ.).

3. Prokusheva, A. P., Prokushev, Ya. E. Modeling and optimization of the choice of software and hardware information protection tools from the point of view of economic and technical feasibility. *Information and safety*, 2012, vol. 15, no. 1, pp. 55–60 (In Russ.).

4. Sitskaya, A. V., Tabakaeva, V. A., Selifanov, V. V. Issues of automation of auditing in accordance with GOST R 57580.2-2018. *Interexpo Geo-Siberia*, 2021, vol. 6, pp. 268–275. DOI: 10.33764/2618-981X-2021-6-268-275 (In Russ.).

5. Yakovleva, A. O., Zhukova, M. N. Development of a software solution for the formation of an adapted set of measures when conducting conformity assessment according to GOST R 57580.2 depending on the requirements of GOST R 57580.1. *Modern methods, means and information security technologies – 2024 : materials of the XV International Scientific and Practical Conference named after Oleg Borisovich Makarevich.* Available at: https://conf-is.tilda.ws/ (In Russ.).

6. *Bank of Russia Regulation 683-P dated April 17, 2019.* Available at: https://base.garant.ru/72246408/ (accessed 15.09.2024) (In Russ.).

7. *Bank of Russia Regulation 802-P dated July 25, 2022.* Available at: https://base.garant.ru/405828183/ (accessed 15.09.2024) (In Russ.).

8. *Bank of Russia Regulation 821-P dated August 17, 2023.* Available at: https://base.garant.ru/408182189/ (accessed 15.09.2024) (In Russ.).

9. *GOST R 57580.2-2018 dated March 28, 2018.* Available at: https://base.garant.ru/72072356/ (accessed 20.09.2024) (In Russ.).

10. Makarenko, S. I. Information security audit: main stages, conceptual foundations, classification of activities. *Management, Communication and Security Systems*, 2018, no. 1. Available at: https://sccs.intelgr.com/20181.html (accessed 10.10.2024) (In Russ.).

11. *How to improve your GOST 57580 score: quickly, efficiently, the first time.* Available at: https://bi.zone /expertise/events/kak-povysit-otsenku-gost-57580-bystro-effektivno-s-pervogo-raza/ (accessed 12.10.2024) (In Russ.).

Статья поступила в редакцию 31.10.2024; одобрена после рецензирования 29.11.2024; принята к публикации 02.12.2024.

The article was submitted 31.10.2024; approved after reviewing 29.11.2024; accepted for publication 02.12.2024.

УДК 004.896

АНАЛИЗ УЯЗВИМОСТИ ЦЕЛЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ К MITRE ATT&CK DEFAULT CREDENTIALS ТЕХНИКИ LATERAL MOVEMENT

Жукова Марина Николаевна, Сибирский государственный университет науки и технологий, 660037, Российская Федерация, г. Красноярск, пр. им. газ. «Красноярский рабочий», 31,
кандидат технических наук, доцент, ORCID: 0000-0003-3441-3041, e-mail: zhukova@sibsau.ru

В работе рассматривается класс техник MITRE ATT&CK Lateral Movement, в частности подтехника MITRE ATT&CK Default Credentials. Исследуется задача и приводятся результаты эксперимента по возможности использования злоумышленником техники Default Credentials класса Lateral Movement (MITRE ATT&CK) в отношении определенного круга ИТ-активов. В рамках проведенных экспериментов показывается, что уязвимым местом являются учетные записи пользователей с настройками значений паролей – «по умолчанию» или со слабыми значениями. Приводится анализ подходов и инструментов, позволяющих работать с учетными записями пользователей с целью поиска паролей «по умолчанию». Выбирается инструмент для осуществления подбора паролей и изучаются словари для данного инструмента. В статье последовательно показаны результаты применения средства для поиска учетных записей с паролями по умолчанию для серверов, сетевого оборудования, веб-камер. Смена пароля «по умолчанию» исключает возможность применения злоумышленником в отношении ИТ-актива техники Default Credentials (ID T0812) класса Lateral Movement (MITRE ATT&CK). В частности, это является защитным механизмом от атак вредоносного программного обеспечения, которое осуществляет поиск в сети устройств с учетными данными по умолчанию.

Ключевые слова: анализ уязвимости, учетные данные, THC Hydra, MITRE ATT&CK Default Credentials

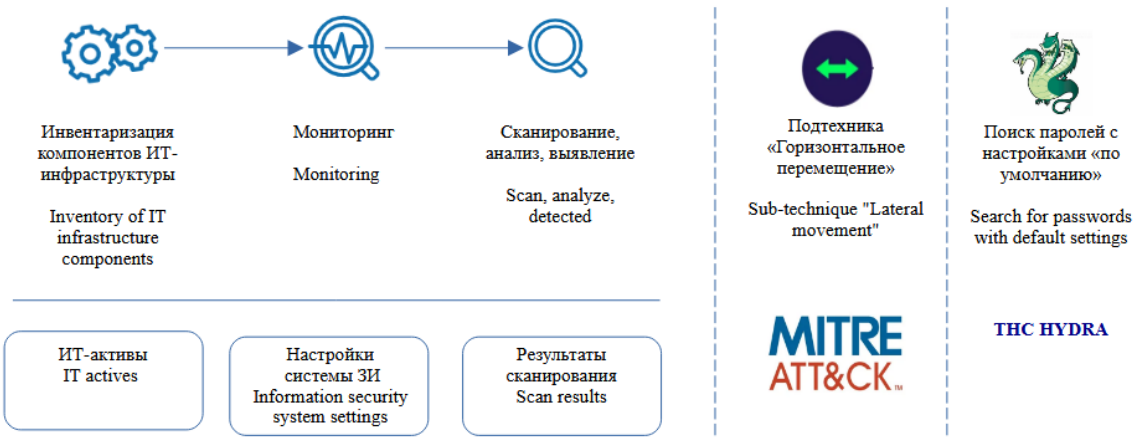
ANALYSIS OF THE VULNERABILITY OF THE TARGET INFORMATION SYSTEM TO MITRE ATT&CK DEFAULT CREDENTIALS LATERAL MOVEMENT TECHNIQUE

Zhukova Marina N., Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy Ave., Krasnoyarsk, 660037, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0003-3441-3041, e-mail: zhukova@sibsau.ru

The work discusses the class of MITER ATT&CK Lateral Movement techniques, in particular the MITER ATT&CK Default Credentials technique. The problem is investigated and the results of an experiment are presented on the possibility of an attacker using the Default Credentials technology of the Lateral Movement class (MITRE ATT&CK) in relation to a certain range of IT assets. As part of the experiments carried out, it is shown that user accounts with password settings – “default” or with weak values - are the vulnerable point. An analysis of approaches and tools is provided that allow you to work with user accounts in order to find “default” passwords. A tool is selected to select passwords and dictionaries for this tool are studied. The article consistently shows the results of using a tool for searching for accounts with default passwords for servers, network equipment, and webcams. Changing the “default” password eliminates the possibility of an attacker using the Default Credentials (ID T0812) Lateral Movement (MITRE ATT&CK) class technology against an IT asset. In particular, this is a protective mechanism against attacks by malware that searches the network for devices with default credentials.

Keywords: vulnerability analysis, credentials, THC Hydra, MITRE ATT&CK Default Credentials

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

Вопросам разработки методов обнаружения вторжений, анализа атак и выбора защитных мер посвящено большое количество научных работ. Задачи управления и обеспечения безопасности информационных систем на основе систем обнаружения вторжений (СОВ) с защищенными процессами обработки и хранения больших объемов информации исследовались в работах П. Д. Зегжды, М. В. Буйневича, И. В. Котенко, и др. [1–3], а также зарубежных исследователей: К. Нейгеля, Э. Таненбаума, М. Клеппмана, Ч. Хоара, Ф. Чезарини, Дж. Паттерсона [4–6].

Современные СОВ направлены в большей степени на выявление внешнего нарушителя, они не скрывают своего существования от внутреннего нарушителя и потому уязвимы для его вмешательства в процессе мониторинга. Сотрудники организаций для осуществления своей рабочей деятельности имеют необходимые регистрации в системе, таким образом накапливается достаточно большой объем учетных данных, каждая запись из которого может представлять определенного вида угрозу для защищаемой информационной системы, в зависимости от уровня прав доступа данной учетной записи. В случае сканирования информационной системы возможно получение информации с определенными характеристиками об этой системе с дополнительными сведениями по учетным записям пользователей системы. При условии четкой постановки задачи с точки зрения определения метрик для формирования системы мониторинга информационной безопасности (например, в соответствии с ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения» [7]) возникает представление о характеристиках получаемых данных, так как положения стандарта определяют какого типа данные необходимо отслеживать при организации систем мониторинга. Это позволяет злоумышленнику определять «ключевые» точки сбора информации об информационной системе, в том числе понимая требования к организации политики контроля учетных данных, а также к политике формирования парольной защиты. Если данные политики недостаточно продуманны и содержат в себе уязвимости, то злоумышленник получает доступ в систему от имени пользователя, уполномоченного выполнять операции с интересующими его данными, что автоматически делает его «невидимым» для СОВ.

Таким образом, одно из самых уязвимых мест автоматизированной информационной системы – точки доступа к ней. Эти точки доступа защищаются протоколами аутентификации (проверки подлинности пользователя). А самая удобная для пользователя и наиболее используемая форма аутентификации – парольная защита. Довольно часто [8] встречаются случаи, когда администраторы, работающие с доступом к различным данным, пренебрегают сменой паролей по умолчанию, и становятся тем самым «слабым звеном», из-за которого взламываются и компрометируются корпоративные системы.

Целью исследования, результаты которого представлены ниже, является решение задачи исключения возможности использования злоумышленником техники Default Credentials класса Lateral Movement (MITRE ATT&CK) в отношении определенного круга компонентов ИТ-инфраструктуры. Основной интерес вызывают результаты аудита паролей с целью выявления ИТ-активов с учетными данными по умолчанию.

Как правило, компонентами ИТ-инфраструктуры являются: серверы – веб-серверы, серверы баз данных, почтовый сервер и т. д.; рабочие места пользователей; принтеры; IP-телефоны; веб-камеры; сетевое оборудование – маршрутизаторы, коммутаторы, шлюзы и т. д. В качестве ИТ-активов в рамках данной статьи будут рассмотрены: серверы, веб-камеры, сетевое оборудование. На основании информации о наиболее часто взламываемых портах [9] и по результатам обследования информационной сети в качестве протоколов, в отношении которых будет осуществлен аудит паролей, выбраны: FTP, SSH, TELNET, HTTP.

МЕТОДЫ ТЕСТИРОВАНИЯ ДЛЯ ПОИСКА УЯЗВИМОСТИ ПАРОЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ

Тестирование методом «белого ящика» – метод тестирования программного обеспечения, который предполагает, что внутренняя структура / устройство / реализация системы известны лицу, проводящему тестирование. Обычно выбирают входные значения, основываясь на знании кода, который будет их обрабатывать. Точно также знают, каким должен быть результат этой обработки. Знание всех особенностей тестируемой программы и ее реализации обязательны для этой техники. Тестирование «белого ящика» – углубление во внутреннее устройство системы за пределы ее внешних интерфейсов [10].

Согласно ISTQB, тестирование в режиме «белого ящика» – это тестирование, основанное на анализе внутренней структуры компонента или системы [10]. В случае аудита паролей тестирование в режиме белого ящика подразумевает проверку конфигурации на соответствие требованиям, установленным парольной политикой исследуемой организации.

Альтернативный метод – тестирование методом «черного ящика». Тестирование методом «черного ящика», также известное как тестирование, основанное на спецификации, или тестирование

поведения – техника тестирования, основанная на работе исключительно с внешними интерфейсами тестируемой системы [10].

Согласно ISTQB, тестирование «черного ящика» – это тестирование, как функциональное, так и нефункциональное, не предполагающее знания внутреннего устройства компонента или системы [10]. В случае аудита паролей тестирование в режиме черного ящика может быть проведено посредством brute force атаки. Причем она может быть произведена в online- или offline-режимах в зависимости от отсутствия или наличия хеша пароля соответственно.

До вступления в силу нормативно-правовых документов в области КИИ аудит паролей в исследуемой организации производился посредством тестирования в режиме «белого ящика». В общем случае специалист по защите информации осуществлял проверку конфигурации устройств на предмет соответствия установленным требованиям парольной политики. В случае паролей пользователей аудит паролей производился посредством Power Shell скрипта, выполняемого с привилегиями администратора домена и выполняющего анализ хешей, поскольку пароли не хранятся в открытом виде.

В соответствии с приказом ФСТЭК № 239 от 25 декабря 2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [11], анализ уязвимостей должен проводиться посредством тестирования на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации. Эта формулировка семантически соответствует тестированию в режиме «черного ящика».

Интерес представляет более сложный случай, поэтому в данном исследовании аудит паролей будет производиться в режиме «черного ящика» посредством online brute force атаки.

АНАЛИЗ И ВЫБОР СРЕДСТВ ПО ПОДБОРУ ПАРОЛЯ

Рассмотрим топ 10 средств подбора паролей [12]: Hashcat; John the Ripper; Brutus; Wfuzz; THC Hydra; Medusa; RainbowCrack; OphCrack; L0phtCrack; Aircrack-ng. Выбор будет осуществляться по следующим критериям:

1) наличие возможности проведения online-атаки по протоколам FTP, TELNET, HTTP, SSH;
2) возможность использования инструмента коммерческой организацией в соответствии с лицензией программного средства подбора пароля;
3) скорость перебора паролей.

Программные средства Hashcat, John the Ripper, RainbowCrack, OphCrack, L0phtCrack не могут быть использованы в рамках поставленной задачи, поскольку являются инструментами подбора паролей по их хешам. Инструменты Brutus, Wfuzz, Aircrack-ng не поддерживают требуемые протоколы. Таким образом, в дальнейшем сравнении будут рассмотрены THC Hydra и Medusa.

Лицензии для THC Hydra и Medusa представлены на рисунках 1 и 2 соответственно.

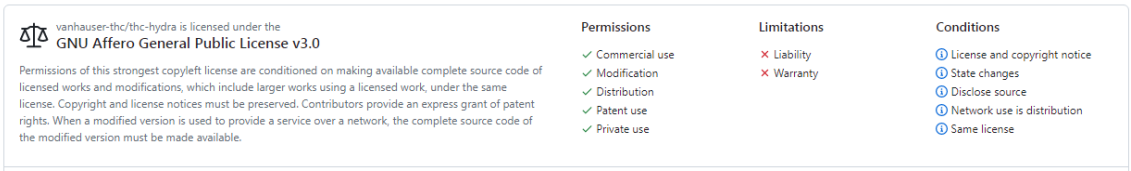


Рисунок 1 – Лицензия THC Hydra

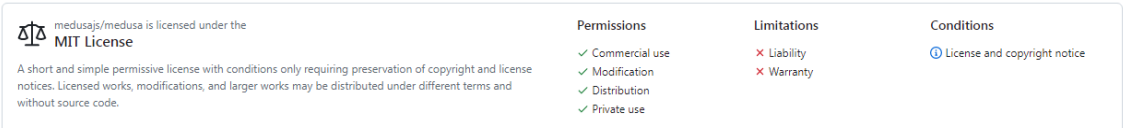


Рисунок 2 – Лицензия Medusa

THC Hydra и Medusa могут быть свободно использованы коммерческой организацией.

Сравним THC Hydra и Medusa по скорости подбора паролей. Первая серия тестов была проведена с использованием SSH. Установлена учетная запись «root» с паролем «toor». Пароль «toor» добавлен в конец списка из 500 паролей под номером 499.

Сравнительная характеристика THC Hydra и Medusa по времени подбора пароля приведена в таблице [13].

Таблица – Сравнение *THC Hydra* и *Medusa* по времени подбора пароля

Наименование программы	Время подбора пароля, с
THC Hydra	191
Medusa	1500

Исходя из сведений, представленных в таблице, можно сделать вывод, что THC Hydra осуществляет подбор пароля быстрее Medusa в 7,85 раз. Таким образом, в качестве средства подбора паролей выбран инструмент THC Hydra.

Эффективность подобных систем сильно зависит от словарей, которые используются в работе решения. В рамках исследования изучены 2 подхода:

1) применение готового словаря, встроенного в программное решение по умолчанию;
2) составление словаря, используя данные после сканирования системы.

Далее необходимо осуществить выбор словарей для THC Hydra.

Рассмотрим пакет словарей wordlists, который установлен по умолчанию в составе операционной системы Kali Linux 2022.1. Интересуют списки с паролями по умолчанию для удаленных служб, таких как SSH, FTP, TELNET:

– для протокола SSH в составе BruteX найдены словари: ssh-default-userpass.txt; ssh_defuser.txt; ssh_defpass.txt;

– для протокола FTP в составе BruteX найдены словари: ftp-default-userpass.txt; ftp_defuser.txt; ftp_defpass.txt;

– для протокола TELNET в составе BruteX найден словарь: telnet-default-userpass.txt.

Тег «userpass» означает, что в словаре представлены связки логин-пароль. Теги «defuser» и «defpass» означают, что в словаре представлены только логины или пароли соответственно.

Для веб-интерфейсов будет осуществлен поиск учетных данных по умолчанию в соответствии с версией программного обеспечения (для веб-камер) и моделью устройства (для сетевого оборудования) в интернете. Перед осуществлением подбора паролей используемые словари будут проверены на наличие в них логинов и паролей по умолчанию. Кроме того, для протокола HTTP в составе Metasploit Framework найдены словари: http_default_pass.txt; http_default_userpass.txt; http_default_users.txt.

ТЕСТИРОВАНИЕ ЦЕЛЕВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА УСТОЙЧИВОСТЬ К ПОДТЕХНИКЕ «MITRE ATT&CK DEFAULT CREDENTIALS»

Далее в статье будет показана возможность поиска серверов, сетевого оборудования, веб-камер, к которым можно подключиться, используя учетные данные по умолчанию, через TELNET, SSH, FTP, веб-интерфейс. Для практической апробации определенного на основе сравнительного анализа инструмента THC Hydra выбрана инфраструктура действующего предприятия. Применимо выбранное решение в виде THC Hydra для сканирования и последующего мониторинга ИТ-инфраструктуры. В статье последовательно показаны результаты применения средства для поиска учетных записей, с паролями по умолчанию для серверов, сетевого оборудования, веб-камер.

Рассмотрим серверную часть инфраструктуры. По результатам сканирования (применялся сканер nmap) выявлены:

1) серверы, осуществлять управление которыми можно через TELNET, отсутствуют;
2) серверы, осуществлять управление которыми можно через SSH, присутствуют в количестве 9 единиц;
3) серверы, которые поддерживают взаимодействие по протоколу HTTP, отсутствуют;
4) серверы, осуществлять взаимодействие с которыми можно через FTP, присутствуют в количестве 2 единиц.

На рисунках 3 и 4 отображен результат попыток THC Hydra подобрать пароль для подключения через SSH и FTP.

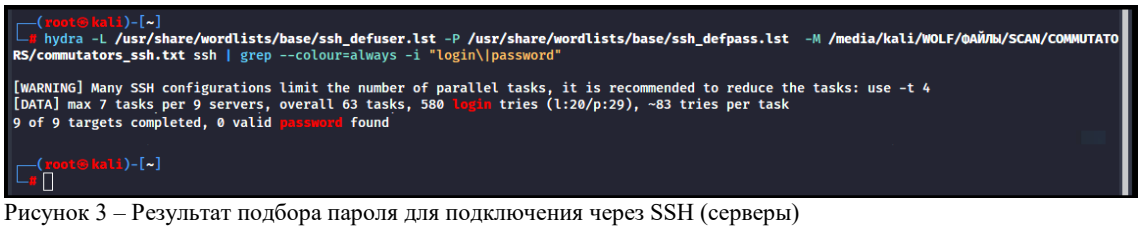


Рисунок 3 – Результат подбора пароля для подключения через SSH (серверы)

Рисунок 4 – Результат подбора пароля для подключения через FTP (серверы)

Результат работы: подобрать пароль для подключения через SSH к серверу не удалось, подобрать пароль для подключения через FTP к серверу не удалось.

Далее в исследовании проводится работа с сетевым оборудованием. По результатам сканирования nmap выявлено, что:

1) сетевое оборудование, осуществлять управление которым можно через TELNET, присутствует в количестве 7 единиц;
2) сетевое оборудование, осуществлять управление которым можно через SSH, присутствует в количестве 9 единиц;
3) сетевое оборудование, которое поддерживает взаимодействие по протоколу HTTP, присутствует в количестве 55 единиц;
4) сетевое оборудование, осуществлять взаимодействие с которым можно через FTP, присутствует в количестве 2 единиц.

Результат работы: подобраны пароли для 2 узлов. Проведена проверка подключения через TELNET, чтобы исключить ложное срабатывание THC Hydra – подключение осуществить удалось.

Подобрать пароль для подключения через SSH к сетевому оборудованию не удалось. Подобрать пароль для подключения через FTP к сетевому оборудованию не удалось.

На рисунке 5 отображен результат попыток THC Hydra подобрать пароль для подключения через HTTP.

Рисунок 5 – Результат подбора пароля для HTTP (сетевое оборудование)

Удалось подобрать пароль для 18 узлов. Проведена проверка аутентификации через веб-интерфейс, чтобы исключить ложное срабатывание THC Hydra – подключение осуществить удалось. На рисунке 6 отображен пример успешного входа через веб-интерфейс для одного из узлов.

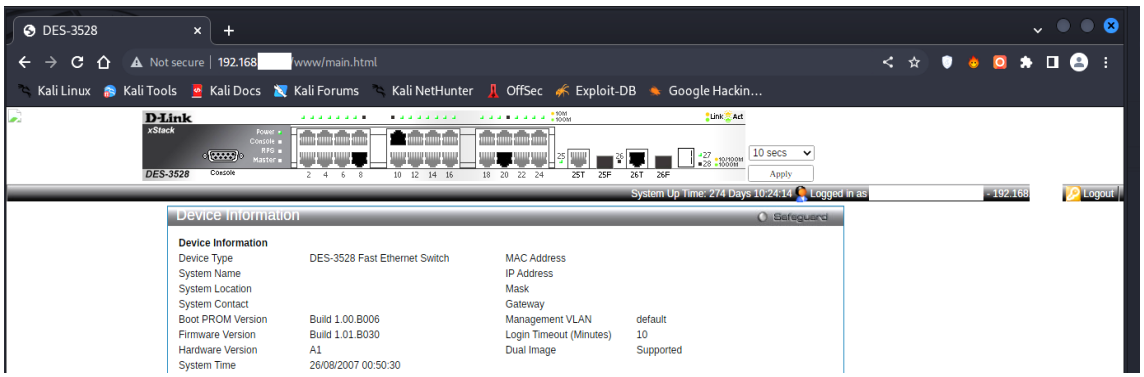


Рисунок 6 – Подключение через веб-интерфейс (сетевое оборудование)

Поиск и мониторинг веб-камер с учетными данными по умолчанию. По результатам сканирования (сканер nmap) выявлено, что:

1) веб-камеры, осуществлять управление которыми можно через TELNET, отсутствуют;
2) веб-камеры, осуществлять управление которыми можно через SSH, отсутствуют;
3) веб-камеры, которые поддерживают взаимодействие по протоколу HTTP, присутствуют в количестве 36 единиц;
4) веб-камеры, осуществлять взаимодействие с которыми можно через FTP, отсутствуют.

Удалось подобрать пароль для 36 узлов. Проведена проверка аутентификации через веб-интерфейс, чтобы исключить ложное срабатывание THC Hydra – подключение осуществить удалось. На рисунке 7 отображен пример успешного входа через веб-интерфейс для одного из узлов.

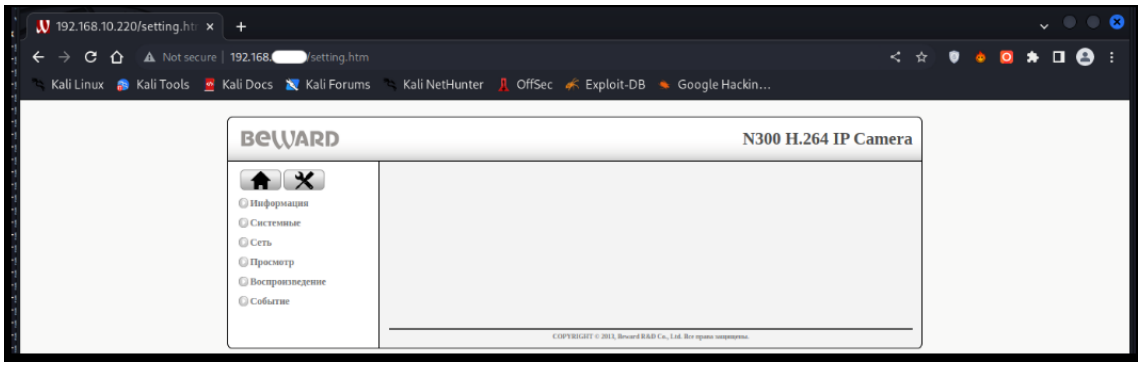


Рисунок 7 – Подключение через веб-интерфейс (веб-камеры)

Таким образом, полученные результаты показывают, что эффективность защиты ИТ-инфраструктуры организации сильно зависит от наличия в системе учетных записей с паролями по умолчанию. Подобные факты существенно снижают уровень защищенности.

ПРИМЕНЕНИЕ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

В рамках проводимого исследования для практического тестирования использовалась достаточно типовая ИТ-инфраструктура, которая присутствует в большинстве организаций. В результате аудита паролей для сетевого оборудования и веб-камер найдены учетные данные по умолчанию. На рисунке 8 отображены количественные графики для каждого из протоколов.

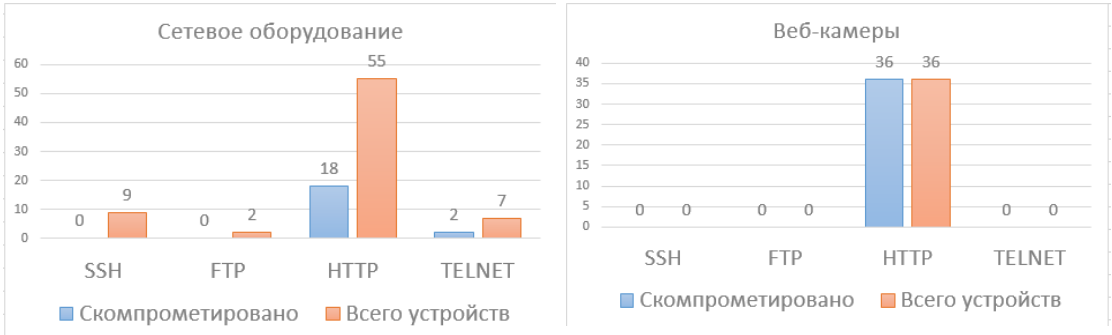


Рисунок 8 – Результат поиска сетевого оборудования и веб-камер с учетными данными по умолчанию

Проведенные эксперименты показали, что аудит паролей должен обеспечиваться как процесс информационной безопасности, а не как разовое мероприятие. Таким образом, аудит паролей должен производиться при появлении новых устройств в сети (неплановый аудит) и систематически (плановый аудит).

В рамках проведения непланового аудита для отслеживания в информационной сети новых устройств используется NeDi. Аудит пароля необходимо производить не позднее 5 дней с момента получения уведомления о появлении нового устройства в информационной сети.

Плановый аудит паролей нужен, поскольку пароль может быть изменен вредоносным программным обеспечением или системным администратором после устранения нарушений, выявленных в ходе проверки. Установленная периодичность проведения планового аудита паролей – 2 месяца.

ЗАКЛЮЧЕНИЕ

Смена пароля по умолчанию исключает возможность применения злоумышленником в отношении ИТ-актива техники Default Credentials (ID T0812) класса Lateral Movement (MITRE ATT&CK) [14]. В частности, это является защитным механизмом от атак вредоносного программного обеспечения, которое осуществляет поиск в сети устройств с учетными данными по умолчанию. В дальнейшем аудит паролей необходимо производить периодически, поскольку в информационной сети могут появиться новые активы.

Исследование сосредоточено на изучении и решении одной из наиболее часто применяемой тактике действий злоумышленников – Default Credentials (ID T0812) MITRE ATT&CK. В случае проведения атаки, при компрометации сетевого узла злоумышленник может найти наличие узла с учетными данными по умолчанию или со слабыми настройками пароля. В этом случае большинство требований и ограничений системы обнаружения и мониторинга инцидентов ИБ теряют свою эффективность.

Проведенные эксперименты показывают, что защищенность ИТ-инфраструктуры зависит от большого количества факторов, немалую роль среди которых играет сильная парольная защита и периодичность аудита по поиску учетных данных с настройками «по умолчанию».

Дальнейшее развитие может иметь направление, связанное с автоматизацией процессов аудита в режиме постоянного анализа, определением источников сбора данных, зависимостях сервисов и формирования подхода, позволяющего отслеживать события возникших векторов атак.

Список источников

1. Смирнов, Д. В. Система сбора и анализа информации из различных источников в условиях Big Data / Д. В. Смирнов, А. А. Грушо, М. И. Забежайло, Е. Е. Тимонина // International Journal of Open Information Technologies. – 2021. – Vol. 9, № 4. – P. 64–74.

2. Штеренберг, С. И. Распределенная система обнаружения вторжений с защитой от внутреннего нарушителя / С. И. Штеренберг, М. А. Полтавцева // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 59–68.

3. Демидов, Р. А. Анализ угроз кибербезопасности в динамических сетях передачи данных с применением гибридной нейросетевой модели / Р. А. Демидов, П. Д. Зегжда, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 27–33.

4. Ha, D. Insider threat assessment: Model, analysis and tool / D. Ha, A. Iyer, H.Q. Ngo, and S. Upadhyaya // Network Security. – Boston : Springer, 2010. – P. 143–174.

5. Sinclair, S. Preventative directions for insider threat mitigation via access control / S. Sinclair, S.W. Smith // Insider Attack and Cyber Security. – Springer, 2008. – P. 165–194.

6. Hussain, S. R. Detecting anomalous database transactions by insiders / S. R. Hussain, A. M. Sallam, E. B. Detanom // Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. CODASPY '15, New York, NY, USA : ACM, 2015. – P. 25–35.

7. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения : национальный стандарт Российской Федерации : дата ведения 2022-04-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2022. – 14 с.

8. «Ростелеком»: 80 % российских компаний не соблюдают базовых требований к паролям // Ростелеком-Солар. – URL: https://rt-solar.ru/events/news/1840/ (дата обращения: 24.08.2024).

9. 28 наиболее часто взламываемых портов [UDP/TCP] // General Software. – URL: https://g-soft.info /articles/8796/28-naibolee-chasto-vzlamyvaemyh-portov-udp-tcp/ (дата обращения: 04.09.2024).

10. White/Black/Grey Box-тестирование // BUGZA. – URL: https://bugza.info/white-black-grey-box-testirovanie/ (дата обращения: 06.09.2024).

11. Top 10 Password Cracking Tools // RuCore.NET. – URL: https://rucore.net/en/top-10-password-cracking-tools/ (дата обращения: 24.08.2024).

12. Brute Forcing Passwords with ncrack, hydra and medusa // Hackonology. – URL: https://hackonology.com /blogs/brute-forcing-passwords-with-ncrack-hydra-and-medusa/ (дата обращения: 24.04.2023).

13. Default Credentials // MITRE ATT&CK. – URL: https://attack.mitre.org/techniques/T0812/ (дата обращения: 04.09.2024).

14. Приказ ФСТЭК «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 года № 239 // Официальный интернет-портал правовой информации. – С изм. и допол. в ред. от 1 января 2023 г.

References

1. Smirnov, D. V., Grusho, A. A., Zabezhaylo, M. I., Timonina, E. E. System for collecting and analyzing information from various sources in Big Data conditions. *International Journal of Open Information Technologies*, 2021, vol. 9, no. 4, pp. 64–74 (In Russ.).

2. Shterenberg, S. I., Poltavtseva, M. A. Distributed intrusion detection system with protection from an internal intruder. *Problems of Information Security. Computer Systems*, 2018, no. 2, pp. 59–68 (In Russ.).

3. Demidov, R. A., Zegzhda, P. D., Kalinin, M. O. Analysis of cybersecurity threats in dynamic data networks using a hybrid neural network model. *Problems of Information Security. Computer Systems*, 2018, no. 2, pp. 27–33 (In Russ.).

4. Ha, D., Iyer, A., Ngo, H. Q., and Upadhyaya, S. Insider threat assessment: Model, analysis and tool. *Network Security*. Boston: Springer, 2010, pp. 143–174.

5. Sinclair, S., Smith, S. W. Preventative directions for insider threat mitigation via access control. *Insider Attack and Cyber Security*. Springer, 2008, pp. 165–194.

6. Hussain, S. R., Sallam, A. M., Detanom, E. B. Detecting anomalous database transactions by insiders. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. CODASPY '15, New York, NY, USA.* ACM, 2015, pp. 25–35.

7. *GOST R 59547-2021. Information protection. Information security monitoring. General provisions: national standard of the Russian Federation: date of reference 2022-04-01.* Federal Agency for Technical Regulation and Metrology. .Ed. official. .Moscow: Standartinform, 2022. 14 p. (In Russ.).

8. Rostelecom: 80 % of Russian companies do not comply with basic password requirements. *Rostelecom-Solar.* Available at: https://rt-solar.ru/events/news/1840/ (accessed 24.08.2024) (In Russ.).

9. 28 most frequently hacked ports [UDP/TCP]. *General Software.* Available at: https://g-soft.info /articles/8796/28-naibolee-chasto-vzlamyvaemyh-portov-udp-tcp/ (accessed 04.09.2024) (In Russ.).

10. White/Black/Grey Box-testing. *BUGZA.* Available at: https://bugza.info/white-black-grey-box-testirovanie/ (accessed 06.09.2024) (In Russ.).

11. Top 10 Password Cracking Tools. *RuCore.NET*. Available at: https://rucore.net/en/top-10-password-cracking-tools/ (Accessed 24.08.2024).

12. Brute Forcing Passwords with ncrack, hydra and medusa. *Hackonology.* Available at: https://hackonology. com/blogs/brute-forcing-passwords-with-ncrack-hydra-and-medusa/ (accessed 24.04.2023).

13. *Default Credentials. MITRE ATT&CK.* Available at: https://attack.mitre.org/techniques/T0812/ (accessed 04.09.2024).

14. Order of the FSTEC "On approval of the Requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation" dated December 25, 2017 No. 239. *Official Internet portal of legal information. With changes and additional in ed. from January 1, 2023.*

Статья поступила в редакцию 08.09.2024; одобрена после рецензирования 23.09.2024; принята к публикации 23.09.2024.

The article was submitted 08.09.2024; approved after reviewing 23.09.2024; accepted for publication 23.09.2024.

УПРАВЛЕНИЕ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ

УДК 004.001

ФОРМИРОВАНИЕ И УПРАВЛЕНИЕ КОМАНДАМИ ПРИ РЕАЛИЗАЦИИ УНИКАЛЬНЫХ ПРОЕКТОВ

***Кашаев Кирилл Владимирович*,** Астраханский государственный университет имени В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,

аспирант, ORCID: 0009-0008-0562-8901, e-mail: abc8512@mail.ru

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

доктор технических наук, профессор, профессор кафедры информационной безопасности, ORCID: 0000-0001-9058-123X, e-mail: aim_agtu@mail.ru

***Зубова Анастасия Алексеевна*,** Астраханский государственный университет имени В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, аспирант ORCID: 0000-0002-0042-5346, e-mail: an_vesnaa@mail.ru

Проектные команды, независимо от вида организационных систем, в которых они функционируют, ставят перед собой задачи достижения конкретных целей оптимальным способом. Дефицит кадровых ресурсов, как с точки зрения компетенций, так и численности, всегда оказывает серьезное влияние на результаты и темпы выполнения проекта. В данной статье рассматриваются подходы к формированию и управлению командами при реализации уникальных проектов. Под уникальными в рамках настоящей статьи понимаются проекты, обладающие признаками эксклюзивности в независимости от их типа. Это могут быть, например, проекты IT, обустройства морских месторождений, проекты организационной трансформации и т. п. Ключевым фактором уникальности является редкая встречаемость проекта, его сложность, а также объем уникальных компетенций, требуемых для его реализации. Основной задачей рассматриваемых в статье подходов, является эффективное распределение имеющегося кадрового ресурса.

Ключевые слова: формирование проектных команд, организационные системы, методика управления проектными командами, цифровой клон

TEAM BUILDING AND MANAGEMENT IN THE IMPLEMENTATION OF UNIQUE PROJECTS

Kashaev Kirill V., Astrakhan Tatishchev State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

graduate student, ORCID: 0009-0008-0562-8901, e-mail: abc8512@mail.ru

Azhmukhamedov Iskandar M., Astrakhan Tatishchev 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: 0000-0001-9058-123X, e-mail: aim_agtu@mail.ru,

Zubova Anastasia A., Astrakhan Tatishchev State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,

graduate student, ORCID: 0000-0002-0042-5346, e-mail: an_vesnaa@mail.ru

Project teams, regardless of the type of organizational systems in which they operate, set themselves the task of achieving specific goals in an optimal way. The shortage of human resources, both in terms of competencies and numbers, always has a serious impact on the results and pace of project implementation. This article discusses approaches to the formation and management of teams in the implementation of unique projects. Unique projects in this article are those that have exclusivity characteristics, regardless of their type. These may be, for example, IT projects, offshore field development projects, organizational transformation projects, etc. The key factor in uniqueness is the rare occurrence of the project, its complexity, as well as the volume of unique competencies required for its implementation. The main objective of the approaches considered in the article is the effective distribution of available human resources.

Keywords: formation of project teams, organizational systems, project team management methods, digital clone

ВВЕДЕНИЕ

Дефицит ресурсов был, есть и будет всегда. Каждый проект, каждая организационная система испытывает нехватку чего-либо. Но есть организационные системы, в которых требования к компетенциям достаточно высоки и невосполнимы за короткий промежуток времени и разумные средства. Следовательно, целесообразно пересмотреть подходы к формированию и управлению проектными командами, дополнив их и разработав соответствующий инструментарий.

Проектные команды создаются для реализации конкретной поставленной задачи – проекта. Как правило, они ограничены во времени и средствах. Сами по себе проекты, в которых задействованы проектные команды, могут иметь разную направленность. Это могут быть проекты инжиниринга уникальных объектов, обустройства морских месторождений, внедрения современных IT-систем, проекты трансформации и оптимизации бизнес-процессов и т. п.

Организации, которые реализуют уникальные проекты, требующие эксклюзивных знаний, умений и навыков, как правило, параллельно осуществляют и стандартную операционную деятельность. Примером могут служить предприятия морской добычи нефти и газа, космическая отрасль, оборонная промышленность и т. п. Инженерный состав, обладающий компетенциями в высокотехнологичной области и имеющий значительный опыт работы на данных предприятиях, – это ценный кадровый ресурс. В условиях высокой загрузки по основному виду деятельности участие в проектах становится для таких сотрудников сложной задачей, так как требует постоянного участия и отвлечения от основной деятельности для выполнения проектных задач.

При этом «на рынке труда остро ощущается нехватка специалистов с инженерно-техническими знаниями, так как значительное количество абитуриентов заинтересованы в выборе бизнес-экономических, а не инженерных специальностей» [1].

КОМАНДЫ УНИКАЛЬНЫХ ПРОЕКТОВ

При распределении человеческих ресурсов между основной деятельностью и выполнением задач уникальных проектов необходимо учитывать сложившуюся архитектуру бизнес-процессов, их операционную сложность и стоимость.

Как правило, организации и предприятия, которые реализуют уникальные проекты, обладают достаточно развитой архитектурой бизнес-процессов. Чем более развита организационная система с точки зрения архитектуры бизнес-процессов, тем сложнее интегрировать в нее новые проекты и перераспределять имеющиеся ресурсы. В подобных организационных системах предъявляются достаточно высокие требования к компетенции сотрудников, так как цена ошибки может стоить сотни миллионов рублей.

Примером может служить морская платформа Deepwater Horizon компании British Petroleum, на которой в 2010 г. произошёл взрыв. Инженеры компании неверно интерпретировали данные о давлении внутри скважины, которые указывали на то, что выброс газа и последовавший за ним взрыв был неизбежным, что привело к техногенной катастрофе [2]. К 2016 г. общая сумма затрат компании British Petroleum на устранение последствий аварии превысила $ 56 млрд. В том числе 5 американских штатов получат от компании в течение 16 лет компенсацию за причиненный ущерб в размере $ 20,8 млрд [3].

При подобных рисках у руководителей нет права на ошибку. Нагрузка на персонал должна распределяться оптимальным способом. Новые проекты должны реализовываться не в ущерб основной деятельности, а проектные команды должны калиброваться не только по профессиональным, но и по личностным качествам. Это представляет собой достаточно сложную задачу, которую предстоит решить.

Основным ядром проекта, с точки зрения компетенций, является проектная команда. Как указывает В. А. Заренков, «она представляет собой группу специалистов, работающих над реализацией проекта, представляющих интересы различных участников проекта и подчиняющихся руководителю проекта» [4].

Непосредственно к участникам проектной команды предъявляются серьезные требования в части необходимого уровня компетенций.

Еще одной категорией по степени вовлеченности в проект может быть вспомогательная команда. Для вспомогательной проектной команды требования к компетенциям могут отличаться не только по уровню, но и по степени востребованности, а также широте перечня компетенций [5].

Учитывая тот факт, что для реализации уникальных проектов может привлекаться сторонний подрядчик, обладающий узкоспециальными навыками и опытом, существует необходимость построения проектной команды, которая состоит в том числе из сотрудников заказчика, которые формируют требования, отвечают за качество и контроль проекта.

Для построения эффективных проектных команд при реализации уникальных проектов немаловажным фактором является способ их формирования. Существуют различные способы построения проектных команд в зависимости от задач проекта.

Например, И. Мазур, В. Шапиро и Н. Ольдерогге выделяют следующие разновидности организационных структур проектов: функциональная, матричная и проектно-целевая [6] (табл.).

Таблица – Сравнение способов построения организационных структур проектов

Организационная структура / Характеристика проекта	Функциональная	Матричная			Проектно-целевая
		Слабая	Сбалансированная	Сильная	
Полномочия руководителя проекта	Крайне незначительные	Ограниченные	От слабых до средних	От средних до высоких	От высоких до неограниченных
Доля организационных ресурсов, задействованных для выполнения проекта	Практически 0 %	От 0 до 25 %	От 15 до 60 %	От 50 до 95 %	От 85 до 100 %
Роль руководителя проекта	Временная	Временная	Постоянная	Постоянная	Постоянная
Обычные названия руководителя проекта	Координатор / лидер проекта	Координатор / лидер проекта	Проект-менеджер / руководитель проекта	Проект-менеджер / руководитель программы	Проект-менеджер / руководитель программы
Статус команды проекта	Временный	Временный	Временный	Постоянный	Постоянный

Учитывая тот факт, что при реализации уникальных проектов отсутствует возможность быстрой замены ключевых участников, обладающих знаниями в высокотехнологичных областях, оптимальным способом построения проектной команды является сбалансированная или сильная матрица. При этом ключевые эксперты, обладающие знаниями в узких областях, могут продолжать свою работу по основной деятельности на предприятии, а руководители проекта со стороны подрядчика имеют достаточное количество полномочий на их мобилизацию в проект.

Главным фактором успеха в рамках такого взаимодействия является грамотно составленный ресурсный план проекта, который в обязательном порядке должен учитывать финансовую мотивацию сотрудников, обладающих знаниями в высокотехнологичных областях. По результатам выполнения ключевых фаз проекта руководитель проектной команды организует выплаты денежных средств (финансовой мотивации) всей проектной команде. При таком сценарии возможно применение различных правовых инструментов перечисления денежных средств. В случае, если сотрудник работает на постоянной основе, либо является совместителем, он в рамках трудового договора ежемесячно получает выплаты в рамках заключенного трудового договора. Если постоянная ставка в организационно-штатной структуре отсутствует, либо требуется периодическое привлечение сотрудника, обладающего необходимыми знаниями, возможно разовое заключение договоров гражданско-правового характера с указанием конкретно выполняемых объемов услуг.

В отсутствие механизмов материального стимулирования сотрудников, обладающих знаниями в высокотехнологичных областях, проект рано или поздно столкнется с негативным отношением указанных сотрудников, которые будут воспринимать проект как повинность и быстро утратят интерес к его реализации.

Таким образом, из состава специалистов предприятия, реализующего уникальные проекты, и специалистов внешнего подрядчика необходимо создать сильную проектную команду, которая будет обладать достаточным ресурсом для эффективной реализации проекта, а также специфическими знаниями, что, безусловно, положительно скажется на качестве его реализации. Открытым остается вопрос подбора кандидатов в проектную команду и оптимального распределения ролей и функций.

МЕТОДОЛОГИЯ И. АДИЗЕСА КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ ПРОЕКТНЫХ КОМАНД

Задача формирования проектной команды является многокритериальной и слабоструктурированной. Значительная часть параметров, влияющих на решение по подбору кандидатов, часто носит экспертный характер и выражается в виде нечисловых оценок [7].

И. Адизес видит основной задачей успешной организационной системы построение эффективной и результативной команды.

При этом для обеспечения надлежащего уровня управления такими командами необходимо выполнять четыре функции [8]:

1. (P)roducing – производство результатов, ради которых существует данная организация и которые определяют ее эффективность.

2. (A)dministering – администрирование, обеспечивающее производительность.

3. (E)ntrepreneuring – предпринимательство, с помощью которого происходит управление изменениями.

4. (I)ntegrating – интеграция, то есть объединение элементов организации для обеспечения ее жизнеспособности в долгосрочной перспективе.

Данная методология PAEI широко распространена по всему миру. Она является самостоятельным научным открытием, опирающимся на многолетний опыт работы профессора И. Адизеса.

Однако, как подчеркивал А. М. Иванов, «…без учета ментальных особенностей народа, без отечественной адаптации иностранных заимствований любые новации обречены на торможение» [9].

Исходя из классификации профессора И.иАдизеса, можно определить функциональные особенности и роли каждого участника проектной команды.

Вне зависимости от задач проектной команды каждый из ее участников может выполнять одну или несколько ролей и функций.

Для успешного функционирования команды необходимо, чтобы в ней были представлены на высоком уровне все четыре функции. Однако, по мнению И. Адизеса, сотрудник одновременно может эффективно выполнять не более двух функций (рис. 1).

Рисунок 1 – Роли участников проектной команды

Для систем с ограниченным кадровым ресурсом, вне зависимости от их типологии, успешность взаимодействия участников проектной команды является ключевым фактором успеха. Таким образом, правильный подбор кандидатов на роли в проектные команды не только позволяет эффективно достигать поставленных задач, но и экономит ресурсы проекта.

Мобилизация качеств, присущих человеку, позволяет создавать системы, направленные на долговременное инновационное развитие предприятия [10].

Смена участника проектной команды до момента его 100% реализации несет в себе множество рисков, таких как: срыв сроков, удорожание проекта, необходимость постоянного перераспределений функций внутри команды. На определенном этапе проекта потеря ключевых экспертов может сделать его нерентабельным.

Применение методологии И. Адизеса при подборе кандидатов на роли в проектные команды может нивелировать серьезные последствия для всех участников проекта, в том числе и для заказчика. Для того чтобы понять, насколько кандидат подходит на конкретную роль/должность в проектной команде, для начала необходимо с помощью анкетирования определить его ключевые навыки с точки зрения методологии И. Адизеса PAIE и определить удельный показатель соответствия кандидата на определенную роль в проектной команде. Указанные анкеты должны иметь машиночитаемый вид для автоматизированной обработки. При формировании многочисленных проектных команд это существенно облегчит работу кадрового персонала, занимающегося ресурсным планированием и ускорит принятие решений по выбору нужного кандидата на роль в проектную команду.

Также необходимо произвести отсев кандидатов с точки зрения компетентности в конкретной профессиональной области. Особенности тестирования кандидатов в профессиональных областях эксклюзивны для каждого конкретного проекта и должны быть адаптированы под цели проекта.

Для достижения оптимальной пропорции профессиональных и личностных (PAEI) качеств кандидата при его оценке на должность необходимо определить вес данного показателя.

Если V – удельный показатель соответствия кандидата на должность/роль/функцию, то формула оптимального подбора будет иметь следующий вид:

$$V = \alpha_1 \cdot K_1 + \alpha_2 \cdot K_2, \quad (1)$$

где K_1 – профессиональные качества кандидата;

K_2 – личностные качества кандидата;

α_1, α_2 – значимость качеств, определенная лицом, принимающим решение.

По результатам проведенного расчета необходимо утвердить кандидатов на конкретные позиции в проектной команде. Эта задача может быть выполнена специалистом по кадровому обеспечению, либо руководителем проектной команды. В каждом конкретном случае, в зависимости от особенностей проекта, его целей и задач, утверждение на должность кандидата должно проходить верификацию лицом, принимающим решение.

Указанным способом предлагается достичь оптимального баланса профессиональных и личностных качеств при формировании проектных команд для реализации уникальных проектов (рис. 2).

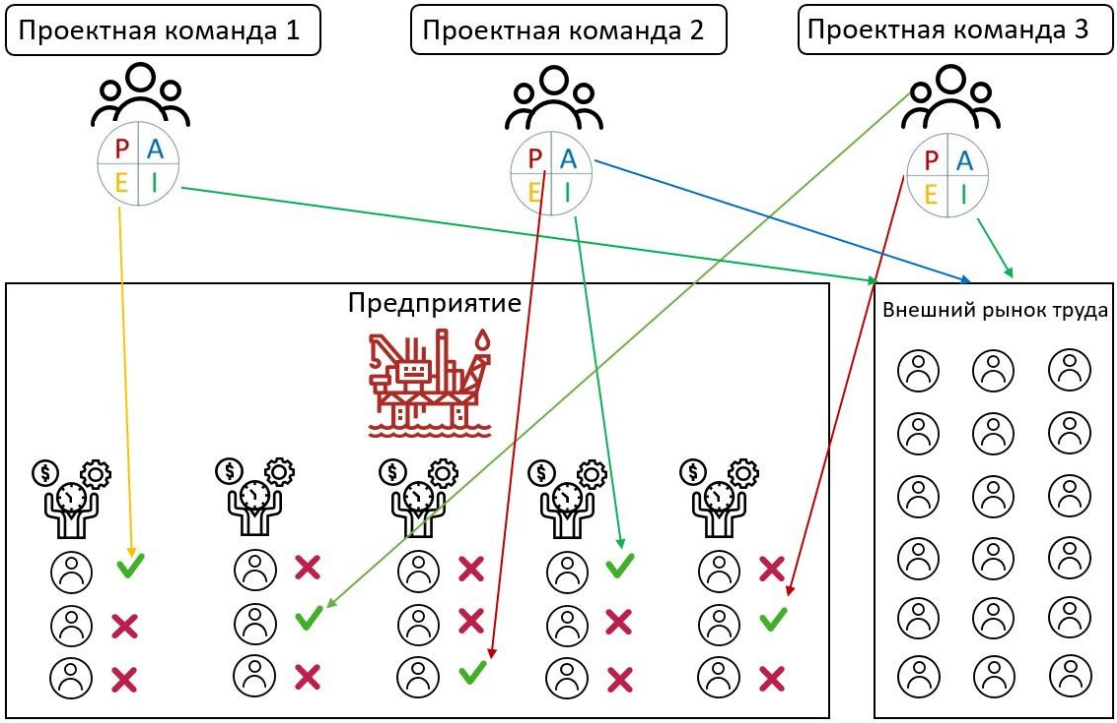


Рисунок 2 – Предлагаемый принцип построения проектных команд

ЦИФРОВОЙ КЛОН СОТРУДНИКА КАК ИНСТРУМЕНТ УПРАВЛЕНИЯ ПРОЕКТНЫМИ КОМАНДАМИ

Вышеупомянутый метод PAEI может не только помогать принимать решение по подбору состава проектных команд оптимальным способом, но и эффективно управлять проектом с точки зрения риск-контроля такого показателя, как сменяемость команды.

После формирования состава участников проектной команды, утверждения плана проекта, его целей и KPI до момента реализации проекта необходимо пройти путь длиною от нескольких месяцев до нескольких лет. Причем чем крупнее проект и длительней, тем сильнее влияние организационных перемен в составе его участников.

Избежать смены участников проектной команды является сложной задачей для любого руководителя проекта. Чем больше проектная команда и дольше проект, тем больше шансов потерять кого-то из ключевых игроков. Помимо внешних факторов (политические, социальные, эпидемиологические) существуют и внутренние факторы (борьба за лидерство, различные точки зрения на ситуацию, неспособность нести ответственность за свои действия, перекладывание ответственности

на смежные направления и другие внутренние разногласия проектной команды). В организационных системах с небольшой численностью такие разногласия могут стать губительными. Например, требуется компетенция узкого специалиста по бурению многоствольных скважин на дне моря, который один на весь регион. В случае потери такого ключевого специалиста проект может быть остановлен до момента появления кандидата с аналогичной компетенцией, что, в свою очередь, несет колоссальные убытки. Привлечение же специалиста с меньшими навыками и опытом потребует времени на его ознакомление со всеми ключевыми решениями по проекту и несет в себе риски для качества предлагаемых решений.

Таким образом, высокие требования к узкоспециальным навыкам членов проектной команды являются одним из ключевых критериев при реализации уникальных проектов.

Для решения проблемы оперативной замены ключевого сотрудника и сохранения его наработанной базы знаний по проекту предлагается разработать программное обеспечение «Цифровой клон сотрудника», которое будет установлено на рабочие компьютеры всех членов проектных команд. Данный продукт может отслеживать ключевые активности персонала с точки зрения методологии PAIE. Принцип работы программного продукта может быть построен на сборе данных, которые сам пользователь загружает в свой профиль. По факту выполнения какого-либо задания член проектный команды получает результат своей работы в виде файла, который он будет загружать в свой «Цифровой клон». Если функционал участника проектной команды не связан с созданием текстовых или иных документов, например, он занимается организацией совещаний, телефонным общением с клиентами, подготовкой макетов объекта строительства, то в данном случае можно загружать скриншот календаря Outlook, протоколы проведенных совещаний, либо любой другой отчет о проделанной работе. По факту загрузки каждого файла пользователь будет получать уведомление об уровне «прокаченности» конкретного навыка P, A, E или I. Система «Цифровой клон» будет определять категорию навыка P, A, E или I, исходя из данных, которые пользователь укажет при загрузке файла.

В рамках реализации проекта «Цифровой клон» необходимо отмечать особо активных пользователей и поощрять их материальным и нематериальным стимулированием. По факту накопления информации о результатах работы каждого сотрудника мы получим его «портфолио работ» – цифровой след о его деятельности на проекте.

Таким образом, мы не только сохраним результаты его работы на случай его увольнения, но также при его вынужденной замене сможем предоставить доступ к этим файлам новому сотруднику, замещающему предыдущего. Новый сотрудник сможет с помощью этого архива гораздо быстрее вникнуть в объем и суть выполненных ранее задач.

Еще одним плюсом данного программного продукта будет то, что при увольнении сотрудника, например, по причине неудовлетворенности в заработной плате, можно будет всегда посмотреть его профиль с загруженными файлами и оценить риски. В каждой организации есть сотрудники, которые выполняют огромный массив работы, но не делают это публично. Бывают случаи, когда человек постоянно жалуется на перегрузку, требует повышения оплаты за выполняемую работу, а по факту регулярно генерирует несколько типовых отчетов. Анализ профиля данного сотрудника позволит руководителю быстрее принять решение о замене такого сотрудника.

Актуальность развития направления цифровых клонов с каждым годом растет. По мнению аналитиков MarketsandMarkets, объем рынка цифровых клонов, который в 2022 г. оценивался в 12,9 млрд долларов США, будет расти со среднегодовыми темпами роста на 36,3 % до 2030 г. [11].

В Российской Федерации глобальных исследований на тему цифровых клонов и объемов этого рынка не проводилось, хотя крупные компании, такие как «ЛУКОЙЛ», «Ростелеком», и «СИБУР» активно прорабатывают это направление [12].

Необходимо отметить, что применение такого рода программного продукта и его администрирование имеет смысл прежде всего на проектах с достаточным для этого бюджетом, так как требует дополнительных денежных затрат. Необходим обученный администратор по работе с данной системой. Также необходимо приобрести и настроить сервер данных с возможностью их безопасного хранения. В проектных командах небольших типовых проектов это может быть неоправданно и не принесет значительного результата.

Руководитель проекта или иное лицо, принимающее решение, должны определить необходимость внедрения данной системы на начальном этапе проекта с точки зрения ее оправданности в каждом конкретном случае, оценив все риски по потере персонала.

ЗАКЛЮЧЕНИЕ

Предложенные подходы к формированию и управлению командами при реализации уникальных проектов могут помочь их руководителям в принятии кадровых решений, позволяют регулировать вопросы мотивации участников проектных команд, минимизируют негативные последствия при потере ключевых участников. Кроме того, создается «бэкап» всех значимых документов пользователя, который в дальнейшем можно модернизировать в систему отчетности со сведениями об участии сотрудников в проектах и бизнес-процессах, а при экспертном анализе данных система также позволит понять объем и качество результатов работы каждого сотрудника.

Список источников

1. Подольский, А. Г. Система показателей оценки уровня компетенций молодых специалистов на соответствие их требованиям оборонно-промышленного комплекса / А. Г. Подольский, А. С. Красникова // Экономика высокотехнологичных производств. – 2022. – Т. 9, № 10. – С. 1618.

2. BP выяснила причины взрыва на нефтяной платформе // РИА Новости. – URL: https://ria.ru /20100829/270138434.html.

3. Качалин, А. BP в течение 16 лет выплатит пяти штатам США $20,8 млрд за разлив нефти 2010 года / А. Качалин // ТАСС. – URL: https://tass.ru/ekonomika/3176091.

4. Заренков, В. А. Управление проектами : учеб. пос. / В. А. Заренков. – Москва : Изд-во АСВ ; Санкт-Петербрг : СПбГАСУ, 2005. – 36 с.

5. Бандурин, А. В. Особенности проектно-ориентированной компании как среды проявления компетенций персонала / А. В. Бандурин // Креативная экономика. – 2023. – Том 17, № 5. – С. 1671–1688. DOI: 10.18334/ce.17.5.117779.

6. Мазур, И. И. Управление проектами : учеб. пос. / И. И. Мазур, В. Д. Шапиро, Н. Г. Ольдерогге. – Москва : Омега-Л, 2004. – С. 82.

7. Зубова, А. А. Проблемы формирования проектных команд в IT-сфере / А. А. Зубова // Прикаспийский журнал: управление и высокие технологии. – 2024. – № 2 (66). – С. 42.

8. Адизес, И. К. Идеальный руководитель. Почему им нельзя стать и что из этого следует / И. К. Адизес. – Альпина Диджитал, 2004. – С. 16.

9. Иванов, А. М. Синергия стратегического превосходства и наставничества как технология передачи компетенций в качестве инструмента повышения конкурентоспособности высокотехнологичных производств / А. М. Иванов, Д. А. Стюхин // Экономика высокотехнологичных производств. – 2021. – Т. 2, № 1. – С. 63–79.

10. Кохно, П. А. Уровень высокотехнологичного производства определяет человеческий капитал / П. А. Кохно // Экономика высокотехнологичных производств. – 2021. – Т. 2, № 3. – С. 172.

11. O'Gorman, Tristan. How digital twins optimize the performance of your assets in a sustainable way / Tristan O'Gorman // IBM. 4 апреля 2023. – URL: https://www.ibm.com/blog/how-digital-twins-optimize-the-performance-of-your-assets-in-a-sustainable-way/.

12. Подборка московских решений: цифровые двойники и моделирование производственных процессов. – URL: https://ict.moscow/news/cards-digital-twins/.

References

1. Podolsky, A. G., Krasnikova, A. S. System of indicators for assessing the level of competencies of young specialists to meet the requirements of the defense-industrial complex. *Economics of High-tech Industries*, 2022, vol. 9, no. 10, p. 1618 (In Russ.).

2. BP reveals causes of oil platform explosion. *RIA Novosti.* Available at: https://ria.ru /20100829/270138434.html (In Russ.).

3. Kachalin, A. BP will pay five US states $20.8 bln for the 2010 oil spill within 16 years. *TASS.* Available at: https://tass.ru/ekonomika/3176091 (In Russ.).

4. Zarenkov, V. A. *Project management: training manual.* Moscow, ASV Publishing House ; St. Petersburg, SPbGASU, 2005. 36 p. (In Russ.).

5. Bandurin, A. V. Features of the project-oriented company as an environment of manifestation of personnel competencies. *Creative Economy*, 2023, vol. 17, no. 5, pp. 1671–1688. DOI: 10.18334/ce.17.5.117779 (In Russ.).

6. Mazur, I. I., Shapiro, V. D., Olderogge, N. G. *Project management: training manual.* Moscow, Omega-L, 2004, p. 82 (In Russ.).

7. Zubova, A. A. Problems of forming project teams in IT-sphere. *Caspian Journal: Management and High Technologies,* 2024, no. 2 (66), p. 42 (In Russ.).

8. Adizes, I. K. *The Ideal Leader. Why it is impossible to become one and what follows from it.* Alpina Digital, 2004, p. 16 (In Russ.).

9. Ivanov, A. M., Stukhin, D. A. Synergy of strategic excellence and mentoring as a technology of competence transfer as a tool to improve the competitiveness of high-tech industries. *Economics of High-tech Industries*, 2021, vol. 2, no. 1, pp. 63–79 (In Russ.).

10. Kokhno, P. A. The level of high-tech production determines human capital. *Economics of High-tech Industries*, 2021, vol. 2, no. 3, p. 172 (In Russ.).

11. O'Gorman, Tristan. How digital twins optimize the performance of your assets in a sustainable way. *IBM*, 4 April 2023. Available at: https://www.ibm.com/blog/how-digital-twins-optimize-the-performance-of-your-assets-in-a-sustainable-way/.

12. *A selection of Moscow solutions: digital twins and modeling of production processes.* Available at: https://ict.moscow/news/cards-digital-twins/ (In Russ.).

Статья поступила в редакцию 04.09.2024; одобрена после рецензирования 23.09.2024; принята к публикации 24.09.2024.

The article was submitted 04.09.2024; approved after reviewing 23.09.2024; accepted for publication 24.09.2024.

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УДК 303.732.4

МОДЕЛИРОВАНИЕ, ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СИСТЕМЫ ГЕНЕРАЦИИ АНКОРОВ ДЛЯ ОПТИМИЗАЦИИ ПОКАЗАТЕЛЕЙ ССЫЛОЧНОГО РАНЖИРОВАНИЯ САЙТА

Соловьев Денис Сергеевич, Тамбовский государственный университет имени Г.Р. Державина, 392036, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,

кандидат технических наук, доцент, ORCID: 0000-0001-6613-3218, e-mail: solovjevdenis @mail.ru

Соловьева Инна Александровна, Тамбовский государственный университет имени Г.Р. Державина, 392036, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,

кандидат технических наук, старший преподаватель, ORCID: 0000-0002-1798-1859, e-mail: good.win32@yandex.ru

***Самохвалов Алексей Владимирович*,** Тамбовский государственный университет имени Г.Р. Державина, 392036, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,

кандидат педагогических наук, доцент, ORCID: 0000-0002-3151-3250, e-mail: samohvalov @gmail.com

***Михайлова Елена Михайловна*,** Тамбовский государственный университет имени Г.Р. Державина, 392036, Российская Федерация, г. Тамбов, ул. Интернациональная, 33,

кандидат педагогических наук, доцент, ORCID: 0000-0002-8860-6562, e-mail: 277lena@mail.ru

В условиях роста числа веб-сайтов и ужесточения критериев ранжирования поисковыми системами автоматизация генерации анкоров для увеличения ссылочной массы является актуальной задачей в области SEO, поскольку их ручное создание требует значительных временных и трудовых затрат. С использованием методологии IDEF0 построена функциональная модель системы для генерации анкоров. Выполнено проектирование диаграммы компонентов системы генерации анкоров при помощи стандарта UML. Реализация системы представляет собой веб-приложение, которое позволяет формировать список анкоров на основе автоматической генерации ссылки с учетом заданных пользовательских параметров, а также предоставляет возможность пополнения встроенного словаря для расширения функциональности системы.

Ключевые слова: система генерации анкоров, функциональное моделирование, IDEF0, проектирование, UML, диаграмма компонентов, веб-приложение, интерфейс

MODELING, DESIGNING AND IMPLEMENTING AN ANCHOR GENERATION SYSTEM FOR OPTIMIZING SITE LINK RANKING INDICATORS

Solovjev Denis S., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392036, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-6613-3218, e-mail: solovjevdenis @mail.ru

Solovjeva Inna A., Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392036, Russian Federation,

Cand. Sci. (Engineering), Senior Lecturer, ORCID: 0000-0002-1798-1859, e-mail: good.win32@ yandex.ru

***Samokhvalov Alexey V.*,** Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392036, Russian Federation,

Cand. Sci. (Pedagogics), Associate Professor, ORCID: 0000-0002-3151-3250, e-mail: samohvalov @gmail.com

***Mikhailova Elena M.*,** Tambov State University named after G.R. Derzhavin, 33 Internatsionalnaya St., Tambov, 392036, Russian Federation,

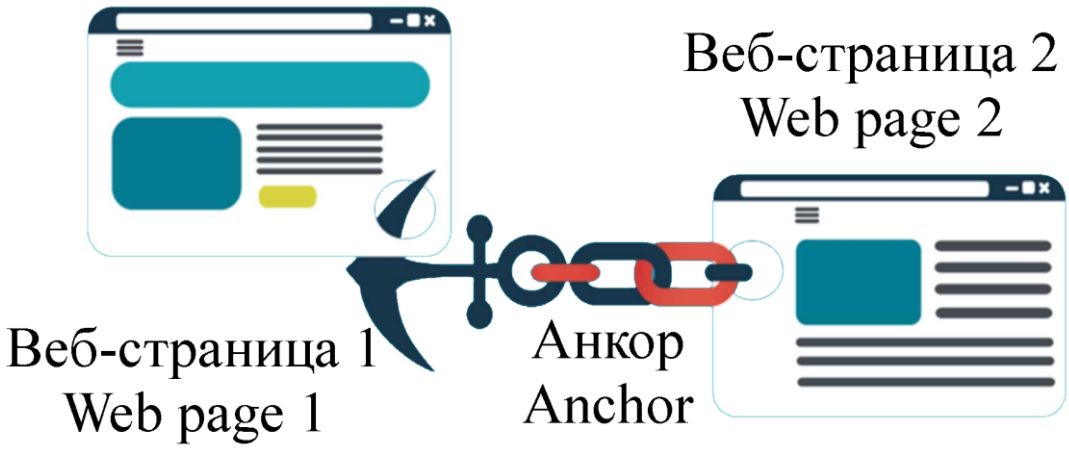
Cand. Sci. (Pedagogics), Associate Professor, ORCID: 0000-0002-8860-6562, e-mail: 277lena @mail.ru

Automation of anchor generation for increasing link mass is a relevant task in the field of SEO in the context of the websites growing number and tightening ranking criteria by search engines, since their manual creation requires significant time and labor costs. The functional model of the anchor generation system using the IDEF0 methodology is built. Design of the component

diagram for anchor generation system using the UML standard is completed. The implementation of the system is a web application that allows you to create a list of anchors based on automatic link generation taking into account specified user parameters. Additionally, there is the ability to replenish the built-in dictionary to expand the functionality of the system.

Keywords: anchor generation system, functional modeling, IDEF0, design, UML, component diagram, web application, interface

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

С учетом стремительного проникновения интернета в повседневную жизнь и постоянного увеличения числа веб-сайтов разнообразной тематики, особое внимание следует уделить продвижению сайтов в поисковых системах [1, 2]. Увеличение количества веб-страниц в сети обусловливает ужесточение критериев, применяемых поисковыми системами для определения релевантности страниц запросам пользователей, что усложняет процесс влияния на результаты выдачи [3, 4]. Одним из ключевых факторов, определяющих релевантность страниц в выдаче поисковых систем, является ссылочное ранжирование [5, 6]. Чем большее количество внешних ссылок указывает на сайт, тем выше вероятность его посещаемости и признания поисковой системой как релевантного по определенному запросу. В условиях высокой конкуренции среди сайтов с аналогичной тематикой, а также учитывая принципы работы поисковых алгоритмов, оптимизаторы вынуждены вручную создавать и размещать значительное количество ссылок на сторонних ресурсах, что требует значительных временных и трудовых затрат. В связи с этим разработка системы генерации анкоров представляет собой актуальную задачу в области SEO.

Когда речь идет о продвижении небольшого сайта, создание качественных анкоров для увеличения ссылочной массы не вызывает особых затруднений. Однако ситуация значительно усложняется при необходимости наращивания ссылок для крупных сайтов с тысячами страниц и множеством запросов. В таком контексте трудоемкость генерации анкоров возрастает многократно, что является общей проблемой для компаний, занимающихся оптимизацией сайтов [7, 8]. Количество необходимых ссылок для каждого конкретного запроса зависит от тематики сайта и ряда значимых показателей, таких как тематический индекс цитирования, количество внешних ссылок на ресурс, вес запроса и планируемое количество ссылок на различных этапах продвижения. Определение необходимого количества ссылок и процесс создания анкоров требует значительных усилий и внимания со стороны оптимизаторов. Таким образом, разработка системы автоматизации генерации анкоров может существенно облегчить задачи по улучшению ссылочного ранжирования.

Цель данной работы заключается в повышении показателей ссылочного ранжирования за счет автоматизации процессов и улучшения качества ссылочной массы оптимизируемых сайтов с минимальными затратами времени и ресурсов.

ФУНКЦИОНАЛЬНОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ ГЕНЕРАЦИИ АНКОРОВ

На рисунке 1 представлена функциональная модель системы, предназначенной для генерации анкоров, построенная с использованием методологии IDEF0 [9].

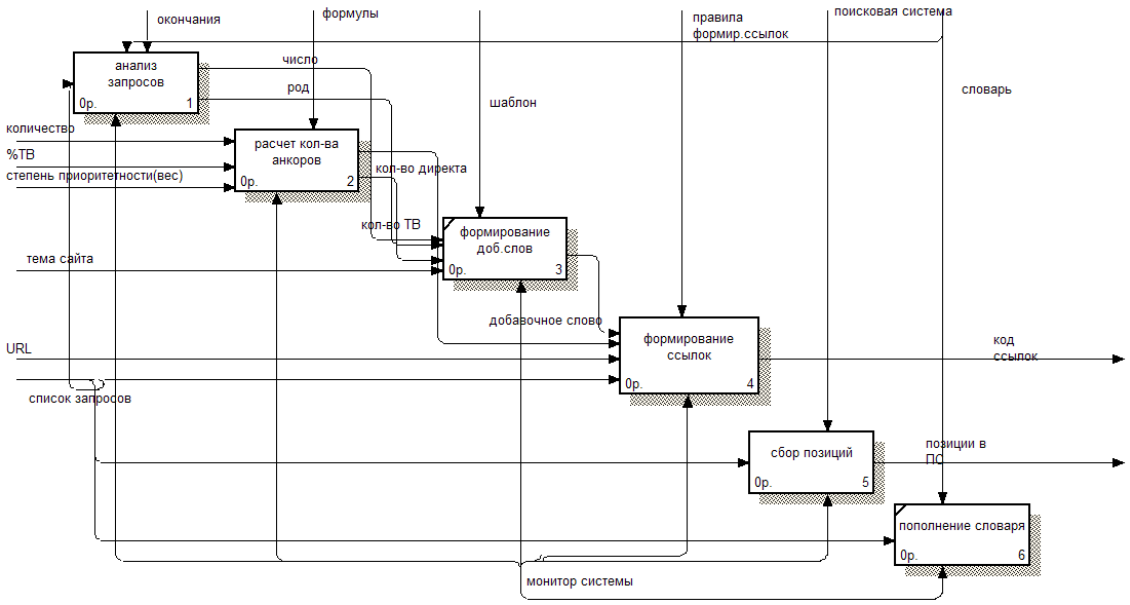


Рисунок 1 – Процесс генерации анкоров

Для работы системы необходимы следующие входные данные: список запросов с соответствующими URL продвигаемых страниц, общее количество требуемых ссылок и процентное соотношение ссылок, которые необходимо оставить без изменений; тематика сайта и степень приоритетности каждого запроса. Результатом работы системы является вывод списка анкоров и позиций запросов в поисковой системе Яндекс. Управляющими факторами системы выступают: формула расчета количества ссылок для каждой фразы из списка, словарь, окончания, правила формирования ссылок, поисковая система и шаблон добавочных фраз. Процесс генерации анкоров осуществляется монитором системы и может быть разделен на две основные стадии: определение количества анкоров для каждого запроса и формирование анкор-листа.

На первом этапе, используя общее количество необходимых ссылок и процент ссылок, которые следует оставить без изменений, рассчитывается количество анкоров для каждого запроса, которое останется неизменным, а также количество анкоров с добавочными словами. Для формирования анкоров в качестве входных параметров используются: список запросов, соответствующие им URL, тематика сайта и рассчитанное на предыдущем этапе необходимое и допустимое количество анкоров. Управляющими факторами на этом этапе являются шаблон анкоров, правила формирования ссылок в HTML и набор слов различной тематики.

Задача определения количества анкоров делится на подзадачи: расчет количества ссылок без изменения исходной фразы и расчет количества директовых анкоров. Процесс анализа исходных данных представлен на рисунке 2.

Задача формирования анкор-листа также подразделяется на несколько подзадач: формирование анкоров с точным вхождением (ТВ), генерация директовых анкоров и составление общего анкор-листа. Процесс формирования анкор-листа иллюстрируется на рисунке 3.

Анализ исходных слов необходим для определения словоформ добавочных слов из шаблона. В каждой фразе исходного списка, состоящей более чем из одного слова, выделяется главное слово. Далее осуществляется поиск точного совпадения исходного слова со словарным. В случае нахождения совпадения исходному слову присваивается тот же род и число, что и у словарного. Если совпадение не найдено, производится выделение основы исходных и словарных слов с последующим поиском точных совпадений измененных пар слов. При отсутствии совпадений исходное слово записывается в словарь.

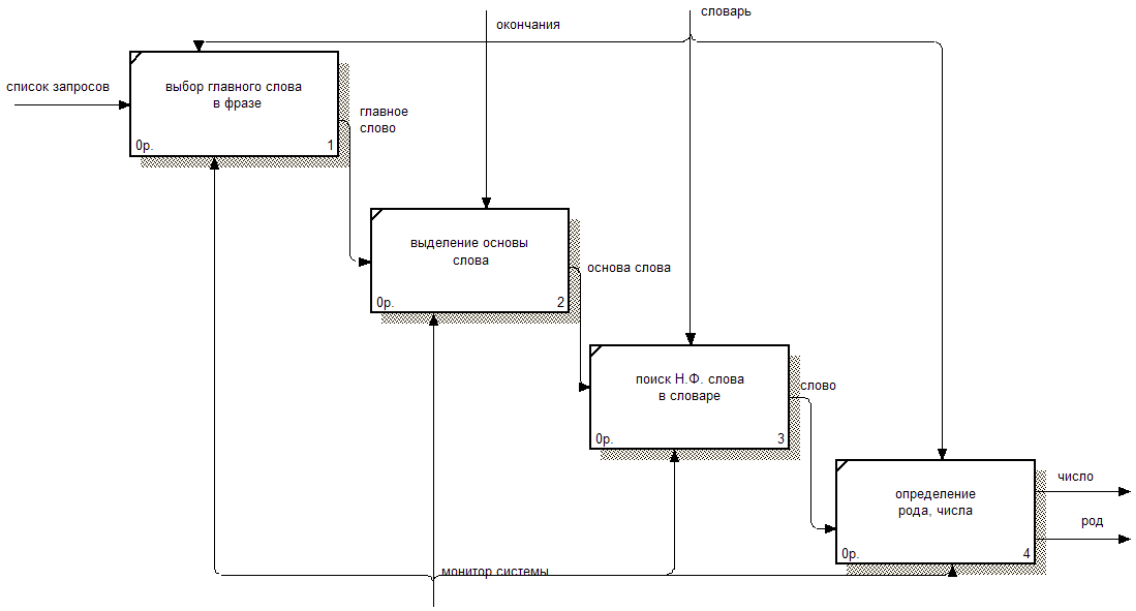


Рисунок 2 – Анализ исходного запроса

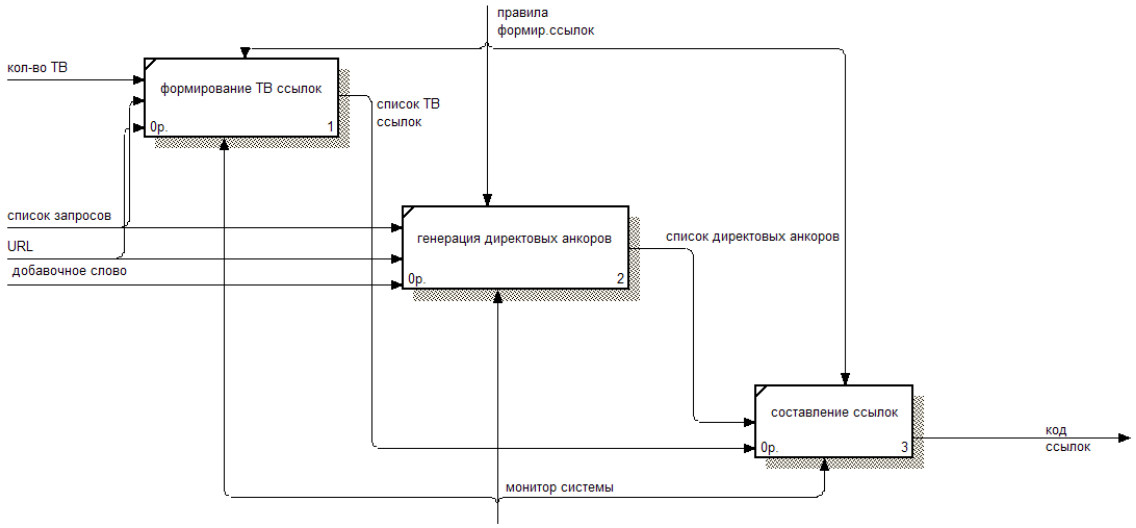


Рисунок 3 – Формирование анкор-листа

Применение функции Левенштейна в системе генерации анкоров позволяет сократить время, затрачиваемое на определение рода, числа и падежа исходного слова [10]. Поскольку в словаре может отсутствовать точное совпадение с исходным словом, выделяются основы как исходных, так и словарных слов с последующим повторным поиском по словарю. Учитывая большой объем словаря, сравнение исходного слова со словарными занимает значительное время; поэтому необходимо производить отсев словарных слов на определенных этапах работы системы. После первого прохождения по циклу выбираются словарные слова с наименьшим значением расстояния Левенштейна. Максимально допустимое значение расстояния зависит от длины исходного слова. Дальнейший анализ осуществляется с учетом слов с минимальным значением расстояния Левенштейна.

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ГЕНЕРАЦИИ АНКОРОВ

На рисунке 4 изображена диаграмма компонентов проектируемой системы, построенная с использованием стандарта UML [11].

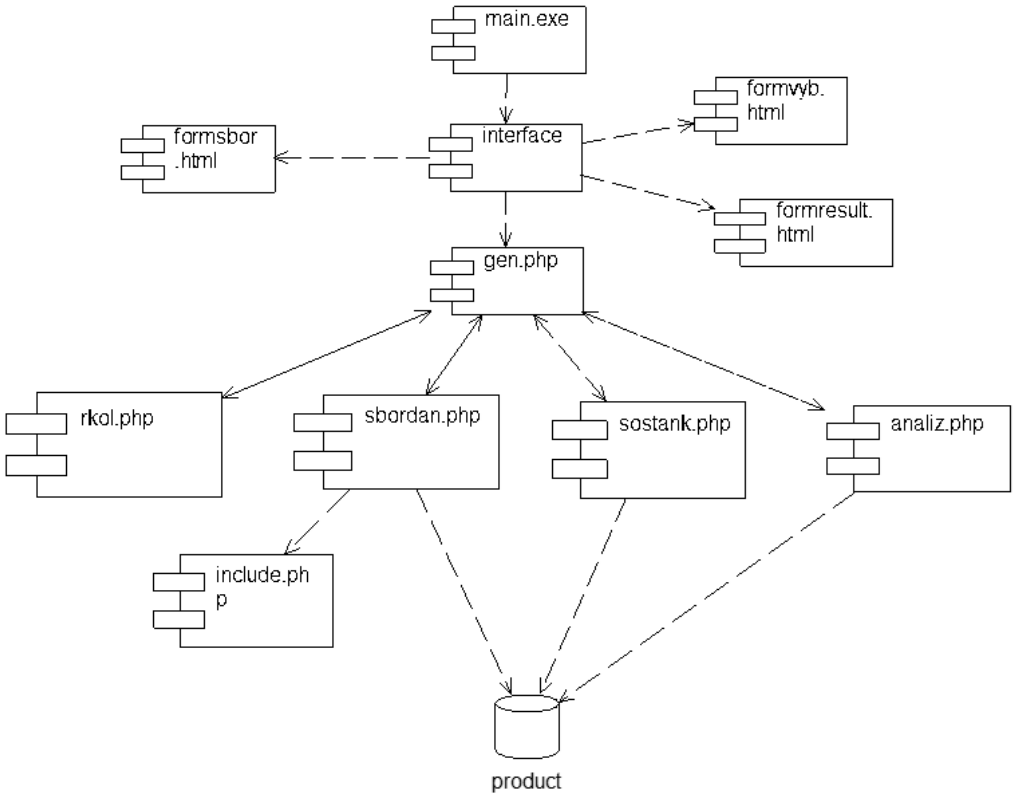


Рисунок 4 – Диаграмма компонентов системы генерации анкоров

В системе генерации анкоров можно выделить несколько ключевых компонентов, среди которых: исполняемый файл системы, файлы со скриптами функций, файлы подключаемых библиотек, база данных (БД) и описание интерфейса системы.

Основным исполняемым файлом является файл main, который отвечает за реализацию работы системы. Этот файл зависит от MainInterface, обеспечивающего интерфейсные функции системы. В свою очередь, MainInterface зависит от файла gen, содержащего основные функции, выполняемые системой, а также от файлов formsbor, formvyb и formresult.

Файлы formsbor, formvyb и formresult являются HTML-страницами, которые содержат код форм для сбора данных, выбора режима работы и отображения результатов функционирования системы. Эти файлы формируют интерфейс на различных этапах работы системы, следуя стандартам языка разметки HTML.

Файл gen напрямую зависит от реализации файлов rkol, sbor.dan, analiz и sostavlenieanc, которые представляют собой рабочие компоненты с исходным кодом проектируемой системы. В файле sbor.dan реализован код обработки данных, полученных от пользователя. Список запросов, URL и вес каждого запроса записываются в таблицу БД, а данные о необходимом количестве ссылок и проценте точных вхождений сохраняются в соответствующих переменных. Пользователь может предоставить список запросов в формате Excel, из которого данные программно извлекаются и записываются в таблицу базы данных для удобства дальнейшего использования. Компонент sbor.dan зависит от файла include, содержащего код для преобразования данных из Excel в общепринятую кодировку символов, что упрощает последующую обработку исходных данных.

Файл rkol включает исходный код для расчета необходимого количества анкоров, которые содержат только точные вхождения запросов, а также количество директовых анкоров для каждого запроса. В файле analiz представлен код анализа введенных запросов: если запрос состоит из нескольких слов, выбирается главное слово; если запрос однословный, анализируется только оно. Определяются род и число продвигаемого запроса, что необходимо для выбора правильных окончаний добавочных слов и фраз. Для этого устанавливается соединение с базой данных, и по словарю определяется род и число запрашиваемого слова.

Файл sostavlenieanc содержит код для формирования анкоров. Учитывая общее количество необходимых анкоров и количество ссылок для каждого запроса с точными вхождениями, а также тематику сайта, выбирается шаблон для формирования директовых анкоров. В соответствии с установленными родом и числом запрашиваемого слова из БД выбираются соответствующие окончания, которые добавляются к словам и словосочетаниям шаблона. Затем формируется HTML-код ссылок, который отображается пользователю.

Поскольку таблицы списка запросов, словарь и шаблоны добавочных слов/словосочетаний хранятся в БД, они необходимы для работы исходного кода файлов sbor.dan, analiz и sostavlenieanc. Все эти компоненты зависят от компонента product, представляющего собой базу данных.

РЕАЛИЗАЦИЯ СИСТЕМЫ ГЕНЕРАЦИИ АНКОРОВ

Система функционирует как веб-приложение и ее основные модули размещены на удаленном сервере, к которому подключаются рабочие компьютеры пользователей для взаимодействия с приложением.

В начале взаимодействия пользователя с системой отображается меню, в котором он может выбрать соответствующий пункт для определения типа задачи, требующей решения. При выборе опции «генерация анкоров без окружающего текста» пользователь сталкивается с необходимостью выбрать режим генерации анкоров: с заранее распределенным количеством ссылок или с автоматическим распределением ссылок.

Следующий этап работы системы, вне зависимости от предыдущего выбора, включает загрузку файла с распределенными запросами, для которых требуется сформировать ссылки. Содержимое загружаемого Excel-файла должно содержать следующие столбцы: запросы для формирования ссылок, соответствующие URL страниц сайта и степень приоритетности каждого запроса, т. е. вес запроса. В случае предварительного определения количества необходимых анкоров для каждого запроса, в третьем столбце указывается не вес запроса, а количество анкоров, которое необходимо сформировать. Для подтверждения корректности загруженного файла данные отображаются для предпросмотра. На данном этапе пользователь имеет возможность внести изменения в исходные данные и продолжить процесс, нажав кнопку «Далее». Данный этап представлен на рисунке 5.

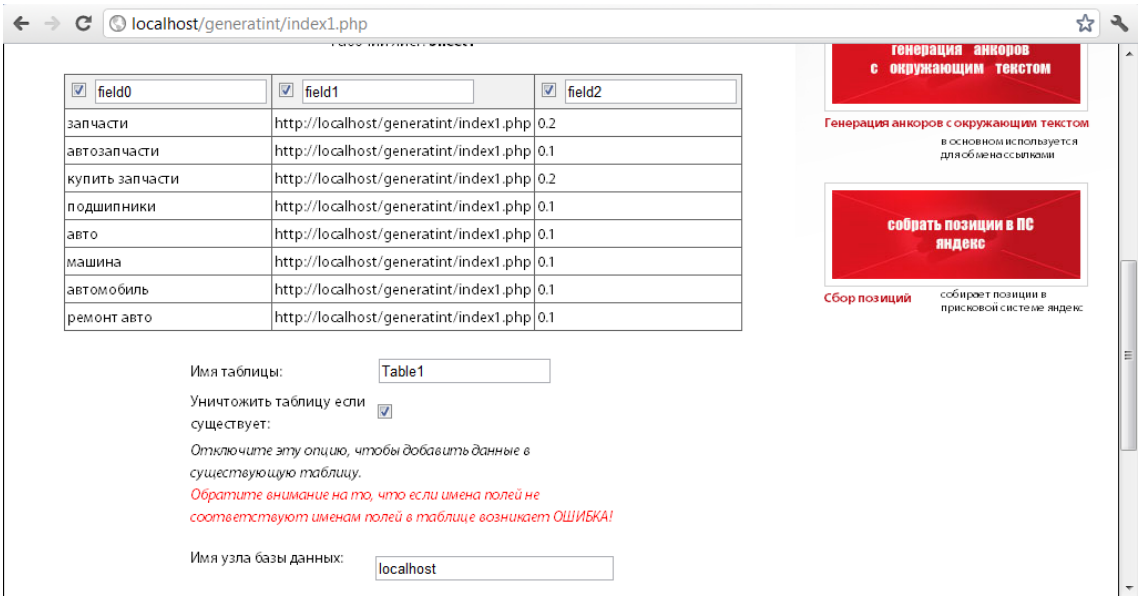


Рисунок 5 – Предварительный просмотр исходных данных

Следующим шагом, независимо от изначально выбранного режима работы системы, является определение процента ссылок от общего числа, которые останутся без изменений, а также общее количество ссылок в случае выбора режима «Генерация анкоров с расчетом количества ссылок на каждый запрос». Кроме того, на этом этапе пользователю предлагается определить категорию проекта, как показано на рисунке 6.

После нажатия кнопки «Далее» система обрабатывает все полученные данные и выводит результат в соответствующую форму. Пользователь может отредактировать результирующие данные или оставить их без изменений. Результат работы системы в режиме «Генерация анкоров с автоматическим расчетом количества ссылок на каждый запрос» представлен на рисунке 7.

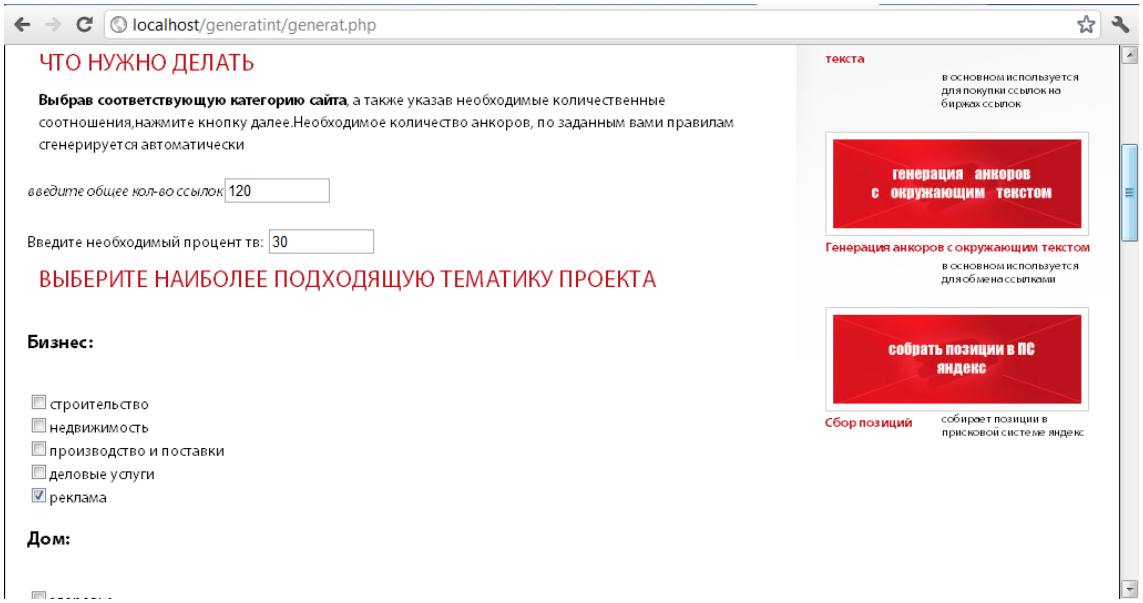


Рисунок 6 – Выбор категории сайта

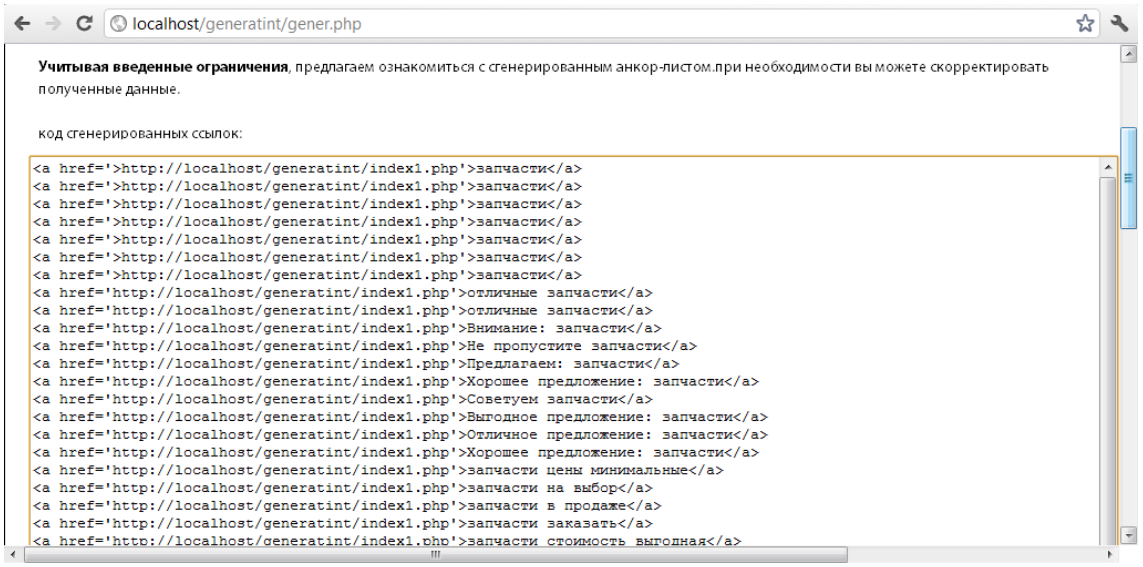


Рисунок 7 – Вывод анкор-листа

В процессе работы системы, особенно на этапе обработки исходных данных, могут возникнуть следующие ошибки: неверно указан путь к загружаемому файлу; загруженный файл пуст и/или имеет неверный формат; поле процента ссылок, которые необходимо оставить без изменений, не заполнено; не указано количество необходимых ссылок; в словаре не найдено слово в начальной форме для указанного в файле запроса.

В случае возникновения ошибок пользователю предоставляется возможность их исправить, введя недостающие данные или пополнив словарь. Если после многочисленных преобразований определить начальную форму слова по словарю не удается, на экран выводится сообщение об ошибке с указанием отсутствия слова в словаре.

Пользователь может пополнить словарь системы, заполнив соответствующие поля формы: ввести слово в начальной форме (именительном падеже, единственном числе); указать род этого слова. При нажатии кнопки «Пополнить словарь» вызывается соответствующий скрипт для обработки введенных данных.

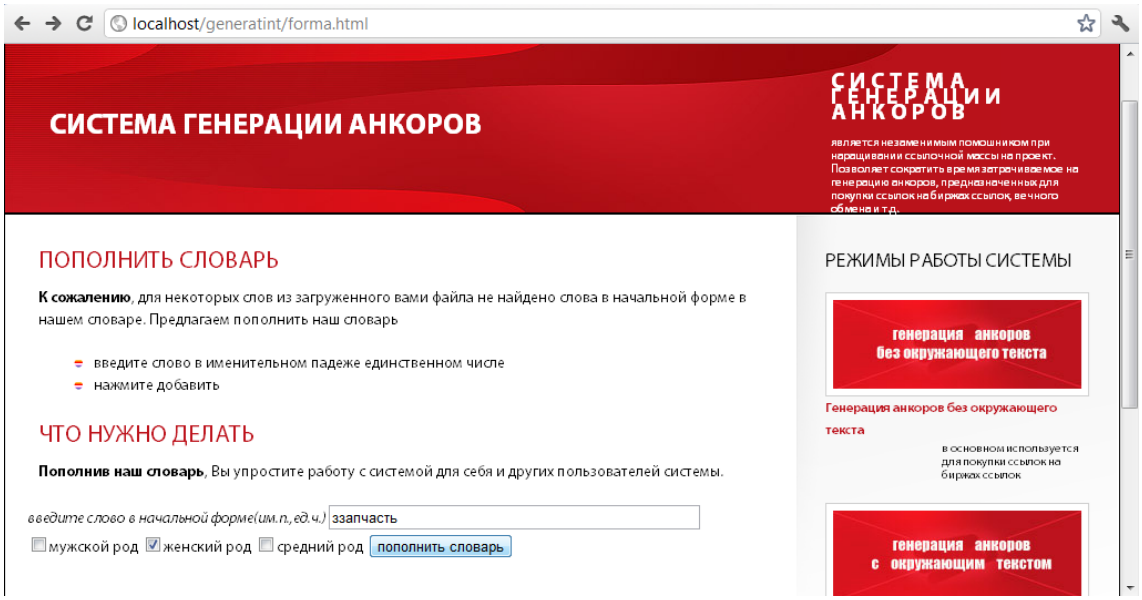


Рисунок 8 – Добавление словарного слова

Система также предоставляет возможность сбора позиций по продвигаемым запросам в поисковой системе. Выбрав соответствующий пункт меню в начале работы системы, пользователю предлагается заполнить необходимые поля формы, на основе которых она формирует ответ пользователю в виде таблицы.

ЗАКЛЮЧЕНИЕ

Ссылочное ранжирование представляет собой один из ключевых факторов, влияющих на позиционирование документов в результатах поиска. Данный процесс основывается на оценке текста ссылок, который указывает на документ, и его влиянии на релевантность этого документа по отношению к конкретному запросу. В частности, наличие слов запроса в тексте ссылок, ссылающихся на документ из других источников, способствует повышению его релевантности. В условиях высокой конкуренции среди сайтов с аналогичной тематикой SEO-оптимизаторы уделяют особое внимание ссылочному ранжированию и улучшению качества ссылочной массы продвигаемых ресурсов. Это обусловлено необходимостью ручного создания значительного количества анкоров и их размещения на сторонних платформах, что требует дополнительных временных и трудовых затрат. Разработанная система автоматизации направлена на решение ряда задач, связанных с оптимизацией ссылочного ранжирования, включая: генерацию ссылок без окружающего текста, что актуально для покупки мест под ссылки на специализированных биржах; создание ссылок с окружающим текстом для участия в обменах ссылками и размещения их в статьях; расчет необходимого количества ссылок для достижения заданных целей; сбор данных о позициях запросов продвигаемого сайта в поисковой системе. Реализация указанных задач приводит к повышению качества ссылочной массы оптимизируемых сайтов при минимальных затратах ресурсов, времени и усилий со стороны оптимизаторов, а также улучшению показателей ссылочного ранжирования благодаря внедрению автоматизированных решений.

Список источников

1. Брумштейн, Ю. М. Отражение научной деятельности региональных вузов на сайтах в Интернете: системный анализ вопросов информационной безопасности / Ю. М. Брумштейн, А. А. Бондарев, А. В. Федотова, М. В. Иванова // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 2 (26). – С. 85–100.

2. Коспай, Д. К. SEO-оптимизация как ключевой инструмент продвижения бренда и продуктов компании: исследование методов / Д. К. Коспай, Л. М. Алимжанова // Интеллектуальные технологии на транспорте. – 2023. – № S1 (35–1). – С. 70–76.

3. Фитеров, Д. SEO-продвижение сайта практические рекомендации / Д. Фитеров // БИТ. Бизнес & Информационные технологии. – 2019. – № 7 (90). – С. 46–50.

4. Ласкавнев, А. С. Сравнительный анализ традиционных и инновационных подходов в SEO / А. С. Ласкавнев // Практический маркетинг. – 2024. – № 4 (322). – С. 39–42.

5. Ширай, М. А. Исследование ранжирования интернет-ресурсов и методов построения обратного ссылочного индекса / М. А. Ширай, О. Г. Григорьев // Труды Института системного анализа Российской академии наук. – 2010. – Т. 58. – С. 127–136.

6. Ширай, М. А. Решение задачи тематического ссылочного ранжирования интернет-ресурсов / М. А. Ширай, О. Г. Григорьев // Информационные технологии и вычислительные системы. – 2012. – № 4. – С. 6–15.

7. Hashmi, K. A. Guided Table Structure Recognition Through Anchor Optimization / K. A. Hashmi, D. Stricker, M. Liwicki, M. N. Afzal, M. Z. Afzal // IEEE Access. – 2021. – Vol. 9. – P. 113521–113534.

8. Zhao, J. Optimization of anchor position allocation considering efficiency and safety demand / J. Zhao, C. Zhou, Z. Li, Y. Xu, L. Gan // Ocean & Coastal Management. – 2023. – Vol. 241. – P. 106644.

9. Черемных, С. В. Структурный анализ систем: IDEF-технологии / С. В. Черемных, И. О. Семенов, В. С. Ручкин. – Москва : Финансы и статистика, 2003. – 208 с.

10. Сапаров, А. Ю. Уточнение результатов распознавания математических формул с использованием расстояния Левенштейна / А. Ю. Сапаров, А. П. Бельтюков, С. Г. Маслов // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. – 2020. – Т. 30, № 3. – С. 513–529.

11. Буч, Г. Язык UML. Руководство пользователя / Г. Буч, Дж. Рамбо, А. Джекобсон. – Москва : ДМК, 2015. – 432 с.

References

1. Brumsteyn, Yu. M., Bondarev, A. A., Fedotova, A. V., Ivanova, M. V. Reflection of regional univesities scientific activity on internet-sites: system analysis of information security questions. *Caspian Journal: Control and High Technologies*, 2014, no. 2 (26), pp. 85–100 (In Russ.).

2. Kospay, D. K., Alimzhanova, L. M. Seo optimization as a key tool for promoting a company's brand and products: research methods. *Intelligent Technologies in Transport*, 2023, no. S1 (35–1), pp. 70–76 (In Russ.).

3. Fiterov, D. SEO website promotion: practical recommendations. *BIT. Business & Information Technologies*, 2019, no. 7 (90), pp. 46–50 (In Russ.).

4. Laskavnyov, A. S. Comparative analysis of traditional and innovative approaches in SEO. *Practical Marketing*, 2024, no. 4 (322), pp. 39–42 (In Russ.).

5. Shiray, M. A., Grigoryev, O. G. Research of Internet resource ranking and methods of constructing a reverse link index. *Proceedings of the Institute of Systems Analysis of the Russian Academy of Sciences*, 2010, no. 58, pp. 127–136 (In Russ.).

6. Shiray, M. A., Grigoryev, O. G. Solution of topical reference ranking web resources. *Information Technologies and Computing Systems*, 2012, no. 4, pp. 6–15 (In Russ.).

7. Hashmi, K. A., Stricker, D., Liwicki, M., Afzal, M. N., Afzal, M. Z. Guided Table Structure Recognition Through Anchor Optimization. *IEEE Access*, 2021, vol. 9, pp. 113521–113534.

8. Zhao, J., Zhou, C., Li, Z., Xu, Y., Gan, L. Optimization of anchor position allocation considering efficiency and safety demand. *Ocean & Coastal Management*, 2023, vol. 241, p. 106644.

9. Cheremnyh, S. V., Semenov, I. O., Ruchkin, B. C. *Structural analysis of systems: IDEF technologies.* Moscow, Finansy i statistika Publ., 2003. 208 p. (In Russ.).

10. Saparov, A. Yu., Beltyukov, A. P., Maslov, S. G. Refinement of the results of recognition of mathematical formulas using the Levenshtein distance. *Bulletin of Udmurtia Universitety: Mathematics, Mechanics, Computer Science*, 2020, vol, 30, no. 3, pp. 513–529 (In Russ.).

11. Booch, G., Rumbaugh, J., Jacobson, A. *UML Language. User's Guide.* Moscow, DMK Publ, 2015. 432 p. (In Russ.).

Статья поступила в редакцию 08.10.2024; одобрена после рецензирования 21.10.2024; принята к публикации 23.10.2024.

The article was submitted 08.10.2024; approved after reviewing 21.10.2024; accepted for publication 23.10.2024.

УДК 004.056

ИССЛЕДОВАНИЕ УГРОЗ СЕТЕВОЙ БЕЗОПАСНОСТИ

Калмыков Игорь Анатольевич, Северо-Кавказский Федеральный университет, 355001, Российская Федерация, г. Ставрополь, пр. Кулакова 2,

доктор технических наук, профессор кафедры вычислительной математики и кибернетики, профессор, ORCID: 0000-0002-9854-5310, e-mail: kia762@yandex.ru

Кандаурова Наталья Владимировна, Ставропольский многопрофильный колледж, 355001, Российская Федерация, г. Ставрополь, пр. Кулакова, 8а,

доктор технических наук, профессор, директор Ставропольского многопрофильного колледжа, ORCID: 0000-0003-0928-4022, e-mail: candaur18@yandex.ru

Кононова Наталия Владимировна, Ставропольский многопрофильный колледж, 355001, Российская Федерация, г. Ставрополь, пр. Кулакова, 8а,

кандидат физико-математических наук, доцент, заведующая кафедрой информационной безопасности, ORCID: 0000-0002-8988-0694, e-mail: knv_fm@mail.ru

Воробьева Лариса Викторовна, Ставропольский многопрофильный колледж, 355001, Российская Федерация, г. Ставрополь, пр. Кулакова, 8а,

преподаватель кафедры информационной безопасности, ORCID: 0009-0005-1674-659X, e-mail: laravorob@yandex.ru

Пелешенко Татьяна Александровна, Северо-Кавказский Федеральный университет, 355001, Российская Федерация, г. Ставрополь, пр. Кулакова 2,

кандидат технических наук, доцент кафедры вычислительной математики и кибернетики, ORCID: 0000-0003-2761-7847, e-mail: gtanya09@mail.ru

В данной статье проведено исследование актуальных угроз информационной безопасности в настоящее время, ведь в современном мире зачастую умалчиваются вопросы кибербезопасности, чтобы не навредить репутации компании. Очень сложно дать оценку и посчитать количество кибератак, поэтому мы используем официальную информацию из различных источников, занимающихся расследованием инцидентов и анализом действий хакерских групп. С развитием современных технологий, искусственного интеллекта, облачных решений и систем доставки контента увеличиваются и усложняются варианты кибератак. Злоумышленники используют все более усовершенствованные пути вторжения в системы безопасности. Специалисты по кибербезопасности должны адекватно реагировать и своевременно предотвращать инциденты. Вызовы современности требуют решения проблем по выявлению мотивов атак, эффективных методов выявления, предупреждения угроз, защиты информационной безопасности.

Ключевые слова: кибератаки, инциденты, вредоносное программное обеспечение, злоумышленники, системы безопасности

RESEARCH ON NETWORK SECURITY

Kalmykov Igor A., North Caucasus Federal University, 2 Kulakov Ave., Stavropol, 355001, Russian Federation,

Doct. Sci. (Engineering), Professor, Professor of the Department of Computational Mathematics and Cybernetics, ORCID: 0000-0002-9854-5310, e-mail: kia762@yandex.ru

Kandaurova Nataliya V., Stavropol Multidisciplinary College, 8A Kulakov Ave., Stavropol, 355001, Russian Federation,

Doct. Sci. (Engineering), Professor, Director of the Stavropol Multidisciplinary College, ORCID: 0000-0003-0928-4022, e-mail: candaur18@yandex.ru

Kononova Nataliya V., Stavropol Multidisciplinary College, 8A Kulakov Ave., Stavropol, 355001, Russian Federation,

Cand. Sci. (Physics & Mathematics), Associate Professor, Head of the Department of Information Security, ORCID: 0000-0002-8988-0694, e-mail: knv_fm@mail.ru

Vorobeva Larisa V., Stavropol Multidisciplinary College, 8A Kulakov Ave., Stavropol, 355001, Russian Federation,

Lecturer at the Department of Information Security, ORCID: 0009-0005-1674-659X, e-mail: laravorob@yandex.ru

Peleshenko Tatiana A., North Caucasus Federal University, 2 Kulakov Ave., Stavropol, 355001, Russian Federation,

Cand. Sci. (Engineering), Associate Professor of the Department of Computational Mathematics and Cybernetics, ORCID: 0000-0003-2761-7847, e-mail: gtanya09@mail.ru

This article examines the current threats to information security at the present time, because in the modern world cybersecurity issues are often ignored so as not to harm the reputation of the company. It is very difficult to assess and calculate the number of cyberattacks, so we use official information from various sources involved in investigating incidents and analyzing the actions of hacker groups. With the development of modern technologies, artificial intelligence, cloud solutions and content delivery systems, cyberattack options are increasing and becoming more complex. Attackers are using increasingly sophisticated ways to break into security systems. Cybersecurity specialists must respond adequately and prevent incidents in a timely manner. The challenges of our time require solving problems to identify the motives of attacks, effective methods of detecting, preventing threats, and protecting information security.

Keywords: cyberattacks, incidents, malicious software, intruders, security systems

ВВЕДЕНИЕ

Вопросы безопасности в сети всегда актуальны, с каждым годом решение этих задач становится не тривиальнее. Появление систем искусственного интеллекта усложняет защиту от взломов. Технологии машинного обучения в руках хакеров становятся серьёзной угрозой информационной безопасности. Искусственный интеллект облегчает взлом паролей и автоматизацию атак, поэтому эксперты по кибербезопасности разрабатывают новые способы пресечения попыток вторжения. Контролируя и анализируя трафик внутри сети, в настоящее время выявляется и обезвреживается огромное количество угроз. Так, количество кибератак на российские ресурсы, которое ежедневно фиксируют регуляторы, составило 170. В 2024 г. зафиксировали мировой рекорд DDos-атаки – 201 миллион запросов в секунду. Причем доля организаций с недостаточным уровнем защиты от внутреннего нарушителя составляет 91 %, а доля компаний, регулярно сталкивающихся с сетевыми атаками, – 85 % [1].

Поскольку увеличиваются темпы роста кибератак на мировые компании, государственный сектор и критически важную инфраструктуру, растет необходимость в повышении киберустойчивости корпораций. Одним из факторов роста инцидентов с использованием программ-вымогателей являются ошибки пользователей, поэтому необходимо правильно подбирать квалифицированные кадры, своевременно обучать IT-специалистов. Вопрос проведения устойчивых и успешных мер по обучению воспринимается неоднозначно, несоответствие между требованиями и эмпирически обоснованным опытом создает пространство для неэффективных консультационных предложений, недооценки сложности темы и риска разочарования.

РОССИЙСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

С уходом основных иностранных компаний IT-индустрии российский бизнес столкнулся с множеством проблем. Для их решения необходимо было в кратчайшие сроки создать и развить отечественные системы и технологии. Рейтинг CNews100 показал, что выручка крупнейших российских IT-компаний выросла на 9 %, в 2024 г. отечественное программное обеспечение заняло 70 % рынка IT-продукции в государственных компаниях, а к 2025 г. Россия перейдет на собственный программный продукт.

Замещение европейского программного обеспечения российским привело еще и к развитию отечественных систем безопасности. Например, в 2024 г. стали популярны подходы, сочетающие защиту от DDoS-атак и функции CDN для быстрого реагирования на киберугрозы, обеспечения стабильности и защиты ресурсов. Тенденция к импортозамещению также послужила мощным стимулом для развития интернет-технологий отечественного производства, как оценивает «EdgeЦентр» [2]. CDN (content delivery network) – это географически распределенные сети доставки контента, состоящие из главного узла и точек по всему миру, где кэшируются тяжелые элементы интернет-ресурсов.

В области сетевой безопасности активно развивается комплекс Гарда NDR – удобная, современная российская система, повышающая устойчивость сетевой инфраструктуры и обеспечивающая бесперебойную работу сервисов, исполняющая требования регуляторов с сфере защиты конфиденциальных данных. Система Гарда может проводить анализ метаданных пакетов сетевого трафика, а также детектировать аномалии и отклонения от нормального поведения в сети. Это дает возможность выявлять даже скрытые атаки и продвинутые угрозы и реагировать на сетевые инциденты.

Возможности Гарда NDR [3] включают в себя не только защиту сетевой инфраструктуры от сложных целевых атак и эксплуатации уязвимостей «нулевого дня», но и обнаружение обходов территории защиты информационной безопасности и неконтролируемых точек доступа, туннелей и shadow it. Также с помощью Гарда NDR обеспечивается безопасность устройств, не поддерживающих агентов АРМ, таких как Iot, Industrial IoT, Scada, Industrial Control Systems и ОС, и гарантия безопасного взаимодействия и обеспечение проактивного выявления угроз при работе с подрядчиками.

К преимуществам Гарды можно отнести:

- хранение более 100 терабайт трафика;
- 100 GE + скорость выявления и реагирования Гарда NDR на инциденты ИБ в сетевом трафике;
- более 250 типов протоколов 5 ML-моделей для обнаружения аномалий в сетевом трафике;

– высокая производительность комплекса (до 10 Гбит/с на сенсор);

– возможность работы только с телеметрией, анализ телеметрии поведенческими ML- и пороговыми моделями, проверка репутационными списками и анализ трафика, сетевого взаимодействия;

– выявление аномалий 3 видами поведенческой аналитики, репутационных списков и сетевого взаимодействия;

– активное реагирование NDR на инциденты через интеграции с внешними системами защиты информации посредством API;

– анализ промышленных протоколов, детектирование и глубокий анализ промышленных протоколов;

– функциональность решения;

– высокая производительность и масштабируемость (более 100 Гбит/с на систему), отсутствие программных ограничений по глубине хранения данных;

– горизонтально масштабируемая производительность, централизованное развертывание и конфигурирование;

– геораспределение, поддержка геораспределенного сценария внедрения, возможность размещения локальной инсталляции системы в филиалах в сочетании с централизованным управлением и анализом данных со всех инсталляций;

– сквозной поиск по всем хранимым данным.

Возможности системы Гарда NDR [4]:

– анализ всего сетевого трафика;

– выявление атак и аномалий в сети;

– перехват подозрительных файлов;

– выявление теневых ИТ-инфраструктур;

– запись и хранение всего сетевого трафика;

– активное реагирование и блокирование атак.

Современный опыт применения Гарда NDR доказывает, что данная российская система – эффективное средство обнаружения уязвимостей и противодействия угрозам сетевой безопасности, как внешним, так и внутренним.

Компании, в которых специалисты имеют права работы в бизнес-приложениях и привилегированные пользователи имеют доступ к сетевой инфраструктуре, успешно применяют системы Privileged Access Management (RAM) – совокупность решений для обеспечения мониторинга и контроля учетных записей сотрудников с высоким уровнем доступа к конфиденциальной информации [5].

По прогнозам руководителя отдела развития бизнеса и поддержки продаж ГК «Солар» Юрия Губанова, «рынок PAM будет расти на 7 % ежегодно и превысит отметку в два миллиарда рублей к 2025 году. Управление привилегированным доступом – активно растущий сегмент отрасли кибербезопасности. PAM-решения помогают контролировать работу пользователей с расширенными правами и пресекать риск ошибки или неправомерных действий с их стороны» [6].

Востребованность таких систем обусловлена необходимостью крупным компаниям обеспечивать безопасность внутренних сетей и высокой степенью защиты периметра, а также исполнение регуляторных требований, включая политику импортозамещения. Применение таких систем решает проблему различных штрафных санкций в случае инцидентов. Ужесточена ответственность за утечку персональных данных, штрафы увеличены от 3 до 15 миллионов рублей, при повторном нарушении – 0,1–3 % от выручки.

Важнейшим аспектом существования сетевой безопасности является защита от внутренних угроз. Ошибаясь или имея злой умысел, сотрудники могут компрометировать чувствительные данные своего предприятия. Для привилегированных пользователей, т. е. пользователей с расширенным доступом к информационным системам организации, сетевой инфраструктуре и конфиденциальной информации, риски возрастают. Системные администраторы или поставщики программных продуктов, имея расширенные полномочия, могут изменить конфигурацию системы или оборудования, а также отключить систему безопасности и использовать конфиденциальную информацию [7]. В таких случаях PAM-решение выявляет недобросовестных подрядчиков. При использовании PAM-систем в прозрачном режиме подключения подрядчики не замечают контроля их действий в реальном времени, затем изучается запись сессии и устанавливаются неправомерные действия.

Функция подмены паролей и подстановки данных учетных записей PAM-системы не дает хакерам самой возможности кражи паролей. При каждом подключении привилегированного пользователя создается новый уникальный пароль, неизвестный пользователю, воспользоваться им извне невозможно, а по окончании сессии он не срабатывает [8].

В настоящее время функциональные возможности решений PAM-систем развиваются для удаленного и облачного доступа, используются технологии машинного обучения. Существует возможность объединить различные технологии для защиты привилегированного доступа и обеспечения безопасности конечных пользователей, что позволит эффективно подавлять все попытки злоумышленников. Преимуществом PAM-системы является легкость установки и настройки, простота управления, не требующая специальных знания, эргономичность, постоянное развитие, но даже в случае несложных в управлении PAM-систем важна сервисная поддержка на постоянной основе.

СЕТЕВАЯ БЕЗОПАСНОСТЬ В МИРЕ

Кибератаки представляют собой хорошо продуманное и упорядоченное поведение злоумышленников, тех, кто не действует случайным образом, а тщательно продумывают стратегию, используя огромный арсенал инструментов, таких как брутфорс, распространение вирусов и методы социальной инженерии.

Распространена следующая схема: для поиска активных профилей администраторов хакеры сканируют учетные записи при помощи известных уязвимостей решений OpenSSH (набор программ, предоставляющих шифрование сеансов связи в компьютерных сетях по протоколу SSH – Secure Shell). Следующим шагом атакующего является подбор пароля методом перебора символов. При успешной реализации злоумышленники получают доступ к учетным записям и наносят ущерб корпорации.

Специалисты уверены в росте рынка искусственного интеллекта и его участии в обеспечении кибербезопасности. Сотрудничество экспертов по кибербезопасности и искусственному интеллекту совместно с LLMs необходимо для успешного выявления и противодействия угрозам.

Проведя анализ данных, полученных Positive Technologies, можно сделать вывод о количестве инцидентов за последние два года, представленных в таблице 1.

Таблица 1 – Динамика инцидентов

Период	I квартал	II квартал	III квартал	IV квартал
2023	786	821	807	872
2024	935	993	1011	

Категории жертв среди организаций: госучреждения – 15 %, IT-компании – 9 %, промышленность – 8 %, финансовые организации – 6 %, наука и образование – 4 %, сфера услуг – 3 %, транспорт – 3 %, телекоммуникации – 3 %, ОПК – 3 %, без привязки к отрасли – 24 %, иные – 15 %. Против частных лиц направлено 22 % атак.

Последствия инцидентов в начале 2024 г. таковы: нарушена деятельность крупной компании. Основными целями злоумышленников является получение конфиденциальной информации (доля таких атак составляет 54 %), нарушение основной деятельности организации (доля таких атак составляет 33 %).

Использование вредоносного ПО для удаленного управления стало обычным явлением, но не стоит забывать и о наличии программ-шифровальщиков. Такие атаки могут привести к неприемлемым инцидентам [9].

Доля успешных сетевых атак приведена в таблице 2.

Таблица 2 – Доля успешных сетевых атак

Назначение	Юридические лица	Физические лица
ПК, серверы, сетевое оборудование	81 %	57 %
Пользователи	52 %	85 %
Веб-ресурсы	19 %	5 %
Мобильные устройства	–	18 %
Иные	2%	3 %

В начале 2024 г. массовое распространение ВПО и фишинговых кампаний увеличило долю корпоративных учетных данных, подвергающихся атакам. В марте 2024 г. PT Expert Security Center обнаружил фишинговую атаку по электронной почте, выдававшую себя за рассылку Microsoft. К фишинговому письму, выдаваемому за информационный бюллетень Microsoft, был прикреплен документ в формате PDF. Документ сопровождался контентом, имитирующим DocuSign, и QR-кодом [10].

Способы распространения вредоносного ПО в успешных атаках представлена в таблице 3.

Вредоносное ПО было наиболее часто используемым против индивидуальных пользователей, причем доля таких инцидентов увеличилась по сравнению с предыдущим кварталом до 68 %. В то же время снизилась доля программ-шифровальщиков, используемых в атаках на индивидуальных пользователей. По сравнению с предыдущим кварталом доля атак на организации снизилась с 54 до 43 %. Исследование показало увеличение доли использования вредоносного программного обеспечения для удаленного управления как в атаках на организации (32 %), так и на частных лиц (37 %) [11].

Таблица 3 – Способы распространения вредоносного ПО

Назначение	Юридические лица	Физические лица
Электронная почта	51 %	21 %
ПК, серверы, сетевое оборудование	35 %	8 %
Сайты	5 %	33 %
Социальные сети	2 %	5 %
Мессенджеры	1 %	33 %
Ложные обновления	1 %	5 %
Компрометация линии поставок ПО	1 %	4 %
Иные	4 %	12 %

Самой опасной угрозой для пользователей оставалось раскрытие конфиденциальной информации, на долю таких инцидентов пришлось 85 %. Наиболее распространенным вектором атак на юридические лица была социальная инженерия, что составило 52 % таких инцидентов [12].

Крупные утечки персональных данных пользователей и масштабные атаки осуществляются путем эксплуатации уязвимости конечной поставки вредоносного ПО, причем для доставки вредоносного ПО злоумышленники используют легитимные сервисы для совместной разработки ИТ-проектов и открытые репозитории пакетов для разработки программного обеспечения.

Доля целевых ОС в успешных атаках с использованием ВПО представлена на рисунке.

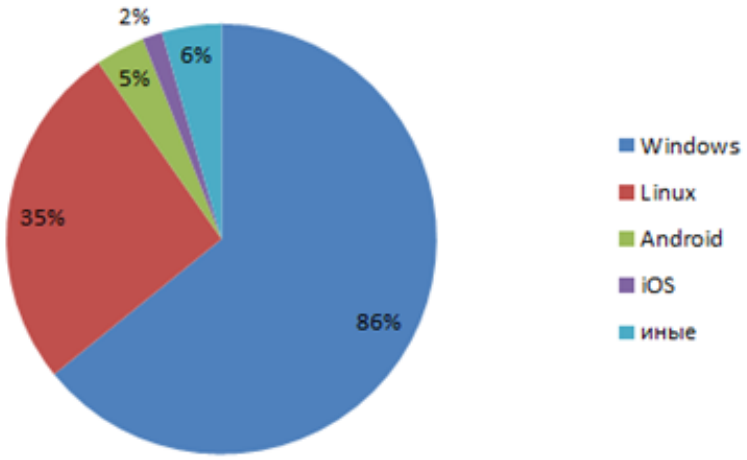


Рисунок – Последствия сетевых атак

В феврале детская больница Lurie в Чикаго подверглась кибератаке, которая затронула доступ к интернету, электронной почте, телефонии и платформе MyChart. Стали недоступными запланированные процедуры, результаты ультразвуковых исследований и компьютерной томографии, рецепты выписывали вручную. Взлом был осуществлен группой вымогателей Rhysida, которая потребовала выкуп в размере 4000000 долларов США за кражу 600 Гб данных больницы [13].

Последствия таких атак приведены в таблице 4.

Таблица 4 – Доля успешных атак

Назначение	Юридические лица	Физические лица
Утечка конфиденциальной информации	54 %	72 %
Нарушения основной деятельности	33 %	3 %
Прямые финансовые потери	5 %	22 %
Ущерб государственным интересам	8 %	–
Использование ресурсов	6 %	3 %
Иное	23 %	20 %

Самыми громкими инцидентами 2024 г., повлекшими негативные последствия, можно признать работу программы Акира, затронувшей центр обработки данных. Пострадавшими являются крупные компании:

– крупнейшая сеть кинотеатров Швеции не смогла осуществить онлайн-продажу билетов;
– компания по поставке строительных материалов Moelven;

– поставщик сельскохозяйственной продукции Granngarden закрыл магазины на восстановительный период.

А также взлом в феврале 2024 г. системы немецкого производителя аккумуляторов Варта повлек остановку производства на пяти заводах, следствием чего акции компании снизились на 4,75 %.

В то же время компания Optum, предоставляющая медицинские услуги, также подверглась атаке мошенников BlackCat. В результате была выведена из строя платформа Change Healthcare, крупнейший платежный обменник в системе здравоохранения США. В результате врачи, медицинские работники и пациенты были вынуждены использовать альтернативные методы для оформления страховки. Эти препятствия привели к 100000000 $ убытков ежедневно для поставщиков медицинских услуг [14].

В успешных атаках на организации, которые привели к компрометации конфиденциальной информации, злоумышленники чаще всего фокусировались на краже личной информации (37 % похищенной информации), информации для аутентификации (17 %) и коммерческой тайны (22 %). При атаках, направленных на отдельных людей, злоумышленники, как правило, концентрировались на краже аутентификационной информации (39 %) и персональной (25 %).

При успешных атаках типы похищенных данных представлены в таблице 5.

Таблица 5 – Классификация похищенных данных

Назначение	Юридические лица	Физические лица
Персональные данные	37 %	25 %
Учетные данные	17 %	39 %
Данные платежных карт	4 %	13 %
Коммерческая тайна	22 %	4 %
Медицинская информация	6 %	2 %
Переписка	3 %	5 %
Иное	11 %	12 %

По данным Ассоциации потребительских технологий, на ИТ-рынке преобладают технологии искусственного интеллекта. Более 40 % от общего числа пользователей используются для доступа и предотвращения компьютерных атак. Российские специалисты применяют искусственный интеллект для предотвращения заражения, вредоносного ПО и других компьютерных атак. Искусственный интеллект и большие языковые модели (LLM) также являются важной частью современной системы ИТ-безопасности, включая анализ больших данных, обнаружение несанкционированного доступа, идентификацию рисков и автоматическое реагирование на инциденты. В случае обнаружения фишинговых писем и других видов социальной инженерии модели GPT-3 и GPT4 могут помочь в распознавании с помощью анализа естественного языка. Применение искусственного интеллекта для обеспечения безопасности в компьютерной сфере предполагает прогнозирование возможных угроз и инцидентов с учетом информации о прошлых атаках или инцидентах, чтобы их можно было выявить и устранить в «нулевой день», руководствуясь рекомендациями безопасности [15].

Однако использование искусственного интеллекта LLM несет проблемы, связанные с наличием предвзятости при обучении моделей, что может вызвать ошибки в результатах системы [15]. Также хакеры могут использовать LLM, создавая убедительные фишинговые письма, для поиска и использования уязвимости. Искусственный интеллект – не самый мощный и крайне уязвимый инструмент, требующий особого внимания специалистов для эффективной работы. По этой причине создание знаний в области информационной безопасности и систем искусственного интеллекта в связке с опытом специалистов необходимо для успешной работы.

Алгоритм машинного обучения способен выявить аномальный трафик и отличить его от легального, что позволит облегчить или нейтрализовать атаки. Преимуществом нейронной сети является способность использовать анализ и обработку больших объемов информации в режиме реального времени. Экспертами центра стратегических разработок прогнозируется рост технологий до 24 % в год, при этом искусственный интеллект и кибербезопасность будут развиваться в связке.

ЗАКЛЮЧЕНИЕ

Для эффективности информационной защиты необходимо использовать следующую стратегию. Сначала необходимо упростить программный комплекс. Чем понятнее и легче все правила и процессы в использовании, тем лучше шанс их соблюдения. Соблюдение сложных процедур и выполнение их без сбоев – сложная задача. В повседневные будни легче интегрировать безопасные практики при уменьшении когнитивной нагрузки сотрудников. Обучение способам и мерам безопасности повышает продуктивность и стимулирует пользователей соблюдать правила безопасности. Злоумышленники постоянно усложняют варианты атак, а значит, угрозы постоянно меняются. Поэтому обучающие курсы тоже должны адаптироваться в современных условиях.

Исследования показывают, что разные страны решают проблему кибербезопасности по особым сценариям. Австралия вносит законы о защите данных и борьбе с атаками, такими как программы-вымогатели. США сделали акцент на кибербезопасности, ориентированной на пользователя, его мотивации, потребности и поведение, что создает более гибкие и устойчивые системы. В европейских странах общественные деятели вносят предложения об уменьшении рабочей недели. Так, предполагают повысить производительность труда, снизить уровень стресса и усилить контроль за поведением на рабочем месте. Идеальных методик не существует, но правильно подобранный подход благодаря мотивации пользователей позволит снизить шансы взлома.

Список источников

1. Гладков, А. Н. Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности / А. Н. Гладков, С. Н. Горячев, Н. С. Кобяков // Защита информации. Инсайд. – 2023. – № 1. – С. 32–37.

2. Белов, А. С. Модернизация системы информационной безопасности / А. С. Белов, М. М. Добрышин, Д. Е. Шугуров // Защита информации. Инсайд. – 2022. – № 4. – С. 76–80.

3. Савин, М. В. Методика выявления и оценки недопустимых событий на основе модели зрелости управления информационной безопасностью / М. В. Савин, М. А. Кондратенко // Защита информации. Инсайд. – 2023. – № 1. – С. 24–31.

4. Голубев, Г. Д. Обзор безопасности маломощных глобальных сетей: угрозы, проблемы и потенциальные решения / Г. Д. Голубев // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.). – Екатеринбург, 2022. – С. 5–11.

5. Федотова, Г. В. Угрозы кибербезопасности устойчивости цифровых платформ / Г. В. Федотова, Д. А. Куразова // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики : материалы IX Междунар. науч.-практ. конф. (Екатеринбург, 2 декабря 2021 г.). – Екатеринбург, 2021. – С.118–122.

6. Догучаева, С. М. Анализ современных проблем информационной безопасности в российских компаниях / С. М. Догучаева // Риск: ресурсы, информация, снабжение, конкуренция. – 2022. – № 2. – С. 65–68.

7. Долганов, К. А. Технология блокчейн с точки зрения информационной безопасности / К. А. Долганов // Цифровая трансформация общества и информационная безопасность : материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.). – Екатеринбург, 2022. – С. 14–17.

8. Смирнов, С. И. Комплексная методика проведения расследования инцидента информационной безопасности / С. И. Смирнов, А. Н. Киселев, В. Д. Азерский [и др.] // Защита информации. Инсайд. – 2023. – № 2. – С. 14–26.

9. Гладких, А. В. Методы защиты от DDoS-атак в интеллектуальных сетях / А. В. Гладких // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.-практ. конф. (Екатеринбург, 18 мая 2022 г.). – Екатеринбург, 2022. – С. 3–5.

10. Пучков, А. Ю. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления / А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов // Прикладная информатика. – 2023. – Т. 18, № 2. – С. 85–102.

11. Прудникова, Л. Б. Информация и информационная безопасность как атрибуты гражданского общества (краткий обзор взаимосвязи) / Л. Б. Прудникова, В. М. Шеншин, Н. С. Глейберман // Государственная власть и местное самоуправление. – 2022. – № 7. – С. 7–9.

12. Раткин, Л. С. Информационная безопасность промышленных предприятий в условиях санкций на примере импортозамещения квантовых систем // Защита информации. Инсайд. – 2022. – № 5. – С. 14–16.

13. Васильев, В. И. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. – 2022. – № 2. – С. 27–38.

14. Горбунов, Д. Д. Криптовалюта и блокчейн: перспективы развития с точки зрения информационной безопасности / Д. Д. Горбунов // Цифровая трансформация общества и информационная безопасность: материалы Всеросс. науч.–практ. конф. (Екатеринбург, 18 мая 2022 г.). – Екатеринбург, 2022. – С. 11–17.

15. Чучкалова, И. Ю. Информационная безопасность в условиях трансформации общества / И. Ю. Чучкалова // BI-технологии и корпоративные информационные системы в оптимизации бизнес–процессов цифровой экономики : материалы IX Междунар. науч.-практ. конф. (Екатеринбург, 2 дек. 2021 г.). – Екатеринбург, 2021. – С.120–122.

References

1. Gladkov, A. N., Goryachev, S. N., Kobyakov, N. S. Visualization of Cyber Threats as an Aspect of the Formation of Competencies in the field of Information Security. *Information Security. Inside*, 2023, no. 1, pp. 32–37.

2. Belov, A. S., Dobryshin, M. M., Shugurov, D. E. Modernization of the Information Security System: The Approach to Determining the Frequency: approach to determining the frequency. *Information Security. Inside*, 2022, no. 4, pp. 76–80.

3. Savin, M. V., Kondratenko M. A. Methodology for Identifying and Evaluating Unacceptable Events Based on the Maturity Model of Information Security Management. *Information Security. Inside*, 2023, no. 1, pp. 24–31.

4. Golubev, G. D. Review of the security of low–power global networks: threats, problems and potential solutions. *Digital transformation of society and information security : materials of the All-Russian scientific-practical. conf. (Ekaterinburg, May 18, 2022).* Ekaterinburg, 2022, pp. 5–11.

5. Fedotova, G. V., Kurazova, D. A. Cybersecurity Threats to the Resilience of Digital Platforms. *BI technologies and corporate information systems in optimizing business processes in the digital economy : proc. of the IX Int. sci.-pract. conf. (Ekaterinburg, December 2, 2021).* Ekaterinburg, 2021, pp. 118–122.

6. Doguchaeva, S. M. Analysis of modern problems of information security in Russian companies. *Risk: resources, information, supply, competition*, 2022, no. 2, pp. 65–68.

7. Dolganov, K. A. Blockchain technology from the point of view of information security. *Digital transformation of society and information security: materials of the All-Russian scientific and practical conf. (Ekaterinburg, May 18, 2022).* Ekaterinburg, 2022, pp. 14–17.

8. Smirnov, S. I., Kiselev, A. N., Azersky ,V. D. et al. Comprehensive Methodology for Conducting an Information Security Incident Investigation. *Information Protection. Insider*, 2023, no. 2, pp. 14–26.

9. Gladkikh, A. V. Methods of protection against DDoS attacks in intelligent networks. *Digital transformation of society and information security : materials of the All-Russian scientific and practical conf. (Ekaterinburg, May 18, 2022)*. Ekaterinburg, 2022, pp. 3–5.

10. Puchkov, A. Yu., Sokolov, A. M., Shirokov, S. S., Prokimnov, N. N. Algorithm for identifying information security threats in distributed multiservice networks of government agencies. *Applied Informatics*, 2023, vol. 18, no. 2, p. 85–102.

11. Prudnikova, L. B., Shenshin, V. M., Gleiberman, N. S. Information and information security as attributes of civil society (a brief overview of the relationship). *State Power and Local Self-government*, 2022, no. 7, pp. 7–9.

12. Ratkin, L. S. Information Security of Industrial Enterprises in Sanction Conditions on the Example of Import Substitution of Quantum Systems. *Information Security. Inside*, 2022, no. 5, pp. 14–16.

13. Vasiliev, V. I., Vulfin, A. M., Kuchkarova, N. V. Assessment of current threats to information security using transformer technology. *Cybersecurity Issues*, 2022, no. 2, pp. 27–38.

14. Gorbunov, D. D. Cryptocurrency and blockchain: development prospects from the point of view of information security. *Digital transformation of society and information security: materials of the All-Russian scientific and practical conf. (Ekaterinburg, May 18, 2022)*. Ekaterinburg, 2022, pp. 11–17.

15. Chuchkalova, I. Yu. Information Security in the Context of Society Transformation. *BI technologies and corporate information systems in optimizing business processes in the digital economy : proc. of the IX Int. sci.-pract. conf. (Ekaterinburg, December 2, 2021).* Ekaterinburg, 2021, pp. 120–122.

Статья поступила в редакцию 30.10.2024; одобрена после рецензирования 29.11.2024; принята к публикации 29.11.2024.

The article was submitted 30.10.2024; approved after reviewing 29.11.2024; accepted for publication 29.11.2024.

УДК 004.855.5

МОДЕЛЬ ПРОГНОЗИРОВАНИЯ ПАТТЕРНОВ ПОВЕДЕНИЯ ИДИВИДА ПРИ ОБРАБОТКЕ ВИДЕОИЗОБРАЖЕНИЙ

Забержинский Борислав Эдуардович, Самарский государственный технический университет, 443100, Российская Федерация, г.Самара, ул. Молодогвардейская, 244,

кандидат технических наук, доцент, ORCID: 0000-0002-5715-2289, e-mail: zab.borislav@gmail.com

Золин Алексей Георгиевич, Самарский государственный технический университет», 443100, Российская Федерация, г. Самара, ул. Молодогвардейская, 244,

кандидат технических наук, доцент, ORCID: 0000-0001-7117-8509, e-mail: zolin.a.g.@gmail.com

Портнов Константин Валерьянович, Самарский государственный экономический университет», 443090, Российская Федерация, г. Самара, ул. Советской Армии, 141,

кандидат технических наук, доцент, ORCID: 0009-0002-6778-7998, e-mail: sk7@mail.ru

Предсказание действий индивида на основе визуальных данных представляет собой многогранную и значимую проблемную область, охватывающую множество направлений в сфере искусственного интеллекта. В этом обзоре предлагается предиктивная модель, которая используется для прогнозирования человеческого поведения. Основная задача модели заключается в предсказании поведения на основе новых данных, однако она также должна способствовать выявлению конкретных действий, даже когда информация неполная. Для решения этой задачи предлагается подход, основанный на анализе вектора активности индивидуума. В процессе обучения модели анализируются полные циклы человеческих действий, в то время как неполные последовательности применяются для тестирования и оценки ее функциональности. Использование полноценных циклов действий дает модели обширный контекст для обучения, в то время как анализ неполных последовательностей способствует оценке ее способности к обобщению и адаптации к реальным обстоятельствам. В ходе экспериментов применялись разнообразные классификаторы для обеспечения высокой точности на начальной стадии разработки модели. Это важно для подтверждения ее эффективности и возможности точно предсказывать и категоризировать разнообразные человеческие действия. Все эти меры направлены на формирование надежного инструмента для прогнозирования поведения, который мог бы эффективно использоваться в разнообразных ситуациях повседневной жизни.

Ключевые слова: прогнозирование, предиктивная модель, поведение человека, распознавание, вектор описания активности

MODEL FOR PREDICTING PATTERNS OF INDIVIDUAL BEHAVIOR WHEN PROCESSING VIDEO

***Zaberzhinsky Borislav E.*,** Samara State Technical University, 244 Molodogvardeyskaya St., Samara, 443100, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-5715-2289, e-mail: zab.borislav@gmail.com

***Zolin Alexey G.*,** Samara State Technical University, 244 Molodogvardeyskaya St., Samara, 443100, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0001-7117-8509, e-mail: zolin.a.g.@gmail.com

***Portnov Konstantin V.*,** Samara State University of Economics, 141 Sovetskoy Armii St., Samara, 443090, Russian Federation,

Cand. Sci. (Engineering), Associate Professor, ORCID: 0009-0002-6778-7998, e-mail: sk7@mail.ru

Predicting an individual's actions based on visual data is a multifaceted and significant problem area that covers many areas in the field of artificial intelligence. This review proposes a predictive model that is used to predict human behavior. The main purpose of a model is to predict behavior based on new data, but it should also help identify specific actions even when the information is incomplete. To solve this problem, an approach based on the analysis of the individual's activity vector is proposed. During model training, complete cycles of human actions are analyzed, while partial sequences are used to test and evaluate its functionality. The use of complete action cycles gives the model a rich context for training, while the analysis of partial sequences helps evaluate its ability to generalize and adapt to real-world circumstances. During the experiments, a variety of classifiers were used to ensure high accuracy at the initial stage of model development. This is important to confirm its effectiveness and ability to accurately predict and categorize a variety of human activities. All these measures are aimed at developing a reliable tool for predicting behavior that could be effectively used in a variety of situations in everyday life.

Keywords: prediction, predictive model, human behavior, recognition, activity description vector

ВВЕДЕНИЕ

Задачи идентификации двигательной активности человека и распознавание паттернов его поведения – одна из актуальных задач современного компьютерного зрения.

Сферы приложения данной задачи безграничны и включают в себя такие области, как безопасность в общественных местах в результате обработки записи видеонаблюдения, идентификация нарушений на старых видеозаписях, диагностика медицинских заболеваний на основании обработки видеоизображений, выявление паттернов поведения потребителей для задач маркетинга. Анализ научной литературы показал четыре класса сложности основных задач при решении данной проблемы – от распознавания простой двигательной активности на первом уровне сложности до распознавания сложных паттернов человеческого поведения на последнем уровне сложности.

В ходе нашего исследования мы тщательно анализировали проблемные аспекты, методы и цели на всех четырех уровнях. Несмотря на то, что ученые за последнее время разработали множество методик, способных распознавать сложные движения и жесты, они не способны определять шаблонное поведение, которое бы позволяло предсказать намерения человека на изображении. Однако если рассматривать распознавание поведения как одно из направлений классификации, то выявление паттернов поведения дает возможность предсказать будущие действия индивида на основе ограниченного набора данных о его активности.

В системах, работающих в режиме реального времени, анализ видеопотока может применяться для обнаружения нарушителей и преступников, прогнозирования непредвиденных ситуаций, в системах помощи водителям, а также для диагностики заболеваний.

В данной статье предлагается предиктивная модель для анализа и прогнозирования движений индивидуумов при обработке кадров видеоизображений.

Анализ современных авторов в этой области показал ориентацию ученых на внедрение предиктивной модели для анализа отдельно взятых действий, а не на цепочках действий, составляющих паттерн поведения.

Большинство работ в данной области используют последовательную информацию для прогнозирования поведения без учета нормализации и разрывов во времени. Определение вектора, отражающего характер активности, открывает двери для его использования в более сложных и продолжительных сценариях, зафиксированных на видео. Наша задача заключается в адаптации этого описательного элемента для предсказания движений и оценки надежности вытекающих из этого метода заключений, даже при наличии неполной информации. В рамках нашего исследования мы намерены применить универсальные классификаторы, чтобы сравнить и оценить результативность разработанных нами алгоритмов.

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ИНДИВИДОВ

На первом шаге, для достижения поставленных целей, производится обработка набора видеоизображения, разбитого на массив растровых изображений для их очистки от помех. Кадры в условно «хорошем» качестве, выше среднестатистического уровня, мы используем для задач отслеживания, разделяя их на сегменты. Алгоритм работает лишь с частью кадра, так называемой областью обработки (ROI), которая обладает более высоким разрешением в кадре. В рамках нашего исследования область обработки соответствует месту, где находится движущийся человек. Извлекая информацию о положении человека из каждого кадра видеопоследовательности, мы можем составить список его координат, что даст возможность предсказать его будущую траекторию движения.

Мы предлагаем метод определения пути движения на основе предварительно разработанной раскадровки, применяя вектор, который отражает активность (BOA), как показано на рисунке 1.

Вектор активности человека получается на основе анализа кадров, в ходе которого выявляется степень локализации человека в определенной точке кадра и характер местных движений его отдельных частей тела [4].

График отражает поведенческую модель проходящих индивидов во время осмотра витрин как при входе, так и при выходе из торгового заведения. На нем представлены следующие элементы:

– оси X: это временная шкала, на которой отмечены моменты проведения наблюдений, отражающие конкретные временные интервалы, когда фиксировалась активность;

– оси Y: здесь находится диапазон значений, отражающих измеренную активность поведения. Каждая точка на этой оси отвечает за определенное значение поведенческого паттерна при прохождении через входные и выходные двери магазина.

Рисунок 1 – Модели поведения индивидов

Функция делит кадр S[i, j] на участки, представленные матрицей C, где ячейка описывает данные о движениях, происходящих в четырех направлениях координатной плоскости. Также там содержится показатель частоты этих движений φ(z). Величины, описывающие эти перемещения, определяются на основе мгновенных изменений между двумя соседними точками в последовательности. В частности, для определения UP(b_i) используется следующее уравнение, представляющее собой формулу для предиктивной модели, указанную как (1):

$$UP(b_i) = \begin{cases} (b_i - b_{i-1}) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \frac{(b_i - b_{i-1}) \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}}{\|(b_i - b_{i-1})\|} > 0 \\ 0 \qquad \text{в иных случаях} \end{cases}, \quad (1)$$

Где b_i – точка в i-момент времени;

b_{i-1} – точка в предыдущий момент времени.

Эти точки в кадре хронологически упорядочены при условии сдвига в положительной вертикальной оси y.

Формула (1) применима и для остальных трех направлений движения. Вычисление вектора описания активности производится внутри выбранной матрицы как совокупные гистограммы движений в четырех плоскостях, ранее обозначенных функциями UP(), DOWN(), LEFT(), RIGHT() и частоты **φ** для точек кадра{S} ячейки $\{C_{i,j}\}$ матрицы {C}. Положим, q x w – фактический размер кадра, g x h – ячейки разделения, $b_{k,l}$ – точка, расположенная в (k,l) пространства кадра {S}, каждый вектор в ячейке равен:

$$\forall c_{i,j} \in C \wedge \forall z_{k,l} \in \frac{S}{i} = \left\lfloor \frac{k \times g}{q} \right\rfloor \wedge j = \left\lfloor \frac{k \times h}{w} \right\rfloor,$$
$$ADV_{i,j} = \begin{pmatrix} \sum \varphi(b_{k,l}), UP(b_{k,l}), \sum Down(b_{k,l}), \\ \sum Left(b_{k.l}), \sum Right\,(b_{k,l}) \end{pmatrix}. \quad (2)$$

Этот метод представляет собой разбиение кадра на элементы и упаковку информации в сокращенные значения, что дает возможность отображать траекторию. Примечательно, что вектор движения содержит в себе данные о пути любых размеров и последовательности точек пути, что открывает двери для его применения в предсказании.

ПРОЦЕСС ПРОГНОЗИРОВАНИЯ ДЕЙСТВИЙ

Процесс предсказания поведения основан на синтезирующей способности модели, которая анализирует введенные образы. Особенностью разработанной модели является ее способность предсказывать действия человека, исходя из неполной информации о его движении в кадре, которое мы определим как период наблюдения.

Данная модель строит траекторию движения шаг за шагом, непрерывно обрабатывая данные с каждого кадра. В зоне внимания находятся те участки кадра, которые следуют для определения траектории движения объектов и в которых могут встречаться мелкие неточности из-за ошибок в сегментации. Процесс коррекции таких неточностей осуществляется с помощью метода сплайновой аппроксимации, описанной в источнике [5].

Одной из ключевых задач, стоящих перед нами на этапе прогнозирования, является определение набора параметров, характеризующих активность (вектор ADV). Эти параметры вычисляются и затем сохраняются, формируя базу данных всех известных нам видов активности. Эта база будет использоваться в дальнейшем для тренировки нашей модели.

В каждом конкретном векторе, описывающем активность, каждый элемент должен быть уравнен в рамках от 0 до 1. Это достигается путем разделения каждого значения в векторе на максимальное значение этого же элемента среди всех имеющихся векторов активности. Таким образом, все векторы активности, приведенные к стандартному виду, служат образцами для настройки параметров классификатора, который применяется в нашей модели.

Такой же метод применяется и для предсказания действий человека, перемещающегося на фоне кадра. Это достигается посредством расчета вектора активности(BOA), который служит основой для создания модели прогнозирования. В этой модели формируется набор контролируемых точек. В процессе работы также происходит стандартизация этих векторов, чтобы их компоненты были ограничены максимальными значениями и приведены в интервале от 0 до 1. Это позволяет использовать классификационную модель для определения поведения человека.

ИССЛЕДОВАНИЕ МОДЕЛИ

Необходимо осуществить экспериментальное изучение модели, разработанной нами. Прогнозирование перемещения объекта в кадре осуществляется с использованием более простых математических методов, связанных с определением траектории движения, где используется только контекстная метка последовательности в качестве более сложной интерпретации поведения человека в кадре. Для ввода данных мы применяем метки в форме ограничивающего прямоугольника.

В рамках экспериментального анализа точности прогнозирующей модели были использованы 20 видеозаписей, взятых с камер наблюдения в торговом центре Самары, снятых с фронтальной точки зрения. Среднее количество кадров в каждом видео составляет 1000, с разрешением 384x288 пикселей и частотой дискретизации в 24–25 кадров в секунду. На видеозаписях фиксировано около 200 человек. Все видео были тщательно отмечены организаторами кадра за кадром, присваивая каждому человеку уникальный идентификационный номер. В большинстве кадров присутствуют несколько зарегистрированных лиц, каждый из которых обозначен индивидуальным идентификатором и ограничен рамкой, указывающей на область интереса. Для каждого человека в кадре были установлены метки, отражающие разнообразные уровни абстракции, описывающие контекст, типы движения и роль участников.

Каждый посетитель демонстрирует уникальную последовательность поведения, охватывающую множество этапов: прохождение контрольно-пропускного пункта, периоды покоя, перемещения внутри помещения, вход и выход из магазина. В каждой итерации присутствуют уникальные характеристики – темп двигательной активности, даже при выполнении одинаковых задач. В частности, ряд действий – «вход в помещение»->«выход из помещения»->«повторный вход» – обычно занимает от 6 до 15 секунд в среднем. Более сложные действия, связанные с изучением различных товаров на витринах, назовем их «осмотр витрин», «осмотр ассортимента», занимают существенно большее количество времени и составляют в среднем от 30 до 90 секунд. На основе проведенных экспериментов мы выяснили, что максимальное время, которое потребовалось для осмотра витрин, составило 93 секунды.

В рамках нашей статьи было принято решение использовать равное количество векторов, отражающих двигательную активность, для каждого типа двигательного контекста. Это было достигнуто благодаря применению техники синтетического увеличения миноритета (SMOTE). В результате мы получили по 60 векторов для каждого из двигательных контекстов. Однако стоит отметить, что применение упомянутого метода приводит к случайному сокращению количества образцов, относящихся к сценариям «просмотр» и «выход из помещения».

Мы также осуществили экспериментальные исследования с применением традиционных методов классификации, включая самоорганизующуюся карту (SOM), Supervised Self-Organizing Map (SSOM), нейронный газ (NGAS), линейный дискриминантный анализ (LDA) и алгоритм k-ближайших соседей [5–6].

Исследование эффективности разработанных предиктивных моделей, учитывающее временные характеристики активности участников, было проведено методом десятикратной кросс-валидации с адаптацией размера сетки, который был определен ранее.

В ходе эксперимента для формирования обучающего набора были выбраны 327 случайных описаний активности. Остальные образцы служили для создания набора для проверки. Векторы описания активности, включенные в обучающий набор, были получены с учетом всей последовательности данных.

ИТОГИ ИССЛЕДОВАНИЯ

В ходе практического анализа функционирования этой модели была проведена оценка эффективности классификации, основанная на показателях чувствительности, специфичности и точности. Процесс классификации, проводимый с помощью данной модели, был изучен на динамическом уровне, учитывая временной фактор, для серии видеофрагментов, описывающих различные виды активности.

Средний показатель точности классификации, полученный в результате тестирования модели на обработке видеоматериалов и зависящий от продолжительности наблюдения при разнообразных размерностях сеток чувствительности (от 1x1 до 7x11), представлен на графиках 2 и 3 в форме гистограммы.

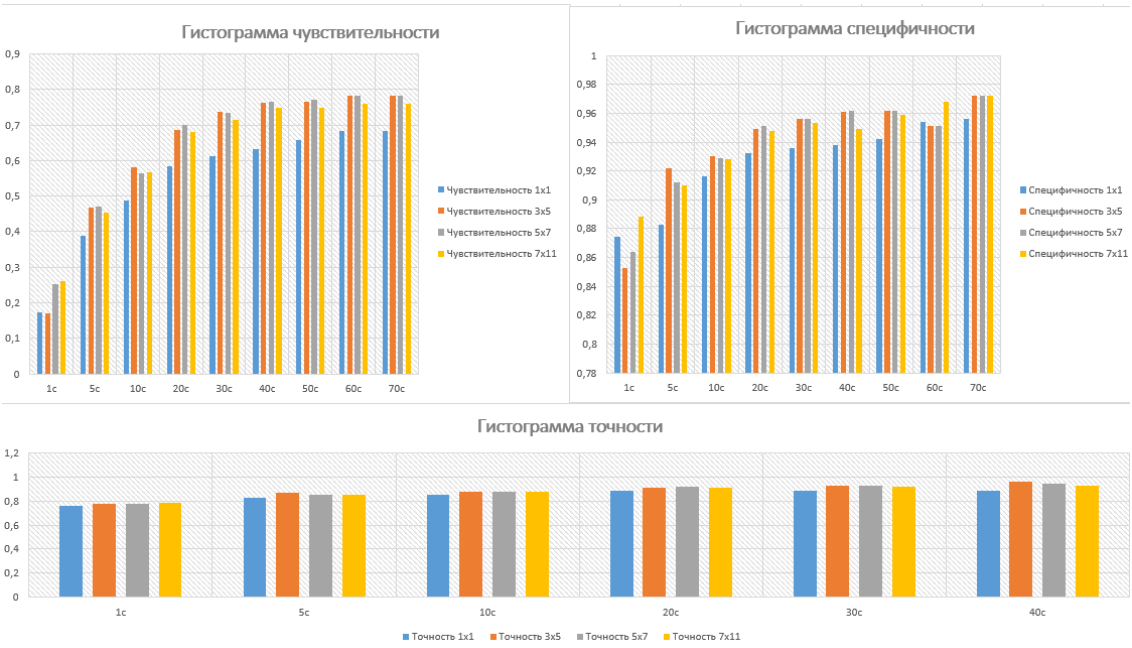


Рисунок 2 – Анализ точности классификационных результатов

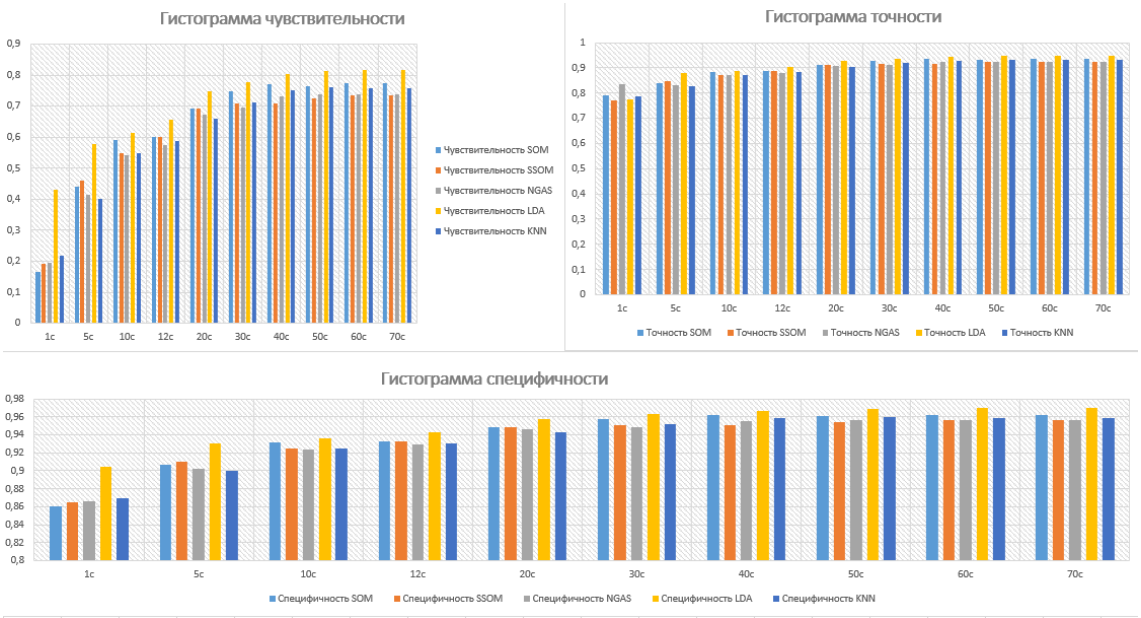


Рисунок 3 – Анализ точности классификационных результатов

Лучшие эффекты достигаются при продолжительном анализе (69 секунд) с использованием сетки размером 1 на 1, в то время как для краткосрочных наблюдений менее 10 секунд оптимальны более крупные сетки, что приводит к увеличению чувствительности, специфичности и точности результатов. Оптимальные прогнозы по активности человека на участке кадра формируются при сетке размером 5 на 7 и наблюдении продолжительностью свыше 11 секунд. При анализе промежутков времени в 21 секунд и более средняя точность всех классификаторов превышает 79 %, иногда достигая 92 %.

Предложенный алгоритм позволяет с высокой точностью оперативно обнаруживать и прогнозировать поведение индивидов на видеоизображении по результатам интерполяции данных.

Изучив графики, отражающие результаты анализа экспериментальных данных (рис. 2, 3), можно вывести, что наиболее эффективным временным интервалом для наблюдения является от 34 до 43 секунд.

Все наборы активностей, отображающие модель поведения (кроме события «вход в магазин»), включают действия, длительность которых превышает 38 секунд. Это свидетельствует о необходимости уточнения работоспособности прогнозирующей модели с учетом конкретного поведенческого паттерна человека, так как 38 секунд указывают на полное выполнение активности.

Таблица – Экспериментальная оценка степени эффективности применяемых классификаторов.

	Rule-based	HSMM	PN	LDA, 7 x 11
Чувствительность	0,561	0,639	0,810	0,821
Специфичность	–	0,968	0,961	0,969

Из представленного нами графического материала становится ясно, что для получения максимально эффективных итогов рекомендуется применять кластерный алгоритм LDA с сеткой размером 7 на 11.

ЗАКЛЮЧЕНИЕ

В данном исследовании был изучен опыт использования предиктивной модели для анализа видеоматериалов с целью предсказания действий человека с использованием вектора активности. Разработанная модель определяет путь движения человека на видеоизображениях, полученных из отрывков видеозаписи, на основе анализа отдельных пикселей кадра.

Этот метод основан на применении классификаторной функции, которая обрабатывает векторы, отражающие поведение человека, приведенные в соответствие с диапазоном от нуля до единицы. Это дает возможность применять метод независимо от времени. При формировании модели учитываются все возможные движения человека, учитывая контекст места установки камеры наблюдения, что обеспечивает возможность ее использования в реальном времени и предсказывать поведение человека на основе аналогичного вектора активности.

Исследование эффективности метода было проведено с помощью обширной коллекции видеозаписей, на которых происходило тестирование разработанной модели. По итогам экспериментов можно утверждать, что примененная стратегия способна эффективно предсказывать реакцию людей на изображения независимо от типа классификатора и размерности сетки. Применение традиционных методов классификации, таких как Rule-based, HSMM, PN, LDA, обеспечивает значительную точность в процессах распознавания и прогнозирования поведения человека. Предложенная модель позволяет прогнозировать поведение человека в течение короткого времени, основываясь на обобщенной информации и данных. Разработанная система дает возможность предсказывать действия индивида на ближайшее время, используя синтезированные знания и информационные данные.

Список источников

1. Горячкин, Б. С. Компьютерное зрение / Б. С. Горячкин, М. А. Китов // E-Scio. – 2020. – № 9 (48). – С. 317–345.

2. Портнов, К. В. Анализ методов эмерджентного искусственного интеллекта / К. В. Портнов, Б. Э. Забержинский Р. Р. Габбасов К. А. Агафонов // Актуальные проблемы общества, экономики и права в контексте глобальных вызовов : сборник материалов XX Международной научно-практической конференции, Москва, 17 мая 2023 года. – Санкт-Петербург : Печатный цех, 2023. – Т. 2. – С. 30–36. – EDN GVVLER.

3. Каримов, Б. Ф. Проблемы адаптации генетических алгоритмов к решению задач структурно-параметрической оптимизации / Б. Ф. Каримов, К. В. Портнов // Современные исследования: теория, практика, результаты : сборник материалов Международной научно-практической конференции, Москва, 29 декабря 2023 года. – Москва : Центр развития образования и науки, ООО «Издательство АЛЕФ», 2023. – С. 443–448. – DOI: 10.26118/1590.2023.63.10.010. – EDN PUGPKI.

4. Забержинский, Б. Э. Разработка интеллектуального метода обработки изображения для повышения точности распознавания лиц на основе локальных бинарных шаблонов / Б. Э. Забержинский, А. Г. Золин // Современные наукоемкие технологии. – 2023. – № 7. – С. 22–26. – DOI: 10.17513/snt.39689. – EDN PZDAPQ.

5. Портнов, К. В. Актуальные проблемы и задачи автоматизированных систем в сфере ЖКХ / К. В. Портнов, Е. В. Панюкова // Журнал монетарной экономики и менеджмента. – 2024. – № 2. – С. 230–236. – DOI: 10.26118/2782-4586.2024.35.72.033. – EDN AEQRFJ.

6. Портнов, К. В. Разработка информационной системы на основе многофакторной логистической регрессии / К. В. Портнов // Информационные технологии. Радиоэлектроника. Телекоммуникации. – 2012. – № 2-3. – С. 129–133. – EDN PEDEUX.

7. Портнов К. В. Анализ и совершенствование методов управления закупками сырья на промышленном предприятии : специальность 05.13.01 «Системный анализ, управление и обработка информации (по отраслям)» : дис. … канд. техн. наук / Константин Валерьянович Портнов. – Самара, 2007. – 132 с. – EDN NOZCLT.

8. Портнов, К. В. Автоматизированные информационные системы анализа и обработки данных в медицине / К. В. Портнов, Н. Ю. Портнова, Е. В. Сибарцева // Актуальные проблемы науки и образования в условиях современных вызовов : сборник материалов XXVIIII Международной научно-практической конференции, Москва, 01 марта 2024 года. – Санкт-Петербург : Печатный цех, 2024. – С. 82–88. – DOI: 10.34755 /IROK.2024.12.84.021. – EDN EQBYWG.

References

1. Goryachkin, B. S., Kitov, M. A. Computer vision. *E-Scio*, 2020, no. 9 (48), pp. 317–345.

2. Portnov, K. V., Zaberzhinsky, B. E. Gabbasov, R. R. Agafonov, K. A. Analysis of methods of emergent artificial intelligence. *Actual problems of society, economics and law in the context of global challenges : collection of materials of the XX International scientific and practical conference., Moscow, May 17, 2023.* Saint Petersburg : Printing shop, 2023. Vol. 2, pp. 30–36. EDN GVVLER.

3. Karimov, B. F., Portnov, K. V. Problems of adaptation of genetic algorithms to solving problems of structural-parametric optimization. *Modern research: theory, practice, results : collection of materials of the International scientific and practical conference, Moscow, December 29, 2023.* Moscow, Center for the Development of Education and Science, OOO "ALEF Publishing House", 2023, pp. 443–448. DOI 10.26118/1590.2023.63.10.010. - EDN PUGPKI.

4. Zaberzhinsky, B. E., Zolin, A. G. Development of an intelligent image processing method to improve the accuracy of face recognition based on local binary patterns. *Modern science-intensive technologies*, 2023, no. 7, pp. 22–26. DOI: 10.17513/snt.39689. EDN PZDAPQ.

5. Portnov, K. V., Panyukova, E. V. Actual problems and tasks of automated systems in the housing and communal services sector. *Journal of Monetary Economics and Management*, 2024, no. 2, pp. 230–236. DOI: 10.26118/2782-4586.2024.35.72.033. EDN AEQRFJ.

6. Portnov, K. V. Development of an information system based on multivariate logistic regression. *Information technologies. Radio electronics. Telecommunications*, 2012, no. 2–3, pp. 129–133. EDN PEDEUX.

7. Portnov, K. V. *Analysis and improvement of raw material procurement management methods at an industrial enterprise: specialty 05.13.01 "System analysis, management and information processing (by industry)" : dissertation for the degree of candidate of technical sciences.* Samara, 2007. 132 p. EDN NOZCLT.

8. Portnov, K. V., Portnova, N. Yu., Sibartseva, E. V. Automated information systems for data analysis and processing in medicine. *Actual problems of science and education in the context of modern challenges : collection of materials of the XXVIIII International scientific and practical conference, Moscow, March 01, 2024.* St. Petersburg, Printing shop, 2024, pp. 82–88. DOI: 10.34755/IROK.2024.12.84.021. EDN EQBYWG.

Статья поступила в редакцию 27.09.2024; одобрена после рецензирования 28.10.2024; принята к публикации 28.10.2024.

The article was submitted 27.09.2024; approved after reviewing 28.10.2024; accepted for publication 28.10.2024.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ

УДК 004.82

ФОРМИРОВАНИЕ ВЫБОРОК ДЛЯ АНАЛИЗА ИЗОБРАЖЕНИЙ ГРАФИКОВ ЗАВИСИМОСТЕЙ ФИЗИЧЕСКИХ ВЕЛИЧИН

Коробкин Дмитрий Михайлович, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28,
кандидат технических наук, доцент, ORCID: 0000-0002-4684-1011, e-mail: dkorobkin80@mail.ru
Фоменков Сергей Алексеевич, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр. им. Ленина, 28,
доктор технических наук, профессор, ORCID: 0000-0001-9907-4488, e-mail: saf@vstu.ru

Нередко в исходных материалах, описывающих физический эффект, содержатся графики, иллюстрирующие зависимости между входными и выходными физическими величинами данного эффекта. В данной работе описана концепция и архитектура системы формирования неразмеченных и размеченных выборок изображений для нейросетевого анализа графиков зависимостей физических величин. Сформированы (а) неразмеченный массив изображений графиков зависимостей, (б) размеченный массив изображений с графиками линейного увеличения / уменьшения, постоянства, вогнутого увеличения/уменьшения и т. п. Проведены вычислительные эксперименты для фильтрации изображений графиков зависимостей из общего набора патентных изображений (чертежи, формулы, схемы и т. п.). Получены высокие значения Precision и AUC-ROC, показывающие верное распознавание изображений графиков зависимостей.

Ключевые слова: парсинг, изображения, графики зависимостей, физический эффект, патент, парсинг, нейросеть

Финансирование: *исследование выполнено за счет гранта Российского научного фонда № 24-21-20140, https://rscf.ru/project/24-21-20140/, и Администрации Волгоградской области.*

FORMATION OF SAMPLES FOR ANALYSIS OF IMAGES OF GRAPHS OF DEPENDENCIES OF PHYSICAL QUANTITIES

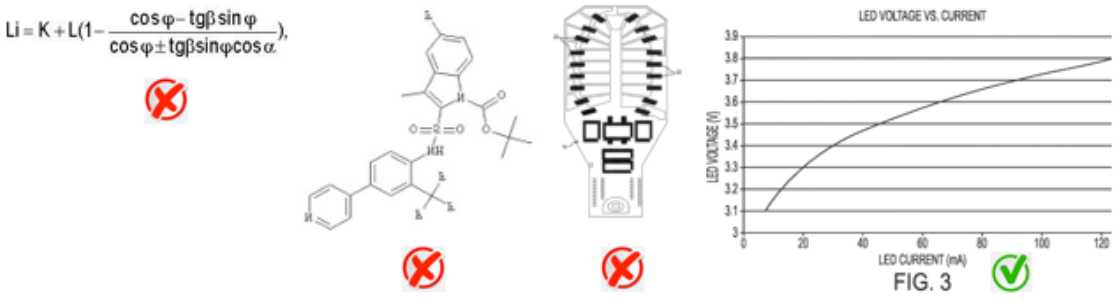
Korobkin Dmitry M., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
Cand. Sci. (Engineering), Associate Professor, ORCID: 0000-0002-4684-1011, e-mail: dkorobkin80 @mail.ru
Fomenkov Sergey A., Volgograd State Technical University, 28 Lenin Ave., Volgograd, 400005, Russian Federation,
Doct. Sci. (Engineering), Professor, ORCID: 0000-0001-9907-4488, e-mail: saf@vstu.ru

Often, the source materials describing a physical effect contain graphs illustrating the dependencies between the input and output physical quantities of the effect. This paper describes the concept and architecture of a system for generating unlabeled and labeled image samples for neural network analysis of dependency graphs of physical quantities. (a) an unlabeled array of dependency graph images, (b) a labeled array of images with graphs of linear increase/decrease, constancy, concave increase / decrease, etc. were generated. Computational experiments were conducted to filter the dependency graph images from a common set of patent images (drawings, formulas, diagrams, etc.). High values of Precision and AUC-ROC were obtained, indicating correct recognition of images of dependence graphs.

Keywords: parsing, images, dependency graphs, physical effect, patent, parsing, neural network.

Financial Support: *the study was supported by a grant from the Russian Science Foundation No. 24-21-20140, https://rscf.ru/project/24-21-20140/, and the Administration of the Volgograd Region.*

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

В процессе разработки новых технических систем одним из наиболее многообещающих подходов считается применение синтеза физического принципа действия (ФПД) [1]. ФПД представляет собой структуру, которая отражает взаимодействие различных физических явлений, обеспечивающих выполнение функций технической системы. На сегодняшний день сформировалась авторитетная научная школа по поиску конструктивных решений на базе систематизированных физических данных (А. И. Половинкин, В. А. Камаев и др.). Был создан фонд, включающий около 1200 физических эффектов [2], требующий автоматизации своего пополнения (обновления) с учетом новейших достижений физики.

Нередко в исходных материалах, описывающих физический эффект, содержатся графики, иллюстрирующие зависимости между входными и выходными физическими величинами данного эффекта. Задача анализа этой информации и ее использования для более полного описания физического явления остается насущной в настоящее время.

Таким образом, целью является разработка концепции и архитектуры системы формирования неразмеченных и размеченных выборок изображений для нейросетевого анализа графиков зависимостей физических величин. Для этого требуется сформировать (а) неразмеченный массив изображений графиков зависимостей, (б) размеченный массив изображений с графиками линейного увеличения / уменьшения, постоянства, вогнутого увеличения / уменьшения, выпуклого увеличения / уменьшения, скачкообразного увеличения / уменьшения, (в) также провести вычислительные эксперименты для фильтрации изображений графиков зависимостей из общего набора патентных изображений (чертежи, формулы, схемы и т. п.).

Необходимо решить следующие задачи:

1. Изучить методы парсинга страниц Google-картинки (Google Images) и патентной системы Google Patents [3].
2. Разработать алгоритмы парсинга изображений Google Images, парсинга изображений из патентов Google Patents, фильтрации изображений графиков зависимостей из патентов Google Patents
3. Разработать концепцию и архитектуру системы формирования неразмеченных и размеченных выборок изображений для нейросетевого анализа графиков зависимостей физических величин.
4. Сформировать неразмеченный массив изображений графиков зависимостей; размеченный массив изображений с графиками линейного увеличения / уменьшения, постоянства, вогнутого увеличения / уменьшения, выпуклого увеличения / уменьшения, скачкообразного увеличения / уменьшения.
5. Провести вычислительные эксперименты для фильтрации изображений графиков зависимостей из общего набора патентных изображений (чертежи, формулы, схемы и т. п.).

КОНЦЕПЦИЯ И АРХИТЕКТУРА

Формирование неразмеченных и размеченных выборок изображений для нейросетевого анализа графиков зависимостей физических величин осуществляется посредством парсинга (веб-скрейпинга). Парсинг – автоматизированный сбор и систематизация информации из открытых источников с помощью скриптов.

В процессе разработки системы формирования неразмеченных и размеченных выборок изображений для нейросетевого анализа графиков зависимостей были использованы следующие библиотеки:

– Selenium [4] – инструмент для имитации работы браузера, используется для сайтов с динамическим контентом, загружаемым через JS. Запускает отдельный браузер и имитирует действия реального пользователя;

– Requests [5] – библиотека для составления HTTP-запросов, которая позволяет легко отправлять различные веб-запросы, а также управлять cookies и сессиями, авторизацией и автоматической организацией пула соединений;

– BeautifulSoup [6] – библиотека для извлечения данных из HTML- и XML-файлов, производит анализ и конвертацию содержимого документов данных форматов. С помощью него гипертекстовую разметку можно преобразовать в полноценные объекты, атрибуты которых являются тегами в html.

АЛГОРИТМ ПАРСИНГА ИЗОБРАЖЕНИЙ GOOGLE IMAGES

На вход алгоритма подаются поисковые запросы (их может быть несколько), а также путь до каталога для сохранения всех картинок. Примеры запросов: «plot linear equation graph», «график линейной зависимости».

Далее запускается эмулятор браузера на странице Google Images по заданному запросу, страница выдачи разворачивается на весь экран (рис. 1). Далее происходит имитация нажатия на каждое изображение, начиная с первого, и для открытого справа в окне изображения по полученной ссылке происходит его скачивание (загрузка). Этот итерационный процесс осуществляется в цикле, пока не закончатся картинки (рис. 2).

Программа может сама листать вниз браузер нажатием на очередную картинку, при этом автоматически происходит загрузка большего количество изображений для показа. После того как нужное количество картинок было загружено, создается корневой каталог и в нем создается подкаталог с названием запроса, куда и загружаются картинки по полученным ссылкам.

В результате получаем сформированные папки с изображениями графиков зависимостей, полученных по соответствующим запросам к системе Google Images. Внутри каталога содержатся скачанные изображения (рис. 3).

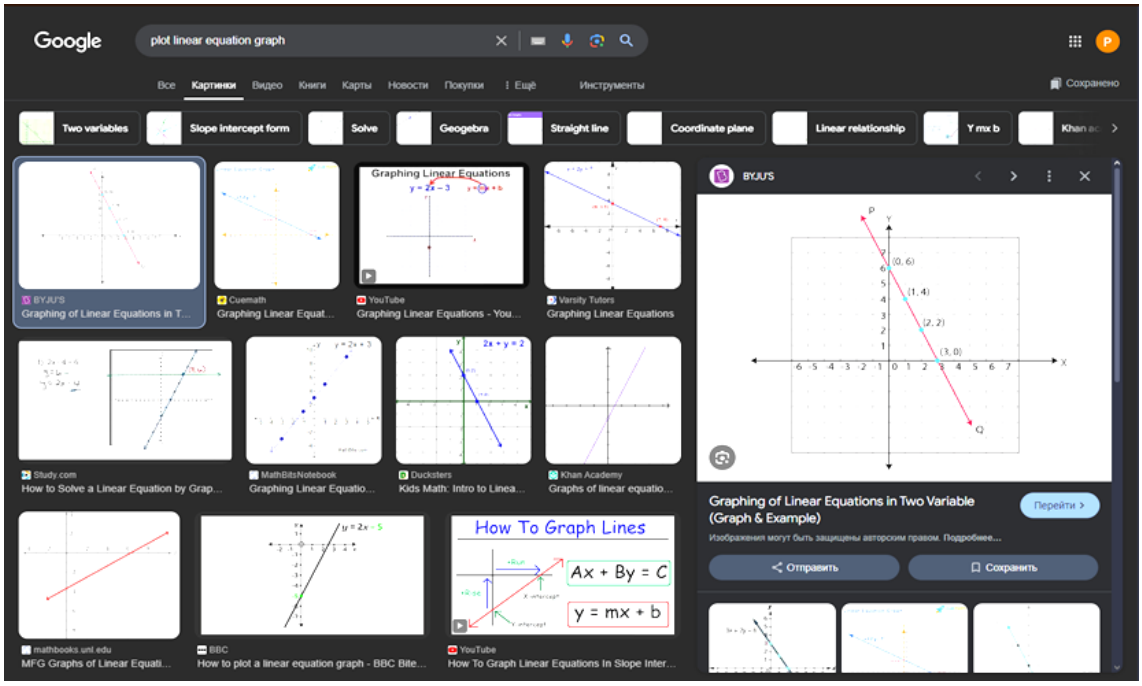


Рисунок 1 – Пример выдачи Google Images на запрос «plot linear equation graph»

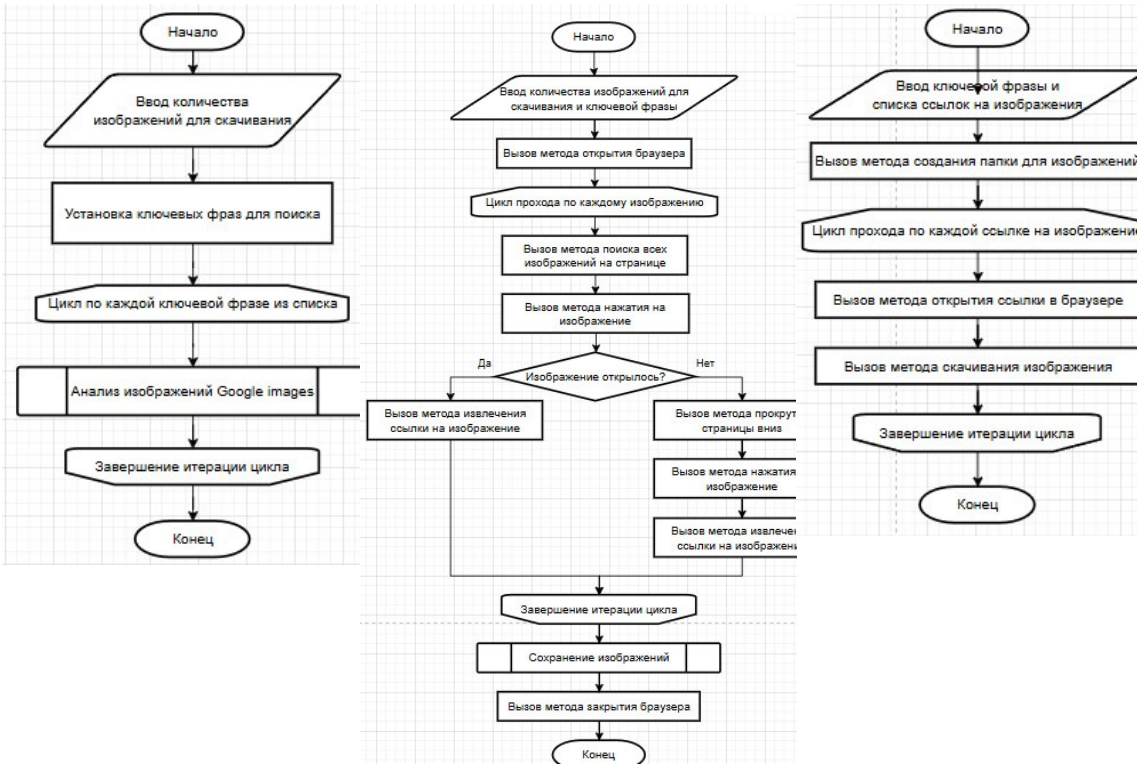


Рисунок 2 – Алгоритм парсинга изображений Google Images

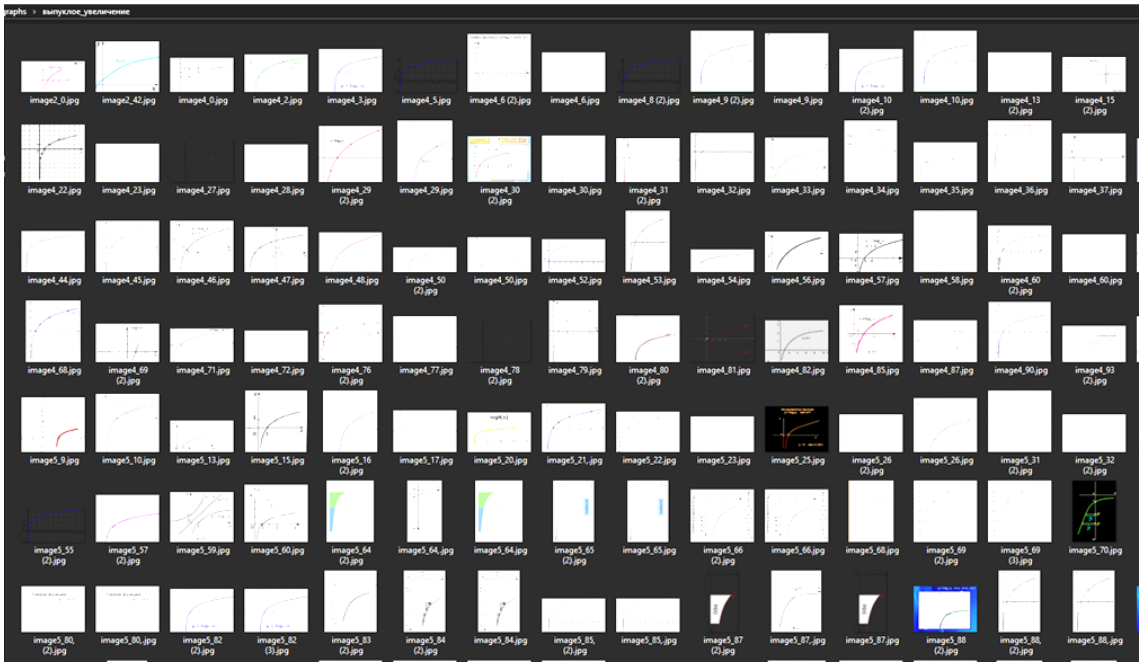


Рисунок 3 – Пример содержимого папки «Выпуклое увеличение»

АЛГОРИТМ ПАРСИНГА ИЗОБРАЖЕНИЙ ИЗ ПАТЕНТОВ GOOGLE PATENTS

На вход алгоритма подаются идентификаторы патентных классов, например, «G01N» (Исследование или анализ материалов путем определения их химических или физических свойств), в которых будет произведен поиск патентов.

Далее запускается эмулятор браузера на странице Google Patents (рис. 4) и сохраняются идентификаторы патентов (ID), которые удовлетворяются нашим запросам, в отдельный Excel-файл (рис. 5).

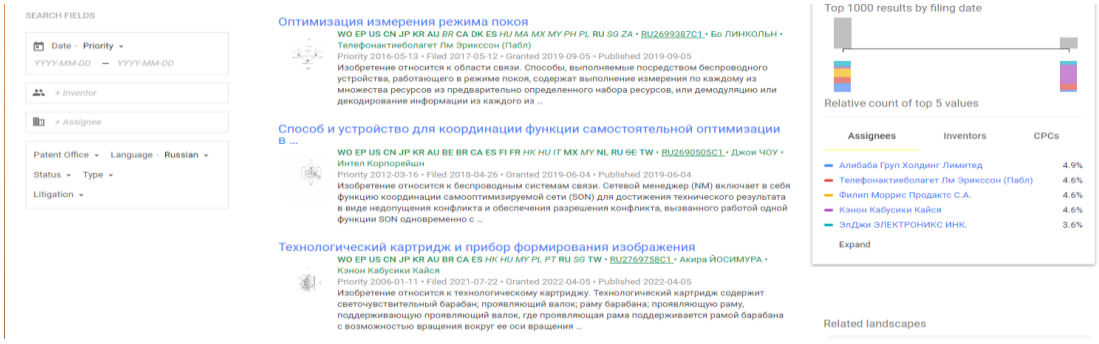


Рисунок 4 – Пример выдачи Google Patents на запрос, содержащий патентный класс

Перед началом скачивания изображений патентов создаются подкаталоги (с названиями патентов), в которые будут загружаться все имеющиеся картинки из патентов (рис. 6).

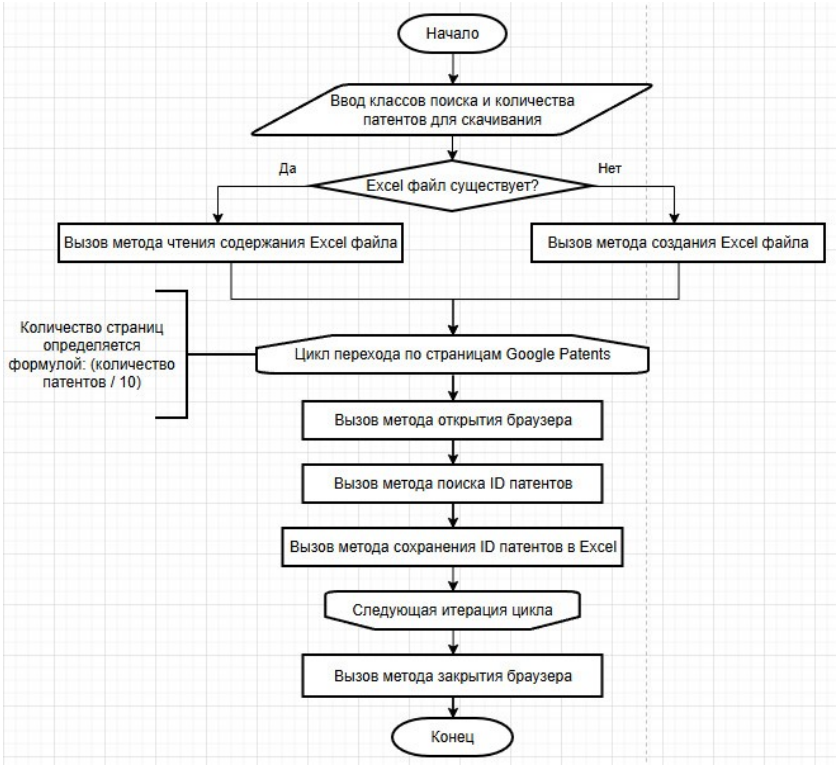


Рисунок 5 – Алгоритм получения идентификаторов (ID) патентов Google Patents

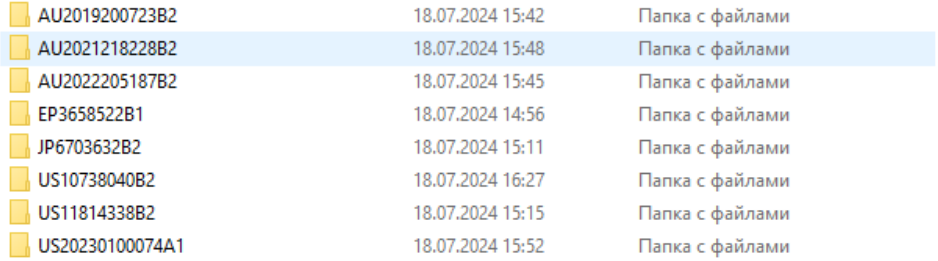


Рисунок 6 – Созданные каталоги с изображениями

Далее на основе имеющихся ID из файла запускается браузер на весь экран (рис. 7). Если на странице есть блок с изображениями, то происходит запуск плагина, отвечающего за имитацию нажатия на каждое изображение, начиная с первого.

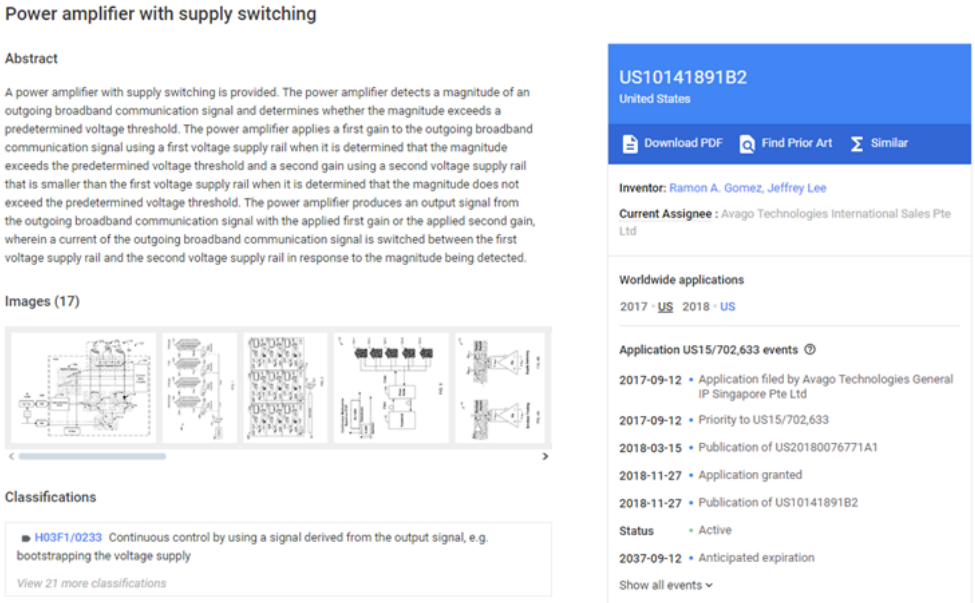


Рисунок 7 – Окно браузера с содержимым патента

В новом окне открывается изображение, осуществляется процедура скачивания (загрузки) изображения. Этот итерационный процесс осуществляется в цикле, пока не закончатся картинки (рис. 8).

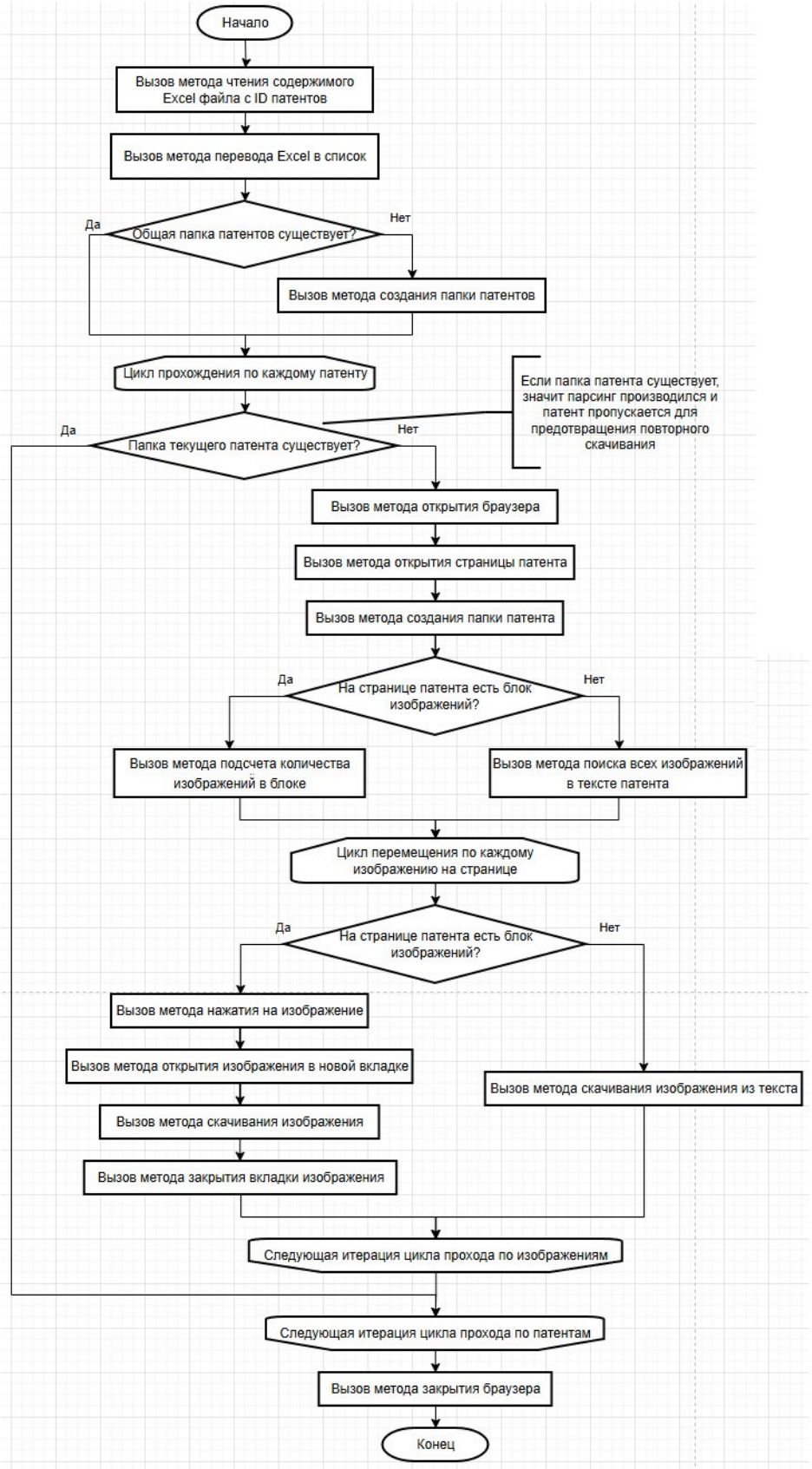


Рисунок 8 – Алгоритм формирования папок с изображениями патентов Google Patents

В результате получаем сформированные папки с патентными изображениями для патентов из выбранных патентных классов. Внутри каталога содержатся скачанные изображения (рис. 9).

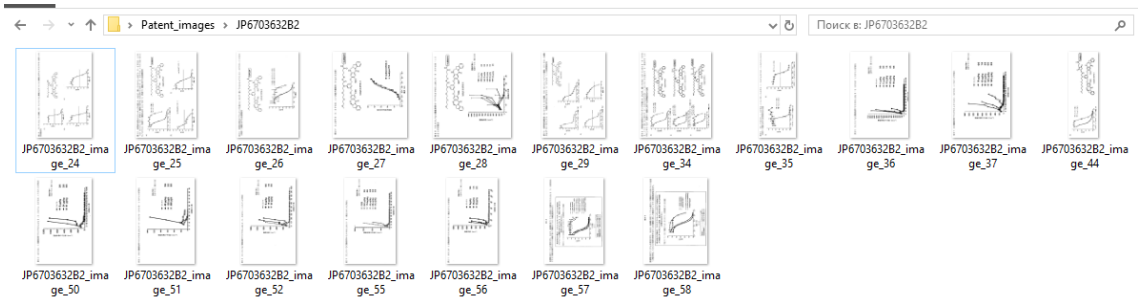
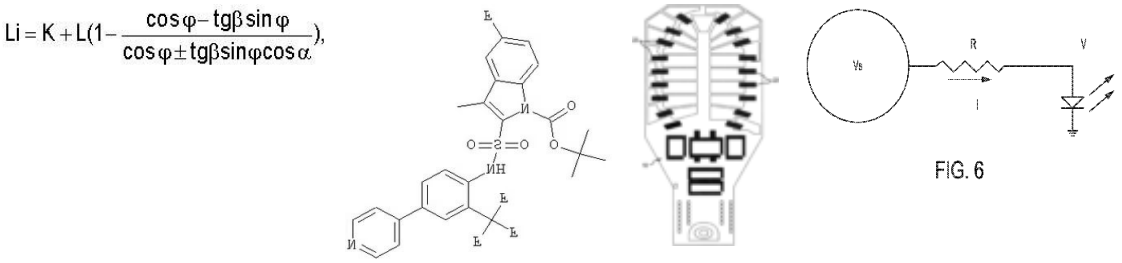


Рисунок 9 – Пример содержимого каталога изображений патентов

АЛГОРИТМ ФИЛЬТРАЦИИ ИЗОБРАЖЕНИЙ ГРАФИКОВ ЗАВИСИМОСТЕЙ ИЗ ПАТЕНТОВ GOOGLE PATENTS

Поскольку в патентных изображениях содержатся не только графики зависимостей, но также чертежи устройств, изображения математических, химических формул и т. п. (рис. 10), то необходимо разработать алгоритм тематической фильтрации изображений графиков зависимостей из патентов Google Patents (рис. 11).



а) математические формулы б) химические формулы в) чертежи г) схемы

Рисунок 10 – Пример изображений патентного массива

Рисунок 11 – Алгоритм фильтрации изображений графиков зависимостей

ПРОВЕРКА ЭФФЕКТИВНОСТИ ФИЛЬТРАЦИИ ИЗОБРАЖЕНИЙ ГРАФИКОВ ЗАВИСИМОСТЕЙ

Для увеличения точности обучения, а также исправления проблемы переобучения модели, была применена аугментация данных перед началом обучения, т. е. генерирование новых данных на основе имеющихся.

Для фильтрации изображений графиков зависимостей применялась библиотека tensorflow [7] и метод CNN [8]. Обучена нейронная сеть, отделяющая графики зависимостей от других изображений патентного массива (рис. 12). В качестве обучающей выборки использовалась база изображений (2 тыс.), содержащих графики зависимостей, из Google Images (рис. 13).

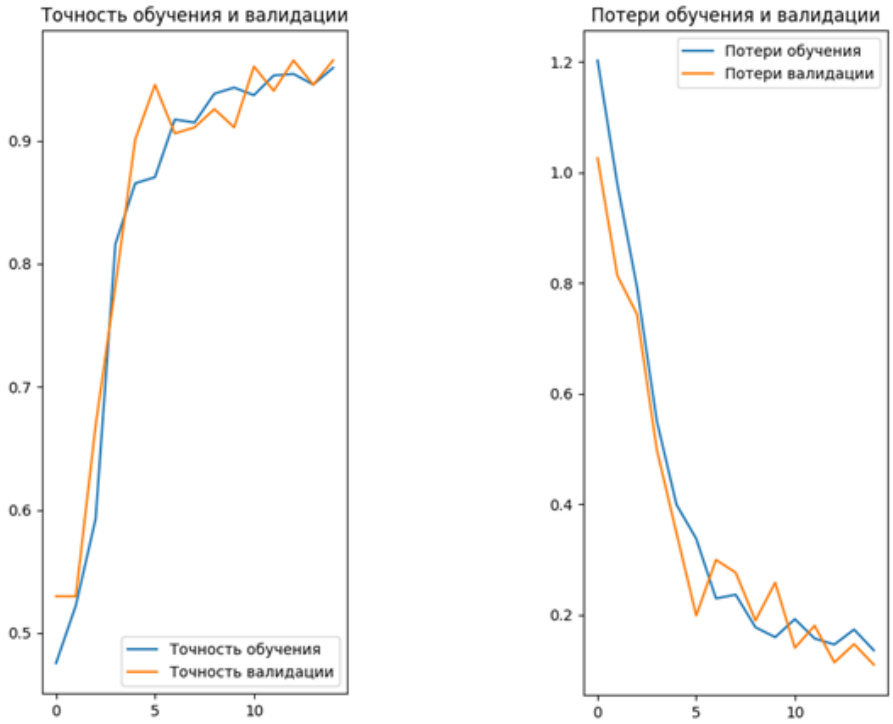


Рисунок 12 – Пример обучения при помощи модели CNN

Метрики проверки эффективности методов показаны на рисунке 10. Метрики получены на тестовых данных, которых не было в обучающем датасете при обучении модели.

```
Validation Accuracy: 0.6875
Validation Precision: 0.797562519784742
Validation Recall: 0.6875
Validation F1 Score: 0.6593573870157167
Validation ROC AUC: 0.9762570112179487
```

Рисунок 13 – Метрики эффективности фильтрации изображений при помощи модели CNN

Для вычисления метрик [9] использовался модуль metrics [10]. Для нахождения accuracy используется: accuracy_score(y_true, y_pred); precision – precision_score(y_true, y_pred); recall – recall_score(y_true, y_pred); f1-score – f1_score(y_true, y_pred); ROC-AUC – roc_auc_score(y_test, y_pred), где y_true – эталонные метки; y_pred – предсказанные метки.

Наиболее точной бинарной оценкой, используемой при оценке качества модели фильтрации, является AUC-площадь (Area Under Curve) под ROC-кривой (Receiver Operating Characteristics), выраженной через отношение доли истинно релевантных прогнозов к доле нерелевантных.

По результатам метрик можно сделать вывод, что Accuracy невелико, так как плохо сбалансированы классы изображений (2 тыс. изображений графиков зависимостей и только по 200 изображений чертежей, математических и химических формул). Полученные значения Precision и AUC-ROC показывают, что верное распознавание изображений графиков зависимостей – высокое.

ЗАКЛЮЧЕНИЕ

В результате работы сформированы (а) неразмеченный массив изображений графиков зависимостей, (б) размеченный массив изображений (2 тыс.) с графиками линейного увеличения / уменьшения, постоянства, вогнутого увеличения / уменьшения, выпуклого увеличения / уменьшения, скачкообразного увеличения / уменьшения. Проведены вычислительные эксперименты для фильтрации изображений графиков зависимостей из общего набора патентных изображений (чертежи, формулы, схемы и т. п.). Получены высокие значения Precision и AUC-ROC, показывающие верное распознавание изображений графиков зависимостей.

Список литературы

1. Bobunov, A. Development of the Concept and Architecture of an Automated System for Updating Physical Knowledge for Information Support of Search Design / A. Bobunov, D. Korobkin, S. Fomenkov // 2023 International Russian Smart Industry Conference (SmartIndustryCon) (Sochi, Russian Federation, 27–31 March 2023) : proceedings / Russia Siberia Section IEEE et al. – IEEE, 2023. – P. 281–288. – DOI: 10.1109/SmartIndustryCon57312.2023.10110764.

2. Козина, С. А. Архитектура системы формирования единой базы знаний по физической тематике / С. А. Козина, Д. М. Коробкин, С. А. Фоменков, С. Г. Колесников // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 1 (61). – С. 27–37. – DOI: 10.54398/20741707_2023_1_27.

3. Google Patents. – URL: https://patents.google.com/ (дата обращения: 15.11.2024).

4. Manukonda, Kodanda. A Comprehensive Evaluation of Selenium Webdriver for Cross-Browser Test Automation: Performance, Reliability, and Usability / Manukonda Kodanda // Journal of Artificial Intelligence Machine Learning and Data Science. – 2023. – № 1.

5. Requests: HTTP for Humans. – URL: https://requests.readthedocs.io/en/latest/ (дата обращения: 15.11.2024).

6. Abodayeh, Ayat. Web Scraping for Data Analytics: A BeautifulSoup Implementation / Abodayeh Ayat, Hejazi Reem, Najjar Ward, Shihadeh Leena & Latif Rabia. –2023. – P. 65–69. – 10.1109/WiDS-PSU57071.2023.00025.

7. Abadi, Martín. TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems / Abadi Martín, Agarwal Ashish, Barham Paul, Brevdo Eugene, Chen Zhifeng, Citro Craig, Corrado G.s, Davis Andy, Dean Jeffrey, Devin Matthieu, Ghemawat Sanjay, Goodfellow Ian, Harp Andrew, Irving Geoffrey, Isard Michael, Jia Yangqing, Jozefowicz Rafal, Kaiser Lukasz, Kudlur Manjunath & Zheng Xiaoqiang. – 2016. – 10.48550/arXiv.1603.04467.

8. Ahmed, Wafaa & Karim, Abdulamir. The Impact of Filter Size and Number of Filters on Classification Accuracy in CNN / Ahmed Wafaa & Karim Abdulamir. – 2020. – P. 88–93. – 10.1109/CSASE48920.2020.9142089.

9. Davis, Jesse. The Relationship Between Precision-Recall and ROC Curves / Davis Jesse & Goadrich Mark // Proceedings of the 23rd International Conference on Machine Learning. – ACM, 2006. – Vol. 6. – 10.1145/1143844.1143874.

10. Module: tf.keras.metrics. – URL: https://www.tensorflow.org/api_docs/python/tf/keras/metrics (дата обращения: 15.11.2024).

References

1. Bobunov, A., Korobkin, D., Fomenkov, S. Development of the Concept and Architecture of an Automated System for Updating Physical Knowledge for Information Support of Search Design. *2023 International Russian Smart Industry Conference (SmartIndustryCon) (Sochi, Russian Federation, 27–31 March 2023) : proceedings / Russia Siberia Section IEEE [et al.].* IEEE, 2023, pp. 281–288. DOI: 10.1109/SmartIndustryCon57312.2023.10110764.

2. Kozina, S. A., Korobkin, D. M., Fomenkov, S. A., Kolesnikov, S. G. Architecture of the system for creating a unified knowledge base on physical topics. *Caspian Journal: Control and High Technologies*, 2023, no. 1 (61), pp. 27–37. DOI: 10.54398/20741707_2023_1_27 (In Russ.).

3. *Google Patents.* Available at: https://patents.google.com/ (accessed 15.11.2024).

4. Manukonda, Kodanda. A Comprehensive Evaluation of Selenium Webdriver for Cross-Browser Test Automation: Performance, Reliability, and Usability. *Journal of Artificial Intelligence Machine Learning and Data Science*, 2023, no. 1.

5. Requests: HTTP for Humans. Available at: https://requests.readthedocs.io/en/latest/ (accessed 15.11.2024).

6. Abodayeh, Ayat, Hejazi, Reem, Najjar, Ward, Shihadeh, Leena, Latif, Rabia. *Web Scraping for Data Analytics: A BeautifulSoup Implementation*, 2023, pp. 65–69. 10.1109/WiDS-PSU57071.2023.00025.

7. Abadi, Martín, Agarwal, Ashish, Barham, Paul, Brevdo, Eugene, Chen, Zhifeng, Citro, Craig, Corrado, G.s, Davis, Andy, Dean, Jeffrey, Devin, Matthieu, Ghemawat, Sanjay, Goodfellow, Ian, Harp, Andrew, Irving, Geoffrey, Isard, Michael, Jia, Yangqing, Jozefowicz, Rafal, Kaiser, Lukasz, Kudlur, Manjunath, Zheng, Xiaoqiang. *TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems*, 2016. 10.48550/arXiv.1603.04467.

8. Ahmed, Wafaa, Karim, Abdulamir. *The Impact of Filter Size and Number of Filters on Classification Accuracy in CNN,* 2020, pp. 88–93. 10.1109/CSASE48920.2020.9142089.

9. Davis, Jesse, Goadrich, Mark. The Relationship Between Precision-Recall and ROC Curves. *Proceedings of the 23rd International Conference on Machine Learning*. ACM, 2006, vol. 06. 10.1145/1143844.1143874.

10. *Module: tf.keras.metrics.* Available at: https://www.tensorflow.org/api_docs/python/tf/keras/metrics (accessed 15.11.2024).

Статья поступила в редакцию 15.11.2024; одобрена после рецензирования 29.11.2024; принята к публикации 29.11.2024.

The article was submitted 15.11.2024; approved after reviewing 29.11.2024; accepted for publication 29.11.2024.

МАТЕМАТИЧЕСКОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ, КОМПЛЕКСОВ И КОМПЬЮТЕРНЫХ СЕТЕЙ

УДК 004.032.26

НЕЙРОСИСТЕМА ДИАГНОСТИКИ ЗАБОЛЕВАНИЙ КОЖИ

Доля Юлия Григорьевна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149.

бакалавр, ORCID: 0009-0004-5570-2832, e-mail: juliadolya06@gmail.com

Лукащик Елена Павловна, Кубанский государственный университет, 350040, Российская Федерация, г. Краснодар, ул. Ставропольская, 149,

кандидат физико-математических наук, доцент, ORCID: 0000-0002-7900-0841, e-mail: lep_9091@mail.ru

Данная работа демонстрирует результаты применения сверточной нейронной сети при создании автоматизированной системы диагностики кожных заболеваний по их изображениям. На сегодняшний день архитектуры, основанные на сверточных сетях, являются лучшим решением для задач распознавания образов. В ходе численного эксперимента подобраны параметры архитектуры сверточной сети, такие как: количество слоев, размерность ядра свертки для каждого из них и количество извлекаемых фильтров на слое, функция активации и другие, влияющие на качество обучения. Большое внимание уделено этапу обучения сети: описаны необходимость и суть применяемых методов. Первичное обучение нейронной сети проводилось на данных открытого архива изображений ImageNet. Предобученная сеть была перенастроена на классификацию кожных заболеваний на подготовленном наборе данных, составленном из открытого датасета ISIC, и протестирована на контрольной выборке, исключенной из общего набора обучающих данных. На контрольных выборках диагностический результат по метрике, отображающей способность сетевой модели давать правильный ответ относительно общего количества исследований, достиг 90 %. Результат по метрике, объединяющей в себе информацию о точности и полноте, составил 89 % и 91 % для классов новообразований: меланомы (злокачественная) и невуса (доброкачественная) соответственно.

Ключевые слова: машинное обучение, распознавание образов, нейронная сеть, свертка, классификация, диагностика, новообразования, меланома, невус

NEUROSYSTEM FOR DIAGNOSTICS OF SKIN DISEASES

Dolya Julia G., Kuban State University, 149 Stavropolskay St., Krasnodar, 350040, Russian Federation,

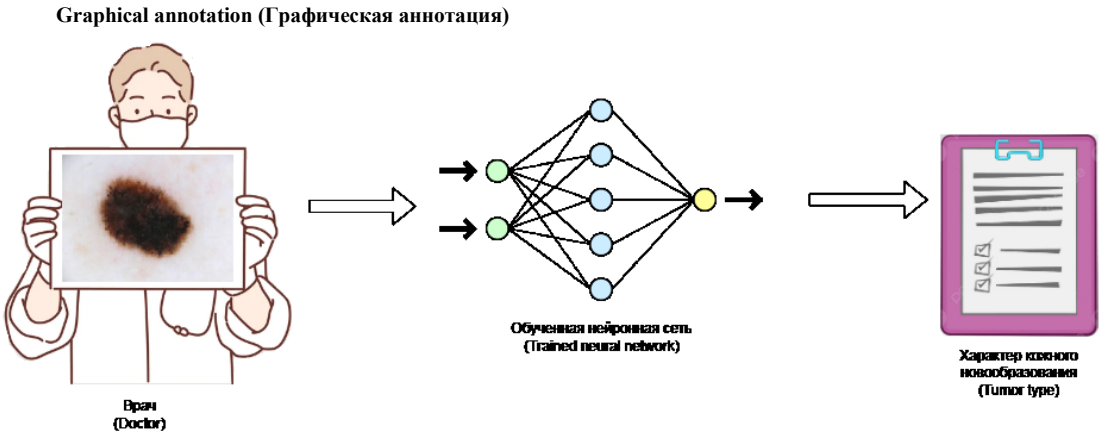
bachelor, ORCID: 0009-0004-5570-2832, e-mail: juliadolya06@gmail.com

Lukashchik Elena P., Kuban State University, 149 Stavropolskay St., Krasnodar, 350040, Russian Federation,

Cand. Sci. (Physics & Mathematics), Associate Professor, ORCID: 0000-0002-7900-0841, e-mail: lep_9091@mail.ru

This work demonstrates the results of using a convolutional neural network to create an automated diagnosing system for skin diseases by their images. Today, architectures based on convolutional networks are the best solution of image recognition problems. During the numerical experiment, the parameters of the convolutional network architecture were selected, such as: the number of layers, the dimension of the convolution kernel for each of them and the number of extracted filters per layer, the activation function and others that affect the quality of training. Much attention is paid to network training. The necessity and essence of the methods used are described. Primary training of the neural network was carried out on data set from the open image archive ImageNet. Then the pre-trained network was reconfigured to classify skin diseases on a prepared data set compiled from the open ISIC dataset, and tested on a control sample excluded from the general training data set. In control samples the diagnostic result reached 90 % by the metric reflecting the ability of the network model to give the correct answer relative to the total number of studies. By the metric combining information on precision and recall the result was 89 % and 91 % for the classes of neoplasms: melanoma (malignant) and nevus (benign), respectively.

Keywords: machine learning, image recognition, neural network, convolution, classification, diagnosis, skin neoplasms, melanoma, nevus



ВВЕДЕНИЕ

Несмотря на достигнутое за последние годы понимание международным сообществом серьезности глобальных экологических проблем, позволившее значительно сократить выбросы химикатов в атмосферу, озоновый слой разрушается. Истощение озонового слоя приводит к повышению уровня ультрафиолетового излучения, что является первопричиной раковых заболеваний кожи. Так, в связи с «увеличением суммарного времени и интенсивности воздействия УФ части спектра солнечного света на человека, генетически к этому неподготовленного», в современном мире наблюдается тревожная тенденция роста заболеваемости кожи [2]. В наше время каждый десятый страдает от заболеваний кожи. Самой злокачественной и агрессивной опухолью является меланома.

Однако диагностика заболеваний кожи значительно затруднена в связи с разнообразием видов и симптомов дерматологических заболеваний. Такая задача требует от врача-дерматолога глубоких знаний и навыков, отнимает много времени и является достаточно трудоемкой. По этой причине дерматологам требуются годы обучения, чтобы развить навыки постановки точного диагноза. При формировании диагноза необходимо учитывать все особенности, наблюдаемые у пациента, и сравнивать их с особенностями, наблюдаемыми при различных заболеваниях. Известно, что точность правильного выявления кожных поражений врачом-дерматологом составляет менее 80 %. На сегодняшний день развитие нейросетевых технологий компьютерного зрения позволяет автоматизировать процесс диагностики этого заболевания. Использование глубоких нейронных сетей позволяет повысить точность определения диагноза, ускорить и облегчить решение многих проблем. Данная работа демонстрирует разработку сверточной нейронной сети для диагностики кожных заболеваний, а именно для определения доброкачественных (невус) и злокачественных (меланома) новообразований кожи.

МОДЕЛЬ СИСТЕМЫ

Нейронная сеть – это метод в искусственном интеллекте, цель которого имитировать структуру и функциональность биологического мозга. Одним из лучших алгоритмов по распознаванию и классификации изображений является сверточная нейронная сеть – модель нейронных сетей глубокого обучения, предложенная Яном Лекуном [3]. Сверточная нейронная сеть позволяет создавать более сложные представления визуальных данных, так как по аналогии со зрительной корой головного мозга простые характеристики извлекаются на ранних стадиях, а более сложные характеристики изучаются на более глубоких уровнях.

Сверточные сети в зависимости от типа исследуемой задачи настраиваются так, чтобы найти лучший признак. Они обеспечивают масштабируемый подход к работе с изображениями, используя принципы линейной алгебры для выявления закономерностей между признаками объектов. Главная идея таких сетей состоит в том, что обработка участка изображения должна происходить независимо от его конкретного расположения.

Сверточная нейронная сеть состоит из нескольких слоев, которые можно условно разделить на три группы: сверточные слои, слои подвыборки и полносвязные слои. По мере прохождения данных через эти слои сложность сети увеличивается, что позволяет ей с каждым следующим слоем последовательно идентифицировать большие части изображения, что в конечном итоге приводит к распознаванию предполагаемого объекта. Объединение всех слоев составляет полную архитектуру сверточной нейронной сети. В основе разработанной системы лежит нейронная сеть с архитектурой ResNet-50 – наиболее популярной и эффективной моделью сверточных нейронных сетей в области обработки растровых изображений [4].

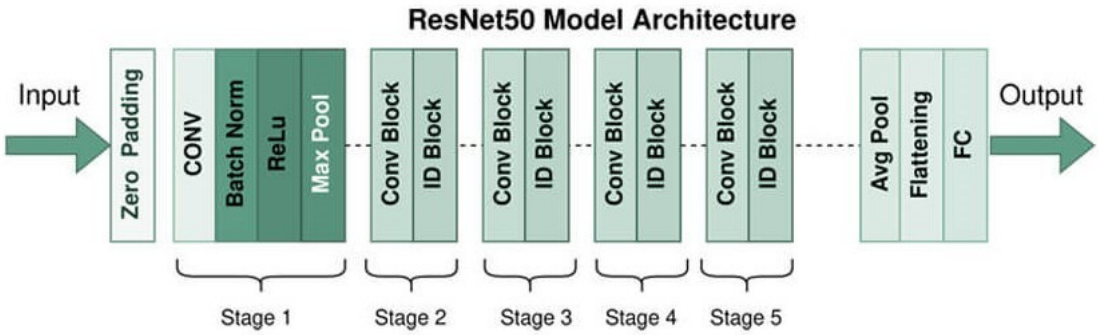


Рисунок 1 – Структура сети ResNet-50

ResNet-50 состоит из 50 слоев, разделенных на 5 блоков, каждый из которых содержит набор блоков с остаточными связями, которые позволяют модели обучаться на глубоких архитектурах, не сталкиваясь с проблемой затухания градиента. Остаточные блоки позволяют сохранить информацию из более ранних слоев, что помогает сети лучше изучить представление входных данных. Каждый остаточный блок состоит из двух сверточных слоев, за каждым из которых следует слой пакетной нормализации и функция активации ReLU. Затем выходные данные второго сверточного слоя добавляются ко входным данным остаточного блока, который затем передается через другую функцию активации ReLU. Выходные данные остаточного блока затем передаются следующему блоку. В архитектуре сети используется идея бутылочного горлышка. Остаточный блок с узким местом использует свертки 1×1, затем свертку 3×3, в конце возвращает количество карт свертками 1×1. Такая процедура позволяет быстрее обучать каждый слой.

СРЕДА РАЗРАБОТКИ СИСТЕМЫ

Для разработки и обучения нейронной сети выбран язык программирования Python, а конкретно его распространенная реализация CPython, написанная на C. Язык предлагает широкие возможности машинного обучения. Также при работе с нейронными сетями немаловажную роль имеет предобработка входных данных для обучения. Для работы с данными Python предоставляет множество удобных библиотек.

Реализация описанной нейронной сети выполнена на основе фреймворка PyTorch. Он предоставляет широкий доступ для манипулирования низкоуровневыми деталями, что позволяет точнее настраивать параметры сети. Фреймворк позволяет переключаться в коде между обычным центральным (CPU) и графическим процессором (GPU). Встроенный модуль Optim включает в себя реализацию всех наиболее часто используемых инструментов оптимизации для работы нейронных сетей, что делает разработку модели эффективнее. Модуль Data Loader позволяет создавать мини-пакеты в рамках одного датасета и подгружать их в модель, перемешивать данные, определять размер мини-пакета, что упрощает и ускоряет загрузку данных, экономит память.

В работе использованы библиотеки Numpy, Scikit-learn и Seaborn. Scikit-Learn – популярная библиотека машинного обучения на Python [5]. Она предоставляет широкий спектр метрик для оценки качества работы обученной нейронной сети, а также позволяет вычислить матрицу ошибок, с помощью которой можно оценить сильные и слабые стороны модели. Библиотека Numpy использовалась для более эффективной работы с многомерными массивами и матрицами. Для визуализации данных применялась библиотека Seaborn.

ОБУЧЕНИЕ СВЕРТОЧНОЙ СЕТИ

Обучение нейронной сети обычно требует большого количества тренировочных данных, вычислительных ресурсов и времени. Однако сверточные нейронные сети имеют общее свойство: на первых слоях модели сеть пытается изучить общую для всех изображений информацию, такую как обнаружение краев, изменений интенсивности цвета и т. д. Такие признаки не являются специфичными для конкретного набора данных, так как не зависят от типа обрабатываемого изображения, по этой причине они могут быть применены и для решения другой задачи. В связи с этим в задачах компьютерного зрения, требующих большого объема данных и огромного количества вычислительных мощностей, наиболее часто используют Transfer learning и Fine-Tuning.

Transfer learning (перенос обучения) – это метод машинного обучения, применяющийся для настройки сети и ее обучения, при котором знания, полученные моделью в задаче с большим количеством доступных обучающих данных, применяются в новой задаче, в которой данных немного [6]. То есть вместо того, чтобы начинать процесс обучения сети с нуля, можно использовать значения весов, полученных в результате решения другой задачи. Другими словами, Transfer

learning позволяет не проводить обучение нейронной сети с самого начала, а использовать в качестве основы готовую предварительно обученную сеть. Такой метод позволяет быстрее и эффективнее обучать новую нейронную сеть, а также может помочь предотвратить переобучение, поскольку модель уже усвоила общие признаки, которые могут оказаться полезными во второй задаче.

Обычно вместе с методом переноса обучения используется Fine-Tuning. Fine-Tuning (тонкая настройка обучения) – это один из методов, который позволяет адаптировать предварительно обученные модели нейронных сетей для конкретных задач или наборов данных. При тонкой настройке берутся существующие параметры сети и дополнительно обучаются для выполнения новой задачи. Одним из важных параметров сети является скорость обучения, определяющая процесс обновления весов во время обучения. Для тонкой настройки необходимо использовать меньшую скорость обучения, чем для обучения с нуля, чтобы сохранить знания, полученные с помощью предварительно обученной сети. Другим способом Fine-Tuning является заморозка и разморозка некоторых слоев модели. Замораживание слоя означает, что его веса не обновляются во время обучения. Обычно в новой сети замораживаются только те слои исходной модели, знания которых должны быть сохранены для нового обучения. Последние слои, фиксирующие более конкретные признаки объектов, участвуют в обучении. Также для адаптации к новой задаче к модели можно добавлять новые слои. Например, добавление выходного слоя, соответствующего количеству классов новой задачи. В качестве тонкой настройки для улучшения способности модели к обобщению используют аугментацию данных, состоящую в применении некоторых преобразований к данным для увеличения их разнообразия и надежности.

Обучение нейронной сети ResNet-50 проводилось на данных открытого архива изображений ImageNet [7]. Предварительно обученная сеть была перенастроена на классификацию кожных заболеваний. В стандартном варианте сети ResNet-50 последний уровень полносвязного слоя предназначен для классификации 1000 классов (количество классов в ImageNet). В исследуемой задаче диагностики заболеваний кожи количество классов отличается от того, которое было в исходном датасете. Так как для распознавания предоставлено два объекта (меланома и невус), то это задача бинарной классификации, т. е. на выходе сети должен быть один нейрон. По этой причине от сети ResNet-50, натренированной на определенную задачу, была взята сверточная часть, выделяющая характерные признаки изображения, а часть классификации была заменена на другую, состоящую из полносвязного слоя и имеющую на выходе один нейрон. Такая замена последнего слоя в архитектуре ResNet-50 позволяет использовать уже полученные знания для решения более конкретной задачи. Для интерпретации выходов сети как вероятностей распознаваемых классов последний слой новой сети представлен функцией активации softmax с двумя классами [8]. В слое softmax количество узлов равно количеству выходов, а значение показывает вероятность каждого выхода.

В архитектурах глубоких нейронных сетей начальные слои изучают общую информацию, а слои на последнем уровне – более специфичные признаки. Данные сформированного для задачи датасета сильно отличаются от архива, на котором обучалась ResNet-50. По этой причине использовался метод Fine Tuning, который захватывает несколько последних сверточных слоев. Чем сильнее исходные данные отличаются от тех, на которых нейронная сеть обучалась, тем большее количество слоев необходимо разморозить. Так, перед обучением разработанной сети были разморожены веса последних 10 слоев, чтобы они тоже участвовали в обучении.

На следующем этапе для правильной корректировки весов была выбрана небольшая начальная скорость обучения. В качестве функции потерь использовалась функция Кросс-энтропия (перекрестная энтропия) [9], которая является более динамичной и устойчивой по сравнению с другими метриками, так как учитывает статистическую достоверность и различия в атрибутах данных. Для изменения весов и скорости обучения применялся оптимизатор Adam, обновляющий скорость обучения для каждого веса нейронной сети индивидуально.

Данные для обучения реализуемой сети были взяты из наиболее популярного архива кожных заболеваний ISIC [10], находящегося в открытом доступе и состоящего из изображений меланом и невусов. В сверточных нейронных сетях обычно используется обучение с учителем. Обучение с учителем предполагает наличие полного набора размеченных данных для тренировки модели на всех этапах ее построения [11]. По этой причине исходный датасет был разделен на три части: обучающую, валидационную и тестовую выборки. Каждая выборка была разделена на две категории – меланома и невус. Обучение сети проводилось на обучающей выборке, составляющей около 70 % от всех имеющихся данных, подбор оптимального набора гиперпараметров, а также контроль за переобучением проводился на валидационной выборке (15 % наблюдений). Для оценки качества работы модели использовалась тестовая выборка (также 15 % наблюдений). Однако изображений в архиве оказалось недостаточно для качественного обучения модели. Кроме того, многие изображения в этом архиве содержат различные зашумления (волосы, разметка на коже, плохое освещение, разная масштабируемость). Совокупность таких обстоятельств затрудняет процесс качественного обучения нейронных сетей [12].

Необходимо отметить, что полученный набор данных является несимметричным: количество изображений меланом значительно меньше количества изображений невусов. Это обусловлено естественными причинами, так как случаи установления диагноза меланомы встречаются реже в общем количестве дерматологических осмотров. Поэтому была проведена стратификация – балансировка классов в выборке. Таким образом получен датасет порядка 17 тысяч изображений.

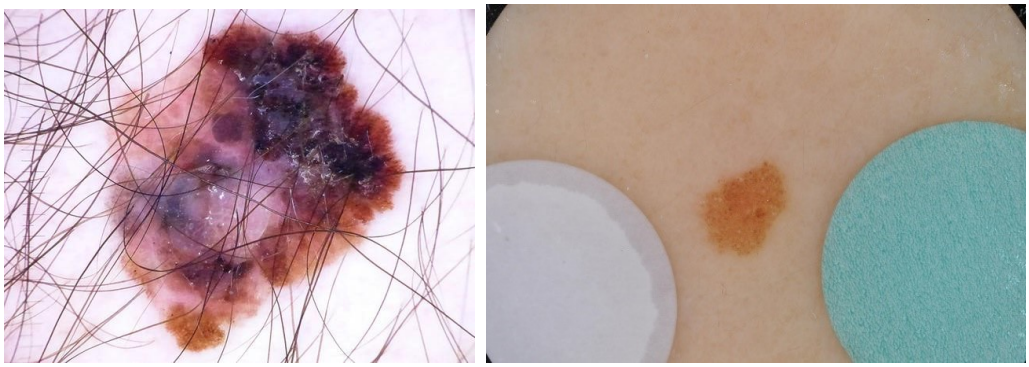


Рисунок 2 – Примеры изображений из датасета

По совокупности причин применен метод аугментации данных на лету. Проводилась модификация данных из тренировочной и валидационной выборки и создание на этой основе дополнительных изображений. Тестовая выборка оставалась неизменной. Было важно задать параметры аугментации так, чтобы они подходили к рассматриваемой задаче. Неправильно подобранные параметры привели бы к искажению изображений и снижению точности работы сети. Поэтому в качестве модификации использовались операции поворота изображений на определенный угол, отображение по горизонтали или вертикали. Такие изменения являются стандартными и хорошо подошли к задаче, так как не влияют на главные признаки объекта.

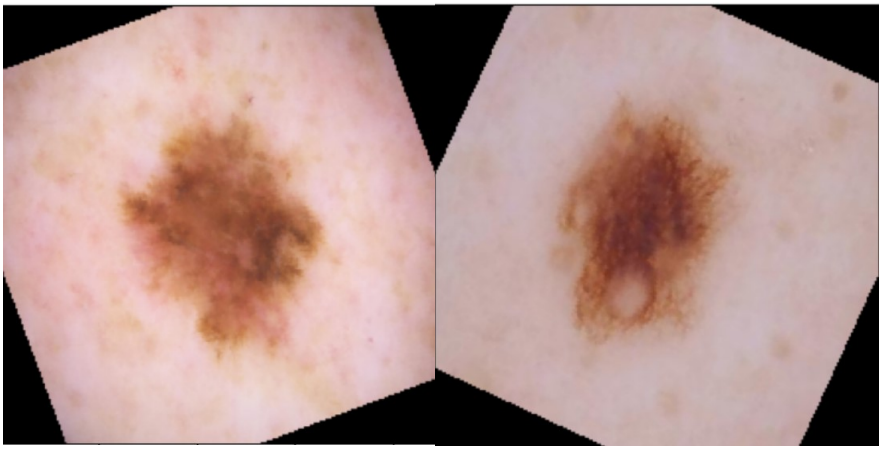


Рисунок 3 – Применение аугментации данных

RGB-значения полученных объектов будут находиться в разных местах трехмерного изображения, т. е. тензорное представление будет другим, что повышает обобщающую способность сети. Такие изменения позволили привести все изображения к одному размеру, а также увеличить объем исходного количества изображений в тренировочном датасете в два раза.

Предобученная нейронная сеть дополнительно обучена на подготовленном тренировочном наборе данных. Оценка работы сети проведена на тестовом датасете, содержащем данные, не участвующие при обучении.

ОЦЕНКА КАЧЕСТВА РАБОТЫ СЕТИ

Для оценки качества обученной нейронной сети, а также для сравнения результатов работы алгоритмов машинного обучения используют численные меры, или метрики. Метрику обычно измеряют на тестовом датасете, содержащем данные, не участвующие в обучении сети. Существует множество метрик, предназначенных для задач разных категорий, таких как задачи классификации, регрессии, ранжирования, обработки естественного языка и т. д.

В случае бинарной классификации для каждого объекта возможны следующие исходы распознаваний [13]:

1) истинно-положительные (True Positive, TP) – класс, предсказанный как положительный, является положительным;

2) истинно-отрицательные (True Negative, TN) – класс, предсказанный как отрицательный, является отрицательным;

3) ложноположительные (False Positive, FP) – класс, предсказанный как положительный, является отрицательным;

4) ложноотрицательные (False Negative, FN) – класс, предсказанный как отрицательный, является положительным.

Для наглядности эти исходы представляют в виде двумерной таблицы, которая называется матрицей ошибок [14]. В матрице ошибок строки представляют экземпляры истинного класса, а столбцы – прогнозируемого класса.

	Predicted: NO	**Predicted: YES**
Actual: NO	TN	FP
Actual: YES	FN	TP

Рисунок 4 – Матрица ошибок

На основе комбинаций элементов матрицы ошибок строятся метрики, позволяющие детальнее оценить полноту, чувствительность и точность нейронной сети.

Самой простой и распространенной является метрика accuracy – количество верно классифицированных объектов среди всех объектов экземпляра [15]:

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN}. \quad (1)$$

Однако в случае несбалансированных по классам данных она мало информативна, так как не учитывает соотношения ложных срабатываний модели.

В случае асимметрии классов, когда необходимо оценить качество работы нейронной сети на каждом классе в отдельности, используются метрики precision, recall, F1. Метрика precision показывает количество истинно положительных объектов из всего набора положительных объектов. Ее значения варьируются в диапазоне от 0 до 1. Результат precision должен быть максимально высоким. Оценка точности, равная 1, будет означать, что нейронная сеть способна хорошо классифицировать правильную и неправильную маркировку классов, так как она не упустила ни одного истинного положительного результата. Недостатком такой метрики является то, что она не учитывает ложноотрицательные результаты:

$$\text{precision} = \frac{TP}{TP + FP}. \quad (2)$$

В отличие от precision метрика recall показывает долю истинно положительных объектов среди всех объектов положительного класса, не учитывая при этом ложноположительные результаты. Метрику recall также часто называют полнотой или чувствительностью нейронной сети:

$$\text{recall} = \frac{TP}{TP + FN}. \quad (3)$$

В случае, когда метрики precision и recall одинаково значимы, можно использовать их среднее гармоническое [16]. Такая оценка называется F1-мерой. Она достигает своего наилучшего значения в 1 и худшего в 0.

$$\text{F1} = 2 * \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}}. \quad (4)$$

Качество применяемой в диагностической системе сверточной сети измерялось по разным метрикам на тестовом датасете, состоящем из 571 изображения. Результат по метрике Accuracy, отображающей способность модели давать правильный ответ относительно общего количества исследований, составил 90 %. Результат по метрике F1, объединяющей в себе информацию о точности и полноте, составил 89 % и 91 % для класса меланомы и невуса соответственно.

ЗАКЛЮЧЕНИЕ

Результаты исследования доказали удачность подобранных параметров сети и успешность сверточных нейронных сетей для диагностики кожных новообразований на основе их изображений.

Так, выбор сверточной архитектуры нейронных сетей обеспечил системе следующие преимущества:

1) гораздо меньшее число настраиваемых весов, по сравнению с полносвязными сетями, связанное с использованием ядра свертки для всего изображения, благодаря чему не нужно для анализа разных фрагментов изображения отводить свои собственные веса;

2) возможность удобного распараллеливания вычислений, а значит, и перенос нагрузки при обучении сети на графический процессор;

3) возможность обучения сети обычным методом обратного распространения ошибки, по аналогии с другими сетями;

4) относительная устойчивость алгоритма к сдвигу и повороту распознаваемого изображения.

Актуальность данной работы состоит в том, что она демонстрирует возможности обучения сети даже на изображениях с разным качеством, на которых объект представляет собой сложный визуальный образ и может плохо выделяться на фоне окружения.

Разработанная модель нейронной сети может использоваться в качестве основы для создания встроенных систем, WEB- и мобильных приложений, которые, в свою очередь, могут быть применены для оказания первичной медицинской помощи, в том числе и доврачебной. Также она может применяться медицинскими работниками как вспомогательное средство в принятии решений во время диагностики кожных заболеваний по фотографиям.

Для дальнейшего совершенствования нейронной сети и повышения точности ее работы необходимо увеличить объем обучающей и валидационной выборок, так как несбалансированный датасет, а также отсутствие достаточного количества примеров определенных видов меланом может привести к ошибкам в распознавании моделью кожных заболеваний в реальных условиях.

Список источников

1. Соробин, А. Б. Сверточные нейронные сети: примеры реализаций / А. Б. Соробин. – Москва : РТУ МИРЭА, 2020. – 159 с.

2. Ганцев, Ш. Х. Онкология : учебник / Ш. Х. Ганцев. – Москва : Гэотар-Медиа, 2023. – 704 с.

3. Ростовцев, В. С. Искусственные нейронные сети : учебник для вузов / В. С. Ростовцев. – Санкт-Петербург : Лань, 2021. – 216 с.

4. Resnet. – URL: https://neurohive.io/ru/vidy-nejrosetej/resnet-34-50-101/ (дата обращения: 03.09.2024).

5. Рашка, С. Python и машинное обучение / С. Рашка, В. Мирджалили. – Санкт-Петербург : Диалектика, 2021. – 848 с.

6. Ферлитш, Э. Шаблоны и практика глубокого обучения / Э. Ферлитш. – Москва : ДМК Пресс, 2022. – 538 с.

7. ImageNet. – URL: https://www.image-net.org/ (дата обращения: 04.09.2024).

8. Данилов, В. В. Нейронные сети : учебное пособие / В. В. Данилов. Донецк : ДонНУ, 2020. – 158 с.

9. Баланов, А. Н. Машинное обучение и искусственный интеллект : учебник для вузов / А. Н. Баланов. – Санкт-Петербург : Лань, 2024. – 172 с.

10. ISIC. – URL: https://www.isic-archive.com/ (дата обращения: 04.09.2024).

11. Сапрыкин, О. Н. Интеллектуальный анализ данных : учебное пособие / О. Н. Сапрыкин. – Самара : Самарский университет, 2020. – 80 с.

12. Колмогорова, С. С. Обработка данных алгоритмами искусственного интеллекта в системе интернета вещей / С. С. Колмогорова. – Санкт-Петербург : Лань, 2023. – 104 с.

13. Пальмов, С. В. Системы и методы искусственного интеллекта : учебное пособие / С. В. Пальмов. – Самара : ПГУТИ, 2020. – 191 с.

14. Tharwat A. Classification assessment methods // Applied Computing and Informatics. – 2021. – Vol. 17, № 1. – P. 168–192.

15. Метрики в машинном обучении. – URL: https://neptune.ai/blog/performance-metrics-in-machine-learning-complete-guide (дата обращения: 06.09.2024).

16. Бинарная классификация. – URL: https://www.learndatasci.com/glossary/binary-classification/ (дата обращения: 05.09.2024).

References

1. Sorobin, A. B. *Convolutional Neural Networks: Examples of Implementations.* Moscow, RTU MIREA, 2020. 159 p. (In Russ.).

2. Gantsev, Sh. H. *Oncology : textbook.* Moscow, Geotar-Media Publ., 2023. 704 p. (In Russ.).

3. Rostovtsev, V. *Artificial Neural Networks : textbook for universities.* Saint Petersburg, Lan Publ., 2021. 216 p. (In Russ.).

4. *Resnet.* Available at: https://neurohive.io/ru/vidy-nejrosetej/resnet-34-50-101/ (accessed 03.09.2024) (In Russ.).

5. Rashka, S. *Python and Machine Learning.* Saint Petersburg, Dialektika Publ., 2021. 848 p. (In Russ.).

6. Ferlitsh, E. *Deep Learning Patterns and Practices.* Moscow, DMK Press, 2022. 538 p. (In Russ.).

7. *ImageNet.* Available at: https://www.image-net.org/ (accessed 04.09.2024).

8. Danilov, V. V. *Neural networks : a textbook.* Donetsk, DonNU, 2020. 158 p. (In Russ.).
9. Balanov, A. N. *Machine learning and artificial intelligence : textbook for universities.* Saint Petersburg, Lan, Publ., 2024. 172 p. (In Russ.).
10. *ISIC.* Available at: https://www.isic-archive.com/ (accessed 04.09.2024).
11. Saprykin, O. N. *Data Mining : a textbook.* Samara, Samara University, 2020. 80 p. (In Russ.).
12. Kolmogorova, S. S. *Data processing by artificial intelligence algorithms in the Internet of Things system.* Saint Petersburg, Lan Publ., 2023. 104 p. (In Russ.).
13. Palmov, S. V. *Artificial Intelligence systems and methods : a textbook.* Samara, PGUTI, 2020. 191 p. (In Russ.).
14. Tharwat, A. Classification assessment methods. *Applied Computing and Informatics*, 2021, vol. 17, no. 1, pp. 168–192.
15. *Metrics in Machine Learning.* Available at: https://neptune.ai/blog/performance-metrics-in-machine-learning-complete-guide (accessed 05.09.2024) (In Russ.).
16. *Binary Classification.* Available at: https://www.learndatasci.com/glossary/binary-classification/ (accessed 05.09.2024) (In Russ.).

Статья поступила в редакцию 26.09.2024; одобрена после рецензирования 05.11.2024; принята к публикации 05.11.2024.
The article was submitted 26.09.2024; approved after reviewing 05.11.2024; accepted for publication 05.11.2024.

УДК 004.089

КОНЦЕПЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ЧАСТНОГО ИНВЕСТОРА ПРИ ФОРМИРОВАНИИ ПОРТФЕЛЯ ЦЕННЫХ БУМАГ

Кондратьева Ольга Владимировна, Уфимский университет науки и технологий, 450005, Российская Федерация, г. Уфа, ул. Карла Маркса, 12,

старший преподаватель, ORCID: 0000-0003-1448-3747, e-mail: kondr_o@mail.ru

Сметанина Ольга Николаевна, Уфимский университет науки и технологий, 450005, Российская Федерация, г. Уфа, ул. Карла Маркса, 12,

доктор технических наук, доцент, профессор кафедры вычислительной математики и кибернетики, ORCID: 0000-0001-6970-1110, e-mail: smoljushka@mail.ru

В статье рассматривается концепция интеллектуальной информационной поддержки принятия решений в процессе формировании портфеля ценных бумаг на основе современных научных разработок инструментов оценки риска, алгоритмов искусственного интеллекта и методов машинного обучения. Сформулированы последовательность решаемых задач и подходы к их решению, стратегии оценки риска портфеля ценных бумаг, используемые методы и принципы, а также условия применимости разработанной концепции. Разработана методика оценки эффективности алгоритма интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг, согласно которой проведен вычислительный эксперимент на основе исторических данных котировок ценных бумаг. Результаты вычислений показали, что в 84–97 % случаев применяемая стратегия оценки риска показала доходность выше, чем традиционные инструменты. Динамика доходности оптимальных портфелей, сформированных на основе предложенной в статье концепции, при сравнении на «будущем» периоде с бенчмарком продемонстрировала лучший результат, независимо от тренда (растущего, бокового, падающего). Таким образом, применение интеллектуальной информационной поддержки позволяет повысить эффективность принимаемых инвестором решений и получить рекордную доходность от вложений.

Ключевые слова: интеллектуальная поддержка принятия решений, адаптация моделей оценки риска, система управления, прецедентный подход, рынок ценных бумаг, инвестор

THE INTELLECTUAL INFORMATION SUPPORT CONCEPT FOR DECISION-MAKING IN THE SECURITIES PORTFOLIO FORMATION BY A PRIVATE INVESTOR

Kondrateva Olga V., Ufa University of Science and Technology, 12 Karl Marx St., Ufa, 450005, Russian Federation,

Senior Lecturer, ORCID: 0000-0003-1448-3747, e-mail: kondr_o@mail.ru

Smetanina Olga N., Ufa University of Science and Technology, 12 Karl Marx St., Ufa, 450005, Russian Federation,

Doct. Sci. (Engineering), Associate Professor, Professor of the Computational Mathematics and Cybernetics Department, ORCID: 0000-0001-6970-1110, e-mail: smoljushka@mail.ru

The article considers the intelligent information support concept for decision-making in the securities portfolio forming process based on modern scientific developments in risk assessment tools, artificial intelligence algorithms and machine learning methods. The sequence of tasks to be solved and approaches to their solution, strategies for assessing the risk of a securities portfolio, the methods and principles used, as well as the conditions for the applicability of the developed concept are formulated. A methodology for assessing the effectiveness of the algorithm for intelligent decision-making support in a securities portfolio forming has been developed, according to which a computational experiment was conducted based on historical data of securities quotations. The calculation results showed that in 84–97 % of cases, the applied risk assessment strategy showed a higher return than traditional instruments. The dynamics of the return on optimal portfolios formed on the basis of the concept proposed in the article, when compared in the "future" period with the benchmark, demonstrated the best result, regardless of the trend. Thus, the use of intelligent information support allows you to increase the effectiveness of decisions made by an investor and get a record return on investment.

Keywords: intellectual decision-making support, risk assessment model adaptation, management system, precedent approach, securities market, investor

ВВЕДЕНИЕ

В связи с развитием финансовых технологий цифровизация и применение искусственного интеллекта получают все большее распространение на фондовом рынке. Для оптимизации инвестиционной деятельности применяются механические торговые системы, автоматические системы, торговые роботы, роботы-советники и др. Удаленное открытие брокерских счетов и идентификация, создание мобильных приложений для заключения сделок на фондовой бирже, низкий денежный порог

для вложений минимизировали путь вхождения на рынок для огромного количества частных инвесторов. Количество физлиц, имеющих брокерские счета на Московской бирже, за 2023 г. увеличилось до 29,7 млн человек [1], а к концу августа 2024 г. – до 33,3 млн человек [2]. В общем объеме торгов акциями на долю частных инвесторов приходится более 80 % сделок. Это характеризует современный тренд поведения частных инвесторов, которые становятся важными игроками на фондовом рынке.

Нестабильная геополитическая ситуация, высокая волантильность рынка, разнообразие новых производных финансовых инструментов ведут к росту неопределенности и сложности в принятии решений неквалифицированным инвестором. При формировании портфеля ценных бумаг необходима информационная поддержка индивидуальных инвесторов для снижения рисков неверных инвестиционных решений, в том числе панического поведения на фондовом рынке, что может повлечь деструктуризацию портфеля и финансовые потери.

На текущий момент активное, динамичное развитие российского финтеха подтверждает рост объемов этого сектора в I полугодии 2024 г. на 14,6 %, в итоге они составили 115,5 млрд рублей [3]. Однако рекомендательный сектор является зоной для роста – персонализация, проактивность в решении проблем, финансовые советы, которые бы учитывали потребности и особенности конкретного человека, только начинают внедряться. В IT-области фондового рынка доминируют решения для алгоритмической торговли, направленные на деятельность трейдеров, а частного инвестора интересуют консервативные цели и долгосрочные вложения.

Существующие рекомендательные системы типа робо-эдвайзеров являются IT-продуктами финансовых институтов (банков, инвесткомпаний и т. д.), например, «Финансовый автопилот» (УК «Финэкс Плюс»), «Персональный финансовый помощник» (УК «Альфа-Капитал»), «Робот-Советник» (ПАО «Банк ВТБ»), «ИИ-советник» (АО «Финам»), «Conomy Terminal» (ООО «М3») [4–8]. Следует отметить, что в интересах данных компаний продвинуть приоритетные услуги и активы, а не обеспечить частному инвестору индивидуальный подход, исходя из его целей и особенностей отношения к риску, т. е. возможен конфликт интересов. Также существенным недостатком робо-эдвайзеров на российском рынке является то, что их алгоритмы, модели для оценки риска основаны на классической теории управления портфелем (Modern Portfolio Theory, MPT), которая предполагает выполнение требования об эффективности рынка, но современный фондовый рынок не соответствует данному условию, что существенно снижает качество работы, прогнозов и рекомендаций этих сервисов.

Поэтому возникла необходимость для создания интеллектуальной информационной поддержки принятия решений при формировании портфеля ценных бумаг, которая бы опиралась на современные модели оценки риска, а не классическую MPT, учитывала бы эмпирическое распределение доходностей ценных бумаг на фондовом рынке, а не базировалась бы на допущении о нормальности распределения. Применение искусственного интеллекта (ИИ) позволяет повысить скорость решения поставленной задачи, более оперативно спрогнозировать показатели, чем традиционные математические методы, и предложить рекомендации по структуре оптимального портфеля, учитывающего когнитивные особенности, финансовые цели инвестора и текущую ситуацию на бирже. Скорость принятия решений является приоритетной метрикой для участников финансового рынка, так как влияет на конечную цель – получение прибыли от инвестиционных вложений. А также алгоритмы ИИ при выполнении поставленной задачи, в отличие от человека, не поддаются эмоциям и переживаниям, которые свойственны любому человеку особенно в периоды сильной волантильности рынка, т. е. возможности таких технологий защищают от искушения поддаться панике и неоправданному риску. По прогнозам Garther [9], к 2025 г. ожидается, что интуиция и личный опыт человека будут играть все меньшую роль при принятии инвестиционных решений.

Целью данного исследования является разработка и оценка эффективности концепции интеллектуальной информационной поддержки принятия решений при формировании портфеля ценных бумаг, которая будет рекомендовать долевую структуру оптимального портфеля инвестору, исходя из его риск-профиля и целей. Концепция должна опираться на современные научные разработки инструментов оценки риска, алгоритмы искусственного интеллекта и методы машинного обучения.

РАЗРАБОТКА КОНЦЕПЦИИ ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ (ИППР)

Концепция интеллектуальной поддержки принятия инвестиционного решения строится вокруг главной цели инвестора – поиска оптимальной, с точки зрения доходности, структуры ПЦБ. Для этого последовательно решаются следующие задачи:

1) разработка комбинированных индексно-энтропийных моделей оценки риска, учитывающих недостатки традиционных мер;

2) разработка модифицированного алгоритма роя частиц для поиска оптимального портфеля ПЦБ на основе двухкритериальной оптимизации;

3) разработка алгоритма интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг;

4) оценка эффективности применения разработанного алгоритма интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг с точки зрения доходности в сравнении с бенчмарком.

В ходе решения поставленных задач применяются системный, прецедентный, динамический подходы, а также трехуровневое управление процессом формирования портфеля ценных бумаг, основанное на инженерии знаний и принципах обратной связи и адаптации моделей оценки риска. Концепция интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг проиллюстрирована в виде ментальной карты на рисунке 1.

Системный подход заключается в том, что процесс формирования портфеля ценных бумаг рассматривается как часть организационной системы (фондового рынка), компоненты которой взаимосвязаны и чувствительны к изменениям всех участников. Задача формирования оптимального портфеля ценных бумаг рассматривается не изолированно, а в единстве связей с динамикой котировок ценных бумаг на фондовом рынке, с предпочтениями инвестора, с общей (инвестиционный портфель с рекордной будущей доходностью) и частной (поиск оптимального набора векторных параметров моделей) целями.

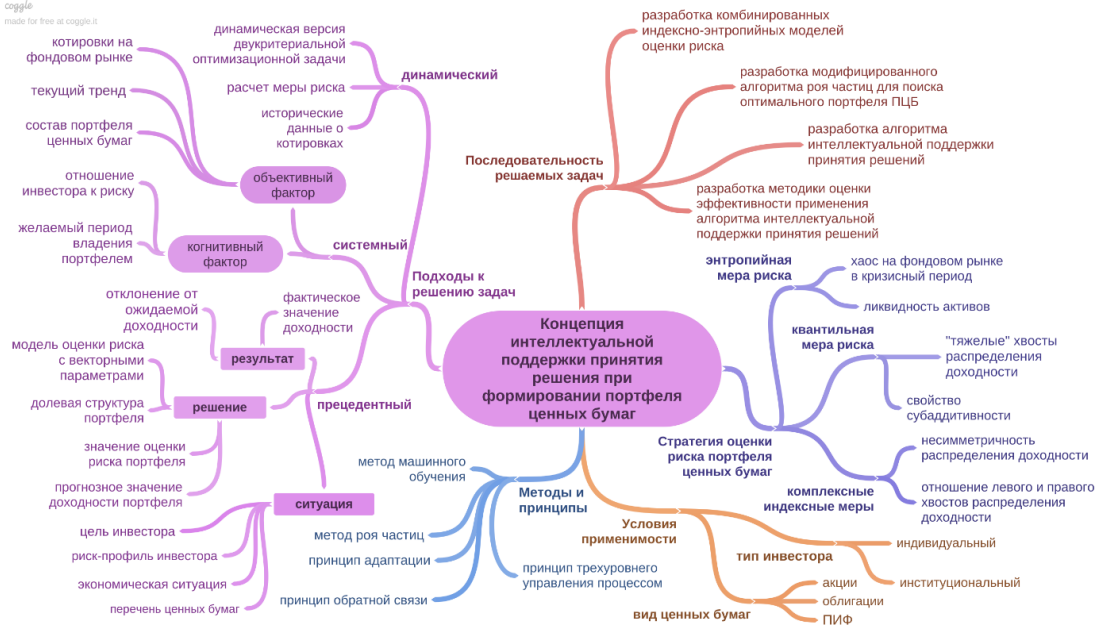


Рисунок 1 – Ментальная карта концепции интеллектуальной поддержки принятия решений инвестора

При определении перечня и долевой структуры тикеров в портфеле учитывается:

а) характер цели вложений (краткосрочный, среднесрочный, долгосрочный) и риск-профиль инвестора (консервативный, агрессивный);

б) текущий тренд экономической ситуации на финансовом рынке;

в) прогнозные показатели ожидаемого риска и ожидаемой доходности портфеля ценных бумаг;

г) метрика финансовой результативности модели, используемой для оценки риска, вычисляемая на основе реальных финансовых доходностей сформированного портфеля ценных бумаг.

Исходя из отношения инвестора к риску, используется соответствующий приоритетной цели (снизить риск или повысить доходность) подход для поиска оптимального портфеля – минимаксный или максиминный, и таким образом формируется агрессивный или консервативный ПЦБ. Так как все расчеты делаются на основе исторических данных о котировках ценных бумаг, то динамика цен финансовых инструментов напрямую влияет на получаемые результаты. Кроме того, вычислительные эксперименты показали зависимость между характером экономической ситуации (рост, кризис) и моделью с ее векторными параметрами, благодаря которой удается сформировать оптимальный ПЦБ.

Прогноз ожидаемой доходности портфеля является критерием для ранжирования и выбора эффективного для вложений портфеля. Рассчитывается ожидаемая и реальная доходность сформированного портфеля ценных бумаг, учитывая срок инвестирования, который, в свою очередь, напрямую зависит от целей инвестора. Учет реальной доходности ПЦБ позволяет оценить эффективность настройки векторных параметров модели – данная метрика используется для информационной поддержки инвестора при принятии решения о выборе модели оценки финансового риска. Таким образом, системный подход позволяет рассматривать процесс формирования инвестиционного

портфеля с учетом когнитивных особенностей инвестора, реальных финансовых результатов от инвестиций и текущего тренда на фондовом рынке.

При формировании портфеля ценных бумаг для измерения риска используется откалиброванная модель, которая выбирается из семейства мер риска, исходя из рассматриваемой ситуации и полученного в прошлом результата, т. е. применяется *прецедентный подход* при интеллектуальной поддержке принятия решений инвестором. Ситуация характеризуется подходом к поиску оптимального портфеля, который, в свою очередь, зависит от отношения инвестора к риску, текущим трендом динамики цен на фондовом рынке, составом и предполагаемым сроком владения ПЦБ. Решением является вектор, в который входит:

– мера риска, которая в прошлом в ситуации с идентичными характеристиками позволила сформировать портфель с позитивным финансовым исходом;
– процентная структура оптимального портфеля;
– ожидаемый риск сформированного оптимального портфеля;
– ожидаемая доходность сформированного оптимального портфеля.

Результатом применения решения является финансовый результат произведенных инвестиций – фактическая доходность ПЦБ и отклонение ее от ожидаемой доходности. Прецедентный подход позволит использовать накопленный опыт от применения мер риска другими инвесторами в прошлом и сократить время на калибровку модели оценки финансового риска благодаря имеющейся базе моделей и, в случае подобной ситуации, базе прецедентов.

Динамический подход применен в решении задач 3 и 4 из списка выше. В рамках интеллектуальной поддержки принятия решений инвестором в части прогнозирования эффективного множества портфелей ценных бумаг используется машинное обучение. Объектами выборки являются все возможные долевые структуры потенциальных портфелей: рассчитанные значения меры риска этих портфелей представляют собой характеристический признак объекта, а будущие доходности потенциальных портфелей определяют целевой признак объекта. Обучающая и валидационная выборки смещаются с определенным временным лагом, и процесс обучения построен на данных по нескольким рассматриваемым периодам, т. е. признаки (характеристический и целевой) портфеля исследуются в динамике. В результате обучения на сходных примерах для потенциальных портфелей формируются пары «значение меры риска, значение доходности» и определяется эффективное множество ПЦБ, которое используется далее для формирования оптимального портфеля. При оценке эффективности применения алгоритма интеллектуальной поддержки принятия решений используется годовая динамика доходности сформированного оптимального ПЦБ и доходности индекса Мосбиржи (бенчмарка) в целях объективного сравнения вариантов на длительном горизонте.

Обученные модели сохраняются в базе знаний и извлекаются согласно продукционным правилам для использования при принятии инвестором решения об инструменте измерения риска портфеля ценных бумаг. В результате оценки ожидаемой доходности и ожидаемого риска потенциального портфеля формируются знания о долевой структуре оптимального ПЦБ, которые фиксируются в базе прецедентов. Далее накопленные прецеденты анализируются на предмет эффективности результатов их применения. Для этого применяется *принцип обратной связи*, когда спустя временной интервал, соответствующий периоду владения ПЦБ, исследуются реальные данные о цене оптимального портфеля согласно фактическим котировкам на фондовом рынке и рассчитывается отклонение доходности. Положительное или отрицательное отклонение между ожидаемой и фактической доходностями оптимального ПЦБ является показателем эффективности применения модели в данных условиях (при соответствующей ситуации на фондовом рынке, при выбранном, исходя из риск-профиля инвестора, подходе к поиску оптимального ПЦБ, при заявленном сроке владения). Знания об эффективности меры риска являются триггером для использования *принципа адаптации модели оценки риска*, который заключается в том, что векторные параметры мер риска могут быть динамически скорректированы на основе информации о дате сделки, предпочтениях инвестора, текущих ценах финансовых инструментов с целью достижения оптимального результата с точки зрения доходности и риска в условиях неопределенности волантильного рынка. В рамках процедуры адаптации происходит не только обновление векторных параметров модели, но и рассматриваются другие меры из семейства мер риска, что расширяет область поиска и возможность настроить модель на отыскание такой долевой структуры портфеля, которая гарантирует позитивный исход инвестиционных вложений.

В качестве инструмента оценки риска портфеля предлагается использовать комбинированные индексно-энтропийные меры риска (1–4):

$$(Entropy - CVaR)_r = \lambda\rho_\gamma(X) - (1-\lambda)CVaR_\alpha(X), \quad (1)$$

$$(Entropy - CIRM_1)_r = \lambda\rho_\gamma(X) + (1-\lambda)\left(\frac{1 - VaR_\alpha^-(X)}{VaR_\alpha^+(X)} - \frac{\mathrm{E}\left[\left(X - \mathrm{E}(X)\right)^3\right]}{\sigma(X)^3}\right), \quad (2)$$

$$(E-CIRM_2)_{r_1} = \lambda\rho_\gamma(X) + (1-\lambda)\left(\frac{1-CVaR_\alpha^-(X)}{CVaR_\alpha^+(X)} + \beta\cdot\frac{Mo}{CVaR_\alpha^+(X)} - (1-\beta)\cdot\frac{\mathrm{E}\left[\left(X-\mathrm{E}(X)\right)^3\right]}{\sigma(X)^3}\right), \quad (3)$$

$$(E-CIRM_3)_{r_1} = \lambda\rho_\gamma(X) + (1-\lambda)\left(\frac{1-CVaR_\alpha^-(X)}{CVaR_\alpha^+(X)} + \beta\cdot\frac{Me}{CVaR_\alpha^+(X)} - (1-\beta)\cdot\frac{\mathrm{E}\left[\left(X-\mathrm{E}(X)\right)^3\right]}{\sigma(X)^3}\right). \quad (4)$$

Разработанные *модели* позволяют учесть волантильность котировок ценных бумаг, хаотичность ситуации на фондовом рынке и ликвидность активов благодаря использованию энропийной меры в составе комбинированной, а применение модифицированных квантильных мер и коэффициента асимметрии – несимметричность распределения доходностей («тяжелые» хвосты, характер скоса). Таким образом, комбинированные индексно-энтропийные меры риска устранят слабые стороны современных портфельных стратегий [10].

Целевые функции оценки риска являются одним из критериев в задаче поиска оптимального портфеля. Вторым критерием является доходность, т. е. необходимо решать двухэтапную оптимизационную задачу, что накладывает свои *ограничения* на выбор и применение численного метода оптимизации. *Метод роя частиц* выбран на основании соответствия требованиям поставленной задачи [11] и следующих преимуществ:

– возможность учесть требование диверсификации портфеля за меньшее число вычислений целевой функции;

– понятность и простота программной реализации алгоритма;

– большая надежность в поиске глобального оптимума;

– возможность применения многороевого варианта алгоритма для семейства комбинированных индексно-энтропийных мер риска;

– особенность метода роя частиц в отыскании лучшего решения частицы и лучшего решения всего роя, позволяющая модифицировать алгоритм для решения поставленной двухкритериальной оптимизационной задачи и использовать две целевые функции.

Разработанный алгоритм интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг может быть использован как индивидуальным, так и институциональным инвестором для любых основных финансовых инструментов на фондовом рынке (акции, облигации, ПИФ).

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ КОНЦЕПЦИИ ИППР

Анализ эффективности разработанного алгоритма интеллектуальной поддержки принятия решений подразумевает сравнение экономического эффекта от вложений в сформированный на основании предложенной концепции портфель ценных бумаг с доходностью портфеля-бенчмарка. Так как рассматриваемая концепция предполагает решение последовательности задач, то уместно оценить эффективность каждого ключевого объекта, от которого зависит финальный результат.

Методика оценки экономической эффективности применения интеллектуальной поддержки принятия решений инвестора при формировании портфеля ценных бумаг представляет собой реализацию следующих этапов:

1) выявление ключевых объектов для анализа эффективности;
2) определение инструментов оценки эффективности в зависимости от критериев оптимальности и вида объекта;
3) установление эталона для сравнения по каждому виду объекта;
4) формирование порядка проведения оценки эффективности;
5) непосредственный расчет показателей;
6) анализ полученных результатов.

Так как главная цель инвестора – сделать денежные вложения в такой портфель ценных бумаг (ПЦБ), который принесет наивысшую доходность, то главным объектом оценки эффективности является оптимальный, с точки зрения доходности, ПЦБ, который формируется с применением описанной концепции интеллектуальной поддержки принятия решений. Вторым критерием при решении задачи поиска оптимальной структуры ПЦБ является риск, поэтому следующим ключевым объектом

для исследования эффективности выступает семейство мер риска, которое является инструментом для выявления эффективного множества портфелей из всего множества потенциальных ПЦБ. Третьим объектом анализа эффективности является модель оценки риска с векторными параметрами, результативность которой влияет на поддержание актуального состояния базы моделей.

Показатели для анализа эффективности выбираются исходя из критериев оптимальности (доходность и риск). Рассчитанное значение доходности, используемое в данной работе, относится к числу относительных показателей. Оно определяется как отношение цены ПЦБ в конечной точке периода владения к цене портфеля в начальный момент совершения денежных вложений. Риск оценивается в двух разрезах – как абсолютная величина (непосредственное значение меры риска из семейства) и относительная (индекс Херфиндаля – Хиршмана показывает степень диверсифицируемости портфеля, которая обратно пропорциональна риску ПЦБ). Качество модели оценки риска определяется с помощью модифицированной метрики $Precision^*$, которая используется в задачах классификации. В отличие от традиционной метрики, которая рассматривает позитивные и негативные прогнозы, в данной задаче негативные прогнозы не рассматриваются, так как убытки не соответствуют целям инвестора, а позитивные прогнозы сравниваются с фактическими результатами. В связи с этим все кейсы, принадлежащие одной модели, делятся на два класса – положительных (R_p) и отрицательных (R_n) результатов в зависимости от знака отклонения фактической (R) и прогнозной (R_{min}) доходностей оптимального ПЦБ (5). Обработка результатов прецедентов производится с использованием дополнительного параметра – минимально приемлемой доходности (*Minimum Acceptable Return, MAR*), которая совпадает с прогнозной доходностью (R_{min}) ПЦБ.

$$R - R_{min} = \begin{cases} R_p, \text{ если } R - R_{min} \geq 0 \\ R_n, \text{ если } R - R_{min} \leq 0 \end{cases}. \quad (5)$$

При этих условиях модифицированная метрика $Precision^*$ (6) означает долю позитивных кейсов в общем числе портфелей, сформированных на основе рассматриваемой модели оценки риска.

$$Precision^* = \frac{R_p}{(R_p + R_n)(L_{max} + 1 - R_p - R_n)} \cdot 100. \quad (6)$$

Модификация метрики необходима для нормализации масштаба получаемой оценки эффективности, так как размерности выборок разнородны и относительное количество положительных исходов не полно отражает качество работы модели. Корректировка оценки с опорой на соотношение с максимальным размером выборки (L_{max}) повышает адекватность интерпретации полученных результатов для дальнейшего использования при интеллектуальной информационной поддержки при принятии решений инвестором.

Для анализа финансовых результатов сформированного оптимального ПЦБ необходимо сравнение с альтернативным вложением инвестиций. В качестве альтернативы принимается индекс Московской биржи (MOEX10), который включает в себя акции крупнейших российских компаний из разных отраслей экономики и отражает общее экономическое состояние рынка, т. е. структура портфеля-бенчмарка повторяет состав индекса MOEX10.

Для подтверждения эффективности и целесообразности разработки семейства комбинированных мер риска в качестве эталонов используются альтернативные традиционные инструменты оценки риска, а именно *VaR*, *CVaR*, и меры, входящие в комбинированные, без модификаций. Доходности портфелей, сформированных на основе оценки риска с помощью разработанных мер и с помощью традиционных инструментов, показывают, какие меры использовать выгоднее.

Эффективность откалиброванной математической модели иллюстрирует финальный результат – отклонение фактического значения доходности оптимального ПЦБ по истечению срока владения от ожидаемой доходности. За позитивный исход принимается отклонение больше или равное нулю, за негативный – меньше нуля. То есть в данном случае в качестве эталона рассматривается значение прогнозной доходности оптимального ПЦБ, по умолчанию оно не может быть меньше единицы, то есть убыточные портфели не рассматриваются как потенциальные к инвестированию.

Экономический эффект от применения интеллектуальной поддержки принятия решений инвестора при формировании ПЦБ можно рассматривать в двух аспектах: прямой – с точки зрения инвестора (прибыль от денежных вложений) и косвенный – с точки зрения компании-эмитента, входящего в ПЦБ (повышение ликвидности ценных бумаг). Также следует отметить получаемый социальный эффект (как результат экономического), который выражается в повышении уровня доходов инвестора (прямое следствие), и в конечном итоге потенциально это приведет к повышению качества жизни и благосостоянию населения в целом (косвенный эффект). Итак, количественная оценка используется для анализа экономического эффекта, а качественная оценка – для исследования социального эффекта от применения интеллектуальной поддержки в процессе принятия решений инвестором о вложениях в оптимальный портфель ценных бумаг.

РЕЗУЛЬТАТЫ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА И ИХ ОБСУЖДЕНИЕ

Для оценки эффективности использования разработанной концепции интеллектуальной поддержки принятия решений были проведены вычислительные эксперименты на основе исторических данных о котировках ценных бумаг: в портфель вошли акции ООО «Яндекс» (YNDX), ПАО «Магнит» (MGNT), ПАО «Сбербанк» (SBER), ПАО «Лукойл» (LKOH), ПАО «ВТБ» (VTBR). Для исследования эффективности семейства комбинированных индексно-энтропийных мер риска проведено сравнение альтернативных оптимальных портфелей, построенных с помощью *CVaR, Entropic, E-CVaR,* M_1, *E-CIRM*$_1$, M_2, *E-CIRM*$_2$, M_3, *E-CIRM*$_3$ (портфели P_{CVaR}, $P_{Entropic}$, $P_{E\text{-}CVaR}$, P_{M1}, P_1, P_{M2}, P_2, P_{M3}, P_3 соответственно). Оценка доходности произведена на интервале с 04.01.2023 г. по 30.08.2024 г., который включал в себя все три вида тренда согласно динамике бенчмарка (рис. 4). Ежедневные доходности портфелей сравнивались тройками, в каждой из которых присутствовали комбинированная индексно-энтропийная мера, энтропийная и индексная меры, например, *E-CIRM*$_1$, *Entropic* и M_1. Расчеты показали, что в рамках 416 наблюдений за 2023–2024 гг. портфели, сформированные на основании комбинированных мер, показали большую доходность, чем альтернативные портфели (рис. 2), в 86,78 % случаев – мера *E-CvaR*, в 84,86 % случаев – мера *E-CIRM*$_1$, в 97,12 % случаев – мера *E-CIRM*$_3$.

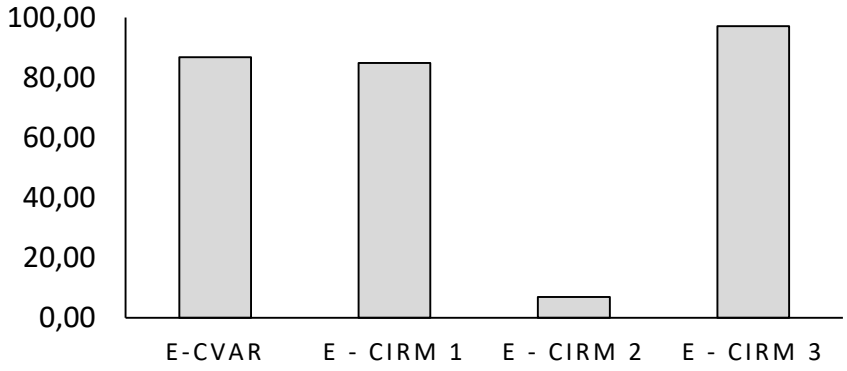


Рисунок 2 – Доля оптимальных портфелей, сформированных с использованием комбинированных индексно-энтропийных мер риска

Гистограмма демонстрирует то, что использование разработанного в рамках концепции семейства комбинированных мер риска более эффективно, чем традиционные инструменты оценки риска. Мера *E-CIRM*$_2$ на рассматриваемом датасете при сравнении с мерой M_2 только в 7-ми % случаев показала эффективность, поэтому портфель P_2, полученный на основании этой меры, далее был исключен из рассмотрения при выборе эффективного множества ПЦБ (рис. 3).

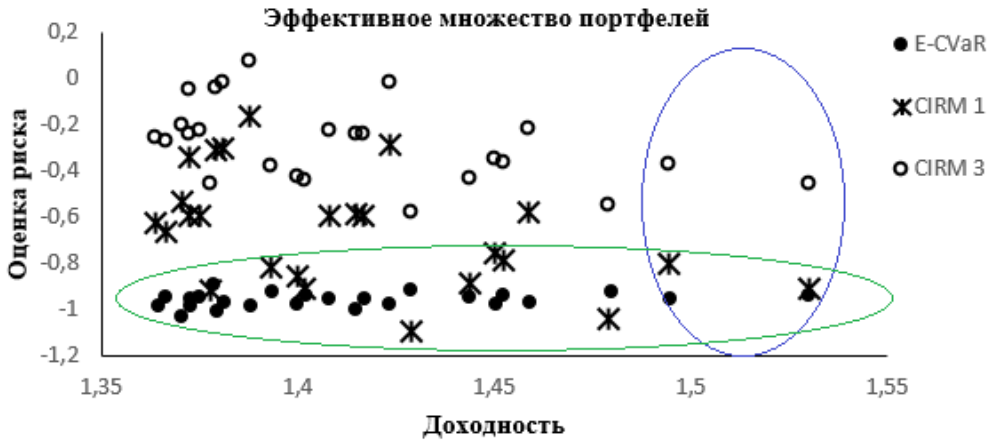


Рисунок 3 – Эффективное множество портфелей

В результате обучения было определено множество эффективных портфелей, каждому из которых соответствует характеризующий признак (долевая структура и значение меры риска портфеля) и результативный признак (прогнозная доходность). Диаграмма рассеяния (рис. 3) показывает, что портфели с наивысшей доходностью сосредоточены в правой области внутри синего контура, портфели наименее рискованные расположены в нижней области внутри зеленого контура, а оптимальные портфели располагаются на пересечении выделенных областей.

Далее анализировалась эффективность оптимальных портфелей на контрольной выборке с 04.01.2023 г. по 30.08.2024 г. Эффективность оптимальных портфелей $P_{E\text{-}CVaR}$, P_1, P_3 определяется путем сравнения динамики доходностей с динамикой индекса Московской биржи. Согласно кривой бенчмарка (рис. 4), с января по сентябрь 2023 г. наблюдается восходящий тренд, с сентября 2023 г. по май 2024 г. – боковой тренд, с июня по август 2024 г. – «падение» рынка.

Исследования показали, что на всех трех периодах портфели, сформированные на основе представленной в статье концепции, имеют доходность выше бенчмарка. Портфели $P_{E\text{-}CVaR}$ и P_1 в период экономического роста более привлекательны, при боковом тренде все три портфеля дают практически одинаковую доходность, а в кризисный период портфель P_3 показал меньшую волантильность, чем два других портфеля. То есть коррекция произошла у всех трех портфелей, но у портфеля P_3 она менее шоковая, что говорит о надежности и меньшем риске.

Рисунок 4 – Динамика доходности оптимальных портфелей $P_{E\text{-}CVaR}$, P_1, P_3 и бенчмарка

Так как параметры алгоритма обучения моделей оценки риска зависят от ситуации, а именно: риск-профиль инвестора влияет на выбор максиминного или минимаксного подхода, срок вложения определяет длину валидационной выборки, текущий тренд обусловливает характер обучающего датасета, то все прецеденты можно разделить на 18 классов, учитывая все возможные комбинации троек «тренд – срок – профиль». Для обучения моделей для каждого вида искусственно создается большое количество прецедентов в разные моменты времени, используя исторические данные о ценах активов на бирже. Обученные модели являются частью решения прецедента, а результат этого решения определяется на основании фактической доходности оптимального портфеля в будущем согласно сроку инвестиционных вложений.

Значения доходностей оптимальных портфелей на контрольной выборке являются фактическими (R), а на валидационной выборке – прогнозными (R_{min}). С помощью модифицированной метрики $Precision^*$ оценивается качество работы моделей оценки риска и производится ранжирование мер риска для большей прозрачности информационной поддержки инвестора при принятии решения. В таблице представлены обученные модели оценки риска для одного типа ситуации (прецедента), которая характеризуется растущим трендом, консервативным риск-профилем и долгосрочными вложениями.

Таблица – Оценка качества работы моделей одного класса прецедентов

Модель оценки риска	$\bar{R}_{min}$	**Положительные кейсы**	$Precision^*$
$(Entropy - CIRM_1)_{r_6}$	1,4	88 % из 112	2,378
$(Entropy - CVaR)_{r_{12}}$	1,45	95 % из 46	0,922
$(Entropy - CIRM_3)_{r1_4}$	1,43	88 % из 53	0,916
$(Entropy - CIRM_2)_{r1_9}$	1,12	32 % из 20	0,248

По показателю прогнозной доходности и проценту положительных исходов преимущество у модели $(Entropy - CVaR)_{r_{12}}$, но размерность выборки положительных прецедентов с данным решением в 2,4 раза меньше, чем у выборки с альтернативным решением, что не позволяет принять метрику количества положительных кейсов (третий столбец в таблице) за истину, поэтому высчитывается модифицированная $Precision^*$. Данные таблицы отсортированы по показателю $Precision^*$ и демонстрируют,

что для текущего инвестора, исходя из его целей и особенностей, предпочтительнее использовать меру $(E - CIRM_1)_{r_6}$, хотя процент положительных исходов и прогнозная доходность больше у $(E - CVaR)_{r_{12}}$. $Precision^*$ позволила дифференцировать модели, которые показали одинаковый результат согласно доли положительных кейсов ($(Entropy - CIRM_1)_{r_6}$ и $(Entropy - CIRM_3)_{r1_4}$).

Аналогично консолидируется информация по всем прецедентам в разрезе классов, и фиксируется наилучшее значение метрики $Precision^*$, т. е. наиболее эффективная модель оценки риска, которую можно рекомендовать инвестору при формировании или ребалансировки ПЦБ. Столбиковая диаграмма отражает наилучшее значение $Precision^*$ для каждого класса прецедентов (рис. 5).

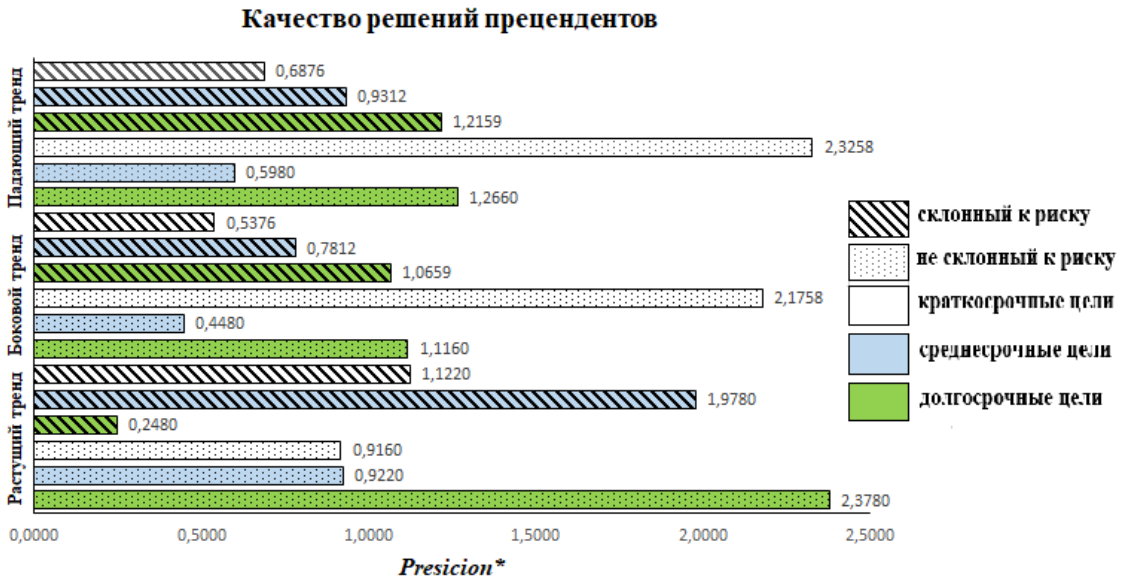


Рисунок 5 – Качество наилучшего решения соответствующего класса прецедентов

Рекордные значения метрики $Precision^*$ соответствуют прецедентам, характеризующимся консервативным (не склонным к риску) риск-профилем инвесторов. Для прецедентов, которым соответствует боковой или нисходящий тренд, более качественными оказались модели для краткосрочных инвестиционных вложений, а для прецедентов в условиях растущего тренда – для долгосрочных.

ЗАКЛЮЧЕНИЕ

Таким образом, интеллектуальная информационная поддержка на основе прецедентного подхода позволяет повысить эффективность принимаемых решений, использование уже обученных, согласно рассматриваемой ситуации, моделей оценки риска дает возможность ускорить процесс формирования диверсифицированного оптимального ПЦБ и улучшить качество управления рисками.

Эффективность подтверждена вычислительными расчетами, которые демонстрируют, что вложения в портфель, сформированный согласно разработанной концепции, более привлекательны, чем альтернативные вложения, так как доходность оптимального портфеля выше бенчмарка на 26 % на растущем рынке, на 55 % – в период бокового и падающего тренда. Экспериментальные исследования показали, что разработанная концепция содержит такие подходы, методы и модели, которые позволяют сформировать оптимальные ПЦБ и произвести значительную интеллектуальную информационную поддержку инвестора.

Список источников

1. Обзор ключевых показателей брокеров № 2 IV квартал 2023 года. Центральный банк Российской Федерации, 2024. – URL: https://cbr.ru/Collection/Collection/File/48976/review_broker_Q4_2023.pdf (дата обращения: 23.09.2024).

2. Пресс-релиз Московской биржи. – URL: https://www.moex.com/n72763?ysclid=m1xtkk2pt3119004924 (дата обращения: 23.09.2024).

3. Исследование аналитического агентства Smart Ranking. – URL: https://smartranking.ru/ru /analytics/FINTECH/fintech-rynok-vyros-na-15-po-itogam-i-polugodiya-2024/ (дата обращения: 23.09.2024).

4. Финансовый автопилот. – URL: https://finance-autopilot.ru/ (дата обращения: 23.09.2024).

5. Персональный финансовый помощник. – URL: https://robo.alfacapital.ru/profile (дата обращения: 23.09.2024).

6. Робот-советник. – URL: https://www.vtb.ru/personal/investicii/robot/ (дата обращения: 23.09.2024).

7. ИИ-советник. – URL: https://broker.finam.ru/landing/ii-sovetnik (дата обращения: 23.09.2024).

8. Conomy Terminal. – URL: https://terminal.conomy.ru/ (дата обращения: 23.09.2024).

9. Пресс-релиз исследовательской компании Gartner. – URL: https://www.gartner.com/en/newsroom/press-releases/2021-03-10-gartner-says-tech-investors-will-prioritize-data-science-and-artificial-intelligence-above-gut-feel-for-investment-decisions-by-20250 (дата обращения: 23.09.2024).

10. Bronshtein, E. M. Security Portfolio Management Based on Combined Entropic Risk Measures / E. M. Bronshtein, O. V. Kondrateva // Journal of Computer and Systems Sciences International. – 2013. – № 52 (5). – P. 837–841. https://doi.org/10.1134/S1064230713050043.

11. Кондратьева, О. В. Алгоритм интеллектуальной поддержки принятия решений при формировании портфеля ценных бумаг на основе роевого интеллекта / О. В. Кондратьева // Моделирование, оптимизация и информационные технологии. – 2021. – № 9 (2). – DOI: 10.26102/2310-6018/2021.33.2.029.

References

1. *Review of key indicators of brokers No. 2 IV quarter 2023. Central Bank of the Russian Federation*. 2024. URL: https://cbr.ru/Collection/Collection/File/48976/review_broker_Q4_2023.pdf (accessed 23.09.2024) (In Russ.).

2. *Moscow Exchange Press Release.* URL: https://www.moex.com/n72763?ysclid=m1xtkk2pt3119004924 (accessed 23.09.2024) (In Russ.).

3. *Research by an Analytical Agency Smart Ranking*. URL: https://smartranking.ru/ru/analytics /FINTECH/fintech-rynok-vyros-na-15-po-itogam-i-polugodiya-2024/ (accessed 23.09.2024) (In Russ.).

4. *Financial Autopilot.* URL: https://finance-autopilot.ru/ (accessed 23.09.2024) (In Russ.).

5. *Personal Financial Assistant.* URL: https://robo.alfacapital.ru/profile (accessed 23.09.2024) (In Russ.).

6. *Robot-Advisor.* URL: https://www.vtb.ru/personal/investicii/robot/ (accessed 23.09.2024) (In Russ.).

7. *AI-Advisor.* URL: https://broker.finam.ru/landing/ii-sovetnik (accessed 23.09.2024) (In Russ.).

8. Conomy Terminal. URL: https://terminal.conomy.ru/ (accessed 23.09.2024) (In Russ.).

9. *Gartner Press Release.* URL: https://www.gartner.com/en/newsroom/press-releases/2021-03-10-gartner-says-tech-investors-will-prioritize-data-science-and-artificial-intelligence-above-gut-feel-for-investment-decisions-by-20250 (accessed 23.09.2024) (In Russ.).

10. Bronshtein, E. M., Kondrateva, O. V. Security Portfolio Management Based on Combined Entropic Risk Measures. *Journal of Computer and Systems Sciences International*, 2013, no. 52 (5), pp. 837–841. https://doi.org/10.1134/S1064230713050043.

11. Kondrateva, O. V. Intellectual decision-making support algorithm on the securities portfolio formation based on the swarm intelligence. *Modeling, Optimization and Information Technology*. 2021;9(2). DOI: 10.26102/2310-6018/2021.33.2.029 (In Russ.).

Статья поступила в редакцию 02.11.2024; одобрена после рецензирования 29.11.2024; принята к публикации 29.11.2024.

The article was submitted 02.11.2024; approved after reviewing 29.11.2024; accepted for publication 29.11.2024.

УДК 004.056

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ АНАЛИЗА ЕГО ПОВЕДЕНЧЕСКИХ ХАРАКТЕРИСТИК

Смагин Кирилл Александрович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
магистрант, e-mail: c.smagin2017@yandex.ru
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: makaryan@kubstu.ru
Путято Михаил Михайлович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
доцент, ORCID: 0000-0003-0414-6034, e-mail: michael.putyato@kubstu.ru
Черкасов Александр Николаевич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, ORCID: 0000-0002-5015-4556, e-mail: cherk@mail.ru
Вихлянцев Владислав Владимирович, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
бакалавр, ORCID: 0009-0003-9914-4206, e-mail: vladikvix@gmail.com

Целью данной работы является разработка системы обнаружения ранее неизвестного вредоносного программного обеспечения на основе анализа его поведенческих характеристик. В данном исследовании был проведен комплексный анализ традиционных методов обнаружения вредоносного программного обеспечения и их сопоставление с инновационными подходами, основанными на моделях глубокого обучения. В рамках исследования была разработана и реализована система, способная эффективно обнаруживать ранее неизвестные виды ВПО. В ходе выполнения работы была разработана и обучена модель глубокого обучения, решающая задачу бинарной классификации на основе входных параметров. Произведено тестирование, оценка эффективности, а также сравнение с существующими аналогами в виде моделей машинного обучения. В результате выполнения работы была разработана система, позволяющая на основании дампов оперативной памяти, полученных из внешних систем, делать оценку параметров и выдавать заключение об обнаружении вредоносного программного обеспечения в загруженном дампе. Внедрение разработанной системы является экономически выгодным, позволяя организациям снизить убытки в результате атак с применением вредоносного программного обеспечения.

Ключевые слова: кибератака, фреймворк, датасет, глубокое обучение

DEVELOPMENT OF A MALWARE DETECTION SYSTEM BASED ON THE ANALYSIS OF ITS BEHAVIORAL CHARACTERISTICS

***Smagin Kirill A.*,** Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
master's student, e-mail: c.smagin2017@yandex.ru
***Makaryan Alexander S.*,** Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Assistant Professor, ORCID: 0000-0002-1801-6137, e-mail: makaryan @kubstu.ru
***Putyato Michael M.*,** Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Assistant Professor, ORCID: 0000-0003-0414-6034, e-mail: michael.putyato@kubstu.ru
***Cherkasov Alexander N.*,** Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
Cand. Sci. (Engineering), Assistant Professor, ORCID: 0000-0002-5015-4556, e-mail: cherk@mail.ru
***Vikhlyantsev Vladislav V.*,** Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,
bachelor, ORCID: 0009-0003-9914-4206, e-mail: vladikvix@gmail.com

The purpose of this work is to develop a system for detecting previously unknown malicious software based on an analysis of its behavioral characteristics. In this study, a comprehensive analysis of traditional malware detection methods was carried out and their comparison with innovative approaches based on deep learning models. As part

of the study, a system capable of effectively detecting previously unknown types of VPO was developed and implemented. In the course of the work, a deep learning model was developed and trained to solve the problem of binary classification based on input parameters. Testing, evaluation of effectiveness, as well as comparison with existing analogues in the form of machine learning models were performed. As a result of the work, a system was developed that allows, based on RAM dumps received from external systems, to evaluate parameters and issue a conclusion on the detection of malicious software in the downloaded dump. The implementation of the developed system is economically beneficial, allowing organizations to reduce losses as a result of attacks using malicious software.

Keywords: cyberattack, framework, dataset, deep learning

ВВЕДЕНИЕ

Кибербезопасность включает в себя перечень методов и технологий, с помощью которых обеспечивается защита инфраструктуры и данных от атак. Различные механизмы кибербезопасности доступны на уровнях сети, хоста, данных и приложений. Существующие механизмы могут быть не эффективны при противодействии атакам нулевого дня, так как ранее данная атака не имела каких-либо записей и не может быть оперативно обнаружена.

Исходя из вышесказанного, можно сказать, что разработка новых методов обнаружения ранее неизвестного вредоносного программного обеспечения является одной из более актуальных задач на сегодняшний день, а применение моделей глубокого обучения для решения данной задачи может повысить эффективность защиты от атак нулевого дня в сравнении с существующими методами.

АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

Ежегодно увеличивается количество атак с применением вредоносного программного обеспечения. Вредоносное ПО представляет собой угрозу для безопасности данных, целостности информации и стабильности работы компьютерных сетей.

По данным компании “Positive Technologies”, в IV квартале 2023 г. вредоносное програмное обеспечение использовалось в более чем 73 % успешных атак на инфраструктуру организаций, и данный показатель продолжает расти из года в год [1].

Исходя из статистики, представленной на рисунках 1 и 2, можно сделать вывод, что существующие методы обнаружения вредоносного программного обеспечения покрывают далеко не все тактики и техники злоумышленников, применяющие ВПО. В текущей ситуации возникает потребность в разработке более совершенных инструментов для отслеживания ранее неизвестного вредоносного программного обеспечения.

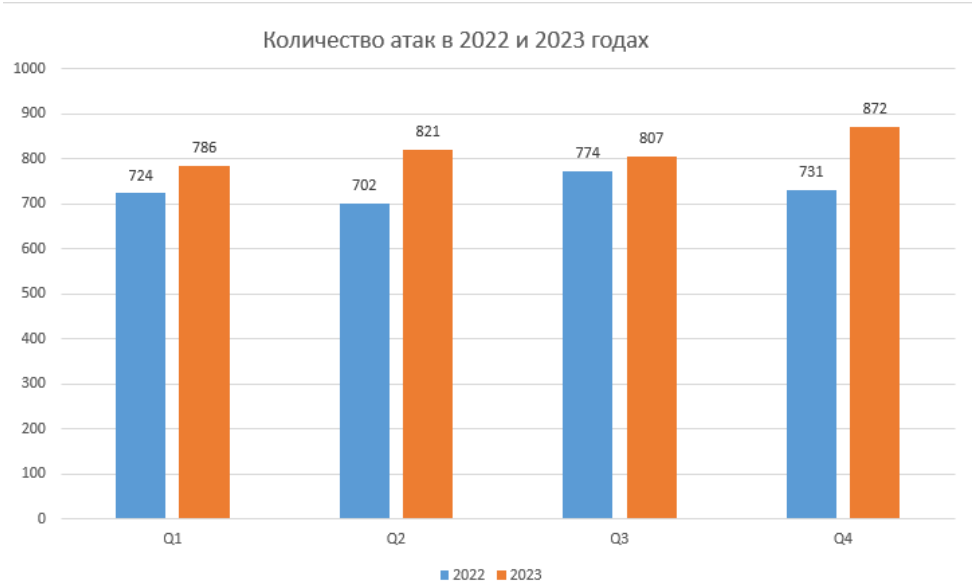


Рисунок 1 – Поквартальный график соотношения количество атак на инфраструктуру в 2022–2023 гг.

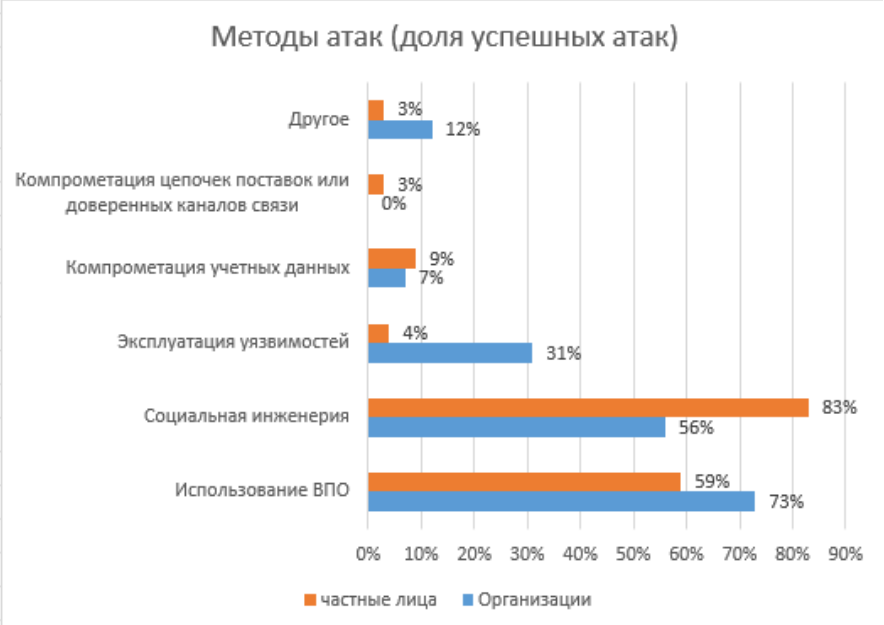


Рисунок 2 – Диаграмма методов атак от доли успешных атак за четвертый квартал 2023 г.

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПО

На сегодняшний день существует ряд устоявшихся методик обнаружения вредоносного программного обеспечения, которые используются по отдельности или в комбинированном исполнении [2]. Данные методы включают в себя:

– сигнатурный анализ;
– эвристический анализ;
– поведенческие блокираторы.

Необходимо оценить преимущества и недостатки представленных методов обнаружения ВПО.

Сигнатурный анализ вредоносных программ (ВПО) – это один из старейших и наиболее распространенных методов обнаружения вредоносных программ [2]. Этот метод основан на поиске характерных признаков, или «сигнатур», которые являются уникальными для каждого вида вредоносного кода. Сигнатуры могут представлять собой последовательности байтов, кодовые последовательности или другие специфические характеристики, которые позволяют идентифицировать конкретный вид вредоносного программного обеспечения.

В современных условиях сигнатурный анализ часто используется в сочетании с другими методами обнаружения, чтобы обеспечить более надежную защиту от широкого спектра угроз.

Эвристический анализатор – это метод обнаружения вредоносных программ, который основан на анализе поведения программного обеспечения и поиске признаков, характерных для вредоносных действий [4]. В отличие от сигнатурного анализа, который ищет конкретные последовательности байтов или кодовые сигнатуры, эвристический анализ пытается определить потенциально опасные действия, которые могут указывать на вредоносность программы.

Поведенческий блокиратор – это тип программного обеспечения для защиты от вредоносных программ, который фокусируется на анализе и контроле поведения приложений в реальном времени [5]. В отличие от сигнатурного и эвристического анализа, который пытается идентифицировать вредоносные программы на основе их кода или поведения, поведенческий блокиратор действует, наблюдая за тем, как программы взаимодействуют с системой и другими ресурсами.

Несмотря на все вышесказанное, продвинутые методы обнаружения ВПО не позволяют полностью отказаться от классических антивирусных баз, а также требуют постоянного развития.

АНАЛИЗ ПРИМЕНЕНИЯ ГЛУБОКОГО ОБУЧЕНИЯ В ЗАДАЧАХ КИБЕРБЕЗОПАСНОСТИ

Основной задачей в рамках обнаружения атак нулевого дня и ранее неизвестного вредоносного программного обеспечения является выявление индикаторов проведенной атаки, которые могут быть использованы в будущем для идентификации новой атаки [6]. Сложность данной задачи заключается в большом количестве данных, генерируемых различными средствами кибербезопасности. Именно для обработки больших объемов данных эффективным решением является обучение и использование моделей глубокого обучения, которые позволят реализовать гибридный подход

к обнаружению атак в сфере кибербезопасности. Данный подход заключается в одновременном выявлении аномального поведения устройств или пользователей, а также повышении скорости обнаружения уже известных атак.

Существуют различные типы моделей глубокого обучения, которые можно применять для решения задач кибербезопасности.

Глубокие сети доверия. Это класс моделей глубокого обучения, состоящий из нескольких взаимосвязанных слоев случайных переменных, внутри которых отсутствуют связи [10]. Фактически глубокие сети доверия объединяют в себе математические методы машинного обучения с нейронными сетями.

Автокодировщик. Метод обучения, при котором исходные данные представлены в форме векторов, позволяет сети искать соответствия, что приводит к формированию на выходе вектора, идентичного входному [9].

Этот процесс можно проиллюстрировать, создавая образцы данных с различной степенью сложности, путем изменения их структуры. В данном контексте функция сжатия информации (или уменьшения размерности признаков) осуществляется посредством сетей с ограниченным количеством скрытых слоев. Важным инструментом в этом процессе является автокодировщик, способный фильтровать шум и восстанавливать первоначальный сигнал из его зашумленной версии.

Рекуррентные нейронные сети – это тип искусственных нейронных сетей, специально разработанных для работы с последовательностями данных, такими как временные ряды, текст, аудио и видео [11]. В отличие от традиционных нейронных сетей, у которых информация передается только в одном направлении (от входа к выходу), рекуррентные сети имеют обратные связи, что позволяет им хранить информацию о прошлых состояниях и учитывать ее при обработке текущих данных.

Рекурсивная нейронная сеть. Данный тип моделей связывает ряд весов рекурсивно. В модели имеется несколько входов, которые рассматриваются в модели как один. Затем выход узла рассматривается как вход для следующего узла. Многие методы обработки естественного языка используют данный тип модели [12].

Количество и разнообразие вредоносного ПО постоянно растет, что усложняет защиту от них стандартными методами. Глубокое обучение позволяет построить обобщающие модели для автоматического обнаружения и классификации вредоносных программ. Это помогает обеспечить защиту от небольших группировок, использующих известное вредоносное ПО, а также от профессиональных группировок, использующих новые или самописные типы вредоносных программ.

Основными задачами в данном случае являются обнаружение вредоносного ПО и его классификация.

Как правило, для обнаружения вредоносного ПО используют динамические и статические функции. Динамические функции являются более предпочтительными, так как их сложнее обфусцировать. В роли входных данных в основном используются данные, полученные в результате запуска ПО в песочнице.

Для обнаружения более сложных программ используются методы, основанные на сетевом поведении, поскольку в данном случае можно изучить траффик вредоносного ПО. Автоматическая классификация вредоносного ПО также может дать важную информацию об источнике и целях злоумышленника, не требуя от аналитиков значительного времени на анализ. Это особенно важно в условиях быстрого роста числа и семейств вредоносных программ.

В результате проведенного анализа были исследованы существующие методы обнаружения вредоносного программного обеспечения, а также применение моделей глубокого обучения в задачах кибербезопасности.

Было определено, что в настоящее время существующих методов обнаружения вредоносного ПО может быть недостаточно в связи со специфичными для каждого метода недостатками.

Также выявлено, что атаки, проведенные с помощью вредоносного ПО, имеют высокий процент успешности и занимают второе место по популярности, что доказывает необходимость применения новых подходов в их обнаружении.

В таблице 1 представлено сравнение существующих методов обнаружения вредоносного ПО с применением моделей глубокого обучения.

Разработка системы обнаружения вредоносного ПО:

Разрабатываемая система будет состоять из нескольких взаимосвязанных блоков:

– модуль сбора данных для анализа представляет собой песочницу, создающую изолированную среду для выполнения вредоносного программного обеспечения и сбора данных для передачи в систему обнаружения вредоносного программного обеспечения;
– модуль обработки данных отвечает за сбор и нормализацию данных для последующего анализа;
– модуль анализа данных обеспечивает процесс разбора данных;
– модуль визуализации отвечает за графическое представление результатов работы системы.

Таблица 1 – Сравнение методов обнаружения вредоносного ПО

Метод	Преимущества	Недостатки
Сигнатурный анализ	Высокая эффективность против известного ВПО	Долгая реакция при появлении новых угроз
Статический эвристический анализ	Простота реализации Высокая скорость работы Возможность обнаружения неизвестного ВПО	Высокая вероятность ложных срабатываний Низкий уровень обнаружения неизвестного ВПО Невозможность лечения ВПО
Динамический эвристический анализатор	Простота реализации Высокая скорость работы Возможность обнаружения неизвестного ВПО	Более высокие требования к вычислительным мощностям Невозможность лечения ВПО
Поведенческий блокиратор	Обнаружение руткитов Контроль целостности приложений	Сработки на легитимные программы Более высокие требования к пользователю
Обнаружение на основе моделей глубокого обучения	Высокая эффективность в обнаружении новых и неизвестных угроз.	Требует больших объемов данных для обучения и может быть сложно настроить и оптимизировать

В рамках разработки системы обнаружения вредоносного ПО необходимо определить перечень инструментов, используемых в дальнейшем для реализации проекта.

Модуль анализа данных будет написан на высокоуровневом языке программирования Python, в связи с чем был определен перечень библиотек и классов, используемых в дальнейшем [13].

Для разработки системы был выбран следующий инструментарий: pandas, tensorflow, sklearn (scikit-learn), seaborn, numpy, matplotlib.pyplot.

Для реализации модулей обработки и анализа данных системы обнаружения вредоносного ПО разработаем и обучим нейронную сеть для корреляции и распознавания поведенческих характеристик вредоносного ПО.

Необходимо заранее подготовить набор обучающих данных для тренировки нейросети. Такой датасет был найден на платформе kaggle, и он имеет следующее название “Malware Detection from Memory Dump” [16]. Набор данных по вредоносным программам был специально разработан для оценки эффективности методов, используемых для обнаружения вредоносных программ с помощью анализа дампов памяти рабочих станций. Он предоставляет сбалансированную коллекцию параметров, которые можно использовать для проверки эффективности систем обнаружения вредоносных программ.

Набор данных на 50 % состоит из вредоносных дампов памяти и на 50 % из доброкачественных дампов памяти. В общей сложности в датасете содержится 58 596 записей, из которых 29 298 доброкачественных и 29 298 вредоносных.

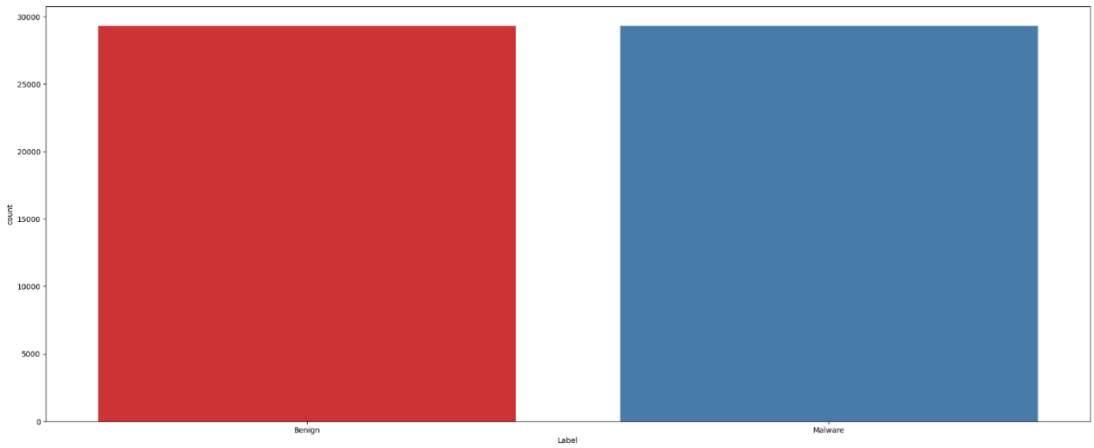


Рисунок 3 – Соотношение обучающих данных в датасете

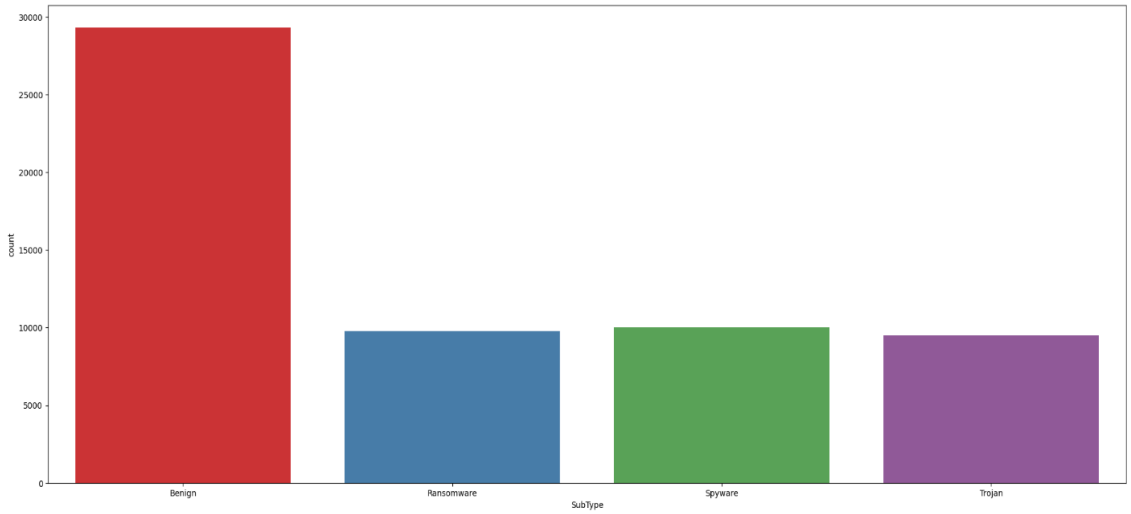


Рисунок 4 – Соотношение типов вредоносного ПО

До начала обучения модели необходимо нормализовать входные данные. Нормализация включает в себя удаление лишних для обучения данных, которые имеются в датасете. Для этого необходимо избавиться от дубликатов и нулевых значений в строках, а также данных, не имеющих ценности для процесса обучения.

Также необходимо разделить данные на признаки и обучающие метки путем удаления этих самых меток из датасета и выделения их в отдельный массив. Дополнительно было выполнено преобразование меток в бинарный формат.

Далее производится стандартизация параметров с использованием функции sklearn. preprocessing.StandardScaler. Стандартизация производится по формуле (1):

$$Z = (X–U)/S, \quad (1)$$

где X – параметр из датасета;

U – среднее значение обучающих выборок;

S – стандартное отклонение обучающих выборок.

Центрирование и масштабирование выполняются независимо для каждого объекта путем вычисления соответствующей статистики по выборкам в обучающем наборе. Затем среднее значение и стандартное отклонение сохраняются для последующего использования в данных с помощью преобразования.

После данных действий данные разделяются на обучающие и тестовые наборы с помощью функции train_test_split.

В рамках данной работы будет решаться задача бинарной классификации. На выходе модель будет выдавать решение касательно того, было ли зафиксировано вредоносное программное обеспечение в дампе памяти или нет.

Для решения данной задачи будет использоваться последовательная нейронная сеть, состоящая из нескольких полносвязных слоев.

Рассмотрим подробнее каждый слой модели:

– первый слой Dense имеет 48 нейронов, функцию активации 'relu' (Rectified Linear Unit) и принимает на вход данные с формой, соответствующей количеству признаков в X_train. Функция активации relu вычисляется как max(0, x), что позволяет нейронам активироваться, когда значение выше нуля, и оставаться неактивными, когда значение ниже или равно нулю.

– первый слой Dropout с коэффициентом 0.5. Dropout – это регуляризационный метод, который помогает предотвратить переобучение модели. В процессе обучения dropout случайным образом выключает (устанавливает в ноль) определенную долю нейронов в слое, тем самым уменьшая зависимость модели от отдельных нейронов;

– второй слой Dense имеет 24 нейрона и функцию активации 'relu';

– второй слой Dropout с коэффициентом 0,5;

– третий слой Dense имеет 12 нейронов и функцию активации 'relu';

– третий слой Dropout с коэффициентом 0,5;

– выходной слой Dense имеет 1 нейрон и функцию активации 'sigmoid'. Функция активации sigmoid вычисляется как 1 / (1 + exp(-x)) и возвращает значение в диапазоне [0, 1], что позволяет интерпретировать выход модели как вероятность принадлежности к определенному классу.

Таким образом, данная модель нейросети состоит из последовательности слоев Dense и Dropout, что позволяет ей обучаться на данных и решать задачу бинарной классификации.

Для оценки модели используется ряд метрик, вычисляемых в процессе обучения, но перед переходом к самим метрикам, необходимо дать определение матрицы ошибок.

Матрица ошибок – макет таблицы, которая позволяет визуализировать производительность алгоритма [17].

	y=1	y=0
x=1	True Positive (TP)	False Positive (FP)
x=0	False Negative (FN)	True Negative (TN)

Рисунок 5 – Матрица классификации ошибок

Таким образом, ошибки классификации бывают двух видов: False Negative (FN) и False Positive (FP).

На основе ошибок классификации вычисляется ряд метрик, отражающих работу алгоритма.

Точность (англ. Accuracy) отражает долю правильных ответов алгоритма и вычисляется по формуле (2):

$$Accuracy = (TP+TN)/(TP+TN+FP+FN), \quad (2)$$

где TP – положительные сработки;

TN – отрицательные сработки;

FP – ложно-положительные сработки;

FN – ложно-отрицательные сработки;

Precision показывает долю объектов, названных нашей моделью положительными и при этом действительно являющихся положительными.

Вычисляется по формуле (3):

$$Precision = TP / (TP + FP), \quad (3)$$

где TP – положительные сработки;

FP – ложно-положительные сработки;

Recall показывает, какую долю объектов положительного класса из всех объектов положительного класса нашел алгоритм. Вычисляется по формуле (4):

$$Recall = TP / (TP + FN), \quad (4)$$

где TP – положительные сработки;

FN – ложно-отрицательные сработки;

F-мера отражает одновременно и Recall, и Precision и вычисляется по формуле (5):

$$F = 2 \cdot (Precision \cdot Recall) / (Precision + Recall). \quad (5)$$

Таким образом, F-мера показывает, насколько корректно модель обнаруживает объекты положительного класса, а также сколько из этих объектов действительно относятся к искомому классу.

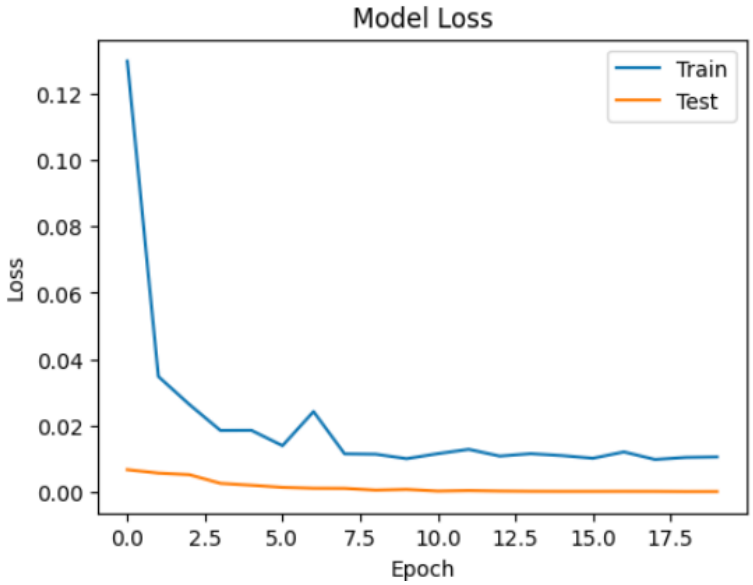


Рисунок 6 – Диаграмма функции потерь

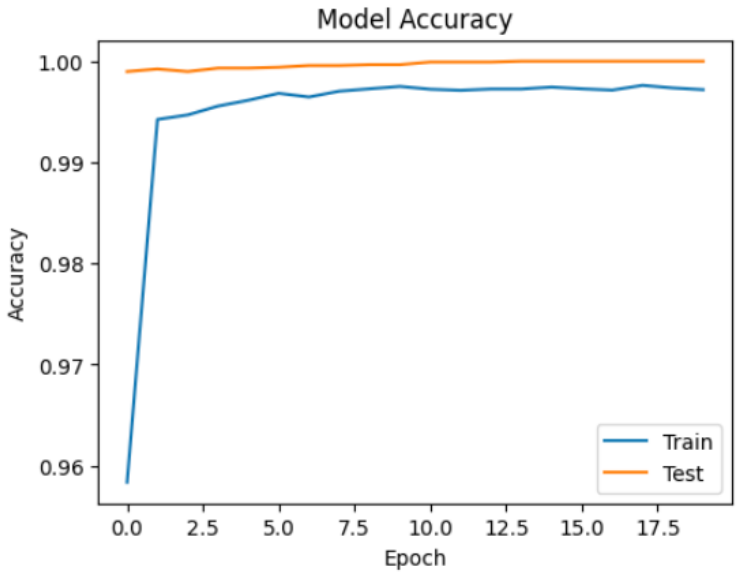


Рисунок 7 – Диаграмма точности модели

Дополнительно стоит обратить внимание на матрицу ошибок. На рисунке 8 можно увидеть матрицу ошибок для данной модели, которая отражает ошибки классификации модели.

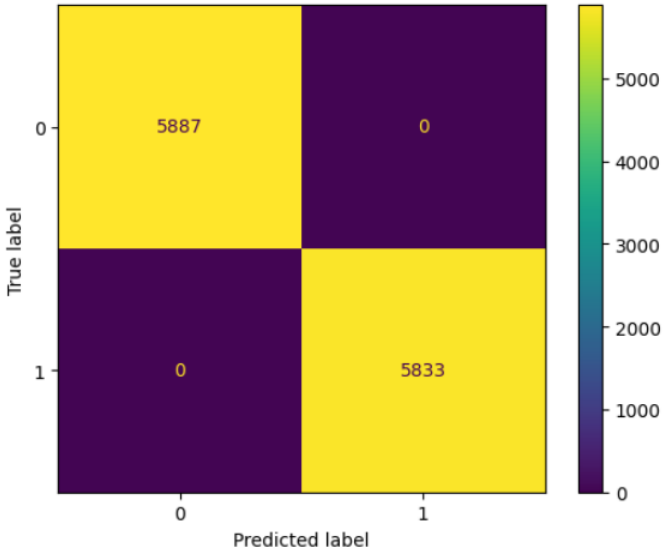


Рисунок 8 – Матрица ошибок

Исходя из полученных данных, можно увидеть, что модель с высокой точностью определяет наличие или отсутствие вредоносного программного обеспечения в получаемых тестовых данных, не участвующих в процессе обучения.

Для оценки эффективности разработанной модели необходимо дополнительно провести ее сравнение с существующими аналогами, а именно с моделями машинного обучения.

Для этого был выбран ряд моделей, способных решать задачи бинарной классификации. На рисунках 9–13 представлены матрицы ошибок моделей, полученные в результате обучения моделей на идентичном датасете.

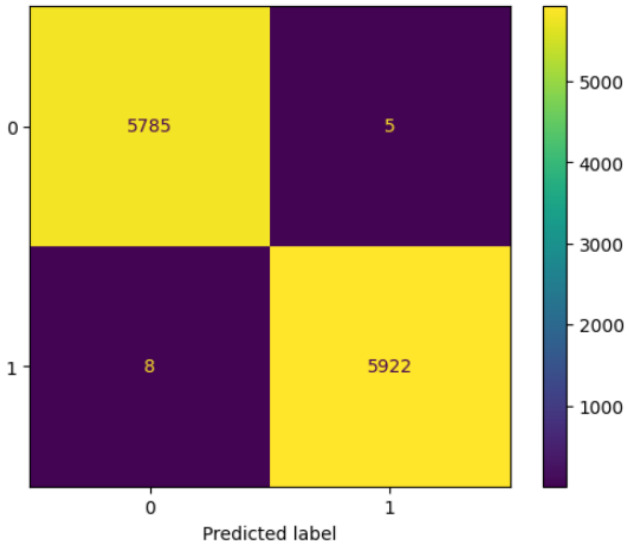


Рисунок 9 – Матрица ошибок модели логистической регрессии

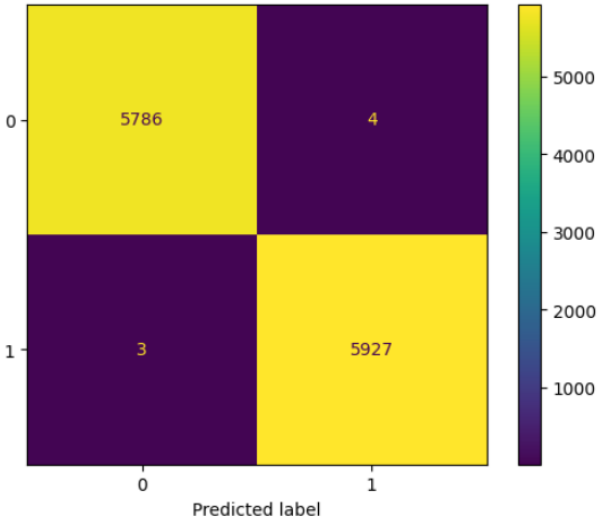


Рисунок 10 – Матрица ошибок модели метода опорных векторов

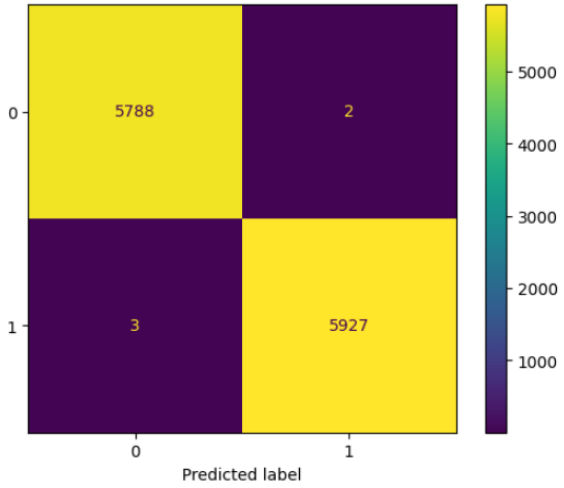


Рисунок 10 – Матрица ошибок модели метода k-ближайших соседей

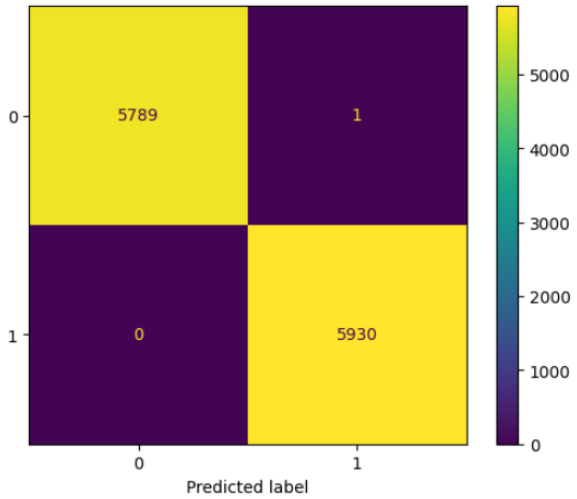


Рисунок 11 – Матрица ошибок модели случайного леса

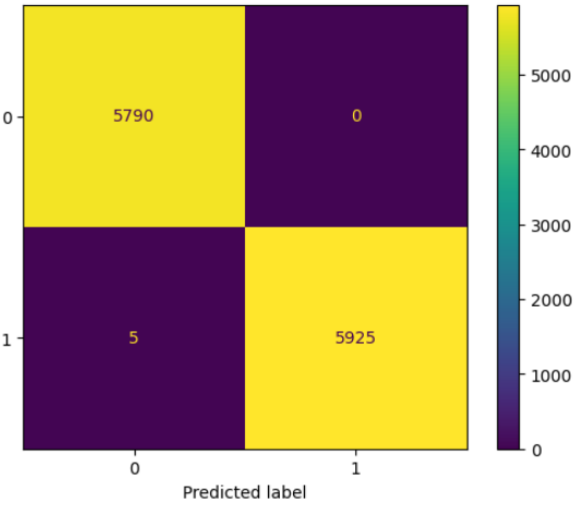


Рисунок 12 – Матрица ошибок модели повышения градиента

ЗАКЛЮЧЕНИЕ

Исходя из вышесказанного, можно сделать вывод, что применение моделей глубокого обучения для обнаружения вредоносного ПО может нивелировать недостатки существующих методов обнаружения, в перспективеувеличивая общую защищенность инфраструктуры.

Дополнительно модели сравниваются по F-мере, которая отражает среднее гармоническое точности и полноты. В таблице 2 представлены показатели F-меры сравниваемых моделей.

Таблица 2 – Сравнение моделей машинного обучения

Модель	F-мера
Логистическая регрессия	0,9989036012482078
Метод опорных векторов	0,9994098305370542
Метод k-ближайших соседей	0,9995783792899906
Случайный лес	0,9999156900767221
Модель	F-мера
Метод повышения градиента	0,9995783792899906
Разрабатываемая модель	1

Исходя из данных выше, можно сделать вывод, что полученная на выходе модель не уступает существующим решениям, что позволяет использовать ее для решения задачи бинарной классификации в рамках разработки системы обнаружения вредоносного ПО. Учитывая более точное определение моделей глубокого обучения при больших объемах данных, использование данной модели будет более предпочтительным.

Список источников

1. Смагин, К. А. Дипломная работа по специальности 10.04.01 «Информационная безопасность» / К. А. Смагин ; Кубанский государственный технический университет. – Краснодар, 2024. – 73 с.
2. Блог компании «Positive Technologies». Актуальные киберугрозы: IV квартал 2023 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (дата обращения: 12.04.2024).
3. Павликов, С. Н. Методы обнаружения вредоносных программ и их элементов / С. Н. Павликов, В. Ю. Коломеец, Ю. Ю. Колесов, П. Н. Петров, Р. К. Афанасьев. – URL: https://cyberleninka.ru/article/n/metod-obnaruzheniya-vredonosnyh-programm-i-ih-elementov (дата обращения: 05.03.2024).
4. Горбунов, А. Н. Принципы использования сигнатурного анализа для обнаружения вредоносных программ / А. Н. Горбунов, Т. Г. Емельяненко. – URL: https://cyberleninka.ru/article/n/printsipy-ispolzovaniya-signaturnogo-analiza-dlya-obnaruzheniya-vredonosnyh-programm (дата обращения: 05.03.2024).
5. Алиев, А. Т., Проактивные системы защиты от вредоносного программного обеспечения / А. Т. Алиев. – URL: https://cyberleninka.ru/article/n/proaktivnye-sistemy-zaschity-ot-vredonosnogo-programmnogo-obespecheniya (дата обращения: 06.03.2024).
6. Проактивные методы антивирусной защиты. – URL: https://www.anti-malware.ru/analytics /Technology_Analysis/antivirus-protection-proactive-methods (дата обращения: 08.03.2024).
7. Buczak, L. A Survey of Data Mining and Machine Learning Methods for Cyber Security / L. Buczak, E. Guven // IEEE Commun. Surv. Tutor. – 2016. – № 18. – P. 1153–1176.
8. Sutskever, I. Sequence to sequence learning with neural networks / I. Sutskever, O. Vinyals, Q. V. Le // Advances in Neural Information Processing Systems. – Cambridge, MA, USA, MIT Press, 2014. – P. 3104–3112.
9. Sainath, T. N. Deep convolutional neural networks for LVCSR / T. N. Sainath, A. R. Mohamed, B. Kingsbury, B. Ramabhadran // Proceedings of the 2013 IEEE International Conference Acoustics, Speech and Signal Processing (ICASSP), Vancouver, BC, Canada, 26–31 May 2013. – P. 8614–8618.
10. Goodfellow, I. Generative adversarial nets / I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, Y. Bengio // Advances in Neural Information Processing Systems. – Cambridge, MA, USA : MIT Press, 2014. – P. 2672–2680.
11. Al-Garadi, M. A. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security / M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, M. Guizani. – arXiv 2018, arXiv:1807.11023.
12. El Hihi, S. Hierarchical recurrent neural networks for long-term dependencies / S. El Hihi, Y. Bengio // Advances in Neural Information Processing Systems. – Cambridge, MA, USA : MIT Press, 1996. – P. 493–499.
13. Deng, L. Deep learning: Methods and applications. Found. Trends Signal Process / L. Deng, D. Yu. – 2014. – № 7. – P. 197–387.
14. Python. – URL: https://www.python.org/ (дата обращения: 04.02.2024).
15. Блог компании RUVDS. О реализации библиотеки для глубокого обучения на Python. – URL: https://habr.com/ru/companies/ruvds/articles/486686/ (дата обращения: 05.02.2024).
16. Cuckoo Sandbox Book. – URL: https://cuckoo.sh/docs/index.html (дата обращения: 15.05.2024).
17. Kaggle: Your Home for Data Science. – URL: https://www.kaggle.com/ (дата обращения: 12.02.2024).
18. Sckit-learn. Confusion matrix // https://scikit-learn.org. – URL: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.confusion_matrix.html (дата обращения: 15.02.2024).
19. Вакансии «Инженер по информационной безопасности». – URL: https://krasnodar.hh.ru/search/resume?text=Инженер+по+информационная+безопасность&area=1&isDefaultArea=true&exp_period=all_time& logic=normal&pos=full_text&hhtmFrom=vacancy_search_list&hhtmFromLabel=resume_search_line (дата обращения: 03.06.2024).
20. Рост ущерба российских копаний от действий злоумышленников. – URL: https://safe.cnews.ru /news/top/2023-07-14_rossijskie_kompanii_teryayut (дата обращения: 03.06.2024).
21. КК «Кубань кредит» ООО Обобщенная бухгалтерская(финансовая) отчетность за 2023 год и аудиторское заключение независимого аудитора. – URL: https://kk.bank/o-banke/raskrytie-informatsii/finansovye-otchety/2023/.
22. Козырь, Н. С. Денежные критерии риска информационной безопасности на основе подхода оценки активов / Н. С. Козырь, А. С. Макарян, Л. Л. Оганесян // Вопросы кибербезопасности. – URL: https://cyberrus.info/wp-content/uploads/2024/05/vokib-2024-3-st06-s051-060.pdf.

References

1. Smagin, K. A. *Thesis on the specialty 10.04.01 "Information security".* Kuban State Technical University. Krasnodar, 2024. 73 p. (In Russ.).
2. *Positive Technologies company blog, Current cyber threats: IV quarter of 2023.* Available at: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q4/ (accessed 12.04.2024) (In Russ.).
3. Pavlikov, S. N., Kolomeets, V. Yu., Kolesov, Yu. Yu., Petrov, P. N., Afanasyev, R. K. *Methods of malware detection and their elements.* Available at: https://cyberleninka.ru/article/n/metod-obnaruzheniya-vredonosnyh-programm-i-ih-elementov (accessed 05.03.2024) (In Russ.).
4. Gorbunov, A. N., Emelianenko, T. G. *Principles of using signature analysis to detect malware.* Available at: https://cyberleninka.ru/article/n/printsipy-ispolzovaniya-signaturnogo-analiza-dlya-obnaruzheniya-vredonosnyh-programm (accessed 05.03.2024) (In Russ.).
5. Aliev, A. T. *Proactive protection systems against malicious software.* Available at: https://cyberleninka.ru/article/n/proaktivnye-sistemy-zaschity-ot-vredonosnogo-programmnogo-obespecheniya (accessed 06.03.2024) (In Russ.).

6. *Proactive methods of antivirus protection.* Available at: https://www.anti-malware.ru/analytics/Technology_Analysis/antivirus-protection-proactive-methods (accessed 08.03.2024) (In Russ.).

7. Buczak, L., Guven, E. A Survey of Data Mining and Machine Learning Methods for Cyber Security. *IEEE Commun. Surv. Tutor.*, 2016, no. 18, pp. 1153–1176.

8. Sutskever, I., Vinyals, O.,Le, Q. V. Sequence to sequence learning with neural networks. *Advances in Neural Information Processing Systems.* Cambridge, MA, USA, MIT Press, 2014, pp. 3104–3112.

9. Sainath, T. N., Mohamed, A. R., Kingsbury, B., Ramabhadran, B. Deep convolutional neural networks for LVCSR. *Proceedings of the 2013 IEEE International Conference Acoustics, Speech and Signal Processing (ICASSP), Vancouver, BC, Canada, 26–31 May 2013*, pp. 8614–8618.

10. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y. Generative adversarial nets. *Advances in Neural Information Processing Systems.* Cambridge, MA, USA, MIT Press, 2014, pp. 2672–2680.

11. Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Guizani, M. *A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security.* arXiv 2018, arXiv:1807.11023.

12. El Hihi, S., Bengio, Y. Hierarchical recurrent neural networks for long-term dependencies. *Advances in Neural Information Processing Systems.* Cambridge, MA, USA, MIT Press,1996, pp. 493–499.

13. Deng, L., Yu, D. *Deep learning: Methods and applications. Found. Trends Signal Process*. 2014, no. 7, pp. 197–387.

14. Python. Available at: https://www.python.org / (accessed: 02/04/2024)

15. RUVDS company blog, About the implementation of a library for deep learning in Python. Available at: https://habr.com/ru/companies/ruvds/articles/486686 / (accessed 05.02.2024) (In Russ.).

16. Cuckoo Sandbox Book. Available at: https://cuckoo.sh/docs/index.html (accessed 15.05.2024).

17. Kaggle: Your Home for Data Science Available at: https://www.kaggle.com / (date of access: 02/12/2024)

18. Sckit-learn. Confusion matrix. Available at: https://scikit-learn.org/stable/modules/generated/sklearn.metrics.confusion_matrix.html (accessed: 02/15/2024)

19. *Vacancies "Information security Engineer".* Available at: https://krasnodar.hh.ru/search/resume?text=Инженер+по+информационная+безопасность&area=1&isDefaultArea=true&exp_period=all_time&logic=normal&pos=full_text&hhtmFrom=vacancy_search_list&hhtmFromLabel= resume_search_line (accessed 03.06.2024) (In Russ.).

20. The growth of damage to Russian digs from the actions of intruders. Available at: https://safe.cnews.ru/news/top/2023-07-14_rossijskie_kompanii_teryayut (accessed 03.06.2024) (In Russ.).

21. *KK "Kuban Credit" LLC Generalized accounting (financial) statements for 2023 and the audit opinion of an independent auditor.* Available at: https://kk.bank/o-banke/raskrytie-informatsii/finansovye-otchety/2023/ (In Russ.).

22. Kozyr, N. S., Makaryan, A. S., Oganesyan, L. L. Monetary criteria for information security risk based on the asset valuation approach. *Issues of cybersecurity.* Available at: https://cyberrus.info/wp-content/uploads/2024/05/vokib-2024-3-st06-s051-060.pdf (In Russ.).

Статья поступила в редакцию 28.10.2024; одобрена после рецензирования 29.11.2024; принята к публикации 10.12.2024.

The article was submitted 28.10.2024; approved after reviewing 29.11.2024; accepted for publication 10.12.2024.

ПРИБОРОСТРОЕНИЕ, МЕТРОЛОГИЯ И ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ ПРИБОРЫ И СИСТЕМЫ

ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫЕ И УПРАВЛЯЮЩИЕ СИСТЕМЫ

УДК 303.732.4

АЛГОРИТМ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫМ КОМПЛЕКСОМ ДЛЯ МОНИТОРИНГА СОСТОЯНИЯ ВОДНЫХ ОБЪЕКТОВ

Новгородов Клим Иванович, Волгоградский государственный технический университет, 400005, Российская Федерация, г. Волгоград, пр-т им. В. И. Ленина, 28,
аспирант, ORCID: 0009-0001-4301-8927, e-mail: novgorodov-klim@mail.ru

В статье представлен новый алгоритм для эффективного мониторинга водоемов. Алгоритм использует возможности информационных и измерительных систем для сбора и анализа данных о различных параметрах качества воды. Объединяя методы дистанционного зондирования с измерениями на месте, алгоритм обеспечивает комплексную оценку качества воды, позволяя на ранней стадии обнаруживать загрязнение и деградацию. Ключевой особенностью разработанного алгоритма является его способность адаптироваться к изменяющимся условиям окружающей среды и включать данные из нескольких источников. Предлагаемый алгоритм устраняет несколько ограничений традиционных методов мониторинга, таких как высокая стоимость и трудоемкость ручного отбора проб. Автоматизируя сбор и анализ данных, алгоритм обеспечивает более частый и масштабный мониторинг качества воды. Более того, алгоритм может быть интегрирован с существующими системами управления водными ресурсами для предоставления информации в режиме реального времени для принятия решений.

Ключевые слова: алгоритм, мониторинг качества, дистанционное зондирование, искусственный интеллект, машинное обучение, нейронные сети, нечеткая логика, водные объекты, информационно-измерительный комплекс

ALGORITHM FOR CONTROL OF INFORMATION AND MEASURING COMPLEX FOR MONITORING THE STATE OF WATER BODIES

Novgorodov Klim I., Volgograd State Technical University, 28, Lenin St., Volgograd, 400005, Russian Federation,
postgraduate student, ORCID: 0009-0001-4301-8927, e-mail: novgorodov-klim@mail.ru

The paper presents a new algorithm for efficient monitoring of water bodies. The algorithm leverages the capabilities of information and measurement systems to collect and analyze data on various water quality parameters. By combining remote sensing methods with in-situ measurements, the algorithm provides a comprehensive assessment of water quality, allowing for early detection of pollution and degradation. A key feature of the developed algorithm is its ability to adapt to changing environmental conditions and incorporate data from multiple sources. The proposed algorithm addresses several limitations of traditional monitoring methods, such as the high cost and labor intensity of manual sampling. By automating data collection and analysis, the algorithm enables more frequent and large-scale water quality monitoring. Moreover, the algorithm can be integrated with existing water management systems to provide real-time information for decision making.

Keywords: algorithm, quality monitoring, remote sensing, artificial intelligence, machine learning, neural networks, fuzzy logic, water bodies, information and measuring complex

ВВЕДЕНИЕ

Деградация водных экосистем, вызванная антропогенным загрязнением, является одной из самых насущных глобальных экологических проблем. Увеличение концентрации загрязняющих веществ в водоемах, таких как промышленные и бытовые стоки, сельскохозяйственные удобрения и пестициды, приводит к эвтрофикации, закислению воды и снижению биоразнообразия. Эти процессы требуют внедрения эффективных систем мониторинга качества воды для своевременного выявления и устранения негативных последствий.

Мониторинг состояния водных объектов является основой для разработки эффективных алгоритмов управления водными ресурсами. Таким образом, мониторинг – система наблюдений, оценки, контроля и прогноза состояния окружающей среды [5].

Полученные в результате мониторинга данные используются для создания математических моделей, которые оценивают динамику водных экосистем и прогнозируют последствия различных антропогенных воздействий. На основе этих моделей разрабатываются алгоритмы управления, направленные на оптимизацию использования водных ресурсов и сохранение их качества.

Информационно-измерительные комплексы являются неотъемлемой частью современных систем мониторинга водных объектов. Они обеспечивают сбор, обработку и анализ данных о физико-химических и биологических характеристиках водной среды. Благодаря использованию современных датчиков и программного обеспечения, комплексы осуществляют непрерывный мониторинг в режиме реального времени и выявляют отклонения от нормативных показателей. Полученная информация используется для оценки экологического состояния водных объектов, прогнозирования его изменений и разработки мер по улучшению качества воды.

Для обеспечения эффективного мониторинга состояния водных объектов и разработки мероприятий по их защите необходимо использование современных информационно-измерительных комплексов. Современные информационно-измерительные комплексы осуществляют непрерывный контроль за качеством воды, чтобы выявлять источники загрязнения и оценивать эффективность природоохранных мероприятий.

ЛИТЕРАТУРНЫЙ ОБЗОР

Проблема мониторинга качества поверхностных вод приобретает все большую актуальность в связи с ростом антропогенной нагрузки на водные экосистемы. Современные методы мониторинга получают обширные данные о состоянии водных объектов, что необходимо для принятия обоснованных решений в области охраны окружающей среды.

В представленном литературном обзоре рассмотрены различные подходы к мониторингу качества воды, основанные на использовании автоматизированных систем, дистанционного зондирования и инновационных датчиков.

И. А. Серебрицкий, Д. Т. Азёмов, Н. А. Жигунова, Е. С. Бородин провели комплексный анализ состояния поверхностных вод в Санкт-Петербурге с использованием автоматизированной системы мониторинга (АСМ-ПВ). Цель исследования заключалась в оценке качества поверхностных вод на территории Санкт-Петербурга с использованием АСМ-ПВ. Данные, полученные с трех автоматических станций, расположенных на различных водных объектах города, анализируют и сравниваются с установленными нормативами. Основной акцент делается на динамике изменения показателей качества воды в течение года и выявлении возможных тенденций [1].

Для осуществления мониторинга авторы использовали АСМ-ПВ. Используемая система АСМ-ПВ представляет собой комплекс технических средств, программного обеспечения и организационных процедур, чтобы осуществлять непрерывный мониторинг качества воды в автоматическом режиме. Система включает автоматические станции, оснащенные датчиками для измерения различных параметров (растворенный кислород, pH, мутность, нитратный азот), а также центр сбора и обработки данных. Полученные данные передаются в единый государственный фонд данных и используются для информирования органов власти, населения и научного сообщества.

В целом качество воды в исследованных водных объектах Санкт-Петербурга соответствует установленным нормативам. Однако были отмечены сезонные колебания некоторых показателей, особенно уровня растворенного кислорода. И. А. Серебрицкий и др. проанализировали динамику изменений показателей качества воды за несколько лет и выявили определенные тенденции. Например, было отмечено повышение уровня мутности в летний период, что может быть связано с усилением антропогенного воздействия. Исследование выявило ряд проблем, связанных с качеством воды в отдельных водных объектах. Авторы предлагают продолжать мониторинг и разрабатывать меры по улучшению экологического состояния водных ресурсов Санкт-Петербурга. Проведенное исследование, основанное на данных автоматизированной системы мониторинга поверхностных вод Санкт-Петербурга, оценило текущее состояние водных объектов города, выявить сезонные и долгосрочные тенденции изменения качества воды и определить основные факторы, влияющие на эти изменения, что является важным вкладом в разработку стратегий рационального использования водных ресурсов и охраны окружающей среды.

Автоматизированная система мониторинга поверхностных вод, используемая в исследовании, представляет собой эффективный инструмент для сбора, обработки и анализа данных о качестве воды в режиме реального времени, чтобы оперативно выявлять отклонения от нормативных значений и принимать необходимые меры для предотвращения негативных экологических последствий.

Результаты исследования свидетельствуют о необходимости постоянного мониторинга качества поверхностных вод Санкт-Петербурга для обеспечения экологической безопасности города и сохранения водных ресурсов для будущих поколений.

Б. В. Соколов, В. А. Палицын, Д. И. Назаров предложили алгоритм совместного планирования измерительных и вычислительных операций при мониторинге обстановки в локальной акватории, который направлен на решение задачи оптимального планирования измерительно-вычислительных операций в системе мониторинга надводной обстановки [2]. Они определили оптимальную последовательность выполнения операций, обеспечивающую наиболее эффективное наблюдение за движением судов в заданной акватории при соблюдении ограничений на ресурсы системы. Алгоритм объединяет моделирование различных аспектов системы, включая движение объектов, взаимодействие между ними, проведение измерений и обработку данных. Для описания процесса мониторинга используется сложная математическая модель, включающая в себя дифференциальные уравнения, ограничения и целевые функции. Формализация задачи и разработка алгоритма основаны на аппарате теории оптимального управления, чтобы обеспечить оптимальность решений [12]. Модель учитывает наличие возмущений и неопределенностей, что повышает ее реалистичность. Также алгоритм может быть адаптирован к различным конкретным условиям путем изменения параметров модели.

В сравнении с другими методами данного алгоритма необходимо отметить, что традиционные методы планирования часто основаны на экспертных оценках и не учитывают все факторы, влияющие на эффективность системы. Методы искусственного интеллекта, такие как нейронные сети и машинное обучение, могут быть использованы для решения задач планирования, но они требуют больших объемов данных для обучения и могут быть менее прозрачными по сравнению с аналитическими методами. Децентрализованные методы распределяют вычисления между различными компонентами системы, что повышает отказоустойчивость. Однако они могут быть более сложными в реализации и требуют эффективных механизмов координации. Однако реализация алгоритма требует значительных вычислительных ресурсов и глубоких знаний в области теории оптимального управления и математического моделирования. Алгоритм предполагает наличие полной информации о состоянии системы, что может быть не всегда выполнимо на практике.

Предложенный алгоритм А. И. Юхно представляет собой интеллектуальную систему управления дозированием хлорагента на станциях водоподготовки, которая направлена на оптимизацию процесса обеззараживания воды и снижение риска образования вредных хлорорганических соединений. Ключевой особенностью алгоритма является использование нечеткой логики и нейронных сетей для принятия решений в условиях неопределенности и неполной информации о качестве исходной воды. Целью алгоритма является минимизация риска образования хлорорганических соединений при одновременном обеспечении достаточного уровня обеззараживания и достигается путем динамической регулировки дозы хлора в зависимости от текущего качества воды [3].

По мнению автора, использование методов искусственного интеллекта (нечеткой логики и нейронных сетей) дает возможность системе адаптироваться к изменяющимся условиям и принимать более точные решения по сравнению с традиционными методами управления. Алгоритм учитывает множество факторов, влияющих на качество воды и эффективность обеззараживания (таких как концентрация исходного хлора, pH, температура, органические вещества и др.) и точно оценивает необходимую дозу хлорагента, чтобы минимизировать образование вредных побочных продуктов. Система работает в режиме реального времени, чтобы оперативно реагировать на изменения качества воды и предотвращать образование опасных концентраций хлорорганических соединений.

В сравнении с иными методами, традиционные методы контроля дозирования хлорагента основаны на фиксированных значениях дозы, рассчитанных на основе средних характеристик воды. Такие методы не учитывают динамические изменения качества воды и могут приводить к перехлорированию или недостаточному обеззараживанию.

Предложенный алгоритм обладает преимуществами по сравнению с традиционными методами. Благодаря использованию интеллектуальных методов алгоритм точно определяет необходимую дозу хлорагента, что снижает риск образования вредных веществ. Система способна адаптироваться к изменяющимся условиям качества воды, что обеспечивает более эффективную и безопасную работу станции водоподготовки. Оптимизация дозирования хлорагента снижает расход химических реагентов и уменьшает нагрузку на оборудование.

Нечеткая логика моделирует неопределенность и неточность, которые неизбежно присутствуют в реальных системах водоподготовки, что особенно важно при работе с биологическими объектами, такими как вода, свойства которой могут значительно варьироваться во времени и пространстве. Нечеткие правила описывают сложные зависимости между входными и выходными переменными, что делает систему более гибкой и адаптивной. Нейронные сети обнаруживают нелинейные зависимости между различными параметрами воды и эффективно обучаются на больших

объемах данных, помогая системе адаптироваться к новым условиям и улучшать свою производительность со временем.

Разработанный алгоритм А. И. Юхно представляет собой значительный шаг вперед в области контроля качества питьевой воды, так как помогает повысить эффективность и безопасность процессов водоподготовки, снизить риск образования вредных веществ и улучшить качество жизни населения.

G. Jakovljevic, M. Govedarica, F. Alvarez-Taboada в своем исследовании разработали алгоритм мониторинга, основанный на дистанционном зондировании для определения качества воды во внутренних водных объектах. Алгоритм использует возможности спутниковых снимков и машинного обучения, чтобы обеспечить эффективный и комплексный подход к мониторингу качества воды по сравнению с традиционными методами [10].

Основным компонентом информационно-измерительного комплекса является искусственная нейронная сеть (ANN), сложная модель машинного обучения. Используя обширный набор данных, включающий спутниковые снимки и соответствующие измерения параметров качества воды на месте, ANN устанавливает надежную корреляцию между спектральными характеристиками воды (полученными на спутниковых снимках) и различными показателями качества воды. ANN способна точно прогнозировать параметры качества воды на основе спутниковых данных.

Для подготовки и проверки модели ANN авторы использовали обширный набор данных за 22 года, включающий спутниковые снимки Landsat и Sentinel 2 и натурные измерения, полученные от Транснациональной сети мониторинга (TNMN). TNMN, сеть из 101 станции, стратегически расположенных по всему бассейну реки Дунай, двенадцать раз в год собирает данные о качестве воды, предоставляя ценный ресурс для понимания долгосрочных тенденций и характера загрязнения [11].

Модель ANN была успешно обучена для прогнозирования шести важнейших параметров качества воды: хлорофилла-а, взвешенных веществ, мутности, общего содержания азота, общего содержания фосфора и растворенного кислорода. Параметры необходимы для оценки общего состояния здоровья и экологической целостности водных объектов. Способность модели точно оценивать указанные параметры по спутниковым снимкам демонстрирует точность дистанционного зондирования для эффективного и крупномасштабного мониторинга качества воды.

Используя алгоритм ANN, основанный на дистанционном зондировании, авторы добились значительных успехов в развитии области мониторинга качества воды. G. Jakovljevic предлагает многообещающее решение для решения проблем, связанных с традиционными методами на месте, таких как нехватка ресурсов и ограниченный пространственный и временной охват. Поскольку технологии дистанционного зондирования продолжают развиваться, а алгоритмы машинного обучения становятся все более сложными, то можем ожидать еще больших достижений в области мониторинга качества воды.

A. Delgado, C. Briciu-Burghina, F. Regan провели всесторонний обзор стратегий защиты от обрастания датчиков, используемых в мониторинге воды. Защита от обрастания – предотвращение прикрепления нежелательных организмов к поверхности датчиков и их роста на ней, что может значительно ухудшить их работу. Авторы обсудили различные методы борьбы с обрастанием, включая физические, химические и биологические методы. Они также подчеркнули важность выбора подходящих стратегий борьбы с обрастанием, основанных на конкретном типе датчика, водной среде и желаемых целях мониторинга [4].

J. Droujko, I. Alameddine, M. El-Fadel исследовали использование датчиков Landsat ETM+ и OLI для мониторинга качества воды в гиперэвтрофных водоемах. Гиперэвтрофные водоемы характеризуются избыточным содержанием питательных веществ, что приводит к цветению водорослей и другим проблемам с качеством воды [6]. Авторы разработали и апробировали алгоритмы для оценки различных параметров качества воды, таких как содержание хлорофилла-а, взвешенных веществ и мутности, с использованием спутниковых снимков. Они обнаружили, что эти алгоритмы, как правило, применимы к различным периодам времени и типам датчиков, демонстрируя потенциал дистанционного зондирования для долгосрочного мониторинга качества воды.

J. Droujko, F. Kunz, P. Molnar представили разработку датчика мутности с открытым исходным кодом Ötz-T, предназначенного для мониторинга взвешенных отложений в водоемах. Датчик выполнен на основе 3D-печати и использует Arduino shield для простой интеграции с другими системами мониторинга. Авторы подчеркнули важность недорогих решений с открытым исходным кодом для мониторинга качества воды, особенно в развивающихся странах [6].

M. H. Gholizadeh, A. M. Melesse, L. Reddi провели всесторонний обзор методов дистанционного зондирования для оценки параметров качества воды. Они изучили использование различных спутниковых датчиков и методов обработки данных для получения информации о показателях качества воды, таких как содержание хлорофилла-а, мутность и общее количество взвешенных веществ. Авторы подчеркнули преимущества дистанционного зондирования для крупномасштабного долгосрочного мониторинга качества воды и его потенциал в дополнение к традиционным измерениям на месте [7].

T. Goblirsch, T. Mayer, S. Penzel, M. Rudolph, H. Borsdorf описали разработку и применение оптического многопараметрического сенсорного зонда для мониторинга качества воды на месте. Зонд способен измерять множество параметров одновременно, включая pH, растворенный кислород, электропроводность, мутность и содержание хлорофилла-a. Авторы продемонстрировали эффективность датчика для оценки качества воды в различных водных средах в режиме реального времени [8].

H. Gunter, C. Bradley, D.M. Hannah, S. Manaseki-Holland, R. Stevens, K. Khamis сосредоточили внимание на появляющейся области сенсорных технологий на основе флуоресценции для количественной оценки микробного загрязнения питьевой воды. Они проанализировали последние достижения в данной области, подчеркнув потенциал флуоресцентных датчиков для обеспечения быстрого и чувствительного обнаружения микробных патогенов. Авторы обсудили проблемы и возможности, связанные с внедрением датчиков на основе флуоресценции в системах очистки и распределения воды [9].

В целом эти исследования подчеркивают растущую важность передовых технологий для мониторинга качества воды. Дистанционное зондирование, датчики на месте и инновационные аналитические методы играют решающую роль в решении проблем загрязнения воды и обеспечении доступности безопасной питьевой воды.

РЕЗУЛЬТАТЫ

Наше исследование направлено на дальнейшее совершенствование технологий и их интеграцию в комплексные системы мониторинга состояния водных объектов. Предлагается математическая модель водных сред для прикладных задач контроля параметров их загрязнения на основе мультиспектральных изображений.

Модель основана на принципе, что изменение биомассы фитопланктона и соотношения между пигментами в воде приводит к изменениям в спектральных характеристиках отраженного света. То есть свет, падающий на водную поверхность, взаимодействует с различными компонентами воды (включая фитопланктон) и в результате отражается с определенным спектральным составом. Один из ключевых факторов, влияющих на спектральные характеристики воды, – увеличение биомассы фитопланктона. Оно приводит к изменению интенсивности поглощения и рассеяния света в определенных спектральных диапазонах, что отражается в спектре отраженного излучения. Различные пигменты (хлорофилл, фикоцианин и др.), присутствующие в фитопланктоне, имеют свои характерные спектры поглощения. Изменение соотношения между этими пигментами также приводит к изменению спектральных характеристик воды.

Суть модели заключается в получении цифровых изображений исследуемого водного объекта в нескольких спектральных диапазонах. Каждый пиксель такого изображения содержит информацию о количестве света, отраженного от соответствующей точки объекта в каждом из этих диапазонов. Процесс анализа спектральных характеристик водных сред представлен на рисунке 1.

Спектральные характеристики каждого пикселя можно представить в виде вектора в многомерном пространстве, где каждая координата соответствует интенсивности в определенном спектральном канале (пространство называется мультиспектральным).

Координаты точки в мультиспектральном пространстве определяются на основе следующих параметров:

– спектральные характеристики источников излучения определяют спектральный состав падающего на объект излучения. Описывают, какой спектр излучения испускает источник света (например, Солнце, искусственный источник);

– чувствительность камеры описывает её способность регистрировать свет в разных спектральных диапазонах;

– спектральная характеристика коэффициента диффузного отражения объекта характеризует способность объекта отражать свет в разных спектральных диапазонах. Описывает, как объект (в данном случае, водная поверхность) отражает свет в зависимости от длины волны. Именно эта характеристика напрямую связана с составом воды и является ключевым параметром для анализа.

Усовершенствованная математическая модель спектральных характеристик водных сред реализуется при изменении биомассы фитопланктона и соотношения между пигментами. Метод мультиспектрального контроля заключается в анализе цифровых изображений объекта, полученных в соответствующих спектральных диапазонах.

Рисунок 1 – Процесс анализа спектральных характеристик водных сред

Но координаты в мультиспектральном пространстве определяются на основе спектральных характеристик источников излучения $P_j(\lambda_i)$, чувствительности камеры в каждом спектральном канале $m_j(\lambda_i)$ и спектральной характеристики коэффициента диффузного отражения объекта контроля $p(\lambda_i)$:

$$\{M_1 = \sum_{i=1}^{i_{max}} P_1(\lambda_i)\underline{m_1}(\lambda_i)p(\lambda_i)\Delta\lambda\ M_2 = \sum_{i=1}^{i_{max}} P_2(\lambda_i)\underline{m_2}(\lambda_i)p(\lambda_i)\Delta\lambda\ M_n =$$

$$= \sum_{i=1}^{i_{max}} P_n(\lambda_i)\underline{m_n}(\lambda_i)p(\lambda_i)\Delta\lambda\ .$$

Математическая модель одного слоя водной среды с частицами фитопланктона связывает его биофизические и структурные параметры и спектральные характеристики. На основе индикатрис рассеяния частиц фитопланктона $p\ (\theta, \lambda)$ рассчитаны спектральные характеристики фактора анизотропии для частиц разного диаметра:

$$g(\lambda) = \frac{\int_{4\pi}^{0} \times\, p(\theta,\lambda)\cos(\theta) \times d\omega}{\int_{4\pi}^{0} \times\, p(\theta,\lambda) \times d\omega},$$

где $d\omega, cos(\theta)$ – элементарный телесный угол.

Фактор анизотропии $g(\theta, \lambda)$ нужен, чтобы рассчитать эффективный показатель рассеяния $\mu_s'\ (\lambda)$, эффективный показатель ослабления (экстинкцией) $\mu_e'\ (\lambda)$, долю света, рассеянного в переднюю полусферу $F_e(\lambda)$, вероятность выживания фотона $\Lambda_e(\lambda)$. Далее рассчитывается коэффициент диффузного отражения $R_d(\lambda)$ и коэффициент направленного пропускания $T(\lambda)$, которые измеряются мультиспектральными методами в зависимости от схемы реализации средства измерений. Однако эффективный показатель рассеяния зависит от фактора анизотропии $g(\lambda)$ следующим образом:

$$\mu_s' = \mu_s(1 - g(\lambda)).$$

Общее ослабление оптического излучения структуры с учетом потерь за счет поглощения и рассеяния выражается эффективным показателем ослабления (экстинкцией):

$$\mu'_e = \mu_a + \mu'_s ,$$

где μ_a – показатель поглощения среды;

μ'_s– эффективный показатель рассеяния.

Потери интенсивности оптического излучения вследствие рассеяния зависят от формы и размеров рассеивающих частиц. Также часть излучения рассеивается назад, проходит все слои водной среды и попадает на поверхность, а часть рассеивается в прямом направлении и проходит вглубь среды:

$$I(z)I_0 exp(-\mu'_e z),$$

где μ'_e – эффективный показатель ослабления (экстинкция).

На основе анализа и аппроксимации индикатрис с большой степенью вытянутости «вперед» использовано выражение для доли света, рассеянного в переднюю полусферу:

$$F_e(\lambda) = 0{,}5 \int_0^{\pi/2} p(\theta,\lambda) sin\theta d\theta \approx \frac{1-[1-g(\lambda)]}{3}.$$

Оптическая толщина находится по выражению

$$\tau_e(\lambda) = \mu'_e d_e,$$

где d_e – геометрическая толщина.

Вероятность выживания фотона

$$\Lambda_e(\lambda) = \frac{\mu'_s(\lambda)}{\mu'_e(\lambda)}.$$

При малоугловом приближении коэффициент диффузного отражения при освещении по нормали к поверхности имеет вид:

$$R_d(\lambda) = \Lambda_e(\lambda) \frac{1 - F_e(\lambda)}{1 - F_e(\lambda)\Lambda_e(\lambda)} \int_0^1 \left\{1 - \exp\left[\alpha(\lambda) d_e \frac{1+\nu}{\nu}\right]\right\} d\nu,$$

где $\alpha(\lambda) = \mu'_e(\lambda)\big(1 - \Lambda_e(\lambda)F_e(\lambda)\big)$– показатель ослабления в малоугловом приближении;

$\upsilon = cos(\gamma), \gamma$ – угол рассеяния.

Коэффициент направленного пропускания

$$T(\lambda) = exp[-\alpha(\lambda) d_e].$$

Спектральные характеристики показателей поглощения и рассеяния пигментов частиц, а также природной водной среды без зависших частиц вводятся в математическую модель по справочным данным с использованием линейной сплайн-аппроксимации. После проведения математического моделирования получаем зависимости спектральной характеристики коэффициента диффузного отражения или направленного пропускания от определенных параметров водных сред.

Подставив известные значения параметров в математическую модель суспензии частиц, можно получить зависимости коэффициента диффузного отражения $Rd(\lambda)$ от направленного пропускания $T(\lambda)$ суспензии, т. е. решить прямую оптическую задачу. И, соответственно, появляется возможность получить регрессионные уравнения, связывающие значения параметров водной среды и спектральные параметры на определенных длинах волн.

После проведения мультиспектральных измерений с помощью соответствующих технических средств опосредованно измеряют необходимые параметры среды с использованием этих регрессионных уравнений.

Далее рассчитывается вклад для каждого из слоев водной среды в общий коэффициент диффузного отражения на его поверхности, чтобы оценить, на какой глубине влияние на спектральные характеристики станет меньшим погрешности измерения:

$$R_d = \sum_{i=1}^{n} (1 - R_{01})^2 \prod_{j=1}^{i} \quad T^2_{\iota(j-1)} T_{\iota j} R_{\iota j},$$

где R_{01} – составляющая коэффициента отражения на границе воздух – водная среда;

T_ι – коэффициент направленного пропускания слоя природной водной среды;

R_ι – коэффициент диффузного отражения слоя природной водной среды.

Общая схема оценки достоверности мультиспектрального контроля параметров водных сред, полученных после решения обратной оптической задачи, приведена на рисунке 2. Также проводится статистический анализ влияния изменения биомассы и пигментных параметров фитопланктона на спектральные характеристики коэффициента диффузного отражения на поверхности водных сред, размах на рабочих длинах волн спектральных каналов средств мультиспектрального контроля. При этом определяется влияние эффекта локализованного поглощения излучения высшими водными растениями на их спектральные характеристики. Далее рассчитываются оптические характеристики водной среды с учетом воздействия всех слоев.

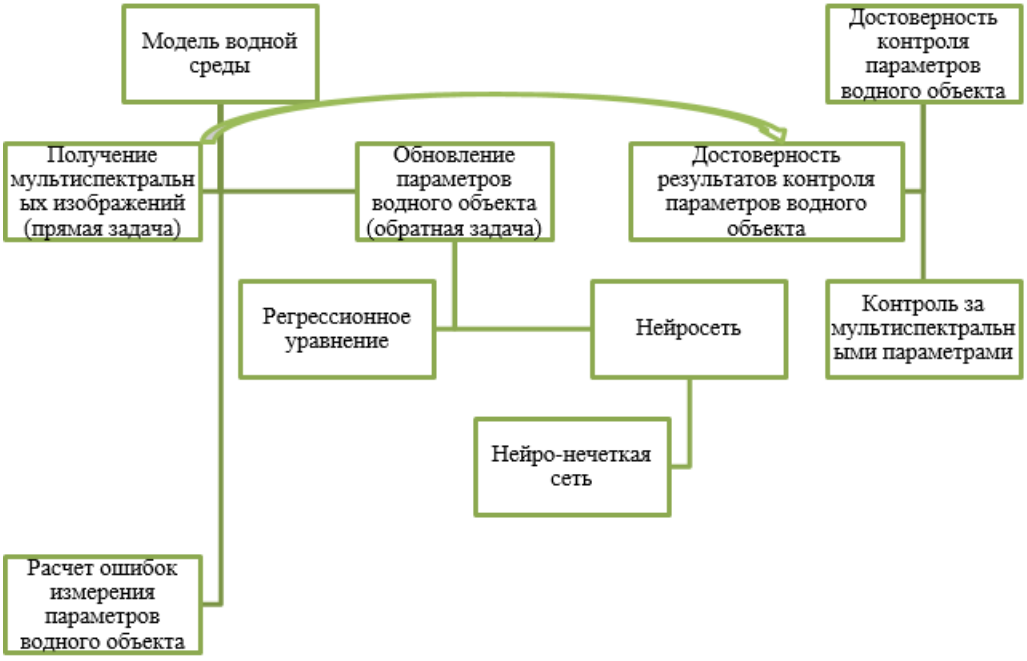


Рисунок 2 – Модель достоверности результатов оценки мультиспектрального контроля параметров водной среды

На основе полученных спектральных характеристик водной среды, с учетом спектральных характеристик камеры, фильтров и источника излучения получаем мультиспектральные параметры в каждом пикселе мультиспектрального изображения. Для получения тест-параметров для водных сред из мультиспектральных изображений необходимо решить обратную оптическую задачу с помощью множественной регрессии, нейронной сети и нейро-нечеткой сети. Другим вариантом реализации мультиспектрального контроля является многопараметрический контроль непосредственно по результатам мультиспектральных измерений без использования регрессионного уравнения.

Разработанная модель может быть интегрирована в систему управления информационно-измерительным комплексом, так как мультиспектральные изображения, полученные с помощью спутников или беспилотных летательных аппаратов, передаются в систему. Алгоритм, основанный на предложенной модели, обрабатывает изображения и вычисляет необходимые параметры качества воды. Полученные данные анализируются на предмет выявления отклонений от нормы и прогнозирования развития ситуации. На основе результатов анализа принимаются решения о необходимости проведения дополнительных исследований, корректировки технологических процессов или других мер по охране окружающей среды.

Преимущества использования предложенной модели:

1. Модель основана на анализе изображений в различных спектральных диапазонах, чтобы получить детальную информацию о составе и состоянии воды, а также напрямую связана с задачей мониторинга водных объектов, где необходимо оценить качество воды, наличие загрязнений и т. д.
2. Модель учитывает влияние фитопланктона и его пигментов на спектральные характеристики воды и оценивает биологическую продуктивность водоема, наличие цветения воды и другие экологические показатели, что является важной составляющей мониторинга.
3. Разработана математическая модель, связывающая спектральные характеристики с физическими параметрами воды, чтобы перейти от спектральных данных к количественным характеристикам загрязнения, что необходимо для принятия управленческих решений.

ЗАКЛЮЧЕНИЕ

Таким образом, предложенный алгоритм открывает новые перспективы для развития систем мониторинга водных объектов и может внести значительный вклад в обеспечение безопасности и экологической устойчивости водных экосистем. Усовершенствованная математическая модель спектральных характеристик водных сред представляет собой мощный инструмент для изучения и мониторинга состояния водоемов. Ее применение дает возможность получать объективную и оперативную информацию о качестве воды, что необходимо для принятия обоснованных решений в области охраны окружающей среды и рационального использования водных ресурсов. Также предложенная модель спектральных характеристик водных сред представляет собой перспектив-

ный инструмент для мониторинга состояния водных объектов. Ее применение повысит эффективность контроля за качеством воды, поможет принимать обоснованные управленческие решения и обеспечивать устойчивое развитие водных экосистем. Разработанная модель открывает новые возможности для развития систем мониторинга водных объектов.

Исследование вносит вклад в область мониторинга качества воды, предлагая надежный и эффективный инструмент для оценки здоровья водных экосистем. Предлагаемый алгоритм может улучшить практику управления водными ресурсами и способствовать защите водных ресурсов.

Список источников

1. Серебрицкий, И. А. Территориальная система мониторинга поверхностных вод водных объектов в Санкт-Петербурге / И. А. Серебрицкий, Д. Т. Азёмов, Н. А. Жигунова, Е. С. Бородин // Окружающая среда. 2024. – URL: https://ecopeterburg.ru/2024/01/20/(дата обращения: 12.10.2024).

2. Соколов, Б. В. Математическая модель и алгоритм совместного планирования измерительных и вычислительных операций при мониторинге обстановки в локальной акватории / Б. В. Соколов, В. А. Палицын, Д. И. Назаров // Завалишинские чтения 17 : сборник докладов. Санкт-Петербург, 10–14 апреля 2017 года. – Санкт-Петербург : Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2017. – С. 81–87.

3. Юхно, А. И. Исследование алгоритма работы информационно-измерительной и управляющей системы контроля качества питьевой воды / А. И. Юхно // Измерение. Мониторинг. Управление. Контроль. – 2019. – № 4 (30). – С. 5–11.

4. Delgado, A. Antifouling strategies for sensors used in water monitoring: Review and future perspectives / A. Delgado, C. Briciu-Burghina, F. Regan // Sensors (Switzerland). – 2021. – № 21. – P. 1–25. DOI: 10.3390/s21020389.

5. Deutsch, E. S. Monitoring water quality in a hypereutrophic reservoir using Landsat ETM+ and OLI sensors: how transferable are the water quality algorithms? / E. S. Deutsch, I. Alameddine, M. El-Fadel // Environ. Monit. Assess. – 2018. – № 190 (3). – P. 141–154. – DOI: 10.1007/s10661-018-6506-9.

6. Droujko, J. Ötz-T: 3D-printed open-source turbidity sensor with Arduino shield for suspended sediment monitoring / J. Droujko, F. Kunz, P. Molnar. – 2023. – Vol. 13. – P. 1–15. – DOI: 10.1016/j.ohx.2023.e00395.

7. Gholizadeh, M. H. A comprehensive review on water quality parameters estimation using remote sensing techniques / M. H. Gholizadeh, A. M. Melesse, L. Reddi // Sensors (Switzerland). – 2016. – № 16. – P. 1298. – DOI: 10.3390/s16081298.

8. Goblirsch, T. In situ water quality monitoring using an optical multiparameter sensor probe / T. Goblirsch, T. Mayer, S. Penzel, M. Rudolph, H. Borsdorf. – 2023. – № 23 (23). – P. 9545. – DOI: 10.3390/s23239545.

9. Gunter, H. Advances in quantifying microbial contamination in potable water: Potential of fluorescence-based sensor technology / H. Gunter, C. Bradley, D. M. Hannah, S. Manaseki-Holland, R. Stevens, K. Khamis // Wiley Interdiscip. Rev. – 2023. – Vol. 10. – P. 1–19. – DOI: 10.1002/wat2.1622.

10. Jakovljevic, G. Remote sensingbased algorithm for monitoring water quality of inland water bodies / G. Jakovljevic, M. Govedarica, F. Alvarez-Taboada // Conference: 41st EARSeL Symposium 6 th EARSeL Workshop on Developing. – 2022. – P. 1–20. – DOI: 10.1175/JCLI-D-20- 0311.1.

11. Jakovljevic, G. Long-Term Monitoring of Inland Water Quality Parameters Using Landsat Time-Series and Back-Propagated ANN: Assessment and Usability in a Real-Case Scenario / G. Jakovljevic, F. Álvarez-Taboada, M. Govedarica // Remote Sens. – 2024. – № 16. – P. 68. https://doi.org/10.3390/rs16010068.

12. Sokolov, B. V. Mathematical model and algorithm of operation scheduling for monitoring situation in local waters / B. V. Sokolov, V. A. Palitsyn, D. I. Nazarov // MATEC Web of Conferences. – 2017. – P. 113–120. – DOI: 02012.10.1051/matecconf/201711302012.

References

1. Serebritsky, I. A., Azemov, D. T., Zhigunova, N. A., Borodin, E. S. Territorial system for monitoring surface waters of water bodies in St. Petersburg. *Environment*, 2024. Available at: https://ecopeterburg.ru/2024/ (accessed 12.10.2024) (In Russ.).

2. Sokolov, B. V., Palitsyn, V. A., Nazarov, D. I. Mathematical model and algorithm for joint planning of measuring and computing operations when monitoring the situation in a local water area. *Zavalishinskie readings 17 : collection of reports. St. Petersburg, April 10–14, 2017.* St. Petersburg, St. Petersburg State University of Aerospace Instrumentation, 2017, pp. 81–87 (In Russ.).

3. Yukhno, A. I. Study of the algorithm for the operation of the information, measuring and control system for monitoring the quality of drinking water. *Measurement. Monitoring. Management. Control*, 2019, no. 4 (30), pp. 5–11 (In Russ.).

4. Delgado, A., Briciu-Burghina, C., Regan, F. Antifouling strategies for sensors used in water monitoring: Review and future perspectives. *Sensors (Switzerland)*, 2021, no. 21, pp. 1–25. DOI: 10.3390/s21020389.

5. Deutsch, E. S., Alameddine, I., El-Fadel, M. Monitoring water quality in a hypereutrophic reservoir using Landsat ETM+ and OLI sensors: how transferable are the water quality algorithms? *Environ. Monit. Assess*., 2018, no. 190 (3), pp. 141–154. DOI: 10.1007/s10661-018-6506-9.

6. Droujko, J., Kunz, F., Molnar, P. *Ötz-T: 3D-printed open-source turbidity sensor with Arduino shield for suspended sediment monitoring*, 2023, vol. 13, pp. 1–15. DOI: 10.1016/j.ohx.2023.e00395.

7. Gholizadeh, M. H., Melesse, A. M., Reddi, L. A comprehensive review on water quality parameters estimation using remote sensing techniques. *Sensors (Switzerland)*, 2016, no. 16, p. 1298. DOI: 10.3390/s16081298.

8. Goblirsch, T., Mayer, T., Penzel, S., Rudolph, M., Borsdorf, H. *In situ water quality monitoring using an optical multiparameter sensor probe*, 2023, no. 23 (23), p. 9545. DOI: 10.3390/s23239545.

9. Gunter, H., Bradley, C., Hannah, D. M., Manaseki-Holland, S., Stevens, R., Khamis, K. Advances in quantifying microbial contamination in potable water: Potential of fluorescence-based sensor technology. *Wiley Interdiscip. Rev.*, 2023, vol. 10, pp. 1–19. DOI: 10.1002/wat2.1622.

10. Jakovljevic, G., Govedarica, M., Alvarez-Taboada, F. Remote sensingbased algorithm for monitoring water quality of inland water bodies. *Conference: 41st EARSeL Symposium 6th EARSeL Workshop on Development*, 2022, pp. 1–20. DOI: 10.1175/JCLI-D-20-0311.1.

11. Jakovljevic, G., Álvarez-Taboada, F., Govedarica, M. Long-Term Monitoring of Inland Water Quality Parameters Using Landsat Time-Series and Back-Propagated ANN: Assessment and Usability in a Real-Case Scenario. *Remote Sens.*, 2024, no. 16, p. 68. https://doi.org/10.3390/rs16010068.

12. Sokolov, B. V., Palitsyn, V. A. Nazarov, D. I. Mathematical model and algorithm of operation scheduling for monitoring situation in local waters. *MATEC Web of Conferences*, 2017, pp. 113–120. DOI: 02012. 10.1051/matecconf/201711302012.

Статья поступила в редакцию 27.10.2024; одобрена после рецензирования 29.11.2024; принята к публикации 13.12.2024.

The article was submitted 27.10.2024; approved after reviewing 29.11.2024; accepted for publication 13.12.2024.

УДК 004.3

РАЗРАБОТКА АППАРАТНОЙ ПЛАТФОРМЫ ДЛЯ СИСТЕМЫ УПРАВЛЕНИЯ ПОЛИВОМ СЕЛЬСКОХОЗЯЙСТВЕННЫХ УЧАСТКОВ

Старов Дмитрий Владимирович, Астраханский государственный университет имени В. Н. Татищева, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а,
старший преподаватель кафедры технологии материалов и промышленной инженерии, ORCID: 0009-0002-0377-3044, e-mail: bortv715ke@mail.ru

В статье представлена разработка аппаратной платформы для системы управления поливом сельскохозяйственных участков, направленная на оптимизацию процессов орошения и повышение эффективности использования водных ресурсов. Рассматриваются ключевые аспекты проектирования, включая выбор датчиков для мониторинга влажности почвы, системы управления и передачи данных. Описываются технические характеристики платформы, а также ее интеграция с современными технологиями, что позволяет обеспечить удаленный доступ к данным и управлению системой полива. В результате проведенных испытаний подтверждается эффективность предложенного решения, что может существенно повлиять на агрономическую практику, повысить урожайность и снизить затраты на водоснабжение.

Ключевые слова: умное земледелие, контроль микроклимата почвы, система управления поливом, сельскохозяйственные культуры

Финансирование: *исследование выполнено при поддержке Программы развития Астраханского государственного университета (Приоритет-2030)».*

DEVELOPMENT OF A HARDWARE PLATFORM FOR A SYSTEM FOR CONTROLLING IRRIGATION OF AGRICULTURAL AREAS

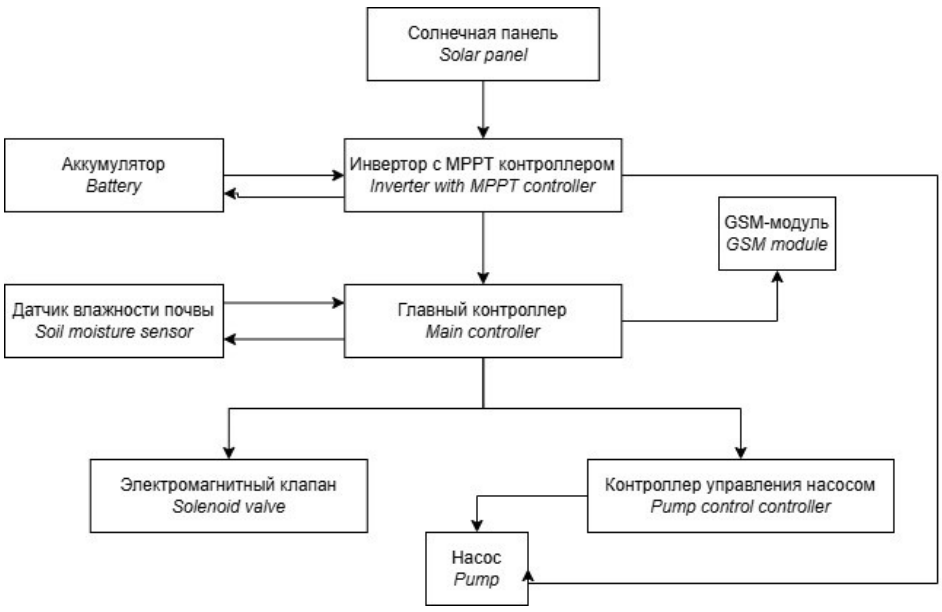
Starov Dmitriy V., Astrakhan Tatishchev State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation,
Senior Lecturer of the Department of Materials Technology and Industrial Engineering, ORCID: 0009-0002-0377-3044, e-mail: bortv715ke@mail.ru

The article presents the development of a hardware platform for an agricultural irrigation management system aimed at optimizing irrigation processes and increasing the efficiency of water resource use. Key design aspects are considered, including the selection of sensors for soil moisture monitoring, control systems, and data transmission. The technical characteristics of the platform are described, as well as its integration with modern technologies, which allows for remote access to data and irrigation system management. The tests confirm the effectiveness of the proposed solution, which can significantly affect agronomic practice, increase crop yields, and reduce water supply costs.

Keywords: smart farming, soil microclimate control, irrigation control system, crops

Financial support: *this research was supported by the Astrakhan State University Development Program (Priority-2030)».*

Graphical annotation (Графическая аннотация)



ВВЕДЕНИЕ

Любая среда выращивания растений представляет собой сложную нелинейную систему, которая должна обеспечить растениям подходящий климат. К сожалению, на хозяйственных участках не всегда получается создать оптимальные условия. Удаленность сельскохозяйственных участков от места постоянного проживания также вызывает трудности с регулярным поливом. В результате этого растения находятся в неблагоприятной среде выращивания [1–3].

На большинстве сельскохозяйственных участков отсутствует автоматизированная система полива. Участки поливаются по расписанию благодаря насосу, который качает воду либо с центральной системы водоснабжения, либо с реки, поэтому учитывать индивидуальные потребности растений крайне сложно.

В связи с текущими проблемами в сельском хозяйстве, такими как изменение климата, истощение ресурсов и потребление воды, автоматизация полива полей становится не только актуальной, но и необходимой для устойчивого развития аграрной отрасли. Внедрение автоматизированных систем позволяет существенно сократить трудозатраты на полив, освобождая агрономов и рабочих от рутинных задач и позволяя им сосредоточиться на более важных аспектах управления хозяйством [4–8].

Современные технологии полива, такие как капельный и распылительный полив, способствуют улучшению условий для роста растений. Новизна предлагаемого решения заключается в построении интеллектуальной системы контроля микроклимата почв, которая на основании показаний с разработанных датчиков, прогноза погоды и временных изменений погодных условий посредством нейросети будет осуществлять полив определенных зон сельскохозяйственных полей.

АНАЛИЗ ОБЪЕКТА ИССЛЕДОВАНИЯ

В рамках исследования рассматривается проектирование электронной системы регулирования поливочной системы для участка прямоугольной формы. Размеры участка – 190х260 м. Данный участок состоит из участка с виноградом с габаритами 100х30 м, а также сада, в котором выращиваются фрукты.

Эскиз хозяйственного участка представлен на рисунке 1.

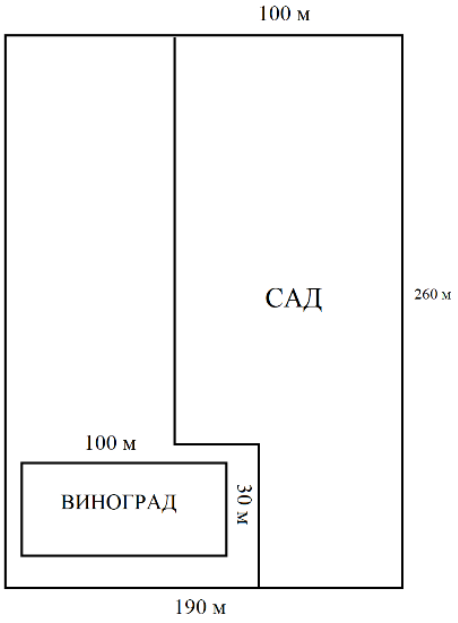


Рисунок 1 – Эскиз сельскохозяйственного участка

Сад разделен на 18 рядов, в которых выращиваются:

- ряды 1 и 2 – вишня;
- ряды 3 и 18 – абрикосы;
- ряды 4 и 5 – персики;
- с 6 по 11 ряд и ряд 15 – яблони;
- с 12 по 14 ряд и ряд 16 – груши;
- ряд 17 – черешня.

На данном участке аллювиальная и суглинистая почва. Аллювиальные почвы являются плодородными почвами. Они сформировались на бывших руслах рек, дельтах и поймах. Во время наводнений эти территории затапливаются. Аллювиальные отложения – это отложения кластического

происхождения, такие как песок или глина, которые приносятся на территорию с наводнением. Они сразу же вовлекаются в процесс почвообразования и способствуют формированию пойменных почв. Суглинистые почвы являются наиболее плодородными почвами и используются для садоводства и крупномасштабных посевов при условии, что в ней присутствует баланс песчаного и горного компонента. В них содержится достаточное количество гумуса и ила, а также других составляющих, которые необходимы для того, чтобы получить богатый урожай.

Существуют распространенные ошибки при проливе: ненормированный и слишком частый. В случае недостаточного полива происходит только поверхностная насыщенность водой, в результате чего корни не прорастают в глубину. При переливе корни загнивают, а растение гибнет. В условиях частых поливов корням не нужно углубляться, чтобы получить воду и питательные вещества. Они растут поверхностно, а это ухудшает их морозостойкость [9–12].

На данном участке деревья поливаются по расписанию (3 раза в неделю). Поэтому нет возможности учитывать индивидуальные потребности деревьев: влажность почвы, нормы полива и частота. Ниже представлена таблица необходимых параметров, которые нужно учитывать (табл. 1).

Таблица 1 – Необходимые параметры для полива деревьев на участке

Название	Необходимая влажность, %	Норма полива, л	Возраст	Частота полива
Вишня	60–70	От 30 до 50	4–5 лет	1 раз в неделю
Абрикос	50–60	От 20 до 30	5	1 раз в неделю
Персик	50–70	От 20 до 30	5	1 раз в неделю
Яблоня	60–80	От 15 до 20	5	1 раз в неделю
Груша	50–60	От 20 до 25	5	1 раз в неделю
Черешня	60–80	От 15 до 25	5	1 раз в неделю

Возникает необходимость в разработке системы регулирования поливочной системы для заданного участка.

РАЗРАБОТКА СИСТЕМЫ УПРАВЛЕНИЯ ПОЛИВОМ

Разрабатываемая система должна соответствовать следующим требованиям:

1. Система должна быть надежной и защищенной от перегрева и перенапряжения.
2. Система должна иметь возможность регулировать частоту и длительность полива для оптимизации потребления воды и минимизации потерь, расходов на воду.
3. Требования к системе должны быть совместимы с местными климатическими условиями, такими как интенсивность солнечного света и температура.
4. Система должна иметь возможность дистанционного управления для облегчения контроля и мониторинга.
5. Система управления должна быть способна автоматически контролировать и управлять подачей воды в ирригационную систему.
6. Солнечные модули должны иметь достаточный КПД для питания всей системы орошения.

Разработка схемы электрической структурной силовой части полива сельскохозяйственного участка

Описываемый принцип работы разрабатываемой электронной системы регулирования поливочной системы базируется на передаче показаний с датчиков почвы, которые измеряют температуру среды, уровень освещения и влажность, на главный контроллер.

В случае обнаружения недостаточной влажности почвы, отсутствия прямых солнечных лучей или снижения показаний температуры окружающей среды, система регулирует мощность насоса путем изменения амплитуды питающей синусоиды с помощью ОВЕН СУНА-122 и открывает соответствующие электромагнитные клапаны, чтобы обеспечить необходимое количество влаги для растений [13–16].

Исходя из функционального назначения устройства была разработана схема структурная (рис. 2).

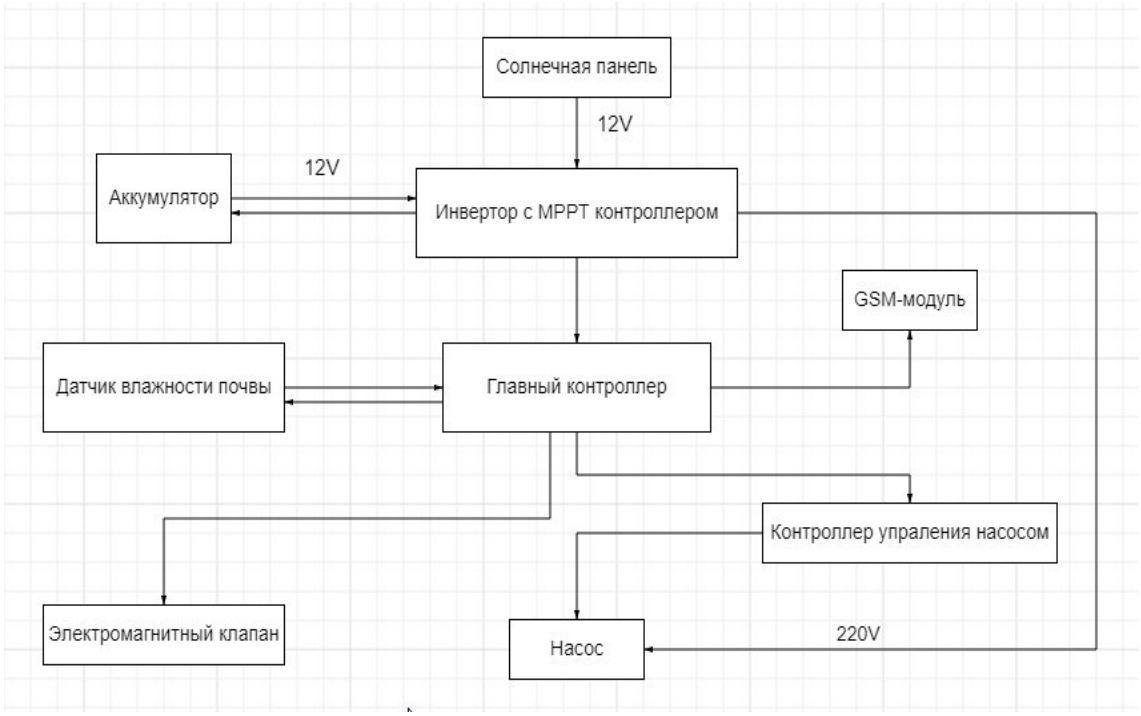


Рисунок 2– Структурная схема электронной системы регулирования поливочной системы от солнечных модулей

Разработанная структурная схема включает в себя: основной контроллер Attiny13, контроллер управления насосом ОВЕН СУНА-122, насос DAB JET 92M, электромагнитный клапан Bi-Stable 3V-12V, аккумулятор SunStonePower ML 150 AH 12B AGM, инвертор Sunways UMX II MPPT 1012, солнечная панель 4,5 кВт.

Микроконтроллер играет ключевую роль в устройстве, поскольку он выполняет функции сбора и обработки информации с датчика, генерации управляющих сигналов для исполнительного блока, настройки необходимых параметров и вывода информации на дисплей. При выборе микроконтроллера следует учитывать возможность расширения функционала путем подключения дополнительного оборудования [17–19].

Основные технические составляющие: быстродействие, объем оперативной памяти и Flash-памяти.

Таблица 2 – Сравнительные характеристики микроконтроллеров

Микроконтроллер	ATtiny13	ATtiny85	ATmega168
Тактовая частота, МГц	20	20	20
ОЗУ, кБ	1	8	16
EEPROM, байт	64	512	512
Цифровые линии ввода/вывода, кол-во	6	6	23
Аналоговые входы, кол-во	4	4	6
Напряжение питания	2,7... 5,5 4,5... 5,5	2,7…5,5 4,5…5,5	2,7…5,5
Рабочая частота	0... 10 0... 20	0…10 0…20	20
Цена, руб.	80	150	200

Данный сравнительный анализ характеристик показал, что с учетом нашей технической и экономической задачи будет достаточно управляющего контроллера на базе экономичного ATtiny13.

ATtiny13 предлагает ряд характеристик, среди которых важно отметить следующие: встроенная программируемая Flash-память программы объемом 1 КБ, EEPROM-память данных на 64 байта, статическое ОЗУ (SRAM) размером также 64 байта. Кроме того, этот микроконтроллер обладает 6 линиями ввода-вывода общего назначения, 32 рабочими регистрами общего назначения и 8-битным таймером/счетчиком с функцией сравнения. Он также поддерживает внутренние и внешние источники прерываний, 4-канальный 10-битный АЦП и программируемый сторожевой таймер с встроенным

генератором. Кроме того, ATtiny13 предлагает три программно инициализируемых режима энергосбережения, включая режим ожидания (Idle), в котором ядро останавливается, но ОЗУ, таймер/счетчик, АЦП, аналоговый компаратор и система прерываний продолжают работать в прежнем режиме. В режиме отключения питания (Power-down) регистры сохраняют значения, но генератор останавливается, полностью блокируя функциональность устройства до последующего прерывания или же аппаратного сброса. Наконец, режим снижения шумов АЦП (ADC Noise Reduction) позволяет остановить вычислительное ядро, сохраняя при этом функциональность всех модулей ввода-вывода, за исключением АЦП, что способствует минимизированию шумов при выполнении преобразования [20, 21].

Устройство было разработано с использованием высокоплотной энергонезависимой памяти технологии компании Atmel. Оно поддерживает программу-загрузчик, работающий на AVR ядре, а также обычный программатор энергонезависимой памяти с встроенной флэш-памятью, который поддерживает внутрисистемное программирование (ISP).

ATtiny13 совместим с широким спектром программных средств и интегрированных средств разработки, включая компиляторы языка C, макроассемблеры, программные отладчики/симуляторы, внутрисхемные эмуляторы и оценочные наборы. Он также обеспечивает полную совместимость с интегрированными средствами разработки.

Разработка датчика почвы

Для измерения влажности почвы можно использовать электронные, резистивные или емкостные датчики влажности. Стоит отметить, что для автоматизации полива загородного участка наиболее подходящими являются емкостные датчики влажности, которые обладают достаточной точностью и низкой стоимостью.

Однако емкостные датчики недостаточно функциональны. Недостатками являются отсутствие возможности измерить температуру среды и уровень освещенности.

По этой причине был разработан датчик почвы, который соответствует необходимым параметрам для должного функционирования электронной системы регулирования поливочной системы. Принципиальная схема датчика почвы показана на рисунке 3.

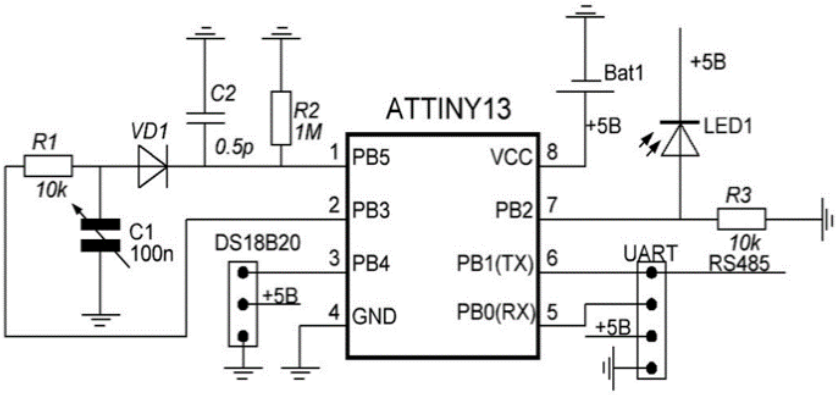


Рисунок 3 – Принципиальная схема датчика почвы

Для создания схемы датчика почвы применяется контроллер DD2 (Attiny13), который основан на принципе измерения емкости между контактами. Изменение емкости происходит в зависимости от проницаемости среды.

Цифровой датчик DS18B20 обеспечивает измерение температуры в широком диапазоне (–55 °C до 125 °C) с точностью до 12 бит. Эта функция позволяет контролировать и регулировать температуру различных материалов, веществ и других объектов в технологических процессах, что является важным условием для обеспечения их безопасности.

Фоторезистор LED1 необходим для измерения уровня освещенности. Дорожки датчика, погруженные в почву, являются конденсатором C1. Диод VD1 используется как диод выпрямитель, а C2 – как сглаживающий конденсатор.

На рисунке 4 представлен внешний вид разработанного датчика влажности почвы.

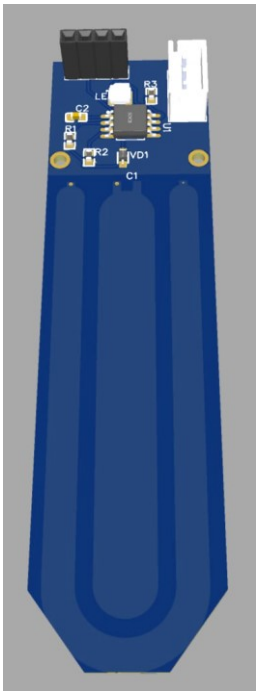


Рисунок 4 – Внешний вид разработанного датчика

Для повышения эффективности дистанционного сбора информации о микроклимате почв также был разработан дополнительный датчик, который будет установлен на равноудаленном расстоянии и по «цепочке» будут передавать показания на контроллер в режиме реального времени. Датчик основан на энергоэффективном микроконтроллере ESP32 и может работать в автономном режиме достаточно большое время. На рисунке 5 представлен внешний вид разработанного датчика.

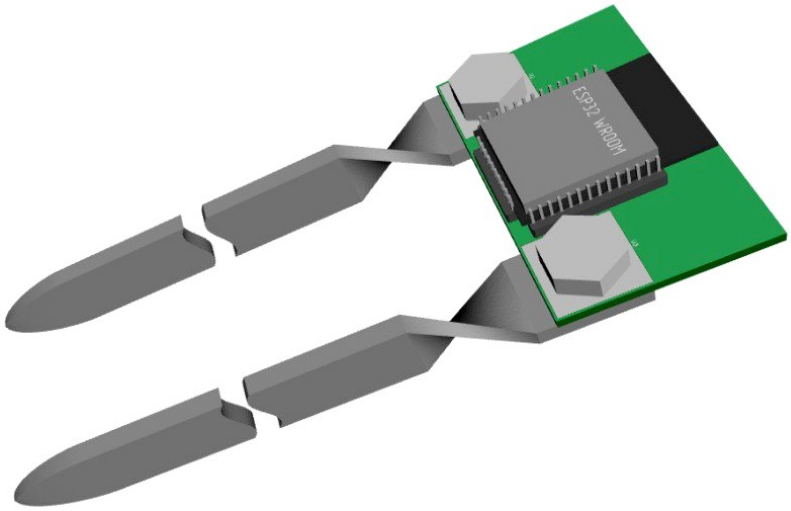


Рисунок 5 – Внешний вид датчика микроклимата почв

Предполагается, что датчик будет устанавливаться на глубину до 50 сантиметров в глубину и резистивным способом производить измерения необходимых параметров почвы. Также используя внутренний генератор, посредством измерения диапазона частот импульсов производить измерение кислотности и загрязненности почв.

Разработка схемы электрической принципиальной

Созданная на базе управляющего контроллера DD2 (Attiny13) схема датчика – почвы – обладает рядом преимуществ. Attiny13 является низкопотребляющим 8-битным микроконтроллером с AVR-RISC-архитектурой (рис. 6).

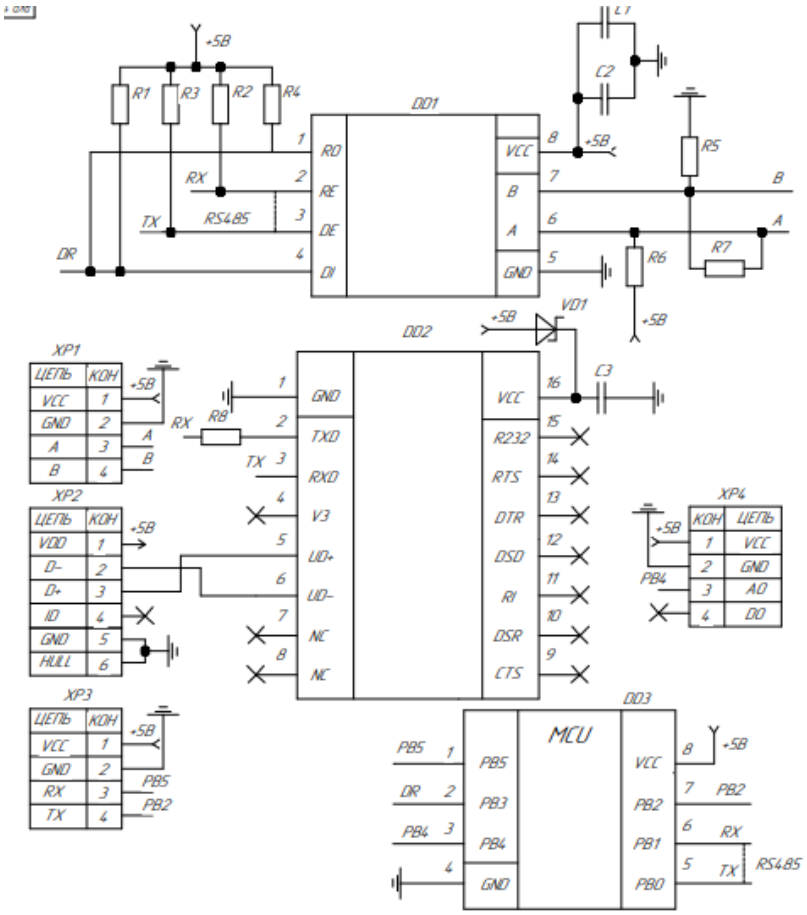


Рисунок 6 – Принципиальная схема

Он способен выполнять команды за один цикл, что позволяет достичь производительности 1 MIPS при частоте задающего генератора 1 МГц и оптимизировать отношение потребления к производительности.

Для измерения показаний с минимальными погрешностями и исключения шумов используется генератор частот ряда высоких импульсов на микросхеме DD1 (NE555) с частотой порядка 5 кГц. Это устройство предназначено для формирования одиночных и повторяющихся импульсов со стабильными временными характеристиками. Частота выходного сигнала определяется обвязкой C1, C2, R1, R2.

Используется диод-выпрямитель VD1 (1N4148WS) и сглаживающий конденсатор C3.

Как уже было сказано, дорожки датчика, погруженные в почву, являются конденсатором (C4), емкость между обкладками которого зависит от среды, в которую его поместили. Чем выше емкость у этого конденсатора, тем больше падение напряжения на резисторе (R3) и тем меньшее напряжение пойдет через диод на аналоговый выход микросхемы (PD5).

Схема аналогична простейшему делителю напряжения, только за место второго резистора используется конденсатор со своим реактивным сопротивлением.

Для определения уровня освещенности используется фоторезистор LDR1, который является резистором, изменяющим свое сопротивление при воздействии света. Считывание аналогового значения осуществляется с помощью этого элемента.

Микросхема DD3 (CH340C) используется для прошивки управляющего контроллера Attiny13 через USB. Она имеет корпус SOIC-16 и встроенный тактовый генератор, но не имеет серийного номера. Микросхема также обеспечивает дополнительный интерфейс RS232, RS485, RS422 и другие интерфейсы через внешнюю микросхему преобразования напряжения.

В нашей разработке используется точный датчик DS18B20, работающий по протоколу 1-Wire, который предназначен для измерения температуры окружающей среды. Это низкоскоростная шина связи, созданная компанией Dallas Semiconductor (впоследствии приобретенной компанией Maxim Integrated). Особенностью этой шины является использование одной и той же пары проводов как для питания устройств, так и для обмена данными.

Микросхема DD4 (MAX485) необходима для передачи данных между текущим контроллером (slave) и управляющим (master) по протоколу RS485.

Все резисторы, используемые в обвязке контроллера, являются подтягивающими по питанию. С6 и С7 – сглаживающие конденсаторы.

Связь между датчиками почвы и главным контроллером будет осуществляться по RS485 (дальность до 800 м).

Кабели «витая пара» с двумя клеммами «А» и «В» используются для объединения устройств через интерфейс RS-485. Чтобы объединить клеммы в общую сеть, применяется цепочка кабелей, проложенных от одного устройства к другому. Обычно применяются кабели, содержащие как минимум две пары проводов, хотя для передачи данных достаточно одной пары, чтобы обеспечить более надежную передачу данных.

Для подавления помех кабели обычно экранируются, а экраны на всей линии должны быть соединены между собой. На устройствах, которые соединяются, помимо клемм «А» и «В», имеется дополнительная клемма «COM», чтобы обеспечить соединение экранов. Линию следует заземлить только в одной точке, обычно в месте расположения контроллера, модема или компьютера. Заземление в двух точках запрещено, чтобы избежать наводок, вызванных различиями в потенциале на экране.

ЗАКЛЮЧЕНИЕ

Разработка аппаратной платформы для системы управления поливом сельскохозяйственных участков представляет собой важный шаг в направлении оптимизации аграрного производства и повышения его эффективности. Создание такой системы не только способствует рациональному использованию водных ресурсов, но и позволяет фермерам более точно контролировать условия роста растений, что, в свою очередь, может значительно увеличить урожайность. Внедрение современных технологий в агрономию открывает новые горизонты для сельского хозяйства, обеспечивая устойчивое развитие и минимизацию негативного воздействия на окружающую среду. Эффективная аппаратная платформа, интегрированная с современными датчиками и системами управления, станет неотъемлемой частью умного сельского хозяйства, способствуя более осознанному и экономически выгодному подходу к ведению аграрного бизнеса. Таким образом, реализация данной разработки имеет значительный потенциал для трансформации подходов к поливу, что в конечном итоге приведет к улучшению качества жизни сельских жителей и обеспечению продовольственной безопасности в регионе.

Список источников

1. F. Rodríguez, M. Modelling and Control for Greenhouse Crop Growth / F. Rodríguez, M. Berenguel, J. L. Guzmán, A. Ramírez. – London : Springer, 2015. – 56 p.

2. Khoshnevisan, B. Application of multi-layer adaptive neuro-fuzzy inference system for estimation of greenhouse strawberry yield / D. Khoshnevisan, S. Rafiee, H. Mousazadeh // Measurement. – 2014. – № 47. – P. 903–910.

3. Liu, L. Design and testing of a solar-powered irrigation system with a variable-frequency water pump for crops / L. Liu et al. // Renewable Energy. – 2017. – Vol. 113. – P. 1227–1236.

4. Radojević, N. Microclimate control in greenhouses / N. Radojević, D. Kostadinović, H. Vlajković, E. Veg // FME Trans. – 2014. – Vol. 42. – P. 167–171.

5. Ажмухамедов, И. М. Инвариантная онтологическая модель процесса обеспечения комплексной безопасности прикаспийских регионов / И. М. Ажмухамедов, В. А. Корякова // Caspium Securitatis: журнал каспийской безопасности. – 2022. – Т. 2, № 2. – С. 11–22. – DOI: 10.54398/2713024X_2022_2_2_11.

6. Авдеенко, К. А. Анализ возможностей автоматизированной системы капельного полива / К. А. Авдеенко, Е. В. Заргарян. – 2020.

7. Абделфаттах, А. Х. Управление орошением почвы с использованием датчиков влажности / А. Х. Абделфаттах, Д. Т. Халиуллин, И. М. Гомаа // Современное состояние, проблемы и перспективы развития механизации и технического сервиса агропромышленного комплекса. – 2018. – С. 18–26.

8. Березина, А. А. Разработка структуры адаптивной системы управления микроклиматом растительного террариума / А. А. Березина, А. И. Денисенко, Ю. В. Коноплев, Д. Б. Арефьева // Техника. Космос : труды тринадцатой общерос. молодежн. науч.-техн. конф. : в 2 т. / Балт. гос. техн. ун-т. – Санкт-Петербург, 2021. – Т. 2. – С. 27–32.

9. Болотин, Д. А. К методике расчета систем капельного орошения / Д. А. Болотин // Орошаемое земледелие. – 2016. – № 3. – С. 17–18.

10. Варзар, Р. Л. Датчик температуры и влажности почвы / Р. Л. Варзар. – 2020.

11. Грабовецкая, К. А. Обзор солнечных панелей для систем автономного питания / К. А. Грабовецкая и др. // Молодой ученый. – 2016. – № 22–3. – С. 29–32.

12. Гусаров, А. В. Проектирование печатных плат в САПР DipTrace / А. В. Гусаров. – Рыбинск : РГАТУ им. П. А. Соловьева, 2018. – Ч. 2: Проектирование простой печатной платы. – 181 с.

13. Гулина, Е. Р. Устройство для дистанционного контроля влажности и температуры почвы / Е. Р. Гулина. – 2018.

14. Данникер, А. А. Особенности использования капельного полива / А. А. Данникер и др. // Инновационные технологии в АПК как фактор развития науки в современных условиях. – 2019. – С. 77–81.

15. Дебрин, А. С. Обзор солнечных панелей и фотоэлектрических станций отечественных производителей / А. С. Дебрин, А. В. Бастрон, В. Н. Урсегов // Вестник Красноярского государственного аграрного университета. – 2018. – № 6 (141). – С. 136–141.

16. Иванов, Б. Л. Автоматизированная система управления полива теплиц / Б. Л. Иванов и др. // Научное сопровождение технологий агропромышленного комплекса: теория, практика, инновации. – 2020. – С. 306–309.

17. Истомина, Е. Е. Программа производства и применения систем автоматического полива растений «Умный дом» / Е. Е. Истомина, М. Н. Куранов // Сельскохозяйственные науки и агропромышленный комплекс на рубеже веков. – 2014. – № 8.

18. Корнилова, Г. С. Анализ датчиков влажности почвы для систем автоматического полива / Г. С. Корнилова, М. Ю. Егоров // Актуальные проблемы науки в области АПК. – 2021. – С. 28–31.

19. Клушин, К. П. Система программируемого полива / К. П. Клушин. – 2018.

20. Муровский, С. П. Разработка блока управления автоматической системы дистанционного полива / С. П. Муровский, А. С. Муровская, Г. Л. Павленко // Успехи современной науки и образования. – 2017. – Т. 4, № 3. – С. 116–133.

21. Нагаев, Д. А. Обзор современных солнечных панелей / Д. А. Нагаев // Вестник современных исследований. – 2018. – № 6.3. – С. 530–534.

References

1. Rodríguez, F., Berenguel, M., Guzmán, J. L., Ramírez, A. *Modeling and Control for Greenhouse Crop Growth.* London, Springer, 2015. 56 p.

2. Khoshnevisan, B., Rafiee, S., Mousazadeh, H. Application of multi-layer adaptive neuro-fuzzy inference system for estimation of greenhouse strawberry yield. *Measurement*, 2014, no. 47, pp. 903–910.

3. Liu, L., et al. Design and testing of a solar-powered irrigation system with a variable-frequency water pump for crops. *Renewable Energy*, 2017, vol. 113, pp. 1227–1236.

4. Radojević, N., Kostadinović, D., Vlajković, H., Veg E. Microclimate control in greenhouses. *FME Trans.*, 2014, vol. 42, pp. 167–171.

5. Azhmukhamedov, I. M., Koryakova, V. A. Invariant ontological model of the process of providing complex security of the Caspian regions. *Caspium Securitatis: journal of Caspian Security*, 2022, vol. 2, no. 2, pp. 11–22. DOI: 10.54398/2713024X_2022_2_2_11 (In Russ.).

6. Avdeenko, K. A., Zargaryan, E. V. *Analysis of the capabilities of an automated drip irrigation system*. 2020. (In Russ.).

7. Abdelfattah, A. H., Khaliullin, D. T., Gomaa, I. M. Soil irrigation management using moisture sensors. *Current state, problems and prospects for the development of mechanization and technical services of the agro-industrial complex*, 2018, pp. 18–26. (In Russ.).

8. Berezina, A. A., Denisenko, A. I., Konoplev, Yu. V., Arefieva, D. B. Development of the structure of an adaptive system for controlling the microclimate of a plant terrarium. *Technique. Space : proceedings of the thirteenth All-Russian youth sci.-tech. conf. In 2 vol.* Baltic state tech. univ. St. Petersburg, 2021, vol. 2, pp. 27–32 (In Russ.).

9. Bolotin, D. A. On the methodology for calculating systems drip irrigation. *Irrigated agriculture*, 2016, no. 3, pp. 17–18 (In Russ.).

10. Varzar, R. L. *Soil temperature and moisture sensor*. 2020 (In Russ.).

11. Grabovetskaya, K. A. et al. Review of solar panels for autonomous power supply systems. *Young scientist*, 2016, no. 22–3, pp. 29–32 (In Russ.).

12. Gusarov, A. V. *Design of printed circuit boards in DipTrace CAD*. Rybinsk, RSATU named after P. A. Solovyov, 2018. Part 2: Design of a simple printed circuit board. 181 p. (In Russ.).

13. Gulina, E. R. *Device for remote monitoring of soil humidity and temperature.* 2018 (In Russ.).

14. Danniker, A. A. et al. Features of using drip irrigation. *Innovative technologies in the agro-industrial complex, as a factor in the development of science in modern conditions*, 2019, pp. 77–81 (In Russ.).

15. Debrin, A. S., Bastron, A. V., Ursegov, V. N. Review of solar panels and photovoltaic stations of domestic manufacturers. *Bulletin of the Krasnoyarsk State Agrarian University*, 2018, no. 6 (141), pp. 136–141 (In Russ.).

16. Ivanov, B. L. et al. Automated control system for greenhouse irrigation. *Scientific support of agro-industrial complex technologies: theory, practice, innovation*, 2020, pp. 306–309 (In Russ.).

17. Istomina, E. E., Kuranov, M. N. The program for the production and application of automatic irrigation systems for plants "Smart House". *Agricultural sciences and agro-industrial complex at the turn of the century*, 2014, no. 8 (In Russ.).

18. Kornilova, G. S., Egorov, M. Yu. Analysis of soil moisture sensors for automatic irrigation systems. *Current problems of science in the field of agro-industrial complex*, 2021, pp. 28–31 (In Russ.).

19. Klushin, K. P. *Programmable irrigation system*. 2018 (In Russ.).

20. Murovsky, S. P., Murovskaya, A. S., Pavlenko, G. L. Development of a control unit for an automatic remote irrigation system. *Advances in modern science and education*, 2017, vol. 4, no. 3, pp. 116–133 (In Russ.).

21. Nagaev, D. A. Review of modern solar panels. *Bulletin of Modern Research*, 2018, no. 6.3, pp. 530–534 (In Russ.).

Статья поступила в редакцию 20.10.2024; одобрена после рецензирования 25.11.2024; принята к публикации 13.12.2024.

The article was submitted 20.10.2024; approved after reviewing 25.11.2024; accepted for publication 13.12.2024.

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 12, 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 – 0,75 см. Кавычки («»), скобки ([ ], ( )), маркеры и другие знаки должны быть аналогичными на протяжении всего предоставляемого для публикации материала.

ПРИКАСПИЙСКИЙ ЖУРНАЛ:
управление и высокие технологии

НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

2024
№ 4 (68)

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
ФГБОУ ВО «Астраханский государственный университет имени В. Н. Татищева»
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Адрес редакции:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20

Адрес издателя:
Российская Федерация, 414056, г. Астрахань, ул. Татищева, 20а

Издание включено в Интернет-каталог
ООО «Агентство «Книга-Сервис» 2022/1

Главный редактор И.М. Ажмухамедов

Редактирование,
компьютерная правка, верстка *Н. Н. Сахно*

Дата выхода в свет 10.03.2025 г.

Цена свободная
Уч.-изд. 12,0. Усл. печ. л. 16,8.
Заказ № 4657. Тираж 500 экз. (первый завод – 22 экз.)

Астраханский государственный университет имени В. Н. Татищева
414056, г. Астрахань, ул. Татищева, 20а
тел. (8512) 24-66-60 (доб. 3; издательско-полиграфический отдел)
Отпечатано в Астраханской цифровой типографии
414040, г. Астрахань, пл. К. Маркса, 33
тел./факс (8512) 54-00-11, 73-40-40,
E-mail: a-d-t@mail.ru