

Зарегистрировано Федеральной службой по надзору
в сфере связи, информационных технологий
и массовых коммуникаций
Свидетельство № 015372 от 01.11.1996 г.

Журнал входит в Перечень научных изданий ВАК,
имеет рейтинг К1, по специальностям:

2.3.1. Системный анализ, управление и обработка
информации (технические, физико-математические
науки); 5.1.2. Публично-правовые (государственно-
правовые) науки (юридические науки).

Главный редактор:

доктор технических наук, профессор
Дмитрий Анатольевич Ловцов

Председатель редакционного совета:

доктор юридических наук, профессор
Сергей Васильевич Запольский

Шеф-редактор,

заместитель главного редактора:
старший научный сотрудник
Григорий Иванович Макаренко

Учредитель и издатель:

Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции
Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.

Печать цветная цифровая.

Подписано в печать 31.03.2025 г.

Общий тираж 100 экз. Цена свободная.

Адрес редакции:

125437, Москва, Михалковская ул.,
65, стр.1

Телефон: +7 (495) 539-25-29

E-mail: inform360@yandex.com

Требования, предъявляемые к рукописям,
размещены на сайте
<http://uzulo.su/prav-inf>

СОДЕРЖАНИЕ

Государственно-правовые науки

АКАДЕМИЧЕСКИЕ РАЗМЫШЛЕНИЯ О ТЕОРИИ ФИНАНСОВ И ЮРИДИЧЕСКИХ ОБЯЗАТЕЛЬСТВАХ

Кобзарь-Фролова М.Н., Запольский С.В. 4

О РОЛИ ПРАВИТЕЛЬСТВА В ПОЛИТИЧЕСКОЙ СИСТЕМЕ РОССИИ

Запольский С.В. 14

ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ СРЕДЫ

Карцхия А.А. 19

О ПРАВОВЫХ СРЕДСТВАХ ОСУЩЕСТВЛЕНИЯ НАЛОГОВОЙ ПОЛИТИКИ

Васянина Е.Л. 32

ПРАВОСУДИЕ И ВИРТУАЛЬНОЕ ПРОСТРАНСТВО

Белякова А.В. 38

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЛОБАЛЬНОГО ПРОТИВОСТОЯНИЯ

Баландин А.Ю. 50

ОТ ПОРОКОВ ДИСКРИМИНАЦИИ К РАЗВИТИЮ ОСНОВ НЕДИСКРИМИНАЦИИ

Фролов В.А. 57

ПЕРСПЕКТИВЫ И ПРОБЛЕМАТИКА МОДЕРНИЗАЦИИ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Чудесенко А.В. 63

Частноправовые науки

СТРАТЕГИЧЕСКИЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОГО И ЦИФРОВОГО СУВЕРЕНИТЕТА: ПРАВОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ НОВОЙ ИНФОРМАЦИОННОЙ СРЕДЫ

Полякова Т.А., Троян Н.А. 70

ТОВАРНЫЕ ЗНАКИ В МЕТАВСЕЛЕННОЙ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Коданева С.И. 79

О НАЛОГОВОЙ ПРАВОСУБЪЕКТНОСТИ ОРГАНИЗАЦИЙ-РЕЗИДЕНТОВ, ОСУЩЕСТВЛЯЮЩИХ СВОЮ ДЕЯТЕЛЬНОСТЬ НА ТЕРРИТОРИЯХ ОСОБЫХ ЭКОНОМИЧЕСКИХ ЗОН

Пименов С.Д. 86

К ВОПРОСУ О СИСТЕМЕ ЗАКОНОДАТЕЛЬСТВА, РЕГУЛИРУЮЩЕГО ВОЗВРАТ СБЕРЕЖЕНИЙ ГРАЖДАН АГЕНТСТВОМ ПО СТРАХОВАНИЮ ВКЛАДОВ

Паршукова А.П. 95

Информационные и автоматизированные системы и сети

АГЕНТНЫЕ МОДЕЛИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бурый А.С., Цаплина О.С. 101

МЕТОДИКА ЗАЩИТЫ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ОТ СОСТЯЗАТЕЛЬНЫХ АТАК НА ОСНОВЕ ШУМОПОДАВЛЯЮЩИХ АВТОЭНКОДЕРОВ

Котенко И.В., Ичетовкин Е.А. 110

ПОДХОДЫ К УПРАВЛЕНИЮ РАЗВИТИЕМ ОТЕЧЕСТВЕННЫХ СИСТЕМ ИНФОРМАЦИОННО-ТЕЛЕМЕТРИЧЕСКОГО ОБЕСПЕЧЕНИЯ

Воронцов В.Л. 121

РАЗРАБОТКА И СИСТЕМНЫЙ АНАЛИЗ МЕТОДА ОЦЕНКИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНОЙ СИСТЕМЫ

Лубенцов А.В. 130

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ БЛЕНДЕРА

Грозов В.А., Будько М.Ю., Гирик А.В. 141

ВИДЕОИГРЫ И ИГРОВЫЕ МЕХАНИКИ: ПРАВОВОЙ РЕЖИМ И ОХРАНА

Пагов А.Ж. 153

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 34077

РЕДАКЦИОННЫЙ СОВЕТ

ЗАПОЛЬСКИЙ Сергей Васильевич
ЕМЕЛИН Николай Михайлович
ИСАКОВ Владимир Борисович
ЛОВЦОВ Дмитрий Анатольевич
СЕРГИН Михаил Юрьевич
ТЮТЮННИК Вячеслав Михайлович
УВАЙСОВ Сайгид Увайсович

Иностранные члены

КРУГЛИКОВ Сергей Владимирович
ШАРШУН Виктор Александрович

председатель редакционного совета, доктор юридических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва
доктор юридических наук, профессор, г. Москва
главный редактор, доктор технических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва

доктор технических наук, профессор, г. Минск, Белоруссия
кандидат юридических наук, г. Минск, Белоруссия

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

АЛЕКСЕЕВ Владимир Витальевич
БЕТАНОВ Владимир Вадимович
БУРЫЙ Алексей Сергеевич
ГАВРИЛОВ Дмитрий Александрович
ЛОВЦОВ Дмитрий Анатольевич
МАКАРЕНКО Григорий Иванович
МАРКОВ Алексей Сергеевич
ОМЕЛЬЧЕНКО Виктор Валентинович
СУХОВ Андрей Владимирович
ФЕДОСЕЕВ Сергей Витальевич
ЦИМБАЛ Владимир Анатольевич
АТАГИМОВА Эльмира Исамудиновна
ЗАХАРЦЕВ Сергей Иванович
КАБАНОВ Павел Александрович
МОИСЕЕВА Татьяна Федоровна
ПОЛЯКОВА Татьяна Анатольевна
ТЕРЕНТЬЕВА Людмила Вячеславовна
ЧУБУКОВА Светлана Георгиевна

доктор технических наук, профессор, г. Тамбов
доктор технических наук, профессор, г. Москва
доктор технических наук, г. Москва
доктор технических наук, г. Москва
главный редактор, доктор технических наук, профессор, г. Москва
шеф-редактор, г. Москва
доктор технических наук, доцент, г. Москва
доктор технических наук, профессор, г. Москва
доктор технических наук, профессор, г. Москва
кандидат технических наук, доцент, г. Москва
доктор технических наук, профессор, г. Серпухов, Московская область
кандидат юридических наук, доцент, г. Москва
доктор юридических наук, профессор, г. Москва
доктор юридических наук, профессор, г. Казань
доктор юридических наук, кандидат биологических наук, профессор, г. Москва
доктор юридических наук, профессор, г. Москва
доктор юридических наук, доцент, г. Москва
кандидат юридических наук, доцент, г. Москва

EDITORIAL COUNCIL

Sergei ZAPOL'SKII
Nikolai EMLIN
Vladimir ISAKOV
Dmitrii LOVTSOV
Mikhail SERGIN
Viacheslav TIUTIUNNIK
Saigid UVAISOV

Foreign members

Sergei KRUGLIKOV
Viktor SHARSHUN

Chairman of the Editorial Council, Doctor of Science in Law, Professor, Moscow
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Law, Professor, Moscow
Editor-in-Chief, Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Professor, Tambov
Doctor of Science in Technology, Professor, Moscow

Doctor of Science in Technology, Professor, Minsk, Belarus
Ph.D. in Law, Minsk, Belarus

EDITORIAL BOARD

Vladimir ALEKSEEV
Vladimir BETANOV
Aleksei BURYI
Dmitrii GAVRILOV
Dmitrii LOVTSOV
Grigoriy MAKARENKO
Aleksei MARKOV
Viktor OMELCHENKO
Andrey SUKHOV
Sergei FEDOSEEV
Vladimir TSIMBAL
El'mira ATAGIMOVA
Sergey ZAKHARTSEV
Pavel KABANOV
Tat'iana MOISEEVA
Tat'iana POLIAKOVA
Liudmila TEREENT'eva
Svetlana CHUBUKOVA

Doctor of Science in Technology, Professor, Tambov
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Moscow
Doctor of Science in Technology, Moscow
Editor-in-Chief, Doctor of Science in Technology, Professor, Moscow
Managing Editor, Moscow
Doctor of Science in Technology, Associate Professor, Moscow
Doctor of Science in Technology, Professor, Moscow
Doctor of Science in Technology, Professor, Moscow
Ph.D. in Technology, Associate Professor, Moscow
Doctor of Science in Technology, Professor, Serpukhov, Moscow Oblast
Ph.D. in Law, Associate Professor, Moscow
Doctor of Science in Law, Professor, Moscow
Doctor of Science in Law, Professor, Kazan
Doctor of Science in Law, Ph.D. in Biology, Professor, Moscow
Doctor of Science in Law, Professor, Moscow
Doctor of Science in Law, Associate Professor, Moscow
Ph.D. in Law, Associate Professor, Moscow

LEGAL INFORMATION

RESEARCH PEER-REVIEWED JOURNAL

2025, No. 1

The journal is published quarterly.

Registered by the Federal Service for Supervision in the
Sphere of Telecom, Information Technologies
and Mass Communications
Registration Certificate No. 015372
of the 1st of November 1996.

The journal is included in the list of scientific publications
of the Higher Attestation Commission by specialty:
2.3.1. System analysis, management and processing
Information (technical, physical and mathematical);
5.1.2. Public-law (state-law) Science (Legal).

Editor-in-Chief:

Doctor of Science in Technology, Professor
Dmitrii Lovtsov

Chair of the Editorial Council:

Doctor of Science in Law, Professor
Sergei Zapol'skii

Managing Editor,

Deputy Editor-in-Chief:
Grigory Makarenko

Founder and publisher:

Federal State-Funded Institution "Scientific
Centre for Legal Information under the
Ministry of Justice
of the Russian Federation"

Printed by the Printing and Publication Division
of the Scientific Centre for Legal Information
under the Ministry of Justice
of the Russian Federation.

Printed in digital colour. Approved for print
on the 31st of March, 2025.
Number of items printed: 100. Free price.

Postal address:

Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia

Telephone: +7 (495) 539-25-29

E-mail: inform360@yandex.com

Guidelines for preparing manuscripts for
publication can be found on the website
<http://uzulo.su/prav-inf>

CONTENTS

Constitutional law

ACADEMIC REFLECTIONS ON THE THEORY OF FINANCE
AND LEGAL OBLIGATIONS

Margarita Kobzar'-Frolova, Sergei Zapol'skii 4

ON THE ROLE OF THE GOVERNMENT IN THE POLITICAL SYSTEM OF RUSSIA

Sergei Zapol'skii 14

THE LEGAL ASPECTS OF REGULATING THE INFORMATION ENVIRONMENT

Aleksandr Kartskhiia 19

ON LEGAL MEANS FOR EXERCISING TAX POLICY

Elena Vasianina 32

ADMINISTRATION OF JUSTICE AND VIRTUAL SPACE

Anna Beliakova 38

SPECIFIC FEATURES OF LEGAL REGULATION OF CYBERSECURITY
IN THE TIMES OF GLOBAL CONFRONTATION

Artur Balandin 50

FROM THE VICES OF DISCRIMINATION TO DEVELOPING
THE FOUNDATIONS OF NON-DISCRIMINATION

Viacheslav Frolov 57

PROSPECTS AND PROBLEMS OF MODERNISING LAWYERS' ACTIVITIES
IN THE CONTEXT OF DIGITAL TRANSFORMATION

Anton Chudesenko 63

Private law

STRATEGIC TASKS OF SECURING TECHNOLOGICAL
AND DIGITAL SOVEREIGNTY: THE LEGAL ASPECTS OF FORMATION
OF A NEW INFORMATION ENVIRONMENT

Tat'iana Poliakova, Natal'ia Troian 70

TRADEMARKS IN THE METAVERSE: PROBLEMS OF LEGAL REGULATION

Svetlana Kodaneva 79

ON TAX LEGAL PERSONALITY OF RESIDENT ORGANIZATIONS OPERATING
IN THE TERRITORIES OF SPECIAL ECONOMIC ZONES

Sergei Pimenov 86

ON THE QUESTION OF THE SYSTEM OF LAWS REGULATING THE REPAYMENT
OF CITIZENS' SAVINGS BY THE DEPOSIT INSURANCE AGENCY

Anastasiia Parshukova 95

Information and automated systems and networks

AGENT-BASED MODELS FOR DECISION-MAKING USING
GENERATIVE ARTIFICIAL INTELLIGENCE

Aleksei Buryi, Ol'ga Tsaplina 101

A TECHNIQUE FOR PROTECTING INTRUSION DETECTION SYSTEMS AGAINST
ADVERSARIAL ATTACKS BASED ON DENOISING AUTOENCODERS

Igor' Kotenko, Egor Ichetovkin 110

APPROACHES TO MANAGING THE DEVELOPMENT
OF DOMESTIC INFORMATION AND TELEMETRY
SUPPORT SYSTEMS

Valerii Vorontsov 121

THE DEVELOPMENT AND SYSTEM ANALYSIS OF A METHOD
FOR EVALUATING THE EFFICIENCY OF INFORMATION SECURITY
OF A COMPLEX SYSTEM

Aleksandr Lubentsov 130

GENERATING CRYPTOGRAPHICALLY STRONG PSEUDORANDOM
SEQUENCES USING A BLENDER

Vladimir Grozov, Mikhail Bud'ko, Alexei Girik 141

VIDEO GAMES AND GAME MECHANICS:
LEGAL REGIME AND PROTECTION

Astemir Pagov 153

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 34077

АКАДЕМИЧЕСКИЕ РАЗМЫШЛЕНИЯ О ТЕОРИИ ФИНАНСОВ И ЮРИДИЧЕСКИХ ОБЯЗАТЕЛЬСТВАХ

Кобзарь-Фролова М.Н.¹, Запольский С.В.²

Ключевые слова: наука финансового права, обязательства, камералистика, экономика, налоги, финансовые отношения, бюджет.

Аннотация

Цель статьи: показать истинное назначение и изначальную суть науки финансового права. Это позволит несколько изменить векторы развития финансовой политики государства и науки финансового права, переориентировав ее в область обязательств.

Исторически наука финансового права формировалась как экономическая дисциплина и прошла долгий путь своего становления. В наши дни финансовое право — самостоятельная ведущая отрасль. Наука финансового права изучает тот круг отношений, который регулируется отраслью, отраслевыми законами.

Результаты: исследование древних источников, зарубежной литературы в области камералистики, финансов и проч., позволило авторам прийти к выводу, что изначально финансовое право формировалось как право, вытекающее из обязательств. Основатели науки финансового права поддержали эту идею, формируя представления о финансовых отношениях, как отношениях, исходящих из взаимных обязательств человека и государства. Известные события начала XX века надолго «притормозили» развитие данной науки, и возродилась она в советском обществе уже через такие понятия, как бюджет и бюджетные отношения. Вместе с тем изначальное сущностное предназначение науки как науки об обязательствах было утеряно.

DOI: 10.24412/1994-1404-2025-1-4-13

Наука финансового права занимает прочное место в системе юридических наук. Необходимые условия для формирования основ науки возникли еще в античные времена. Наука финансового права выкристаллизовалась из системы экономических наук и прошла долгий путь от формирования комплекса знаний об управлении дворцовым хозяйством, политико-экономических представлений о финансовой политике государства и его социальных функциях, идей меркантилизма, получения комплекса знаний о финансах, налогах, таможенных податях и прочем.

Первые упоминания о финансовых отношениях и финансовой деятельности государства встречаются в письменных источниках античного права — например, в Законах XII таблиц³ и Законах Хаммурапи. Там

имеются правила, закрепляющие порядок расчетов между должниками и кредиторами, уплаты долгов, ростовщичества, положения о финансовых рисках, определен порядок и величина сборов и несения иных повинностей, и прочее⁴.

Однако уместно будет заметить, что в Древнем Риме всё право разделяли на публичное и частное, что соответствовало частному и общественному интересу. Публичное право защищало интересы государства, а частное складывалось относительно пользы граждан. Ведущая роль в отношениях отводилась договору как основанию возникновения обязательств⁵. Отсюда

³ Стейнберг С. Двенадцать таблиц и их происхождение: дебаты XVIII века (пер. с англ.) // Журнал истории идей. 1982. Т. 43. № 3. С. 379—396.

⁴ Там же. С. 379—381, 384—389. См. также: Томсинов В.А. Рецепция римского права в Западной Европе в средние века: постановка проблемы // Древнее право. 1998. № 1 (3). С. 169—175.

⁵ Мозолин В.П., Масляев А.И. Гражданское право. Часть первая : учебник. М., Юрист, 2005. С. 251; См. Гай. Институции. Книги 2: Памятники римского права. М. : Юрист, 1997. С. 204—205.

¹ **Кобзарь-Фролова Маргарита Николаевна**, доктор юридических наук, профессор, главный научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Российская Федерация.

E-mail: margokfnn@yandex.ru

² **Запольский Сергей Васильевич**, доктор юридических наук, профессор, главный научный сотрудник сектора административного права и административного процесса Института государства и права РАН, заслуженный юрист РСФСР, г. Москва, Российская Федерация.

E-mail: adminlaw@igpran.ru

отношения мены, долговых обязательств и прочего — это все есть часть обязательственных отношений⁶.

Сборник правовых норм Киевской Руси — Русская Правда — тоже включал нормы, закрепляющие обязательственные имущественные и иные отношения, например, правила взимания податей и иных платежей, правила о поклаже, «простом заёме» и бескорыстной ссуде и прочие.

Вместе с тем и античные законы, и Русская Правда содержали лишь отдельные элементы обязательственных отношений. В них был изложен односторонний подход в части обязательств. Уместно заметить, что обязаны по отношению к государству были только его подданные. Обязательства государства по отношению к гражданам законодательно закреплены не были. Таким образом, рассмотренные отношения можно отнести к видам повинностей, явившихся прообразом правоотношений.

Заметный вклад в развитие науки о финансах внесли германские, австрийские, французские финансисты. Развитие в XVII веке в европейских государствах либеральных идей о свободе, справедливости, солидарности, общественном договоре, достойном существовании человека, объединение в XVIII веке разрозненных германских княжеств в единый союз — Zollverein, с одной стороны, необходимость сохранять, приумножать и более эффективно расходовать доходы государства и княжеств, не допуская неучтенных расходов, с другой, — все это способствовало становлению и бурному развитию науки камералистики⁷. Камералистика разрабатывалась как совокупность знаний, позволяющих управлять государственным имуществом. В университетах Германии и Австрии в XVIII веке открываются специальные факультеты камералистики. Студенты изучали там собственно камералистику, экономику, аудит, финансы, торговое дело и прочее. Это позволило подготовить специалистов и теоретиков в этих областях знаний. Появляются первые учебники и книги по вопросам управления государственным хозяйством.

Так, германский историк и юрист, исследователь государственных финансов XVII века Фейт Людвиг фон Зекендорф (1626—1692) в 1655 г. выпускает работу «Немецкое княжеское государство». На основе состояния финансов в раздробленной Германии он формулирует предложения по управлению княжескими финансами. Фон Зекендорф одним из первых задался проблемой зависимости поступлений в казну от состояния податной силы населения. Он наста-

ивал на участии государства в заботах о духовной и материальной жизни населения⁸.

Немецкий экономист, камералист Иоганн Генрих фон Юсти (1720—1771) выпускает работу «Система финансового хозяйства»⁹. В работе Юсти рассматривал вопросы сущности и назначения финансовой науки. Книга содержит учения о доходах государства, его расходах и управления государственным хозяйством.

Оба ученых были сторонниками теории обязательств. Они полагали, что государство должно принимать на себя обязательство участия в социальных процессах общества и финансировать общественные блага населения.

Профессор экономики и финансов Карл Теодор фон Эгеберг (Eheberg; 1855—1941) в книге «Курс финансовой науки» (1913) упорядочил многообразие институтов финансовой науки Германии, разъяснил и дал характеристику многим ее терминам. Широко известны его труды о налогах, например, «Налоги на доходы, имущество и на переход имущества» (1923)¹⁰.

Рост мануфактурного производства во Франции в середине XVIII века обусловил дальнейшее развитие экономических наук. Национальное собрание Франции в XVII в. официально вводит налоговую систему; уплата налогов становится не только обязанностью и долгом каждого гражданина, но и ценой тех благ, которые доставляет им государство¹¹.

Теоретик политической экономики Франсуа Кенэ (1694—1774) вывел формулу взаимосвязи сокращения воспроизводства и налогообложения во Франции. Он также доказал, что несправедливо высокое налогообложение приводит к сокращению производства и незаинтересованности производителей в получении прибыли. Он предложил взимать налог не с валового дохода производителя, а с чистого дохода.

Наиболее прогрессивные европейские философы, такие как англичанин Томас Гоббс (1588—1679), француз Франсуа Мари Вольтер (1694—1778), Оноре Габриэль Мирабо (1749—1791) и другие, были сторонниками теории фискального договора, согласно которой каждый гражданин, уплачивая налог, может рассчитывать на некие гарантии от государства и охрану своей собственности. В этом проявляется обоюдная выгода возмездного обязательства как со стороны государства, так и его подданных. Таким образом, сущность

⁸ См., например: Райнерт Эрик С. Краткое введение в изучение Фейта Людвиг фон Зекендорфа (1626—1692) // Европейский журнал права и экономики. Май 2005. Т. 19. Вып. 3. С. 221—230.

⁹ См.: Юсти И.Г. Существенное изображение естества народных обществ и всякого рода законов / Соч. г. Юсти; с нем. на рос. яз. пер. ВРМ. ВЛКВ. [Авраам Волков]. М.: При Имп. Моск. ун-те, 1770. 384 с.

¹⁰ Курс финансовой науки / Пер. с 12-го нем. изд. под ред., [с предисл.] и с доп. по рус. фин. праву М.А. Курчинского, приват-доцента С.-Петерб. ун-та. СПб., 1913. XII, 592 с.; См. также: Современные налоги на Западе: Налоги на доходы, имущество и на переход имущества / Пер. с 19-го нем. изд. под ред. и с доп. по русскому податному законодательству проф. М.И. Боголепова. Петроград: Наука и школа, 1923. 96 с.

¹¹ Грачева Е.Ю. История финансового права // Вестник университета им. О.Е. Кутафина. 2015. № 3. С. 28—45.

⁶ Кобзарь-Фролова М.Н. Административный деликт: самозванец или сформировавшийся правовой феномен? // Сибирское юридическое обозрение. 2020. Т. 17. № 2. С. 267—272.

⁷ Камера, Камеральные науки — учреждение // Энциклопедический словарь Брокгауза и Ефрона: в 86 т. (82 т. и 4 доп.). СПб., 1890—1907.

фиска определяется возвратностью благ и гарантий со стороны государства.

По мнению Е.Ю. Грачевой, на становление науки финансового права наиболее значимое влияние оказали работы Ш.-Л. Монтескье, Ж.-Ж. Руссо, И. Канта, а особенно А. Смита и Д. Риккардо.

Шотландский экономист Адам Смит (1723—1790) в 1776 году публикует книгу «Исследование о природе и причинах богатства народов», в которой представил свои воззрения на экономику. Ему удалось попытка разъяснить действие механизма свободного рынка, сформулировать феномен прибавочной стоимости и развить экономическую теорию природы налога. Однако финансовая наука в его понимании — это составная часть политической экономии. В налоге Смит также развивает идею социального обязательства. За счет налогов государство покрывает расходы на оборону и содержание достоинства верховной власти. Смитом была разработана система принципов налогообложения, общая суть которых — соблюдение баланса частных и публичных интересов¹².

Наиболее полно и системно области финансового права были раскрыты итальянским ученым Ф. Нитти¹³, который, рассуждая о пределах экономической (финансовой) деятельности государства, проводит анализ причин роста общественных расходов, дает характеристику налогам и таможенным платежам и проч.¹⁴. По мнению Ф. Нитти, назначение науки о финансах — познание способов извлечения государством и местными учреждениями самоуправления необходимых для их деятельности материальных средств и того, как они их расходуют. Финансовая наука — дисциплина с весьма обширной сферой ведения. «В круг ее исследования входят все те отношения, которые возникают на почве добывания и употребления средств, собираемых с граждан»¹⁵. Его теория также основана на взаимных обязательствах государства и граждан.

Имперская Россия ощутила проблему управления государственными финансами в начале XIX века. В этой связи на юридических факультетах императорских университетов открываются факультеты и отделения камералистики. В Москве такой факультет был создан в 1835 году, а в Петербурге — в 1843 году. Цель — «приготовление людей, способных к службе хозяйственной или административной»¹⁶. Наряду с камералистикой

преподавали: государственное право европейских держав, законы о благоустройстве и благочинии, политическую экономию, технологию, агрономию, статистику и проч. Годы позже камеральные отделения открылись в университетах Казани и Харькова.

Есть мнение, что первым из русских ученых изложил свои взгляды на науку финансового права И. Посошков, который выпустил произведение «Книга о скудости и богатстве»¹⁷ (1724). Книга написана в духе политической экономии и теории меркантилизма. В ней И. Посошков рассуждает о духовности, правосудии, купечестве, государственном устройстве, просвещении, причинах приключения скудости и что умножает богатство. Его рассуждения пронизаны глубоким патриотизмом и заботой о благополучии страны. Между тем суть науки финансового права в его рассуждениях не отражается.

Интерес к вопросам экономики государства российского, финансов государства, распределения налогов проявлял академик М.В. Ломоносов (1711—1765). Он поставил своим долгом провести инвентаризацию природных, земельных, людских и иных ресурсов России, и добился этой цели. Цель экономики он видел не в приумножении богатства казны, а в увеличении народонаселения, его образовании.

Изучение трудов русских ученых и исследователей в сфере экономики и финансов приводит к выводу о том, что системно все сферы финансовой деятельности государства не охватывались. По большей части исследованию подвергались налоги (Н.И. Тургенев) и таможенные подати (В.Н. Татищев¹⁸, Н.С. Мордвинов).

Чтение лекций в императорских университетах позволило подготовить плеяду молодых ученых, желающих развивать финансовое право. Наиболее известными и авторитетными в этой области признаны профессора Е.Г. Осокин, Н.Я. Горлов, Ф.Б. Мильгаузен, В.А. Лебедев, Д.М. Львов, И.И. Янжул, И.Х. Озеров, С.И. Иловыйский и другие.

В 1890 году в Петербурге выходит книга профессора В.А. Лебедева «Финансовое право»¹⁹. Основываясь на трудах А. Смита, ученый выводит понятия «финансовое хозяйство», «финансовая власть», определяет задачи и дает характеристику субъектов. Ученый рассматривает финансовые отношения как договорные²⁰ и прочее. «Право» в трудах В.А. Лебедева — это свобода отдавать распоряжения, устанавливать и взимать налоги и проч.

¹² Смит А. Исследование о природе и причинах богатства народа. М.: Эксмо, 2007. 443 с.

¹³ Нитти Ф. Основные начала финансовой науки. Русск. пер. И. Шрейдера. Изд. М. и С. Шабашниковых, 1904. С. 13.

¹⁴ Чупров А. Введение к книге Нитти Ф. «Основные начала финансовой науки», русск. пер. И. Шрейдера. Изд. М. и С. Шабашниковых, 1904, с. 1—2 (33—36). (Примечание: в страницах книги имеются расхождения. Так, начинается повествование со с. 33, но в книге пронумеровано — 1.)

¹⁵ Там же. С. 1—2 (33—36).

¹⁶ Томсинов В.А. Университетская реформа 1863 года в России // Подготовка и проведение университетской реформы 1863 года / Составитель и автор вступительных статей В.А. Томсинов. М.: Зерцало, 2012. С. LXVIII—CXVII (Великие реформы).

¹⁷ Посошков И. Книга о скудости и богатстве. М.: Изд-во РИПОЛ Классик, 2021. 324 с.

¹⁸ Татищев В.Н. Избранные труды / Сост., авт., вступ. ст. и коммент. А.Б. Каменский; Ин-т обществ. мысли. М.: Российская политическая энциклопедия (РОССПЭН), 2010. 486 с.

¹⁹ Лебедев В.А. Финансовое право / Соч. В.А. Лебедева, проф. С.-Петерб. ун-та. Т. 1. Вып. 2 / 24. Санкт-Петербург: типо-лит. А.М. Вольфа, 1890. 316—544 с.

²⁰ Там же. С. 334.

В 1904 году академик И.И. Янжул выпускает учебное пособие «Основные начала финансовой науки»²¹. В этой книге академик все юридические науки, которые изучаются на юридическом факультете Московского университета, разделил на 2 большие группы:

- 1) науки государственного, гражданского и уголовного характера,
- 2) науки административные или хозяйственные, такие как политическая экономия, статистика, о государственном хозяйстве или наука о финансах, финансовое право.

Как видим, у И. Янжула феномены науки о финансах и финансовое право тождественны и относятся к общей группе наук о государственном хозяйстве²². Янжул пишет о том, что давно назрела необходимость создать особую отрасль государственоведения, которая изучала бы принципы, долженствующие лежать в основе правильного и целесообразного устроенного организма финансового хозяйства. Этой важной наукой явилась наука о финансах, имеющая своим предметом исследование способов наилучшего удовлетворения материальных потребностей государства²³.

Несомненной заслугой ученого является то, что он вывел систему финансовой науки, включающую в себя учение о государственных доходах и расходах и дает их классификацию. Однако теория общественного договора и обязательств, хоть и подразумевается, но «размывается» на страницах книги.

Ординарный профессор Московского императорского университета И.Х. Озеров предпринял попытки развить учение своего учителя И. Янжула. Он рассматривает содержание *финансовой науки* как принадлежащей к циклу экономических наук, ее задачи, предмет, метод, анализирует финансовое хозяйство государства и приводит его отличия от частного. И.Х. Озеров расписывает, для чего государству (публичным союзам) нужны налоги — «для выполнения лежащих на них задач...». С другой стороны государства имеют затраты, «...одним словом, ведут свое хозяйство»²⁴. И выводит определение: «Финансовая наука изучает финансовое хозяйство, т. е. совокупность отношений, которые возникают на почве добывания союзами публичного характера материальных средств: она изучает те способы, посредством которых эти союзы добывают себе нужные средства и как эти способы отражаются на других сторонах жизни» [20, с. 20—21].

И.Х. Озеров четко определил задачи науки финансового права. Задача первая — изучение хозяйства государства, общин, городов и проч., изучение причин-

ной связи этого круга явлений с точки зрения их формального и материального развития. Вторая задача — изучение причин перемещения налогового бремени с плеч одних на плечи других. Это есть вопрос об общественных отношениях. Третья задача — аналитическая: исследовать влияние налогового бремени на экономическую жизнь [20, с. 21—23]. То есть для профессора И.Х. Озерова понятия «финансовая наука» и «наука финансового права» — тождественны, но вопросы обязательств в финансовых отношениях не размыты, они очевидны, хоть и не названы напрямую.

Теоретик права профессор Г.Ф. Шершеневич на основе анализа трудов профессора И.Х. Озерова и Нитти определил суть финансового права как юридической дисциплины — это «совокупность норм, определяющих способы приобретения и расходования государственных материальных средств, необходимых для осуществления им своих задач». «По существу, финансовое право есть часть административного права, это область внутреннего управления»²⁵.

Между тем события Февральской, а затем Октябрьской революции на долгие годы прервали развитие науки финансового права. Затем на долгие годы (до середины 1930 года) роль финансового права была нивелирована. В условиях развивающегося социализма деньги и их накопление рассматривались как пережиток капитализма, советское общество пропагандировалось как безналоговое общество (хотя налоги были). В ряде университетов стали закрываться кафедры финансового права. К тому же многие ученые покинули Россию. Например, Э.Н. Берендтс (1870—1930), доктор финансового права, став профессором Тартуского университета, издал несколько книг не только по финансовому праву зарубежных стран, но и административному праву²⁶.

Наука финансового права стала робко прокладывать свой путь через развитие представлений о бюджете и бюджетных отношениях, когда пришло понимание необходимости поставить на научную основу вопросы управления государственным бюджетом (лишь конец 20-х — начало 30-х гг.). В этот период появляются первые тематические работы по финансовому праву. Особая заслуга здесь принадлежит советскому ученому, ординарному профессору Московского университета С.А. Котляревскому, который, упорно работая, выпускает ряд работ²⁷ по бюджетному регулированию и действию бюджетного законодательства, бюджетно-финансовым отношениям и бюджетным правам СССР и союзных республик, проблемам местных бюджетов

²¹ Янжул И.И. Основные начала финансовой науки: Учение о гос. доходах. 4-е изд., изм. и доп. Санкт-Петербург: тип. И. Стасюлевича, 1904. IV, 500 с.

²² Там же. С. 3.

²³ Там же. С. 10.

²⁴ Озеров И.Х. Основы финансовой науки. Вып. 1. Учение об обычных доходах: курс лекций, читанный в С.-Петербургском и Московском университетах. 4-е изд., [испр. и доп.]. М.: тип. т-ва И.Д. Сытина, 1911. 544, V с.

²⁵ Шершеневич Г.Ф. Общая теория права. М.: издание бр. Башмаковых, 1910. С. 550.

²⁶ См. например: Берендтс Э.Н. Финансовое право Великого Княжества Финляндского в XIX столетии. Исторический очерк. СПб.: Гос. тип., 1900. 321 с.; Берендтс Э.Н. Опыт системы административного права. Т. I, вып. I. Ярославль, 1898, и др.

²⁷ Котляревский С.А. Бюджетное право РСФСР и СССР. М.: Труды института советского права, 1924. 163 с.; Котляревский С.А. Финансовое право СССР. Л.: Гос. изд-во, 1926. 157 с. (Проблемы советского права под общей редакцией проф. Д.А. Магеровского).

и прочие. Н.В. Кроткова, например, пишет, что С.А. Котляревский более глубоко, нежели дореволюционные исследователи, погрузился в проблему бюджетных отношений и определил бюджет как основной финансовый план государства²⁸. Вслед выходят учебники по советскому бюджетному праву и отдельные работы по налогам и расчетным отношениям, авторы — профессор М.Д. Загряцков²⁹, доктор права Э.Э. Понтович³⁰, Е.А. Ровинский³¹ и другие.

Уместно заметить, что каждая эпоха, каждое событие в политической жизни государства вносило и вносит в теорию финансового права свои коррективы, отражающие специфику социально-экономических отношений в целом, и влияло на особенности развития финансового права.

В 30—40-е годы XX века основные усилия ученых (Е.А. Ровинского, М.А. Гурвича, А.О. Шварцмана, М.Д. Загряцкова, не без влияния трудов М.Я. Залесского, Г.С. Гуревича, А.К. Райдера, К.К. Шамова и других) были ориентированы на познание предмета и системы финансового права³². Такой вектор научных исследований был задан А.Я. Вышинским в его докладе³³ в связи с потребностью формирования отраслевой модели права, определения содержания и границ юридических наук в рамках системы советского права и возрождения науки административного и финансового права³⁴. В этой связи ученым Института государства и права было поручено разработать ключевой инструментарий науки финансового права. Так, в учебнике под редакцией профессора Марка Гурвича³⁵ уже приводятся дефиниции таких важных финансово-правовых категорий, как «финансовые обязательства», «банковская и кредитная система», «эмиссия», «эмиссионное право» и прочие. По справедливому замечанию профессора К.С. Бельского³⁶, в результате творческого мышления ученых

упоминания о финансовых обязательствах привели к развитию современных представлений об этих обязательствах. Основоположниками и идеологами советской теории финансового правоотношения вполне уместно признать ученых Института государства и права АН СССР — А.Я. Вышинского, Е.А. Ровинского, Р.О. Халфину³⁷ и других³⁸.

Это в полной мере относится к послевоенному периоду, когда в СССР в ходе восстановления народного хозяйства и дальнейшего его развития оживилась дискуссия о праве, его соотношения с государственной властью, и появились новые, ранее не использовавшиеся финансовые институты, требовавшие теоретического обоснования.

Первопроходцем стал выдающийся ученый Ефим Абрамович Ровинский, обосновавший методологические подходы к исследованию предмета и системы финансового права³⁹. Его исследования поддержали и продолжили группы ученых, во многом интуитивно угадывавших большое будущее финансового права — Н.И. Химичева, С.Д. Цыпкин, Л.К. Воронова, М.И. Писко-тин, А.А. Жданов, О.Н. Горбунова и ряд их единомышленников. В их понимании финансовое право — публично-правовая наука, имеющая своим предметом имущественные денежные отношения, складывающиеся между государственными органами и субъектами индивидуального и коллективного хозяйствования по поводу формирования и использования публичных денежных фондов, прежде всего средств бюджетной системы.

Этот подход предопределялся превалированием государственной собственности в экономике, безальтернативностью планового хозяйства, императивностью финансового законодательства. В тех условиях обязательственная природа финансовых отношений просто не попадала в фокус внимания ни законодателей, ни практиков. Порядок формирования публичных денежных фондов и их использование целиком и полностью следовали плановым показателям.

Ситуация серьезно изменилась после принятия ряда общегосударственных решений по развитию хозяйства и стимулированию производства в 1965 году. Централизованные капиталовложения, собственные доходы предприятий, платежи в бюджет, фонды экономического стимулирования стали объектами хозяйственных экономических интересов, банковский кредит получил дифференцированный режим применения. Финансовое право из юридической «золушки» стало

²⁸ Кроткова Н.В. Котляревский С.А. как представитель советской юридической науки // Финансовое право и управление. 2014. № 3. С. 184—198.

²⁹ Загряцков М.Д. Бюджетные права местных Советов. М.: Изд-во Гл. упр. Коммун. хоз-ва НКВД, 1924. 60 с.

³⁰ Понтович Э.Э. Финансовый контроль. Л.: Финансовое изд-во НКФ СССР, 1928. 107 с.

³¹ Ровинский Е.А. Основные вопросы теории советского финансового права. М.: Госюриздат, 1960. 193 с.

³² Финансовое право: учебник / Сост.: Гурвич М.А., Залесский М.Я., Райдер А.К., Шварцман А.О., Шамаков К.К.; общ. ред.: Гурвич М.А. М.: Юрид. изд-во НКЮ СССР, 1940.

³³ Вышинский А.Я. Основные задачи науки советского социалистического права (Сокращенная стенограмма доклада на 1-м совещании по вопросам науки советского права и государства 16 июля 1938 г.) // Социалистическая законность. 1938. № 8. С. 1—34.

³⁴ Кобзарь-Фролова М.Н., Андрианова Н.Г., Васянина Е.Л. Эволюция теории финансового правоотношения: (историографические и догматические аспекты становления и развития) // М.: Государство и право, №1, 2025, С. 145–159.

³⁵ Финансовое право: учебник / Сост.: Гурвич М.А., Залесский М.Я., Райдер А.К., Шварцман А.О., Шамаков К.К.; общ. ред.: Гурвич М.А. М.: Юрид. изд-во НКЮ СССР, 1940.

³⁶ Бельский К.С. Забытый «патриарх» советской науки финансового права (к 120-летию со дня рождения М.А. Гурвича) // Государство и право. 2017. № 9. С. 93—100.

³⁷ См., например: Халфина Р.О. К вопросу о предмете и системе советского финансового права // Вопросы советского административного и финансового права. М.: Изд-во АН СССР, 1952. С. 182—214.

³⁸ Андрианова Н.Г., Васянина Е.Л., Кобзарь-Фролова М.Н. Эволюция теории финансового правоотношения: (историографические и догматические аспекты становления и развития) // Государство и право. 2025. № 1. С. 145—159.

³⁹ Ровинский Е.А. Основные вопросы теории советского финансового права. М.: Госюриздат, 1960. 193 с.

неуклонно превращаться в научную и педагогическую ценность.

Многие инициативы правового характера в это время «брали старт» из Министерства финансов СССР, от руководителя юридической службы В.И. Слома. Это касалось, в частности, понимания платежей предприятий в бюджет (налог с оборота, плата за фонды, фиксированные или рентные платежи, свободный остаток прибыли) как особых финансовых обязательств; банковское кредитование стало рассматриваться как обязательства заемщиков, к чему много труда приложил начальник юридического отдела Госбанка СССР М.Л. Коган. «Могучая кучка» учеников и последователей Е.А. Ровинского в этот период опубликовала свои классические работы⁴⁰. Мощный импульс развитию финансового права дали имевшие место в 70-е годы прошедшего века симпозиумы юристов-финансистов социалистических стран, особенно симпозиум, проведенный в октябре 1977 года под эгидой Института государства и права АН СССР в Москве.

Сложный период пережила наука финансового права в период т. н. «перестройки», когда государство добровольно отказывалось от рычагов управления финансами в пользу полукриминальных коммерческих кругов, банков и международных монополий. Этот период запечатлел себя хозяйственно-финансовой разрегулированностью, бесплодными ожиданиями порядка в экономике и в денежном обороте. Это время породило понимание финансового права как всеохватывающего набора юридических приемов совершения сомнительных операций в целях обогащения, в частности, через оборот ценных бумаг, биржевую торговлю, уклонение от налогов и проч. и проч.

Восстановление уважения к праву, чем характерен переживаемый страной текущий период, начатый в 2000 году, вызвал признание финансово-правовой проблематики одним из самых потенциально значимых направлений укрепления государственности.

Принятие Бюджетного кодекса, Налогового кодекса, банковского, таможенного законодательства, другие важные свершения привели к существенным теоретическим подвижкам. Сейчас стало несомненным признание за каждым госорганом, физическим и юридическим лицом круга полномочий и обязанностей, образующих субъективное финансовое право, а вступление в налоговые, бюджетные, расходные и кредитные отношения не чем иным, нежели возникновением соответствующих финансовых обязательств. Это стало возможным вследствие возникновения и завоевания популярности теории юридических лиц публичного права, позволяющей гармонично совместить отправление публичных функций и полномочий с коммерческой деятельностью⁴¹.

Подавляющая часть имущественных денежных отношений между налоговыми органами, банками, социальными фондами, органами отраслевого управления, госкорпорациями, другими носителями статуса юридического лица публичного права, с одной стороны, и юридическими и физическими лицами — участниками хозяйственного оборота, с другой, обладают многими или всеми признаками финансового обязательства. Нельзя не заметить, что смысл понимания финансовых отношений в качестве обязательств состоит в вовлечении предоставительно-обязывающего механизма в дело обеспечения реципиента ассигнованных ему денежных средств к своевременному получению и обязыванию финансирующего субъекта к своевременному и полному исполнению его обязанности, чем достигается эффект де бюрократизации финансового оборота.

Главное достоинство названного эффекта — возможность применения относительно неопределенных или диспозитивных юридических конструкций, что необходимо для экономического стимулирования «активной» стороны финансовых отношений. Эти путем налогоплательщик, получатель бюджетной субсидии, заемщик, инвестор, иной участник финансовой сделки приобретает возможность индивидуализации своих прав и обязанностей с органом публичной власти в зависимости от условий экономической политики государства.

Есть и видимая опасность такого подхода — низведение финансового права до регулирования любых денежных отношений и соответствующих сделок. В нашей стране развивается рынок ценных бумаг, оборот криптовалюты, внедряются расчеты цифровыми рублями, и все эти явления нуждаются в четком правовом регулировании, основанном на защите прав и интересов субъектов частного права и инструментами частного права. Как следствие, все большее распространение получает точка зрения о наличии в финансовом праве ряда частноправовых институтов.

Считая этот комплекс экономических отношений предметом коммерческого, а отчасти гражданского и коммерческого права, не можем признать подобную точку зрения правильной, а перспективу преобразования финансового права в комплексную отрасль (публично-частную) — заслуживающей поддержки. Дело даже не в различии методов правового регулирования, хотя это очень важно, а во «врожденной» особенности финансового права — быть регулятором «вертикальных» имущественных отношений с обязательным участием в них органа государства (публичной власти) или же субъекта, специально уполномоченного на осуществление публичного интереса. Кроме того, вышеназванный правосубъект должен обладать специальной, а не общей правосубъектностью, т. е. правом на совершение финансовых сделок видов, определенных в законе.

Представляется, что причиной возникновения этой и многих подобных проблем служит устаревающая

⁴⁰ См.: Российская наука финансового права конца XX — начала XXI в. М., 2025.

⁴¹ Чиркин В.Е. Юридические лица публичного права. М., 1997.

система российского права, корнями уходящая в 30-е годы прошлого века. Денежные расчеты независимо от их формы заслуживают отдельного места в совокупности регулятивных комплексов экономического развития. Возможно, в будущем получит развитие эмиссионно-денежное право как инструмент упорядочения разнообразных видов платежных, расчетных, инвестиционных и других операций денежного характера. Пока же требуется определенная научная дисциплина, предотвращающая конвергенцию публичного и частного в сфере правового регулирования финансовых отношений.

В целом возникновение подобных проблем свидетельствует, что финансовое право как наука вышло из этапа формирования, доказало свою действенность и накопило потенциал для серьезного вклада в дело интенсификации экономического развития. В нашей стране возникло несколько центров финансово-правовых исследований, объединяющих известных ученых и молодых исследователей. В Москве это Школа финансового права в Московской государственной юридической академии (МГЮА) под руководством профессора Грачевой Е.Ю., в Екатеринбурге — группа исследователей налогового права во главе с профессором Д.В. Винницким, в Воронеже развивается проблематика общих основ финансового права (профессор М.В. Карасева). Финансово-правовые исследования ведут два ведущих в стране научных центра правоведения — Институт государства и права, Институт законодательства и сравнительного правоведения и многие высшие учебные заведения. Результаты исследований публикуются в ряде специализированных журналов — «Финансовое право», «Банковское право», «Налоговед» и другие.

Выводы и заключение

Можно с уверенностью сказать, что наука финансового права в результате социального развития перестала быть юридической «золушкой», а нашла свое применение в широком спектре экономико-правовых исследований, законотворчестве и совершенствовании правоприменения. Перед исследователями правовой стороны финансов стоит перспектива открытия и обоснования тесной связи финансов и всех сфер жизнедеятельности общества, прежде всего с экономикой.

Перед наукой финансового права, которая постепенно выходит на авансцену важнейших правовых исследований, стоит ряд крупных задач и проблем, среди которых выделим следующие.

Целесообразно изучить пути и возможности оснащения отдельных видов финансовых обязательств действенным юридико-техническим аппаратом, с тем чтобы перенести тяжесть регулирования налоговых, бюджетных, инвестиционных отношений с закона

на обязательственные, т. е. двусторонние инструменты, связывающие финансового кредитора с финансовым должником в целях безусловного исполнения обязательств. И здесь была бы весьма уместна рецепция некоторых положений гражданского законодательства, регулирующего сделки и обязательства.

- Назрел вопрос об официальном признании уполномоченных госорганов, а также субъектов с делегированными полномочиями финансового характера юридическими лицами публичного права. Заблуждением постепенно становится понимание государства единым и единственным контрагентом юридических и физических лиц в области финансов. Контрагентом налогоплательщика выступает налоговая инспекция, в сфере бюджетных расходов взаимодействуют орган отраслевого управления и бюджетное учреждение и т. д. Теоретической основой в этом случае может и должно стать признание за юридическими и физическими лицами обладания субъективным финансовым правом.

- Любое финансовое обязательство становится таковым не иначе, как будучи обеспеченным мерами пресечения и превенции от нарушения, а также юридической ответственности за неисполнение или ненадлежащее исполнение. Заметно, что некоторые финансовые обязательства не снабжены мерами юридического понуждения к исполнению. Так, остаются, как правило, без последствий отказы от финансирования бюджетных учреждений, инвестиционных проектов, выплаты различных пособий и компенсаций для граждан. По нашему мнению, неисправность финансового должника должна вызывать юридические последствия: имущественную ответственность, (признание неплатежеспособным и др.), одностипные с гражданско-правовой ответственностью.

В заключение следует отметить, что становление и переход в практическую плоскость концепции финансовых обязательств продиктован ходом развития финансово-правовой мысли, осознания возможности и необходимости правового регулирования финансовой политики. В той степени, в которой любая финансовая операция должна рассматриваться как сделка, совершаемая в целях удовлетворения публичного интереса и протекающая вследствие этого в специальной финансово-правовой форме, она (сделка) носит характер финансового обязательства. Путь к этим выводам был за многие века проторен учеными — нашими предшественниками за рубежом и в России, обоснован теоретически в период планового руководства финансами, получил практическую реализацию в ходе построения новой экономической системы, сочетающей как плановые, так и рыночные правовые ценности.

Литература

1. Стейнберг С. Двенадцать таблиц и их происхождение: дебаты XVIII века (пер. с англ.) // Журнал истории идей. 1982. Т. 43. № 3. С. 379—396.
2. Томсинов В.А. Рецепция римского права в Западной Европе в средние века: постановка проблемы // Древнее право. 1998. № 1 (3). С. 169—175.
3. Мозолин В.П., Масляев А.И. Гражданское право. Часть первая : учебник. М. : Юрист, 2005. С. 251.
4. Гай. Институции. Книги 2: Памятники римского права. М. : Юрист, 1997. С. 204—205.
5. Кобзарь-Фролова М.Н. Административный деликт: самозванец или сформировавшийся правовой феномен? // Сибирское юридическое обозрение. 2020. Т. 17. № 2. С. 267—272.
6. Камера, Камеральные науки — учреждение // Энциклопедический словарь Брокгауза и Ефрона: в 86 т. (82 т. и 4 доп.). СПб., 1890—1907.
7. Райнерт Эрик С. Краткое введение в изучение Фейта Людвиг фон Зекендорфа (1626—1692) // Европейский журнал права и экономики. Май 2005. Т. 19. Вып. 3. С. 221—230.
8. Юсти И.Г.Г. Существенное изображение естества народных обществ и всякого рода законов / Соч. г. Юсти; с нем. на рос. яз. пер. ВРМ. ВЛКВ. [Авраам Волков]. М. : При Имп. Моск. ун-те, 1770. 384 с.
9. Курс финансовой науки / Пер. с 12-го нем. изд. под ред., [с предисл.] и с доп. по рус. фин. праву М.А. Курчинского, приват-доцента С.-Петерб. ун-та. СПб., 1913. XII, 592 с.
10. Современные налоги на Западе: Налоги на доходы, имущество и на переход имущества / Пер. с 19-го нем. изд. под ред. и с доп. по русскому податному законодательству проф. М.И. Боголепова. Петроград: Наука и школа, 1923. 96 с.
11. Грачева Е.Ю. История финансового права // Вестник университета им. О.Е. Кутафина. 2015. № 3. С. 28—45.
12. Смит А. Исследование о природе и причинах богатства народа. М. : Эксмо, 2007. 443 с.
13. Нитти Ф. Основные начала финансовой науки. Русс. пер. И. Шрейдера. Изд. М. и С. Шабашниковых, 1904. С. 13.
14. Чупров А. Введение к книге Нитти Ф. «Основные начала финансовой науки», русс. пер. И. Шрейдера. Изд. М. и С. Шабашниковых, 1904, с. 1—2 (33—36).
15. Томсинов В.А. Университетская реформа 1863 года в России // Подготовка и проведение университетской реформы 1863 года / Составитель и автор вступительных статей В.А. Томсинов. М. : Зерцало, 2012. С. LXVIII—CXVII (Великие реформы).
16. Посошков И. Книга о скудости и богатстве. М. : Изд-во РИПОЛ Классик, 2021. 324 с.
17. Татищев В.Н. Избранные труды / Сост., авт., вступ. ст. и коммент. А.Б. Каменский; Ин-т обществ. мысли. М. : Российская политическая энциклопедия (РОССПЭН), 2010. 486 с.
18. Лебедев В.А. Финансовое право / Соч. В.А. Лебедева, проф. С.-Петерб. ун-та. Т. 1. Вып. 2 / 24. Санкт-Петербург: типо-лит. А.М. Вольфа, 1890. 316—544 с.
19. Янжул И.И. Основные начала финансовой науки: Учение о гос. доходах. 4-е изд., изм. и доп. Санкт-Петербург: тип. И. Стасюлевича, 1904. IV, 500 с.
20. Шершеневич Г.Ф. Общая теория права. М. : издание бр. Башмаковых, 1910. С. 550.
21. Берендтс Э.Н. Финансовое право Великого Княжества Финляндского в XIX столетии. Исторический очерк. СПб. : Гос. тип., 1900. 321 с.
22. Берендтс Э.Н. Опыт системы административного права. Т. I, вып. I. Ярославль, 1898.
23. Котляревский С.А. Бюджетное право РСФСР и СССР. М. : Труды института советского права, 1924. 163 с.; Котляревский С.А. Бюджет СССР, как он составляется, утверждается и исполняется. Л., 1925. 72 с.; Котляревский С.А. Бюджет и местные финансы. М. : Экономическая жизнь, 1926. 146 с.
24. Котляревский С.А. Финансовое право СССР. Л. : Гос. изд-во, 1926. 157 с. (Проблемы советского права под общей редакцией проф. Д.А. Магеровского).
25. Кроткова Н.В. Котляревский С.А. как представитель советской юридической науки // Финансовое право и управление. 2014. № 3. С. 184—198.
26. Загряцков М.Д. Бюджетные права местных Советов. М. : Изд-во Гл. упр. Коммун. хоз-ва НКВД, 1924. 60 с.
27. Понтович Э.Э. Финансовый контроль. Л.: Финансовое изд-во НКФ СССР, 1928. 107 с.
28. Ровинский Е.А. Основные вопросы теории советского финансового права. М. : Госюриздат, 1960. 193 с.
29. Финансовое право : учебник / Сост.: Гурвич М.А., Залесский М.Я., Райдер А.К., Шварцман А.О., Шмаков К.К.; общ. ред.: Гурвич М.А. М. : Юрид. изд-во НКЮ СССР, 1940.
30. Вышинский А.Я. Основные задачи науки советского социалистического права (Сокращенная стенограмма доклада на 1-м совещании по вопросам науки советского права и государства 16 июля 1938 г.) // Социалистическая законность. 1938. № 8. С. 1—34.
31. Андрианова Н.Г., Васянина Е.Л., Кобзарь-Фролова М.Н. Эволюция теории финансового правоотношения: (историографические и догматические аспекты становления и развития) // Государство и право. 2025. № 1. С. 145—159.
32. Бельский К.С. Забытый «патриарх» советской науки финансового права (к 120-летию со дня рождения М.А. Гурвича) // Государство и право. 2017. № 9. С. 93—100.
33. Халфина Р.О. К вопросу о предмете и системе советского финансового права // Вопросы советского административного и финансового права. М. : Изд-во АН СССР, 1952. С. 182—214.

ACADEMIC REFLECTIONS ON THE THEORY OF FINANCE AND LEGAL OBLIGATIONS

Margarita Kobzar'-Frolova, Dr.Sc. (Law), Professor, Principal Researcher at the Sector of Administrative Law and Administrative Process of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.

E-mail: margokfmn@yandex.ru

Sergei Zapol'skii, Dr.Sc. (Law), Professor, Principal Researcher at the Sector of Administrative Law and Administrative Process of the Institute of State and Law of the Russian Academy of Sciences, Honoured Lawyer of the Russian Soviet Federative Socialist Republic, Moscow, Russian Federation.

E-mail: adminlaw@igpran.ru

Keywords: science of financial law, obligations, cameralistics, economics, taxes, financial relations, budget.

Abstract

Purpose of the paper: showing the true destination and original essence of the science of financial law. This will make it possible to somewhat modify the development vectors of the government's financial policy and the science of financial law reorienting it to the field of obligations.

Historically, the science of financial law was formed as an economic discipline and travelled a long way of formation. These days, financial law is an independent branch of law. The science of financial law studies the relations regulated by this branch of law and the laws of this branch.

Study findings: studying ancient sources, foreign literature in the field of cameralistics, finance, etc., allowed the authors to come to the conclusion that financial law was originally formed as a branch of law arising from obligations. The founders of the science of financial law supported this idea, forming the concepts of financial relations as relations arising from mutual obligations of the individual and the government. The well-known events of the begin of the 20th century hindered the development of this branch of science for quite some time, and it reappeared in the Soviet society through such concepts as the budget and budget relations. However, the original essential predestination of this science as a branch of law dealing with obligations was lost.

References

1. Steinberg S. Dvenadtsat' tablits i ikh proiskhozhdenie: debaty XVIII veka (per. s angl.). Zhurnal istorii idei. 1982. T. 43. No. 3. Pp. 379–396.
2. Tomsinov V.A. Retseptsii rimskogo prava v Zapadnoi Evrope v srednie veka: postanovka problemy. Drevnee pravo. 1998. No. 1 (3). Pp. 169–175.
3. Mozolin V.P., Masliaev A.I. Grazhdanskoe pravo. Chast' pervaya : uchebnik. M. : Iurist", 2005. P. 251.
4. Gai. Institutsii. Knigi 2: Pamiatniki rimskogo prava. M. : Iurist", 1997. Pp. 204–205.
5. Kobzar'-Frolova M.N. Administrativnyi delikt: samozvanets ili sformirovavshiisia pravovoi fenomen? Sibirskoe iuridicheskoe obozrenie. 2020. T. 17. No. 2. Pp. 267–272.
6. Kamera, Kameral'nye nauki – uchrezhdenie. Entsiklopedicheskii slovar' Brokgauza i Efrona: v 86 t. (82 t. i 4 dop.). SPb., 1890–1907.
7. Rainert Erik S. Kratkoe vvedenie v izuchenie Feita Liudviga fon Zekendorfa (1626–1692). Evropeiskii zhurnal prava i ekonomiki. Mai 2005. T. 19. Vyp. 3. Pp. 221–230.
8. Iusti I.G.G. Sushchestvennoe izobrazhenie estestva narodnykh obshchestv i vsiakogo roda zakonov. Soch. g. Iusti; s nem. na ros. iaz. per. VRM. VLKV. [Avraam Volkov]. M. : Pri Imp. Mosk. un-te, 1770. 384 pp.
9. Kurs finansovoi nauki. Per. s 12-go nem. izd. pod red., [s predisl.] i s dop. po rus. fin. pravu M.A. Kurchinskogo, privat-dotsenta S.-Peterb. un-ta. SPb., 1913. XII, 592 pp.
10. Sovremennye nalogi na Zapade: Nalogi na dokhody, imushchestvo i na perekhod imushchestva. Per. s 19-go nem. izd. pod red. i s dop. po russkomu podatnomu zakonodatel'stvu prof. M.I. Bogolepova. Petrograd: Nauka i shkola, 1923. 96 pp.
11. Gracheva E.Iu. Istoriia finansovogo prava. Vestnik universiteta im. O.E. Kutafina. 2015. No. 3. Pp. 28–45.
12. Smit A. Issledovanie o prirode i prichinakh bogatstva naroda. M. : Eksmo, 2007. 443 pp.
13. Nitti F. Osnovnye nachala finansovoi nauki. Russ. per. I. Shreidera. Izd. M. i S. Shabashnikovykh, 1904. Pp. 13.

14. Chuprov A. Vvedenie k knige Nitti F. "Osnovnye nachala finansovoi nauki", russ. per. I. Shreidera. Izd. M. i S. Shabashnikovoykh, 1904, pp. 1–2 (33–36).
15. Tomsinov V.A. Universitetskaya reforma 1863 goda v Rossii. Podgotovka i provedenie universitetskoj reformy 1863 goda. Sostavitel' i avtor vstupitel'nykh statei V.A. Tomsinov. M. : Zertsalo, 2012. Pp. LXVIII–CXVII (Velikie reformy).
16. Pososhkov I. Kniga o skudosti i bogatstve. M. : Izd-vo RIPOL Klassik, 2021. 324 pp.
17. Tatishchev V.N. Izbrannye trudy. Sost., avt., vstup. st. i komment. A.B. Kamenskii; In-t obshchestv. mysli. M. : Rossiiskaya politicheskaya entsiklopediya (ROSSPEN), 2010. 486 pp.
18. Lebedev V.A. Finansovoe pravo. Soch. V.A. Lebedeva, prof. S.-Peterb. un-ta. T. 1. Vyp. 2. 24. Sankt-Peterburg: tipo-lit. A.M. Vol'fa, 1890. 316–544 pp.
19. Ianzhul I.I. Osnovnye nachala finansovoi nauki: Uchenie o gos. dokhodakh. 4-e izd., izm. i dop. Sankt-Peterburg: tip. I. Stasiulevicha, 1904. IV, 500 pp.
20. Shershenevich G.F. Obshchaya teoriya prava. M. : izdanie br. Bashmakovykh, 1910. P. 550.
21. Berendts E.N. Finansovoe pravo Velikogo Knyazhestva Finliandskogo v XIX stoletii. Istoricheskii ocherk. SPb. : Gos. tip., 1900. 321 pp.
22. Berendts E.N. Opyt sistemy administrativnogo prava. T. I, vyp. I. Iaroslavl', 1898.
23. Kotliarevskii S.A. Biudzhethoe pravo RSFSR i SSSR. M. : Trudy instituta sovetskogo prava, 1924. 163 pp.; Kotliarevskii S.A. Biudzheth SSSR, kak on sostavliaetsia, utverzhdaetsia i ispolniaetsia. L., 1925. 72 pp.; Kotliarevskii S.A. Biudzheth i mestnye finansy. M. : Ekonomicheskaya zhizn', 1926. 146 pp.
24. Kotliarevskii S.A. Finansovoe pravo SSSR. L. : Gos. izd-vo, 1926. 157 pp. (Problemy sovetskogo prava pod obshchei redaktsiei prof. D.A. Magerovskogo).
25. Krotkova N.V. Kotliarevskii S.A. kak predstavitel' sovetskoi iuridicheskoi nauki. Finansovoe pravo i upravlenie. 2014. No. 3. Pp. 184–198.
26. Zagriatskov M.D. Biudzhethnye prava mestnykh Sovetov. M. : Izd-vo Gl. upr. Kommun. khoz-va NKVD, 1924. 60 pp.
27. Pontovich E.E. Finansovyi kontrol'. L.: Finansovoe izd-vo NKF SSSR, 1928. 107 pp.
28. Rovinskii E.A. Osnovnye voprosy teorii sovetskogo finansovogo prava. M. : Gosizdat, 1960. 193 pp.
29. Finansovoe pravo : uchebnyk. Sost.: Gurvich M.A., Zalesskii M.Ia., Raider A.K., Shvartsman A.O., Shmakov K.K.; obshch. red.: Gurvich M.A. M. : Iurid. izd-vo NKlu SSSR, 1940.
30. Vyshinskii A.Ia. Osnovnye zadachi nauki sovetskogo sotsialisticheskogo prava (Sokrashchennaya stenogramma doklada na 1-m soveshchanii po voprosam nauki sovetskogo prava i gosudarstva 16 iulia 1938 g.). Sotsialisticheskaya zakonnost'. 1938. No. 8. Pp. 1–34.
31. Andrianova N.G., Vasilina E.L., Kobzar'-Frolova M.N. Evoliutsiya teorii finansovogo pravootnosheniia: (istoriograficheskie i dogmaticheskie aspekty stanovleniia i razvitiia). Gosudarstvo i pravo. 2025. No. 1. Pp. 145–159.
32. Bel'skii K.S. Zabytyi "patriarkh" sovetskoi nauki finansovogo prava (k 120-letiiu so dnia rozhdeniia M.A. Gurvicha). Gosudarstvo i pravo. 2017. No. 9. Pp. 93–100.
33. Khalfina R.O. K voprosu o predmete i sisteme sovetskogo finansovogo prava. Voprosy sovetskogo administrativnogo i finansovogo prava. M. : Izd-vo AN SSSR, 1952. Pp. 182–214.

О РОЛИ ПРАВИТЕЛЬСТВА В ПОЛИТИЧЕСКОЙ СИСТЕМЕ РОССИИ

Запольский С.В.¹

Ключевые слова: Конституция, Президент, социальная политика, исполнительная власть, публичная власть, компетенция, администрирование.

Аннотация

Цель. Анализ изменений в правовом положении правительства Российской Федерации.

Метод. Сравнительно-правовой метод правовых механизмов.

Результат. В связи с поправкой к Конституции России, принятой в 2020 году, произошли структурные изменения в механизме государственного управления: кристаллизована (уточнена и конкретизирована) роль Президента РФ, подвергся реконструкции алгоритм взаимоотношений президента с правительством, министерствами и ведомствами. Анализируются изменения в правовом положении кабинета министров как в иерархическом смысле, так и в аспекте расширения функций правительства по влиянию на социальные и экономические процессы, протекающие в стране. Сделан акцент на гармоничном сочетании полномочий президента как главы государства и правительства, осуществляющего исполнительную власть под общим руководством президента; проанализирована конституционная природа общего руководства деятельностью кабинета министров со стороны президента.

DOI: 10.24412/1994-1404-2025-1-14-18

В Конституции России правительству посвящена отдельная глава, шестая, определяющая функции, полномочия, порядок создания, взаимоотношения с президентом и Федеральным Собранием, другие аспекты деятельности кабинета министров; правительству посвящен федеральный конституционный закон, детализирующий правовое положение органа, осуществляющего подавляющий объем исполнительной власти в стране. Тем не менее роль Правительства РФ в организации политической системы и осуществлении социально-экономической политики оставалась весьма противоречивой. Правительство, будучи исполнителем воли Федерального Собрания, выраженного в законах, и воли главы государства, который осуществляет общее руководство его деятельностью, по образной оценке Ю.А. Тихомирова, по-прежнему работает в режиме «чего изволите», либо «что требуется», либо «по моему собственному усмотрению»... Патология усмотрения администрирования стала очень горькой. Конституция живет тогда, когда она является инструментом управления процессами и жизнью, это будет существенно² [1].

² Стенограмма юбилейного заседания Конституционного клуба. Обсуждение статьи В.Д. Зорькина «Буква и дух Конституции». Конституционный вестник. 2019. № 4 (22). С. 73.

¹ **Запольский Сергей Васильевич**, доктор юридических наук, профессор, главный научный сотрудник Института государства и права РАН, заслуженный юрист Российской Федерации, г. Москва, Российская Федерация.

E-mail: zpmoscow@mail.ru

До внесения поправки в Конституцию РФ в 2020 году конституционно-правовое положение правительства не было определено. Сопоставление ст. 10 и 11 Конституции дает основания считать, что Президент Российской Федерации, не относясь ни к законодательной, ни тем более к судебной власти, входит в исполнительную ветвь власти и возглавляет ее. В то же время ст. 110 Конституции в старой редакции гласила, что правительство, и по логике вещей — только оно, осуществляет исполнительную власть.

В уточненной редакции правительство осуществляет исполнительную власть под общим руководством Президента РФ. Тем самым соотношение полномочий и функций Президента РФ и Правительства РФ получило значительно большую определенность, нежели это предполагал текст Конституции РФ до внесения в нее в 2020 году поправки.

Во-первых, получили обоснование практически все нормы статьи 83 Конституции РФ, относящиеся к деятельности кабинета министров, поскольку предусмотренные ею полномочия — не что иное, как общее руководство, упомянутое в ст. 110 Конституции РФ. Полномочия президента по определению структуры федеральных органов исполнительной власти, соотношения этих органов между собой, утверждения поло-

жений о министерствах и ведомствах, оценка деятельности Председателя правительства и всего кабинета министров — есть не что иное, как общее руководство правительством как органом государственного управления.

Во-вторых, Президент РФ как орган федеральной власти приобретает юридическую возможность осуществлять государственную власть по предметам ведения РФ и по предметам совместного ведения РФ и субъектов РФ (см. ст. 72 Конституции РФ), на основе ч. 2 статьи 77 Конституции РФ, говорящей о единстве системы исполнительной власти Российской Федерации и ее субъектов. Безусловно, это не только расширяет возможность Президента РФ влиять на социально-экономическую политику субъектов Федерации, но, прежде всего, организационно обеспечивает выполнение п. 2 статьи 80 Конституции РФ в части согласованного функционирования и взаимодействия органов, входящих в единую систему публичной власти.

В-третьих, возложение на президента общего руководства органами части исполнительной власти, в целом подведомственных Правительству, снимает коллизию между статусом руководителей федеральных органов, самих этих органов (т. н. «силовой блок» — см. ч. «в» и «д» ст. 83 Конституции) и статусом иных органов исполнительной власти и их руководителями, руководство которыми осуществляет Правительство РФ.

Следует принять во внимание и то, что статус главы государства (ч. 1 ст. 80 Конституции) предполагает наличие у президента полномочий и функций по руководству органами государства, не входящими в систему органов исполнительной власти, но выполняющих аналогичные или сходные функции. Достоинством новой редакции Конституции РФ служит четкое разграничение исполнительной власти и достаточно широкого круга органов публичной власти иной правовой и политической природы, таких как прокуратура, Следственный комитет, Судебный департамент, контрольно-счетные органы, включая Счетную палату, социальные страховые фонды, избирательные комиссии, Национальный олимпийский комитет, Администрация Президента, государственные корпорации и др. В сущности, речь идет о дополнении формулы, приведенной в ст. 10 Конституции, путем выделения органов публичной власти, наделяемых компетенцией особого рода, что отграничивает их от системы органов исполнительной власти.

Представляется, что полное слияние полномочий правительства с властью, которой Конституция РФ наделяет президента, было бы неправильно. «Общее руководство» следует отнести не к деятельности правительства в ее полном объеме, но именно к осуществлению исполнительной власти. Далеко не все функции и полномочия кабинета министров реализуются путем административного распорядительства. Здесь речь следует вести о деятельности кабинета министров по инициированию, поддержке, институализации многих программ и проектов, направленных на социальное

развитие российского общества, упомянутых в статье 114 Конституции России. Достаточно сказать, что приоритетные национальные проекты, прежде чем стать предметом администрирования, финансирования и контроля, рождаются и формируются под опекой правительства, его аппарата, а впоследствии осуществляются как правительственные проекты.

Статья 114 Конституции РФ, существенно измененная и дополненная путем утверждения поправки 2020 года, охватывает многие прерогативы, использование которых включает как реализацию исполнительной власти, так и иные виды деятельности организационного, воспитательного и стимулирующего толка, таких как воспитание экологической культуры, формирование ответственного отношения к животным, поддержка институтов гражданского общества, создание доступной среды для инвалидов, укрепление и защита семьи и многое другое.

Уместен вывод о существенном расширении сферы деятельности правительства в результате принятия Закона РФ «О Правительстве РФ» за счет включения в компетенцию кабинета министров функций, однотипных с функциями Президента РФ, в частности, осуществления социальной политики, развития гражданского общества, защиты прав и свобод человека и гражданина, предусмотренных ч. 2 ст. 10 Конституции³.

В теоретическом ключе весьма важным вопросом является установление пределов функций правительства по осуществлению исполнительной власти. В оригинальном варианте Конституции РФ, в частности, правительству предоставлялась возможность издавать постановления и распоряжения только на основании и во исполнение Конституции, федеральных законов, нормативных указов президента.

Продолжительный период действия первоначального варианта Конституции РФ показал, что ограничение полномочий правительства только исполнительной властью, равно как и игнорирование того, что президент как глава государства также обладает исполнительной властью, не служит на пользу дела и недостаточно эффективно. Поправкой 2020 года создан правовой режим, создающий, с одной стороны, возможность для президента осуществлять исполнительную власть самостоятельно, с другой — позволяющий кабинету министров ведение управленческой деятельности по направлениям, ранее относимым только к исключительным полномочиям законодателя. В частности, статья 114 дополнена девятью новыми прерогативами правительства, обеспечивающими его влияние на широкий круг политических, социальных и экономических процессов в стране. Немаловажным обстоятельством является и укрепление способов взаимодействия Президента и Правительства РФ в виде двух новых каналов — распоряжений и поручений главы государства, позволяющих правительству оперативно

³ ФКЗ «О Правительстве Российской Федерации» // Собрание законодательства РФ. 2020. № 45. Ст. 7061.

реагировать на изменяющуюся внешнюю и внутреннюю обстановку.

Общим результатом введения в действие поправки в Конституцию РФ стал отказ от, выражаясь спортивным языком, «сдвоенного центра» и переход к управленческому механизму, характерному для многих иностранных государств, где глава государства осуществляет руководство кабинетом министров, а последний является практически исполнителем функций и полномочий президента. Эти изменения, которые в недалеком будущем должны показать свой созидательный потенциал, вызовут и уже вызывают существенную перенастройку механизма управления.

Прежде всего отметим, что в силу приближения правительства к главе государства как государственному органу уточняется, а со временем, возможно, исчезнет посредник — аппарат кабинета министров для взаимодействия президента с министерствами и ведомствами. Помимо «силового блока», непосредственно на президента выходят и некоторые другие органы исполнительной власти, относящиеся к ареалу правительства — Минздрав, Роспотребнадзор, Минэкономразвития, Антимонопольная служба; они значительное время пользуются повышенным вниманием президента, и круг этих ведомств постепенно расширяется.

Во многом возникновение подобной тенденции нельзя не связывать с принятием Федеральным Собранием РФ ФКЗ «О Правительстве РФ», которым перевод в рабочий режим взаимоотношений президента с министерствами, службами и агентствами, подведомственными правительству, зафиксирован юридически. Достаточно назвать новую функцию президента, согласно названному закону получившего право утверждать положения и другие соответствующие статутные акты, определяющие функцию и компетенцию исполнительных органов, ранее предоставленную правительству.

При известной доле условности можно предположить, что взаимодействие президента с министерствами и ведомствами и руководство их деятельностью со стороны правительства в будущем приведет к созданию структурно-сложного механизма, в рамках которого функция руководства кабинетом министров перейдет к президенту, а на правительство как на консолидированный орган будут возложены функции и полномочия по управлению всей совокупностью исполнительных органов, как федерального значения, так и созданных субъектами федерации. В сущности, в этом ничего необычного нет, так как глава государства в президентских республиках *ex officio* является и главой кабинета министров. Характерно, что первоначально во время создания Правительства России оно понималось как второстепенный орган. Как пишут Ю.Л. Шульженко и Д.Ю. Шульженко, «Совет Министров, созданный в 1861 году, рассматривался как учреждение, созданное для придания деятельности отдельных министров большего единства и солидарности, путем

выработки под непосредственным руководством Императора общего плана управления»⁴ [3].

Положительно оценивая наметившуюся тенденцию, следует предположить ее важный потенциальный результат — отказ от руководства министерствами и ведомствами путем направления поручений правительства (ПП) и иных форм приказаний. Министерство, служба, агентство — самодостаточный правосубъект, на который возложено проведение государственной политики во вверенной отрасли или круге вопросов. Выдача поручений правительства само по себе дифференцирует деятельность органа на приоритетную (во исполнение ПП) и иную, не требующую оперативного отчета. Соответственно, работа ведомства оценивается по выполнению оперативных поручений, а не по общим, возложенным на орган функциям. Думается, что инициативная деятельность министерства, иного ведомства должна стать ведущей формой работы, тогда как поручениям правительства суждено стать инструментом контроля и координации внутри системы органов исполнительной власти.

Перераспределение функций между президентом, правительством, министерствами и ведомствами следует расценивать как процесс естественного совершенствования социально-политической структуры управления. Концепция «сдвоенного центра» как в дореволюционной (Государь и правительство) и послереволюционной интерпретации (ВЦИК и СНК), так и в последний период, предшествовавший распаду СССР (Политбюро и правительство), испытывает потребность преобразования в монорежим, сохраняя одновременно позитивные достижения, выработанные за продолжительный период функционирования органа исполнительной власти, отдельного от главы государства.

Особенностью текущего в настоящее время конституционного развития следовало бы признать то, что на основе поправки Конституции 2020 года президент и правительство не находятся в режиме соподчинения, но взаимодействуют функционально, с одной стороны, как единый исполнительный орган государственной власти, с другой — как соорганизаторы социального и экономического развития, осуществляя эту деятельность принадлежащими им полномочиями в своих сферах деятельности.

Проблемы, затронутые выше, далеко не впервые обсуждаются в печати. обстоятельному анализу соотношения власти президента и правительства подверг в 2003 году В.Е. Чиркин⁵ [2]. Им была высказана мысль о невозможности отнесения Президента РФ к исполнительной власти в связи с тем, что статус главы государства требует от президента распространения его функций на все три ветви власти в равной мере,

⁴ Шульженко Ю.Л., Шульженко Д.Ю. Наука русского государственного права второй половины XIX века. М., 2009. С. 144.

⁵ Чиркин В.Е. Президент и исполнительная власть в системе разделения властей: реалии современной России // В кн.: История становления и современное состояние исполнительной власти в России. М.: Новая правовая культура, 2003. С. 114.

а следовательно, правительство есть единственный важный орган государства, отправляющий исполнительную власть. Возможно, при правоте В.Е. Чиркина тогда, в 2003 году, к современному периоду конституционного развития возникли бы новые побудительные причины и императивы расширения возможностей президента в осуществлении исполнительной власти, а правительство осуществляет и реализует исполнительную волю президента.

Очевидно, дело в расхождении понимания самого существа исполнительной власти. Исходя из формулы, приводимой в ст.10 Конституции, исполнительная власть предполагает в конечном счете материализацию и социализацию федеральных во многом вновь принятых законов, судебная власть — применение этих законов в судопроизводстве. Здесь, действительно, роль президента сводится к подписанию законов и наблюдению за их применением.

Однако исполнительная власть в социально-политическом смысле не может не охватывать каждодневную работу по поддержанию социума в относительной

стабильности, балансировки различных сил и тенденций, наконец, исполнения самой Конституции на основании ст. 71, 72, 114, действующих «напрямую», безотносительно к наличию или отсутствию законов, конкретизирующих эти положения. Поэтому поправка 2020 года к Конституции Российской Федерации в части, относящейся к Правительству, существенно расширяет возможности кабинета министров как в осуществлении исполнительной власти, так и по формированию руководства социально-экономической политикой в стране. Показательно, что новые полномочия у кабинета министров появились практически одновременно с возникновением и расширением эпидемии коронавируса, в борьбе с которой решающую роль играют правительство и федеральный орган исполнительной власти — Минздрав России и Роспотребнадзор, наряду с региональными правительствами. Это не может не свидетельствовать о наличии тенденции углубления и совершенствования значения исполнительной власти в современных непростых внутренних и внешних условиях развития российского общества.

Литература

1. Шульженко Ю.Л., Шульженко Д.Ю. Наука русского государственного права второй половины XIX века. М., 2009. С. 144.
2. Чиркин В.Е. Президент и исполнительная власть в системе разделения властей: реалии современной России // В кн.: История становления и современное состояние исполнительной власти в России. М. : Новая правовая культура, 2003. С. 114—121.
3. Конституционный вестник. 2019. № 4. С. 73.
4. Россинский Б.В. Проблемы государственного управления с позиций теории систем. М. : Норма, 2021. С. 246.
5. Формы и методы государственного управления в современных условиях развития / Коллектив авторов. М. : Прометей, 2017.
6. История становления и современное состояние исполнительной власти в России. М., 2003.
7. Советский государственный строй: реалии, проекты, идеи, споры (1945—1985 гг.). М. : ИГП, 2012.
8. Конин Н.М. Административное право России. М., 2006.
9. Лазарев Б.М. Можно ли было сохранить СССР (правовое исследование). М., 2002.
10. Публичный интерес в административном праве. М. : ИГП, 2015.
11. Махина С.И. Административная децентрализация : история, современность, перспективы : монография. М. : Изд-во Рос. соц. гос. ун-та, 2011. 191 с.

SECTION:
CONSTITUTIONAL LAW

ON THE ROLE OF THE GOVERNMENT IN THE POLITICAL SYSTEM OF RUSSIA

*Sergei Zapol'skii, Dr.Sc. (Law), Professor, Principal Researcher at the Institute of State and Law of the Russian Academy of Sciences, Honoured Lawyer of the Russian Federation, Moscow, Russian Federation.
E-mail: zpmoscow@mail.ru*

Keywords: Constitution, President, social policy, executive power, public authority, competency, administration.

Abstract

Purpose of the study: analysing changes in the legal status of the Government of the Russian Federation.

Method used in the study: the comparative legal method of legal mechanisms.

Study findings: due to an amendment to the Constitution of Russia adopted in 2020, structural changes in the public administration mechanism took place: the role of the President of Russia was crystallised (that is, specified with precision and in more detail), and the procedure for relations between the President and the Government, ministries and institutions underwent a restructuring. Changes in the legal status of the Government are analysed, both in the hierarchical sense and in the aspect of broadening the functions of the Government as regards its impact on social and economic processes in the country. A harmonious combination of the powers of the President as Head of the State and of the Government exercising executive authorities under the general guidance of the President is emphasised, and an analysis of the constitutional nature of the general guidance of the President as regards the Government is given.

References

1. Shul'zhenko Iu.L., Shul'zhenko D.Iu. Nauka russkogo gosudarstvennogo prava vtoroi poloviny XIX veka. M., 2009. P. 144.
2. Chirkin V.E. Prezident i ispolnitel'naia vlast' v sisteme razdeleniia vlastei: realii sovremennoi Rossii. V kn.: Istoriiia stanovleniia i sovremennoe sostoianie ispolnitel'noi vlasti v Rossii. M. : Novaia pravovaia kul'tura, 2003. Pp. 114–121.
3. Konstitutsionnyi vestnik. 2019. No. 4. P. 73.
4. Rossinskii B.V. Problemy gosudarstvennogo upravleniia s pozitsii teorii sistem. M. : Norma, 2021. P. 246.
5. Formy i metody gosudarstvennogo upravleniia v sovremennykh usloviakh razvitiia. Kollektiv avtorov. M. : Prometei, 2017.
6. Istoriiia stanovleniia i sovremennoe sostoianie ispolnitel'noi vlasti v Rossii. M., 2003.
7. Sovetskii gosudarstvennyi stroi: realii, proekty, idei, spory (1945–1985 gg.). M. : IGP, 2012.
8. Konin N.M. Administrativnoe pravo Rossii. M., 2006.
9. Lazarev B.M. Mozhno li bylo sokhranit' SSSR (pravovoe issledovanie). M., 2002.
10. Publichnyi interes v administrativnom prave. M. : IGP, 2015.
11. Makhina S.I. Administrativnaia detsentralizatsiia : istoriia, sovremennost', perspektivy : monografiia. M. : Izd-vo Ros. sots. gos. un-ta, 2011. 191 pp.

ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ СРЕДЫ

Карцхия А.А.¹

Ключевые слова: киберпространство, национальная безопасность, информационное право, цифровое право, персональные данные, кибербезопасность, защита информации.

Аннотация

Цель исследования: правовой анализ информационной среды, ее содержания и особенностей формирования при использовании современных информационно-коммуникационных и цифровых технологий, которые находят свое отражение в национальном и международном праве.

Методы исследования: сравнительно-правовой анализ действующего российского и международного законодательства в сфере информационной цифровой среды и практики применения, а также формально-логическое исследование понятийного аппарата, содержания и структуры предмета исследования.

Результаты исследования: сформулированы особенности информационной цифровой среды и ее содержания, в т. ч. с точки зрения кибербезопасности и национальной безопасности в информационной сфере. Автор полагает закономерным формирование информационной среды, цифрового технологического пространства в новом, не аналоговом физическом измерении как новой сферы правового регулирования, что обуславливает формирование специального законодательства в данной сфере и специального правового регулирования.

Научная новизна исследования: выявление понятия и качественных характеристик, особенностей содержания информационной цифровой среды, ее элементов и степени влияния на реальные отношения.

DOI: 10.24412/1994-1404-2025-1-19-31

Введение

XX век стал свидетелем масштабных социальных преобразований, а 1950-е годы ознаменовались сменой парадигмы — «информационной революцией», связанной с формированием «информационного общества», или общества, основанного на знаниях. Мир изменился и тогда, когда Интернет в 1993 году стал общедоступным пространством, создав цифровую параллель с повседневной «аналоговой» жизнью. За последние два десятилетия цифровые технологии коренным образом изменили восприятие информации и взаимодействие с ней. Интернет позволил создавать контент и делиться им с широкой аудиторией с минимальными затратами, социальные сети стерли границы между личной и массовой коммуникацией, а поисковые системы сделали огромные объемы информации широко, мгновенно и свободно доступными. Однако первоначальный оптимизм по поводу позитивного преобразующего потенциала цифровых технологий уступил место критическому осознанию связанных с ними рисков, включая риски поляризации общества по идеологическим воззрениям и фрагментации политического дискурса, возрастающие риски

недобросовестного распространения дезинформации в Интернете с использованием противоправных способов. В общий лексикон вошел термин «киберпреступность», которая затрагивает уже всех, а не только беспечных граждан или «небрежный» бизнес. Каждый человек и организация могут стать потенциальной мишенью, сталкивались с киберпреступностью в той или иной форме. Информационная безопасность приобретает первостепенное значение как для граждан, так и для компаний. Конфиденциальность все чаще рассматривается как основополагающее требование как для деловой практики, так и для отношений частного характера, а защита конфиденциальной информации стала неотъемлемой частью коммерческой деятельности. В то же время кибербезопасность стала стратегическим приоритетом не только государственной политики, но и предпринимательства и частной жизни. Нарушение конфиденциальности может привести к значительному юридическому, финансовому и репутационному ущербу, что подтверждает необходимость комплексного подхода к защите данных. Соблюдение всемирно признанных

¹ Карцхия Александр Амиранович, доктор юридических наук, профессор РГУ нефти и газа (НИУ) им. И.М. Губкина, г. Москва, Российская Федерация.
E-mail: arhz50@mail.ru

стандартов безопасности обеспечивает прозрачность и всестороннюю ИТ-защиту. Соблюдение глобальных стандартов безопасности, отслеживаемость и подотчетность приобретают решающее значение, особенно в трансграничных контактах или международных сделках, где безопасность обработки данных имеет решающее значение. Соответствие мировым стандартам безопасности должно демонстрировать приверженность компаний и отдельных лиц информационной безопасности, а также обеспечивает структурированные подходы к управлению рисками кибербезопасности.

Технический прогресс, как отмечается в рекомендациях ООН², за несколько коротких десятилетий произвел революцию в сфере коммуникаций, объединив отдельных людей и сообщества в немыслимых ранее масштабах и предоставив беспрецедентные возможности для распространения знаний, культурного обогащения и устойчивого развития. Они во многом повысили стремление к целостности информационной экосистемы, где в полной мере обеспечивается свобода выражения мнений и где точная, надежная информация, свободная от дискриминации и ненависти, доступна всем в открытой, инклюзивной, безопасной информационной среде. Хотя эти достижения позволили массово распространять информацию, они также способствовали распространению дезинформации и разжиганию ненависти многими субъектами с беспрецедентными в истории объемами, скоростью и вирусностью, ставя под угрозу целостность информационной экосистемы. Такие риски включают в себя целый ряд текущих, возникающих и будущих угроз в условиях стремительного развития технологий искусственного интеллекта (ИИ). Такое нарушение целостности информационного пространства может подорвать способность людей осуществлять права человека и помешать усилиям по достижению мира, процветания и достойного будущего на нашей планете. Таким образом, задача укрепления информационной целостности представляет собой одну из наиболее актуальных задач нашего времени. Информационная целостность предполагает плюралистическое информационное пространство, которое защищает права человека, мирные общества и устойчивое будущее. Оно несет в себе обещание цифровой эры, которая способствует доверию, знаниям и индивидуальному выбору для всех. Обеспечение целостности информации предполагает предоставление людям возможности осуществлять свое право искать, получать и распространять информацию и идеи любого рода, а также беспрепятственно придерживаться своего

мнения. Во все более сложной цифровой информационной среде это означает предоставление людям возможности безопасно перемещаться в информационном пространстве, сохраняя конфиденциальность и свободу. Усилия по повышению целостности информации имеют решающее значение для сохранения и дальнейшего продвижения целей в области устойчивого развития.

Разрушительные возможности манипулирования информацией как один из указанных WEF 2025 глобальных рисков³ стремительно возрастают по мере распространения открытого доступа ко всё более совершенным технологиям и снижения доверия к информации и институтам. Число пользователей Интернет и соцсетей неуклонно растет из года в год (см. табл. 1 и табл. 2). Вместе с тем дезинформация — новый лидер топ-10 рейтинга глобальных рисков. Простые в использовании интерфейсы для крупномасштабных моделей ИИ, которые больше не требуют специальных навыков, уже привели к резкому росту количества фальсифицированной информации и так называемого «синтетического» контента — от сложного клонирования голоса до поддельных веб-сайтов. Для борьбы с растущими рисками правительства начинают внедрять новые и постоянно меняющиеся нормативные акты, нацеленные как на владельцев, так и на создателей онлайн-дезинформации и незаконного контента. Зарождающееся регулирование генеративного ИИ сможет дополнить эти усилия. Например, в КНР требования о нанесении водяных знаков на контент, созданный с помощью ИИ, могут помочь идентифицировать ложную информацию, включая непреднамеренную дезинформацию с помощью контента, созданного с помощью ИИ. В течение следующих двух лет искусственный контент будет манипулировать людьми, наносить ущерб экономике и разрушать общество различными способами. Фальсифицированная информация может быть использована для достижения различных целей, от борьбы за изменение климата до эскалации конфликтов. Также будут распространяться новые виды преступлений, такие как подделка порнографии без согласия пользователя или манипулирование фондовым рынком. Существует риск нарушения баланса между предотвращением дезинформации и защитой свободы слова, усиления нормативного контроля со стороны государства за информацией для нарушения прав человека, широкое использование дезинформации и средств ее распространения для разжигания публичных беспорядков и насильственных протестов, преступлений на почве ненависти и даже гражданской конфронтации и терроризма.

² United Nations Global Principles for Information Integrity. Recommendations for Multi-Stakeholder Action. URL: <https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf>

³ Global Risks Report 2024, WEF 2025, p. 18. URL: <https://trendsunplugged.io/wp-content/uploads/2024/01/The-Global-Risks-Report-2024.pdf>

Таблица 1

Число пользователей Интернет в мире (млрд человек)

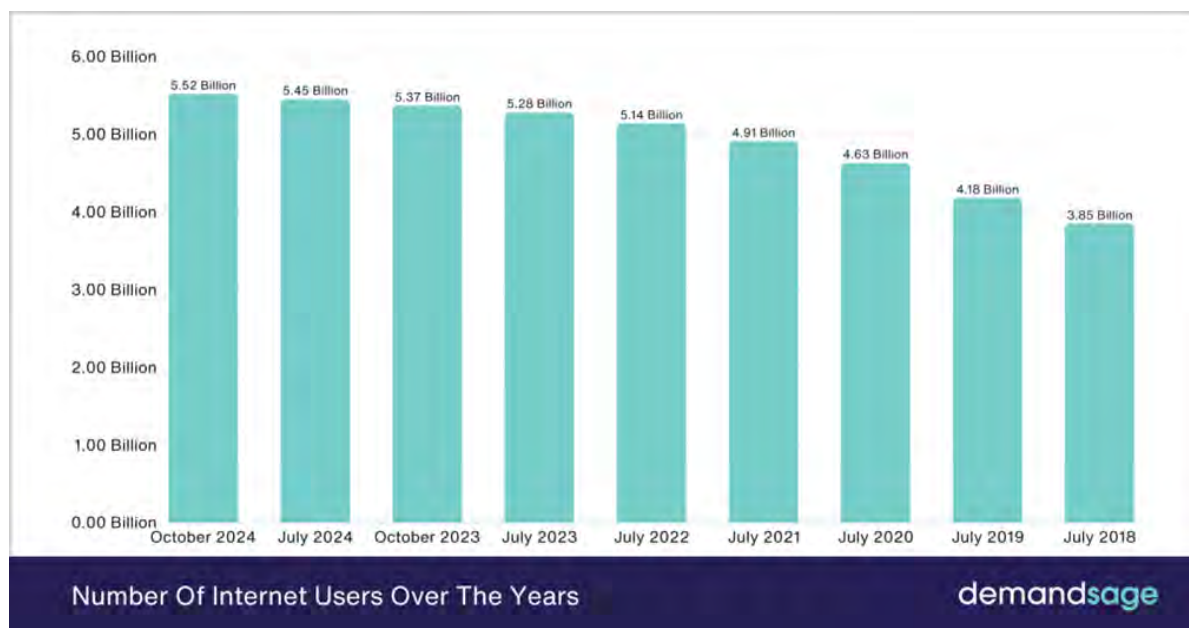
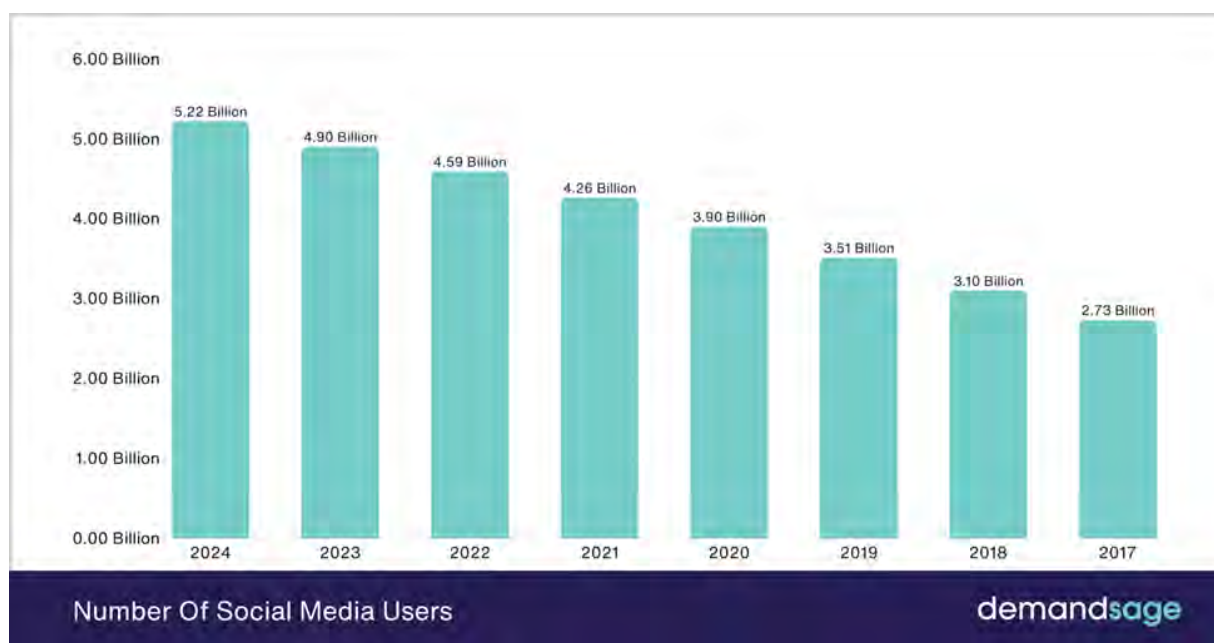


Таблица 2

Число пользователей социальных сетей в мире (млрд человек)



Источник: <https://www.demand sage.com/internet-user-statistics>

Информационная среда: понятие и особенности

Часто информационная среда понимается как пространство, где сходятся человеческое познание, технологии и контент, где информация обрабатывается людьми и, все чаще, машинами и которое включает технологии, используемые для обработки этой инфор-

мации и доступа к ней, в том числе мобильные телефоны, Интернет и дополненная реальность, а также сопутствующий контент. Иными словами, информационная среда представляется адаптивной системой, сложность которой возрастает с появлением новых социальных норм и технологий, которая подвергается негативным влияниям, угрожающим целостности такой среды, психологическому и физическому здоро-

вью ее участников, даже общественной безопасности и государственному строю⁴.

Термин «информация» преимущественно используется как абстрактное массовое понятие и обозначает любой объем данных, кода или текста, который хранится, отправляется, принимается или обрабатывается любым способом. Точное значение термина «информация» в разных философских традициях различно, а его разговорное употребление варьируется географически и в разных прагматических контекстах. Хотя анализ понятия информации был темой западной философии с самого ее зарождения, явный анализ информации как философской концепции появился недавно и восходит ко второй половине XX века. Исторически сложилось так, что изучение концепции информации можно рассматривать как попытку сделать измеримыми обширные свойства человеческого знания. Информация включает в себя широкий спектр понятий и явлений. Они относятся как к процессам, так и к материальным состояниям, которые тесно взаимосвязаны. Информация может быть продуктом, который включает в себя информацию как вещь, как объект, как ресурс, как товар, или то, что передается по каналу, включая сам канал, или даже фактическое содержание носителя. Информация имеет множество различных абстракций. Данные могут быть как отдельными наблюдениями, так и примитивными сообщениями низкого уровня. Информация представляется как отсортированные, классифицированные или проиндексированные данные в организованные наборы. В то же время информация — это отличный товар, которым обычно обмениваются люди-операторы, стремящиеся приобрести достаточно знаний о рассматриваемой проблеме. Понимание информации (знание) обеспечивает определенную степень понимания как статических, так и динамических взаимосвязей объектов данных и способность моделировать структуру и поведение этих объектов в прошлом (и будущем). Знания включают в себя как статическое содержимое, так и динамические процессы. Экспертные знания представляют собой совокупность знаний по определенной теме, предмету или процессу, которое позволяет достичь информационного превосходства, т. е. способности собирать, обрабатывать и распространять непрерывный поток информации, одновременно используя или лишая противника возможности делать то же самое⁵.

Последние десятилетия отечественными исследователями активно развивались воззрения, согласно ко-

торым жизнь человека развёртывается не только в физической среде, мире природы, но и в им же созданном искусственном мире, который делится на два основных компонента — техносферу (мир науки, техники, технологий) и информационную среду⁶. Техносфера рассматривается как часть биосферы, коренным образом преобразованная человеком в технические и техногенные объекты, становящиеся частью ноосферы. Информационная среда общества не представляется статичной, наполняемость ее изменяется по мере развития технических средств.

Изменение взаимодействия участников с информационной средой, беспрецедентный масштаб и уровень детализации при анализе огромных объемов данных в любых сферах жизнедеятельности позволяют с новых позиций рассматривать преимущества и риски цифровых преобразований, оценивать фундаментальные когнитивные механизмы взаимодействия с информацией и выдвигать новые гипотезы о функционировании этих механизмов в эпоху цифровых технологий. Такой подход объективно нуждается в определении термина «информационная среда», который часто используется без предварительного определения и приобретает различные значения в зависимости от контекста, в котором он используется.

Как отмечают современные исследования [3; 8], термин «информация» сам по себе не имеет единого определения. Одна из интересных концепций сформулирована в семиотике, науке о знаках и сигналах в широком спектре биологических, инженерных и социальных систем. Специалисты этой области понимают информацию как неожиданное, новое содержание знака, означающее, что существует двойное понимание информации, поскольку оно относится как к объекту, служащему знаком, так и к когнитивному процессу распознавания новизны в нем. Так, широко используется общее определение информации⁷, основанное на семиотической концепции информации как «текст + контент» (*text + content*)⁸ либо как «данные + значение» (*data + meaning*). Такой концептуальный подход основан на том, что информационное наполнение состоит из данных, которые являются правильно сформированными, т. е. синтаксически корректными, и значимыми (семантически корректными). Данные, в свою очередь, могут быть поняты как неинтерпретируемое отсутствие единообразия в реальном мире, между сигналами или символами. К примеру, новостная статья представляет собой информацию, поскольку она состоит из данных (букв), следует грамматическим пра-

⁴ Alicia Wanless and Jacob N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for International Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/Wanless_Shapiro_CERN_final.pdf

⁵ Michel J. Menou, Richard D. Taylor. A "Grand Challenge": Measuring Information Societies. *Inf. Soc.* 22(5):261–267; Birger Hjørland. Theory and metatheory of information science: A new interpretation. *Journal of Documentation*, December 1998. URL: <https://www.researchgate.net/publication/228717437>; R. Mathar. Information Theory. URL: <https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf>

⁶ Дружилов С.А. Современная информационная среда и экология человека: психологические аспекты // *Hygiene & Sanitation (Russian Journal)*. 2018. № 97. С. 597—602.

⁷ Floridi, Luciano (2005). *Semantic conceptions of information*, Stanford Encyclopedia of Philosophy; Floridi, Luciano (2010). *Information: A Very Short Introduction*. Oxford University Press, 2010.

⁸ Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. *Journal of Documentation*. 2003. 59(5): 505—522. DOI: 10/1108/00220410310499564.

вилам и доносит смысл до читателя. Упрощенно можно определить окружающую среду как физическое, социальное и цифровое окружение индивида, в частности, те аспекты этого окружения, которые могут влиять на поведение индивида.

Следуя этому концепту, информационную среду можно определить как состоящую из всех информационных процессов, услуг и сущностей, включая, таким образом, информационных агентов, а также их свойства, взаимодействия и взаимоотношения. Примечательно, что термин «агент» охватывает как отдельных лиц, так и организации. Отдельные лица могут обрабатывать информацию, которую они получают, и взаимодействовать с ней посредством социальных сетей или средств массовой информации. Они также могут формировать свою информационную среду и вносить в нее свой вклад, самостоятельно создавая информационный контент или делясь им. Они могут действовать в одиночку или группой, скоординированно или нескоординированно. С другой стороны, организации включают в себя новостные агентства и другие учреждения, которые создают и распространяют информацию, а также, в частности, цифровые платформы и социальные сети, которые облегчают обмен информацией между отдельными лицами, а также между отдельными лицами и организациями. Информационная среда динамична и меняется в зависимости от технологических инноваций, а также социальных и политических обстоятельств. Анализ влияния информационной среды на индивидов и группы означает анализ фактических данных о том, как эта среда влияет на индивидуальное и коллективное поведение, а также о том, как индивиды и группы взаимодействуют с ней и друг с другом, находясь в ней⁹.

Такое определение информационной среды наиболее близко к тому, которое используется в политологии или науке о коммуникациях. Но оно формулируется в расширенном контексте в качестве синонима новостной медиасреды, в частности, печати и телевидения, которая охватывает передачу социальной информации, цифровые информационные платформы и социальные медиа, а также политически значимой информации. Такое понимание информации тем не менее исключает описание информации на финансовых рынках, которая позволяет корпорациям принимать решения, или информации, используемой в корпорациях для руководства и организационной структуры. Однако информационная среда не является внутренне сплоченной и универсальной областью. Так, имеются географические различия в информационной среде, связанные с глубокими экономическими и социальными различиями между развитыми и развивающимися странами, которые отражаются в явных различиях в том, как люди воспринимают информацию по всему

миру. Например, доступ в Интернет, который радикально изменил информационную среду, предоставив доступ к онлайн-новостным сайтам и социальным сетям, расширяется во всем мире, но еще не полностью охватил страны Глобального Юга. Так, в 2019 году Международный союз электросвязи ООН сообщил, что уровень использования Интернета в странах Глобального Севера приближается к уровню насыщения: 80,1% и 74,6% пользователей в Европе и Северной и Южной Америке находятся в Сети, в то время как в Африке только 26,3% людей пользовались Интернетом, а в арабских государствах и Азиатско-Тихоокеанском регионе — 49,5% и 46,2% людей соответственно. Помимо географических различий, демографические характеристики являются ключевым фактором, определяющим индивидуальную информационную среду. Возраст, в частности, имеет большое значение, который в первую очередь касается потребления новостей, а не информации в целом. Так, молодое поколение в подавляющем большинстве случаев потребляет новости со своих смартфонов, особенно через социальные сети, в то время как старшие поколения в большей степени полагаются на телевидение, радио и печатные издания. Примечательно, что среди пользователей социальных сетей существует разделение по поколениям, например: 93% подростков в возрасте от 16 до 24 лет имели профиль в социальных сетях, в то время как 58% людей в возрастной категории 55—64 года и 34% — в возрастной группе 65—74 года [8].

Информационная среда и информационная безопасность

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 23.11.2024) (далее — Закон об информации)¹⁰ содержит определение «информация» как сведения (сообщения, данные) независимо от формы их представления, а также понятие «информационно-телекоммуникационная сеть», которая представляет собой технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Информация может носить ограниченный характер доступа и распространения в соответствии с установленным правовым режимом. Так, к охраняемой законом тайне относятся любые сведения, доступ к которым ограничен федеральными законами и указами Президента РФ. К ней, в частности, относится конфиденциальная информация, включая персональные данные, информацию, составляющую профессиональную (адвокатскую, банковскую, аудиторскую и др.), коммерческую, служебную тайну. Особый правовой режим и категорию информации составляет охраняемая законом гостайна. В некоторых случаях для придания информации статуса конфиден-

⁹ Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.

¹⁰ Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

циальной требуется ограничить доступ к сведениям, обладающим коммерческой ценностью, и установить в отношении них режим коммерческой тайны.

В предусмотренных законом случаях установлен запрет на распространение информации (ч. 6 ст. 10 Закона об информации), в т. ч. если эта информация направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, либо за ее распространение предусмотрена уголовная или административная ответственность (напр., административная ответственность за оскорбление, совершенное публично, в том числе с использованием сети Интернет (ч. 2 ст. 5.61 КоАП РФ), незаконное распространение информации о несовершеннолетнем (ч. 3 ст. 13.15 КоАП РФ), за распространение порнографических материалов или предметов среди несовершеннолетних (ч. 2 ст. 242 УК РФ). В п. 1 ч. 5 ст. 15.1 Закона об информации также приведен перечень запрещенной к распространению информации, при выявлении которой в сети Интернет уполномоченные госорганы вправе обращаться для включения страниц сайтов в соответствующий Единый реестр. Запрещается распространять материалы, производимые и (или) распространяемые иностранным агентом в связи с осуществлением им вида деятельности, установленного ст. 4 Закона об иностранном влиянии, а также информацию о таком виде деятельности без указания на то, что эти материалы (информация) произведены и (или) распространены иностранным агентом (ч. 7 ст. 10 Закона об информации, ч. 3 ст. 9 Закона об иностранном влиянии).

Вместе с тем Закон об информации не содержит понятия «информационная среда (сфера)», но дает определение информационной системы как совокупности содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

В **Доктрине информационной безопасности Российской Федерации**¹¹ под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Обеспечение информационной безопасности означает осуществление взаимосвязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению,

отражению информационных угроз и ликвидации последствий их проявления.

В то же время **Основы государственной культурной политики**¹² определяют понятие «информационная среда» как совокупность средств массовой информации, радио- и телевидение, информационно-телекоммуникационная сеть «Интернет» (сеть «Интернет»), распространяемые с их помощью текстовые и визуальные материалы, информацию, а также созданные и создаваемые цифровые архивы, библиотеки, оцифрованные музейные фонды.

Реализация стратегического национального приоритета «Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» предполагает решение ряда задач государственной политики по сохранению и укреплению традиционных ценностей, в т. ч. поддержку проектов, направленных на продвижение традиционных ценностей в информационной среде в соответствии с **Основами государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей**¹³.

Следует особо выделить значение информационного пространства во внешнеполитической сфере. Так, в **Концепции внешней политики Российской Федерации** (далее — Концепция)¹⁴ отмечается, что в международных отношениях используется широкий набор противоправных инструментов и методов, включая применение принудительных мер (санкций) в обход Совета Безопасности ООН, провоцирование государственных переворотов, вооруженных конфликтов, угрозы, шантаж, манипулирование сознанием отдельных социальных групп и целых народов, наступательные и подрывные операции в информационном пространстве, допускается использование информационно-коммуникационных технологий в противоправных целях (п. 9). Концепция выделяет среди современных тенденций развития международных отношений повышение роли фактора силы в международных отношениях, использование военной силы в нарушение международного права, освоение космического и информационного пространства в качестве новых сфер военных действий, стирание грани между военными и невоенными средствами межгосударственного противоборства (п. 11). С учетом этого определены сферы национальных интересов Российской Федерации во внешнеполитической сфере, к которым, в частности, относятся развитие безопасного информационного пространства, защита российского общества от деструктивного иностранного информационно-психологического воздействия, формирование объективного восприятия

¹² Указ Президента РФ от 24.12.2014 № 808 (ред. от 25.01.2023) «Об утверждении Основ государственной культурной политики».

¹³ Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».

¹⁴ Указ Президента РФ от 31.03.2023 № 229 «Об утверждении Концепции внешней политики Российской Федерации».

¹¹ Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

России за рубежом, укрепление ее позиций в мировом информационном пространстве.

Концепция особо оговаривает право Российской Федерации в случае совершения иностранными государствами или их объединениями недружественных действий, представляющих угрозу её суверенитету и территориальной целостности, в том числе связанных с применением ограничительных мер (санкций) политического или экономического характера либо с использованием современных информационно-коммуникационных технологий, принять симметричные и асимметричные меры, необходимые для пресечения таких недружественных действий, а также для предотвращения их повторения в будущем (п. 26).

В целях обеспечения международной информационной безопасности, противодействия угрозам в ее отношении, укрепления российского суверенитета в глобальном информационном пространстве Российская Федерация намерена уделять приоритетное внимание:

(1) укреплению и совершенствованию международно-правового режима предотвращения и разрешения межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве;

(2) формированию и совершенствованию международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях;

(3) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети Интернет на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;

(4) принятию политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства, по использованию информационно-коммуникационных технологий для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым информационно-коммуникационным технологиям и усилению их технологической зависимости.

Стратегия противодействия экстремизму в Российской Федерации¹⁵ констатирует, что наиболее опасным проявлением экстремизма является терроризм, представляющий глобальную угрозу международному миру и безопасности. Современному росту экстремистских и террористических угроз в мире способствует стремительное распространение экстремистской идеологии (включая неонацизм и радикальный национализм), в том числе в информационном пространстве. Информационно-теле-

коммуникационные сети, включая сеть «Интернет», мультимедийные и онлайн-технологии все шире используются в экстремистских целях — для вербовки новых членов, организации и координации совершения преступлений экстремистской направленности, распространения экстремистской идеологии, а также финансирования экстремистской деятельности, распространения призывов к насильственным действиям. Все чаще применяются различные методы манипулирования общественным мнением и распространения недостоверной информации, в т. ч. дискредитация использования Вооруженных Сил Российской Федерации, исполнения государственными органами Российской Федерации своих полномочий. В целях дестабилизации общественно-политической и социально-экономической обстановки в Российской Федерации специальные службы и организации иностранных государств наращивают деструктивное информационно-психологическое воздействие на население России, прежде всего на молодежь. В связи с этими угрозами основными направлениями государственной политики в сфере противодействия экстремизму предусмотрены, в частности: совершенствование законодательства Российской Федерации в части, касающейся пресечения производства экстремистских материалов и их распространения, в том числе на электронных носителях информации, а также в информационно-телекоммуникационных сетях, включая сеть «Интернет»; противодействие пропаганде идей экстремизма в средствах массовой информации и информационно-телекоммуникационных сетях, включая сеть «Интернет».

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» субъекты критической информационной инфраструктуры (государственные органы и учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления), функционирующие в критически важных отраслях здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей, переведены на преимущественное использование доверенных программно-аппаратных комплексов.

В целях обнаружения, предупреждения и ликвидации последствий компьютерных атак на информа-

¹⁵ Указ Президента РФ от 28.12.2024 № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации».

ционные ресурсы Российской Федерации¹⁶ создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которая включает информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и консульских учреждениях Российской Федерации.

Глобальная сфера информационной среды, как отмечает ряд авторов [2], не является физически определенным местом, а преодолевает границы, реализуясь в любом физическом или временном измерении. Такая среда создана слиянием совместных сетей компьютеров, информационных систем и телекоммуникационных инфраструктур, а формируемое таким образом цифровое пространство характеризуется анонимностью и доступностью информации, и обозначается в любых пространственных измерениях (на земле, в открытом море, международном воздушном пространстве или космическом пространстве), что допускает его характеристику как общемирового, общего пространства, или *res communis omnium* (общего блага всех). Это, в свою очередь, позволяет сделать вывод о том, что цифровое пространство полностью не подчинено суверенитету одного государства или группы государств и не защищено от апроприации.

Между тем достаточно показателен подход к регулированию информационной среды в стратегических документах США. Так, в соответствии со Стратегией операций в информационной среде (2023) Министерства обороны США (далее — Стратегия операций МО США)¹⁷ понятие «информационная среда» (*Information Environment*) определено как совокупность социальных, культурных, лингвистических, психологических, технических и физических факторов, которые влияют на то, как люди и автоматизированные системы извлекают смысл из информации, действуют в соответствии с ней и подвергаются ее воздействию, включая отдельных лиц, организации и системы, которые собирают, обрабатывают, распространяют или используют информацию.

Дается определение понятия «информационная сила (мощь)» (*Informational Power*) как способности использовать информацию для достижения целей и получения информационного преимущества. Сущность информационной мощи заключается в способности проявлять свою волю посредством распространения, отрицания использования и сохранения информации

для достижения целей. «Операции в информационной среде» (*Operations in the Information Environment*) рассматриваются в документе как военные действия, предполагающие комплексное использование нескольких информационных сил для воздействия на движущие силы поведения путем

информирования аудитории,
оказания влияния на соответствующих иностранных участников,
атаки и использования соответствующей информации участников, информационных сетей и информационных систем

и защиты дружественной информации, информационных сетей и информационных систем.

Стратегия операций МО США направлена на повышение способности министерства планировать, использовать ресурсы и информационную мощь для обеспечения комплексного сдерживания, проведения кампаний и создания устойчивых преимуществ, как описано в Стратегии национальной обороны (NDS). Эффективное применение информационной мощи должно пониматься более широко и целенаправленно включаться во весь спектр стратегий и операций Министерства обороны, мероприятий и инвестиций (OAI) для поддержки продвижения национальных интересов на дипломатическом уровне, информационные, военные и экономические инструменты национальной мощи в поддержку конкретных целей оборонной политики. Такое изменение обеспечивает способность Министерства обороны позитивно влиять на поведение людей и автоматизированных систем, формируя оперативную среду и укрепляя силу и доверие к Соединенным Штатам. Программа SOIE Министерства обороны направлена на усиление и сбалансирование институциональной и оперативной синергии между операциями военной информационной поддержки, гражданскими вопросами (CA), связями с общественностью (PA), совместными операциями в области электромагнитного спектра (JEMSO), операциями в киберпространстве, космическими операциями, специальными техническими операциями (STO), действиями по дезинформации обороны (DDA), безопасности операций (OPSEC), новые и формирующиеся виды информационной деятельности и другие дисциплины, а также информационные аспекты физической силы.

Это соответствует подходу **Стратегии международной политики Соединенных Штатов в области киберпространства и цифровых технологий** (далее — Стратегия политики)¹⁸, заключающемся в перераспределении ответственности за защиту киберпространства между правительством и организациями частного сектора, которые наиболее способны и располагают наилучшими возможностями для снижения рисков, а также перестройке стимулов в пользу долго-

¹⁶ Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

¹⁷ Strategy for Operations in the Information Environment, July, 2023, US Department of Defense. URL: <https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-department-of-defense-strategy-for-operations-in-the-information-environment.pdf>

¹⁸ United States International Cyberspace & Digital Policy Strategy, US Department of State, 2024. URL: <https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/>

срочных инвестиций в кибербезопасность с помощью дипломатии, партнерских отношений и обмена информацией. В основе Стратегии политики лежат три принципа деятельности Госдепа США:

- (i) позитивное видение киберпространства и цифровых технологий, ориентированное на использование преимуществ технологий и основанное на законе в целях безопасного использования цифровых технологий для поиска, получения и распространения информации и идей онлайн, участвуя в жизни свободных, открытых и информированных обществ, а также получения доступа к образовательным и экономическим возможностям для обеспечения инклюзивного экономического роста и надежного получения важнейших услуг и информации от своих правительств.
- (ii) интеграция кибербезопасности, устойчивого развития и технологических инноваций, где кибербезопасность, защита данных и киберустойчивость являются предпосылками и факторами, способствующими экономическому росту и созданию здорового гражданского пространства, где граждане могут осуществлять свои права;
- (iii) применение комплексного политического подхода, который использует соответствующие инструменты дипломатии и международного государственного управления во всей цифровой экосистеме, которая включает, помимо прочего, аппаратное обеспечение, программное обеспечение, протоколы, технические стандарты, поставщиков, операторов, пользователей и цепочки поставок, охватывающие телекоммуникационные сети, подводные кабели, облачные вычисления, центры обработки данных и инфраструктуру спутниковых сетей, операционные технологии, приложения, веб-платформы и потребительские технологии, а также Интернет вещей (IoT), искусственный интеллект (AI) и другие критически важные и появляющиеся технологии.

Национальная стратегия кибербезопасности США¹⁹ поставила цель создать защищенную, устойчивую цифровую экосистему, в которой атаковать системы дороже, чем защищать их, где конфиденциальная или частная информация надежно защищена и охраняется, и где ни инциденты, ни ошибки не приводят к катастрофическим системным последствиям.

В Стратегии констатируются негативные последствия цифровизации и расширения использования информационного киберпространства. В частности, указывается, что мир вступает в новую фазу углубления цифровой зависимости. Благодаря новым технологиям и все более сложным и взаимозависимым системам кардинальные изменения в предстоящем десятилетии откроют новые возможности для процветания челове-

чества, а также увеличат системные риски, связанные с ненадежностью систем.

Программное обеспечение и системы становятся все более сложными, обеспечивая ценность для компаний и потребителей, но также увеличивая коллективную незащищенность. Слишком часто новые функциональные возможности и технологии внедряются в и без того сложные и хрупкие системы в ущерб безопасности и отказоустойчивости. Широкое внедрение систем ИИ, которые могут действовать неожиданным образом даже для их собственных создателей, повышает сложность и риски, связанные со многими из наших наиболее важных технологических систем.

Цифровые технологии все чаще затрагивают самые чувствительные аспекты нашей жизни, обеспечивая удобство, но также создавая новые, зачастую непредвиденные риски. Пандемия COVID-19 заставила нас все глубже погружаться в цифровой мир. Поскольку наша жизнь тесно связана с потоковой передачей видео и аудио, носимыми устройствами и биометрическими технологиями, объем и конфиденциальность сбора персональных данных растут в геометрической прогрессии. Кража этих данных также растет быстрыми темпами и открывает новые возможности для злоумышленников следить за людьми, манипулировать ими и шантажировать.

Взаимодействие нового поколения стирает границы между цифровым и физическим мирами и подвергает некоторые из наших наиболее важных систем опасности сбоев. Заводы, энергосети, предприятия по очистке воды наряду с другими важными объектами инфраструктуры все чаще отказываются от старых аналоговых систем управления и быстро внедряют цифровые технологии оперативного управления (ОТ). Передовые беспроводные технологии, Интернет вещей и средства космического базирования, в том числе те, которые позволяют определять местоположение, навигацию и время для гражданских и военных целей, мониторинга окружающей среды и погоды, а также повседневных интернет-операций — от банковского дела до телемедицины — ускорят эту тенденцию, переведя многие из наших основных систем в оперативный режим и повысив эффективность кибератак, разрушительных и влияющих на нашу повседневную жизнь.

Вредоносная киберактивность эволюционировала от создания помех к шпионажу и краже интеллектуальной собственности, от разрушительных атак на критически важную инфраструктуру до программ-вымогателей и кампаний влияния с использованием киберпространства, направленных на подрыв общественного доверия к основам нашей демократии. Когда-то доступные лишь небольшому числу стран, обладающих достаточными ресурсами, инструменты и сервисы для взлома, включая зарубежное коммерческое шпионское ПО, теперь широко доступны. Эти инструменты и сервисы расширяют возможности стран, которые ранее не имели возможности нанести ущерб интересам

¹⁹ US National Cybersecurity Strategy, March 2023. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>

США в киберпространстве, и создают растущую угрозу со стороны организованных преступных синдикатов.

Правительства автократических государств с ревизионистскими намерениями агрессивно используют передовые кибернетические возможности для достижения целей, которые противоречат интересам США и общепринятым международным нормам. Их безрассудное пренебрежение верховенством закона и правами человека в киберпространстве угрожает национальной безопасности и экономическому процветанию США.

Новая Национальная стратегия кибербезопасности предусматривает новый подход к кибербезопасности, основанном на значительных достижениях, которые уже формируют стратегическую среду и цифровую экосистему США. Прежде всего это касается формирования современной и гибкой нормативно-правовой базы кибербезопасности, адаптированной к профилю риска каждого сектора, согласованной для сокращения дублирования, дополняющей сотрудничество государственного и частного секторов и учитывающей стоимость внедрения. *Новые и обновленные правила кибербезопасности должны быть выверены с учетом потребностей национальной и общественной безопасности, а также безопасности отдельных лиц, регулируемых организаций, их сотрудников, клиентов, операций и данных.* Ключевые сектора кибербезопасности — нефте- и газопроводы, авиация и железнодорожный транспорт, системы водоснабжения. Важно создать нормативные акты для обеспечения кибербезопасности критически важных объектов инфраструктуры. Кроме того, эти и другие критически важные сектора зависят от кибербезопасности и устойчивости своих сторонних поставщиков услуг. Облачные услуги позволяют применять более эффективные и экономичные методы обеспечения кибербезопасности в масштабах страны, но они также необходимы для обеспечения операционной устойчивости во многих секторах критической инфраструктуры.

Вместе с тем следует помнить и о том, что в стратегических документах США, таких как Национальная оборонная стратегия США (2022 г.), Федеральный закон США № 115-44 «О противодействии противникам Америки посредством санкций» (*Countering America's Adversaries Through Sanctions Act, CAATSA*) 2017 г., а также в Военной стратегии НАТО (2019 г.), Стратегической концепции НАТО от 29.06.2022 г. Российская Федерация рассматривается в качестве враждебного государства.

В КНР в 2017 г. разработан план более активного участия в мировых делах, дальнейшего экономического и социального развития, укрепления вооруженных сил и уделения более пристального внимания промышленным и технологическим инновациям, где поставлена цель добиться значительного обновления китайской нации к 2049 году. Определена приоритетность экономической стратегии для проведения более активной торговой политики, увеличения инвестиций, креди-

тования инфраструктурных проектов развивающихся стран, продвигая экономические программы, такие как инициатива «Пояс и путь», а также использования информации и применении асимметричных методов для противостояния своим противникам и доминирования над ними.

В европейских странах усилен контроль со стороны регулирующих органов, направленный на борьбу с незаконным контентом и рисками, связанными с услугами. Закон о цифровых услугах ЕС (*Digital Services Act, DSA*) налагает серьезные обязательства на поставщиков онлайн-посреднических услуг. В Соединенном Королевстве вступает в силу в марте 2025 г. Закон о безопасности в Интернете (*Online Safety Act, OSA*).

В последние годы на первый план вышли специальные законы по безопасности в Интернете, такие как Закон о цифровых услугах в ЕС, Законы о безопасности в Интернете в Великобритании, Австралии, Сингапуре. Защита детей занимает центральное место во многих из этих инициатив, а в Австралии принято законодательство, требующего от платформ социальных сетей препятствовать доступу пользователей моложе 16 лет к их услугам. В других юрисдикциях, например, в Южной Африке, применяется гибридный подход: регулирующий орган разрабатывает отраслевые кодексы поведения и управляет системой рассмотрения жалоб пользователей, а также обладает полномочиями издавать директивы общего применения.

Учитывая разрозненную динамику законодательства на федеральном уровне и в штатах США, наряду с ограничением Первой поправки к Конституции США о защите свободы слова, ключевое внимание на федеральном уровне уделяется защите детей (проект федерального закона о защите конфиденциальности детей в Интернете еще проходит законодательный процесс). В ожидании принятия всеобъемлющего федерального закона в США частный сектор продолжает саморегулироваться, при этом крупные технологические компании определяют, как действовать в отношении модерации контента, а Верховный суд США вмешивается в случае необходимости.

Как и в случае с другими правовыми режимами, регулирующими трансграничную цифровую экономику, общим для глобальных правил онлайн безопасности является их экстерриториальный характер. Основное внимание в многочисленных нормативно-правовых базах по всему миру уделяется защите пользователей, которые находятся в определённой юрисдикции или выходят в Интернет из неё, независимо от местонахождения сервисов. Это требует от глобальных поставщиков онлайн-услуг ознакомления с множеством правил и их соблюдения. Это особенно сложно, учитывая, что нормативно-правовая база представляет собой разрозненную международную мозаику. В ответ на это и для обеспечения согласованности, правительства и регулирующие органы по всему миру сотрудничают по целому ряду вопросов, включая согласование нормативно-правовой базы и правоприменительной практики

в отношении онлайн-контента. В 2019 году в Заявлении министров юстиции США, Великобритании, Австралии, Канады о противодействии сексуальной эксплуатации и насилию в отношении детей, противодействии насильственному экстремизму и терроризму как в Интернете, так и за его пределами, иностранным боевикам-террористам и шифрованию²⁰, а затем в 2021 году на саммите G7 правительства Великобритании, Канады, Франции, Германии, Италии, Японии, США и ЕС приняли совместную декларацию²¹ о принципах безопасности в Интернете для повышения онлайн-безопасности. С тех пор в феврале 2024 года правительства Австралии и Великобритании подписали совместный меморандум о взаимопонимании для укрепления двустороннего сотрудничества в борьбе с онлайн-угрозами. А в октябре 2024 года правительства США и Великобритании подписали соглашение об онлайн-безопасности, которое предусматривает более тесное сотрудничество, в частности, для обеспечения безопасности детей в Интернете. Хотя глобальное сотрудничество в отношении онлайн-сервисов не является чем-то новым (например, правоохранительные органы по всему миру всегда обменивались информацией о материалах, связанных с эксплуатацией детей), ожидается, что регулирующие органы будут активнее сотрудничать, чтобы решать проблемы быстро развивающейся цифровой экосистемы. Правовые рамки некоторых юрисдикций содержат только ответные требования, такие как уведомления об удалении отдельных фрагментов контента. Однако другие режимы безопасности в Интернете направлены на принятие упреждающих мер поставщиками онлайн-услуг по предотвращению и минимизации онлайн-ущерба (включая Великобританию, Австралию, Сингапур и, возможно, США). В результате наблюдается смещение ответственности за онлайн-ущерб на поставщиков услуг. Усилия по регулированию в этой сфере направлены на охват широкого круга технологических компаний. Законы Австралии, Великобритании, Сингапура, ЕС и других юрисдикций распространяются на широкий спектр онлайн-провайдеров, включая платформы социальных сетей, сервисы электронной коммерции, интернет-провайдеров, а также провайдеров услуг хостинга и хранения данных. В то время как в Великобритании широкое понятие «услуг, предоставляемых пользователям пользователями» (таких как приложения для обмена сообщениями, приложения для знакомств, игры с функциями общения и другие платформы социальных сетей, на которых пользователи взаимодействуют с контентом друг друга) не является отдельной категорией регулируемых субъектов во всех юрисдикциях, в некоторых юрисдикциях, например, в Австралии, это понятие относится к другим

категориям регулируемых субъектов. Исторически сложилось так, что законы о безопасности в Интернете были сосредоточены на регулировании незаконного контента в Даркнете, регулируя такие области, как эксплуатация детей и контент, связанный с терроризмом. Однако такие страны, как США, Индонезия, Австралия и Великобритания стремились устранить по крайней мере некоторые аспекты вредоносного (но не обязательно незаконного) контента, включая кибербуллинг, домогательства или материалы с применением насилия. Некоторые страны также запрещают дезинформацию и мистификации с помощью своих режимов безопасности в Интернете. Учитывая потенциальное воздействие вреда, причиняемого онлайн, неудивительно, что несоблюдение требований влечет за собой целый арсенал правоприменительных полномочий для регулирующих органов, главное из которых — налагать штрафы, подобно Директиве ЕС о персональных данных (GDPR) в размере процента от мирового годового дохода за наиболее серьезные нарушения в соответствии с режимами Великобритании (10%) и ЕС (6%), при этом значительные финансовые штрафы также взимаются в других юрисдикциях — Австралия и Сингапур. Хотя в некоторых юрисдикциях также действуют приказы об удалении контента и блокировке доступа к онлайн-сервисам, не соответствующим требованиям, именно потенциальная уголовная ответственность высшего руководства в таких юрисдикциях, как Великобритания и Сингапур, превратила онлайн-безопасность в проблему, требующую решения на уровне совета директоров.

Последние исследования информационной среды²² позволили сделать ряд выводов, в частности:

(а) наиболее важной характеристикой здоровой информационной среды является наличие достоверной информации;

(б) самой большой угрозой для информационной среды эксперты считают владельцев социальных сетей, за которыми следуют местные власти и иностранные правительства, политики и политические партии;

(с) генеративный ИИ может способствовать сохранению предубеждений, увеличению масштабов преследований и распространения дезинформации.

Информационная среда, таким образом, представляет собой сложно организованную технологическую структуру, которая не идентична информационной системе как совокупности содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Информационная среда представляет собой адаптивную систему, сложность, структура и границы возможного которой возрастают с появлением новых социальных норм и технологий и которая подвергается негатив-

²⁰ URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822818/Joint_Meeting_of_FCM_and_Quintet_of_Attorneys_FINAL.pdf

²¹ URL: <https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration>

²² Опрос экспертов. Глобальная информационная среда, International Panel on the Information Environment (IPIE), 2024. URL: https://cdn.prod.website-files.com/643ecb10be528d2c1da863cb/673c7f24757d3f3b9e930dee_SFP2024.1%20-%20FINAL-3_RU.pdf

ным влияниям, угрожающим ее целостности, психологическому и физическому здоровью ее участников, даже общественной безопасности и государственно-му строю. Это создаваемое цифровыми и информационно-коммуникационными технологиями цифровое, не аналоговое пространство, где сходятся челове-

ское познание, технологии и контент, где информация обрабатывается людьми, ИИ и нейронными сетями и которое включает технологии, используемые для обработки этой информации и доступа к ней, в том числе такие как мобильные телефоны, сеть Интернет и дополненная реальность, а также сопутствующий контент.

Литература

1. Дружилов С.А. Современная информационная среда и экология человека: психологические аспекты // Hygiene & Sanitation (Russian Journal). 2018. № 97. С. 597—602.
2. Моргунова Е.А., Шахназаров Б.А. Право интеллектуальной собственности в условиях развития новых технологий : монография. М. : Норма, ИНФРА-М, 2023. 186 с.
3. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 28—44. DOI: 10.21681/2311-3456-2023-1-28-44 .
4. A. Wanless, J.N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for International Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/Wanless_Shapiro_CERN_final.pdf
5. Michel J. Menou, Richard D. Taylor. A "Grand Challenge": Measuring Information Societies. Inf. Soc. 22(5):261–267.
6. Birger Hjørland. Theory and metatheory of information science: A new interpretation. Journal of Documentation, December 1998. URL: <https://www.researchgate.net/publication/228717437>
7. R. Mathar. Information Theory. URL: <https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf>
8. P. Röttger, B. Vedres. The Information Environment and Its Effects on Individuals and Groups. Oxford Internet Institute, University of Oxford, 2020, pp. 2–4. URL: <https://royalsociety.org/-/media/policy/projects/online-information-environment/oie-the-information-environment>
9. Floridi, Luciano (2010). Information: A Very Short Introduction. Oxford University Press, 2010.
10. Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. Journal of Documentation.
11. Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.

SECTION:
CONSTITUTIONAL LAW

THE LEGAL ASPECTS OF REGULATING THE INFORMATION ENVIRONMENT

Aleksandr Kartskhiia, Dr.Sc. (Law), Professor at the Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russian Federation.
E-mail: arhz50@mail.ru

Keywords: cyberspace, national security, information technology law, digital law, personal data, cybersecurity, information protection.

Abstract

Purpose of the study: a legal analysis of the information environment, its content and specific features of formation when using modern information, communication and digital technologies which are reflected in domestic and international law.

Methods used in the study: comparative legal analysis of current Russian and international laws in the field of digital information environment and the practice of using them as well as a formal logical study of the conceptual apparatus, content and structure of the subject under study.

Study findings: specific features of digital information environment and its content are worded, including from the standpoint of cybersecurity and national security in the information sphere. The author considers it natural that the information environment and digital technological space are formed in a new, non-analog physical dimension as a new area of legal regulation which entails forming special laws and special legal regulation in this field.

Research novelty: the concept, qualitative characteristics, and specific features of the content of digital information environment, its elements and extent of its impact on real relations are identified.

References

1. Druzhilov S.A. Sovremennaya informatsionnaya sreda i ekologiya cheloveka: psikhologicheskie aspekty. Hygiene & Sanitation (Russian Journal). 2018. No. 97. Pp. 597–602.
2. Morgunova E.A., Shakhnazarov B.A. Pravo intellektual'noi sobstvennosti v usloviakh razvitiya novykh tekhnologii : monografiya. M. : Norma, INFRA-M, 2023. 186 pp.
3. Kartskhiya A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeystviya kiberpres-tupnosti. Voprosy kiberbezopasnosti. 2023. No. 1 (53). Pp. 28–44. DOI: 10.21681/2311-3456-2023-1-28-44 .
4. A. Wanless, J.N. Shapiro. A CERN Model for Studying the Information Environment, 2022 Carnegie Endowment for In-ternational Peace and Princeton University. URL: https://carnegie-production-assets.s3.amazonaws.com/static/files/Wanless_Shapiro_CERN_final.pdf
5. Michel J. Menou, Richard D. Taylor. A “Grand Challenge”: Measuring Information Societies. Inf. Soc. 22(5):261–267.
6. Birger Hjørland. Theory and metatheory of information science: A new interpretation. Journal of Documentation, December 1998. URL: <https://www.researchgate.net/publication/228717437>
7. R. Mathar. Information Theory. URL: <https://ti.rwth-aachen.de/teaching/InformationTheory/ws1819/data/InformationTheory.pdf>
8. P. Röttger, B. Vedres. The Information Environment and Its Effects on Individuals and Groups. Oxford Internet In-stitute, University of Oxford, 2020, rr. 2–4. URL: <https://royalsociety.org/-/media/policy/projects/online-informa-tion-environment/oie-the-information-environment>
9. Floridi, Luciano (2010). Information: A Very Short Introduction. Oxford University Press, 2010.
10. Raber, Douglas and John M Budd (2003). Information as sign: semiotics and information science. Journal of Docu-mentation.
11. Habermas, Jürgen (2015). The Theory of Communicative Action: Lifeworld and Systems, a Critique of Functionalist Reason. Vol. 2. John Wiley & Sons.

О ПРАВОВЫХ СРЕДСТВАХ ОСУЩЕСТВЛЕНИЯ НАЛОГОВОЙ ПОЛИТИКИ

Васянина Е.Л.¹

Ключевые слова: налоговое обязательство, налог, налогоплательщик, налоговая система, налоговая реконструкция, ответственность, наука, налоговая политика.

Аннотация

Цели статьи: исследование существа налогового обязательства как одного из основных правовых средств осуществления налоговой политики, а также попытка найти необходимый правовой инструментарий для создания конкурентоспособной и справедливой налоговой системы.

Установлено, что совершенствование конструкции налогового обязательства необходимо осуществлять на основе разработки правовых категорий и структурных элементов налогового обязательственного права. Во избежание формирования противоречивой судебной практики НК РФ целесообразно дополнить положениями о перемене лиц в обязательстве, о специфических мерах налогово-правовой ответственности за нарушение налоговых обязательств, а также об условиях и порядке применения налоговой реконструкции как способа конкретизации элементов юридического состава налога исходя из реального экономического содержания совершаемых налогоплательщиком сделок. Компенсировать недостаток правового инструментария, обеспечивающего инвестиционную активность налогоплательщиков, предлагается посредством введения существовавшего и применяемого в советскую эпоху правового института распределения прибыли предприятий, выступающих в качестве первичного звена экономики государства.

DOI: 10.24412/1994-1404-2025-1-32-37

Введение

Сегодня финансово-правовые исследования сфокусированы на вопросах совершенствования механизма налогообложения, который, будучи сформированным в 90-е годы XX века, в новых экономических реалиях быстро утратил свою эффективность.

В государстве продолжает формироваться околоналоговая фискальная система, в рамках которой число не охватываемых Налоговым кодексом Российской Федерации (далее — НК РФ) обязательных платежей, по данным исследователей, достигло семидесяти [2]. Более того, развитие налоговой системы идет по пути установления оборотных налогов (платежи за распространение рекламы в сети Интернет², курортный сбор), не учитывающих реальные платежные возможности участников гражданского оборота и вызывающих инфляционный эффект [14].

Не подчиняются общим правилам регулирования фискальных взиманий устанавливаемые банками пла-

тежи, к числу которых относятся являющиеся квази-налогами эквайринговые комиссии, а также заградительные комиссии, правомерность введения которых периодически является предметом судебных разбирательств³.

Масштабные поправки в НК РФ, вызванные проведенной в 2024 году «донастройкой» налоговой системы, направленные, с одной стороны, на увеличение, а с другой — на сглаживание фискальной нагрузки для отдельных категорий налогоплательщиков, не позволили обеспечить более справедливое перераспределение налогового бремени между участниками гражданского оборота и не привели к стимулированию их инвестиционной и экономической активности.

Во многом недостижение поставленных целей связано с тем, что в рамках работы по модернизации фискальной системы законодатель крайне мало внимания уделил вопросам совершенствования правового обеспечения налоговых обязательств, а финансово-правовые исследования до сих пор должным образом не сосредоточены на разработке структурных

² Федеральный закон от 26.12.2024 № 479-ФЗ «О внесении изменений в Федеральный закон “О рекламе” и отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2024. № 53 (Часть I). Ст. 8489.

³ Определение ВС РФ от 26.12.2024 № 305-ЭС24-16889.

¹ **Васянина Елена Леонидовна**, доктор юридических наук, доцент, ведущий научный сотрудник сектора административного права и административного процесса Института государства и права РАН, г. Москва, Российская Федерация.
E-mail: elenavasianina@yandex.ru

элементов налогового обязательственного права. Это существенно тормозит развитие законодательства Российской Федерации о налогах и сборах и приводит к многочисленным спорам, связанным с применением тех или иных элементов юридического состава налога.

Вместо конкретизации условий исполнения налоговых обязательств законодатель прибегает к установлению налогово-правовых норм, применение которых потребует разработки дополнительных критериев оценки финансово-хозяйственной деятельности налогоплательщика. В качестве примера можно привести новые положения НК РФ, исключающие возможность перерегистрации бизнеса в регионах с более низкой ставкой по упрощенной системе налогообложения (УСН), а также нормы об амнистии дробления бизнеса, применение которых вкупе с нормами о предельном объеме доходов организаций, по достижении которого освобождение от уплаты НДС невозможно, потребует проведение оценки добросовестности действий налогоплательщиков в процессе оптимизации структуры бизнеса.

Учитывая обозначенные проблемы, цель настоящей статьи заключается в исследовании существа налогового обязательства как одного из основных правовых средств осуществления налоговой политики, а также в попытке найти необходимый правовой инструментарий для обеспечения системной доработки параметров налоговой системы.

О сущности налогового обязательства

Долгое время в юридической науке преобладал подход, в рамках которого отрицалась сама возможность существования финансовых (налоговых) обязательств, поскольку обязательство позиционировалось исключительно в качестве гражданско-правовой конструкции, которая представлялась неприемлемой для обеспечения развития публично-правовой сферы. В связи с этим вопросы фискального обложения в литературе по истории русского права описывались в разделе, посвященном управлению финансами [3].

Во многом такая точка зрения обусловлена особенностями развития древнерусского права. В Русской Правде, закрепляющей зачатки обязательственного права, речь идет преимущественно об обязательствах, возникающих из договоров [9]. О существовании обязательств, не связанных с исполнением договоров и причинением вреда, свидетельствует классификация, разработанная в римском праве, в рамках которой выделены так называемые обязательства, вытекающие из закона [6].

Изучение юридической литературы позволяет констатировать, что исследованию этой особой категории обязательств посвящены некоторые работы, написанные еще в советскую эпоху. Агарков М.М. в работе «Обязательства по советскому гражданскому праву», опубликованной в 1940 году, описывая обязательства в гражданском праве, особое внимание уделил обяза-

тельствам, возникающим из актов государственного управления [1].

В 80-е годы XX века теория финансовых обязательств получает развитие в работах С.В. Запольского, в которых финансовые обязательства рассматриваются в качестве метода управления предприятиями [16]. Основываясь на предоставительно-обязывающем характере права, ученый описывает существо финансового (налогового) обязательства исходя из того, что обязанности налогоплательщика корреспондировано не только право органов публичной власти, осуществляющих исполнение доходной части бюджета, на получении соответствующего платежа, но и их обязанность по управлению этим процессом [10].

В современных финансово-правовых исследованиях изучаются сущность, элементы, виды налоговых обязательственных правоотношений [4, 15]. При этом в науке финансового права «термин «налоговое обязательство» используется не в абстрактном «общенаучном», а совершенно конкретном, узкоспециальном значении» [7].

Недостаточная разработанность в финансово-правовой науке конструкции налогового обязательства приводит к нехватке в действующем законодательстве положений, необходимых для полноценного правового обеспечения механизма налогообложения и, как следствие, — к отсутствию ориентиров формирования правоприменительной практики по налоговым спорам.

На сегодняшний день тренд в развитии налогового законодательства наблюдается в сторону правового обеспечения цифровой трансформации механизма налогообложения в целях его адаптации к параметрам цифровой экономики [13] посредством разработки критериев цифрового присутствия налогоплательщиков, внедрения новых форм контрольно-надзорной деятельности с использованием цифровых платформ, что, несомненно, имеет важное значение для целей исполнения налоговых обязательств, однако не позволяет исчерпывающим образом разрешить возникающие в процессе налогообложения вопросы.

Ключевая проблема в сфере правового регулирования налоговых отношений заключается в том, что цифровая трансформация механизма налогообложения, облегчая процесс сбора, обработки, хранения информации и способствуя сокращению административных процедур, не сопровождается проведением работы по конкретизации условий исполнения налоговых обязательств.

Результатом такого подхода законодателя стало активное применение в сфере налогообложения «метода одностороннего долженствования» [11], исключаящее эффективное взаимодействие субъектов налоговых правоотношений, что в конечном счете привело к ослаблению гарантий защиты права лица на распоряжение финансами.

Ярким примером сказанного является сформированный в русле цифровой трансформации государ-

ственного управления правовой институт единого налогового счета, который привел к нарушению установленного законом принципа определенности налогообложения. Законодатель, существенно расширив полномочия контрольно-надзорного органа, фактически лишил налогоплательщика возможности в рамках возникшего фискального обязательства самостоятельно определять назначение, период и вид платежа, тем самым существенно ограничив его право на распоряжение финансами, защита которого является одним из основных предназначений финансового права.

Проблемы исполнения налоговых обязательств

Определить направления совершенствования правового обеспечения налоговых обязательств можно, основываясь на выработанных в правовой доктрине и экономической науке подходах к пониманию сущности налога, который, с одной стороны, является абстрактной юридической конструкцией, трансформирующейся при наличии установленных законом юридических фактов в налоговую обязанность. С другой стороны, налог есть не что иное, как инструмент, обеспечивающий превращение частной денежной массы в публичный доход. С третьей стороны, с учетом современной денежной теории, налоги необходимы для придания деньгам ценности, а посредством исполнения налоговой обязанности происходит погашение долговых инструментов, в роли которых выступают деньги [8].

Учитывая изложенные подходы к пониманию сущности налога, становится очевидным, что успешная модернизация налоговой системы не представляется возможной без учета целей развития финансово-кредитного механизма, обеспечивающего процесс управления денежной массой.

В контексте сказанного обособленное корректирование отдельных финансово-правовых институтов, к которому периодически прибегает законодатель, имеет негативный для экономики эффект, а именно приводит к рассинхронизации фискальной, бюджетной, денежно-кредитной политики, а также к нехватке правового инструментария, необходимого для обеспечения финансовой самостоятельности участников гражданского оборота и исключающего острую зависимость предприятий от бюджетных инструментов.

В юридической литературе в качестве ядра регулятивного комплекса налогового права выделяют налоговое обязательственное право [5, 15], структурные элементы и юридические категории которого пока недостаточно разработаны в финансово-правовой науке и законодательстве, что существенным образом тормозит процесс системной доработки параметров налоговой системы.

В частности, в налоговом законодательстве отсутствует легальная дефиниция налоговой реконструкции и условий ее применения как способа конкретизации элементов юридического состава налога исходя из ре-

ального экономического смысла совершаемых сделок. В результате на практике сформировался неоднозначный подход к порядку корректировки налогового обязательства. Так, в одном случае при злоупотреблении или искажении фактов хозяйственной деятельности налогоплательщика доначисления рассчитываются с учетом действительной стоимости товара, реально понесенных налогоплательщиком расходов и вычетов НДС, как если бы налогоплательщик не допускал нарушений⁴.

В другом случае по спору о размере доначисленного работодателю НДФЛ в результате подмены трудовых отношений на гражданско-правовые Верховный Суд РФ придерживается несколько иного подхода по вопросу проведения налоговой реконструкции и приходит к выводу о том, что переплата налога на доходы физических лиц не может быть произвольно зачтена в счет исполнения налоговым агентом обязанности по уплате НДФЛ в отсутствие соответствующего волеизъявления плательщика налога на профессиональный доход⁵.

В налоговом праве не разработан институт ответственности за нарушение налоговых обязательств, что привело к появлению параллельных правовых институтов юридической ответственности за нарушения законодательства РФ о налогах и сборах и применению различных отраслевых законодательных актов, к числу которых, помимо НК РФ, относятся КоАП РФ, УК РФ, а также Федеральный закон от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)» в части применения субсидиарной ответственности контролирующих должника лиц.

Во многом сложившийся в правовом регулировании подход вызван наличием стойкого мнения законодателя о том, что финансовое (налоговое) право не имеет собственного правового инструментария для привлечения к ответственности субъектов налоговых правоотношений, что и привело к утяжелению механизма финансово-правового регулирования.

Вместе с тем стоит отметить, что в НК РФ закреплены специфические меры ответственности за нарушение налоговых обязательств, которые рассредоточены по разным главам кодекса с учетом установленных видов налогов. Помимо штрафов, взимаемых за правонарушение, составы которых закреплены в гл. 16 и 18 НК РФ, в главе 21 кодекса установлена такая специфическая мера ответственности за нарушение обязательств, возникающих по поводу обложения НДС, как отказ в предоставлении налогового вычета (возмещения) НДС. В главе 31 НК РФ, посвященной имущественному налогообложению, за неисполнение обязанности по уплате налога на имущество физических лиц предусмотрена уплата налога в многократном размере.

⁴ См.: Письма ФНС России от 10.03.2021 № БВ-4-7/3060@ и от 06.12.2024 № БВ-4-7/1384; Определение Верховного Суда РФ от 9.07.2023 № 305-ЭС23-4066.

⁵ Определение ВС РФ от 20.01.2025 г. № 309-ЭС24-20306.

Учитывая изложенное, законодателю следовало бы продолжить разработку специальных налогово-правовых мер ответственности за нарушение налоговых обязательств, определить общие условия их применения, что позволит исключить сформированные параллельные правовые институты юридической ответственности за налоговые правонарушения.

В налоговом праве не разработаны положения о перемене лиц в обязательствах. Это приводит к тому, что в отдельных случаях лица, которые на определенном этапе развития налоговых правоотношений становятся стороной налогового обязательства, оказываются лишены возможности быть стороной в налоговом споре. Например, контролирующие должника лица, которые несут субсидиарную ответственность за ненадлежащее исполнение налоговой обязанности, долгое время не имели права на оспаривание актов налоговых органов по причине отсутствия соответствующих положений в НК РФ. Применительно к описываемой проблеме ситуация изменилась благодаря формированию обширной правоприменительной практики по вопросам защиты прав контролирующих должника лиц в налоговых спорах [12].

Появление такого рода судебных актов свидетельствует о том, что в целях укрепления конституционных гарантий защиты права лица на распоряжение финансами, настоятельной необходимостью является закрепление в НК РФ положений о перемене лиц в обязательствах.

Существенный объем налоговых споров связан с определением элементов юридического состава налога. В частности, проблемным является вопрос об установлении объекта налогообложения по налогу на имущество организаций в части определения критериев, при наличии которых имущество относится к категории недвижимого. Споры возникают по вопросу формирования налоговой базы по НДС, по поводу проведения оценки стоимости концентрата, содержащего в себе один или несколько драгоценных металлов.

Серьезный вопрос, потребовавший оценки конституционности соответствующих положений НК РФ, возник вследствие отсутствия в НК РФ механизма определения и расчета экономической выгоды в случае передачи денежных средств или имущества в счет выплаты действительной стоимости доли участнику хозяйственного общества⁶.

Недостаточная разработанность конструкции налогового обязательства приводит, во-первых, к тому, что конкретизация условий исполнения фискальных обязательств происходит на уровне правоприменительной практики. Сказанное можно продемонстрировать

на примере остро возникшего вопроса о включении таможенными органами в таможенную стоимость товаров дивидендов⁷ в целях пресечения недобросовестного поведения взаимозависимых лиц, выступающих сторонами внешнеторговой сделки. Сложившийся в судебной практике подход получил подтверждение со стороны Минфина России. Соответствующее письмо, в котором определены условия, при которых дивидендные платежи могут включаться в таможенную стоимость импортируемых товаров на основании подпункта 3 пункта 1 статьи 40 ТК ЕАЭС, опубликовано на сайте ФТС России⁸.

Во-вторых, отсутствие необходимых налогово-правовых инструментов приводит к расширению рецепции частноправовых механизмов в налоговом законодательстве. Однако использование альтернативных правовых средств регулирования налоговых отношений на фоне отсутствия в законодательстве критериев их применения может привести к деформации существующих финансово-правовых институтов, а также к появлению новых видов налоговых споров.

Ярким примером изложенного является такой инструмент, как «налоговая оговорка в договоре», применение которой не позволило разрешить проблему исполнения налоговых обязательств по существу, но привело к появлению новой, ранее не существовавшей категории налоговых споров, вытекающих из хозяйственных договоров.

Заключение

Проведенный анализ позволил сформулировать ряд выводов, которые могут иметь значение для развития финансово-правовой науки и финансового законодательства.

1. Совершенствование конструкции налогового обязательства необходимо осуществлять на основе разработки правовых категорий и структурных элементов налогового обязательственного права, изучению которого в финансово-правовых исследованиях до сих пор не уделяется должного внимания.

В контексте изложенного, во избежание формирования противоречивой судебной практики целесообразно дополнить НК РФ положениями о перемене лиц в обязательстве, об условиях и порядке применения налоговой реконструкции как способа конкретизации элементов юридического состава налога исходя из реального экономического содержания совершаемых налогоплательщиком сделок.

⁶ Постановление Конституционного Суда РФ от 21.01.2025 № 2-П «По делу о проверке конституционности подпункта 5 пункта 3 статьи 39, пункта 1 статьи 41, пунктов 1 и 2 статьи 248, пунктов 1 и 2 статьи 249, а также пункта 1 статьи 346.15 Налогового кодекса Российской Федерации в связи с запросом Верховного Суда Российской Федерации». URL: <http://pravo.gov.ru>, 22.01.2025.

⁷ Определения Судебной коллегии по экономическим спорам Верховного Суда Российской Федерации от 01.12.2022 № 305-ЭС22-11464 по делу № А40-20125/2021; от 02.12.2022 № 310-ЭС22-8937 по делу № А09-1129/2021; от 02.12.2022 № 310-ЭС22-9639 по делу № А09-1751/2021.

⁸ URL: https://customs.gov.ru/storage/document/document_info/2025-02/20/11349.pdf

2. Учитывая наличие в НК РФ специфических наказаний, применяемых за нарушение налоговых обязательств, к числу которых относятся отказ в предоставлении вычета (возврата) налога, уплата налога в двойном (многократном) размере, законодателю следует продолжить разработку специальных налогово-правовых мер ответственности, определить общие условия их применения, что позволит исключить развитие параллельных правовых институтов юридической ответственности за налоговые правонарушения.
3. Компенсировать недостаток правового инструментария, обеспечивающего инвестиционную активность налогоплательщиков, целесообразно посредством введения существовавшего

и применявшегося в советскую эпоху правового института распределения прибыли предприятий, выступающих в качестве первичного звена экономики государства⁹.

Формирование подобной модели распределения прибыли организаций в современных условиях снимет их зависимость от бюджетных инструментов, позволив самостоятельно реализовать инвестиционные проекты.

⁹ Постановление ЦК КПСС, Совмина СССР от 04.10.1965 № 729 «О совершенствовании планирования и усиления экономического стимулирования промышленного производства».

Литература

1. Агарков М.М. Ученые труды. Обязательство по советскому гражданскому праву. М. : Юридическое изд-во, 1940. 190 с.
2. Васянина Е.Л. Теоретические основы правового регулирования публичных доходов в Российской Федерации : автореферат дис. ... докт. юрид. наук: 12.00.04 / Васянина Е.Л.; [Место защиты: Ин-т государства и права РАН]. Москва, 2016. 54 с.
3. Владимирский-Буданов М.Ф. Обзор истории русского права // Соч. проф. М.Ф. Владимирского-Буданова. 5-е изд. Санкт-Петербург, Киев : Н.Я. Оглоблин, 1907. [4], VI, VI, 694 с.
4. Васянина Е.Л. Обязательства в финансовом праве. М. : ООО «КноРус», 2020. 130 с.
5. Винницкий Д.В. Российское налоговое право: проблемы теории и практики. СПб. : Юридический центр Пресс, 2003. 397 с.
6. Годэмэ Е. Общая теория обязательств / Евгений Годэмэ, профессор гражданского права юридического факультета Страсбургского университета / Пер. с франц. И.Б. Новицкого. М. : Юридическое издательство Министерства юстиции СССР, 1948. 512 с. (Всесоюзный институт юридических наук Министерства юстиции СССР. Ученые труды; Выпуск XIII).
7. Голубцов В.Г. Реформа обязательственного права: теоретический и практический эффект состоявшихся изменений // Вестник Пермского университета. Юридические науки. 2018. № 3. С. 396—419.
8. Грищенко В., Остапенко В., Ткачев В., Трунев В. Современная денежная теория (ММТ): новая парадигма или набор рекомендаций для макроэкономической политики // Экономическая политика. 2021. Т. 16. № 3. С. 8—43.
9. Загоровский А.И. Исторический очерк займа по русскому праву до конца XIII столетия / Соч. А. Загоровского. Киев : в Университетской тип., 1875. 78 с.
10. Запольский С.В. Правовые вопросы самофинансирования предприятий в условиях полного хозяйственного расчета (финансово-правовой аспект) : автореферат дис. ... докт. юрид. наук: 12.00.02 / ВНИИ сов. гос. стр-ва и законодательства. М., 1989. 45 с.
11. Запольский С.В. Эмиссия как элемент правового регулирования финансов // Финансовое право. 2024. № 10. С. 2—6.
12. Литовцева Ю.В. Защита прав контролирующих должника лиц в налоговых спорах // Налоговед. 2022. № 11. С. 43—49.
13. Новые горизонты развития системы информационного права в условиях цифровой трансформации / Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов [и др.]. М. : Институт государства и права РАН, 2022. 368 с.
14. Пепеляев С.Г. Акциз на рекламу // Налоговед. 2025. № 2. URL: <https://nalogoved.ru/art/15304.html>
15. Порохов Е.В. Налоговое право : учебник для вузов (академический курс). Алматы : Научно-исследовательский институт финансового и налогового права, 2023. 1148 с.
16. Предприятие. Закон. Управление : практ. пособие / С.В. Запольский и др.; под ред. М.К. Юкова. М. : Юрид. лит., 1989. 239 с.

ON LEGAL MEANS FOR EXERCISING TAX POLICY

Elena Vasianina, Dr.Sc. (Law), Associate Professor, Leading Researcher at the Sector of Administrative Law and Administrative Process of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.

E-mail: elenavasianina@yandex.ru

Keywords: tax obligation, tax, taxpayer, tax system, tax reconstruction, responsibility, science, tax policy.

Abstract

Purposes of the study: studying the essence of tax obligation as one of the main legal means for exercising tax policy and attempting to find the necessary legal tools for setting up a competitive and fair tax system.

It was established that improving the tax obligation construct should be based on developing legal categories and structural elements of tax obligation law. To avoid forming a contradictory judicial practice, it would be advisable to supplement the Tax Code of the Russian Federation with provisions on subrogation of persons in an obligation, specific measures of tax law responsibility for violating tax obligations as well as on the terms and procedure for using tax reconstruction as a way for specifying the elements of the legal composition of the tax considering the actual economic content of transactions effected by the taxpayer. It is proposed to compensate the shortcomings of legal tools ensuring the investing activity of taxpayers by introducing the legal institution of distribution of profit of enterprises constituting the primary section of the country's economy, an institution that existed and was used in the Soviet times.

References

1. Agarkov M.M. Uchenye trudy. Obiazatel'stvo po sovetскому grazhdanskomu pravu. M. : Iuridicheskoe izd-vo, 1940. 190 pp.
2. Vasianina E.L. Teoreticheskie osnovy pravovogo regulirovaniia publichnykh dokhodov v Rossiiskoi Federatsii : avtoreferat dis. ... dokt. iurid. nauk: 12.00.04. Vasianina E.L.; [Mesto zashchity: In-t gosudarstva i prava RAN]. Moskva, 2016. 54 pp.
3. Vladimirskii-Budanov M.F. Obzor istorii russkogo prava. Soch. prof. M.F. Vladimirskogo-Budanova. 5-e izd. Sankt-Peterburg, Kiev : N.Ia. Ogloblin, 1907. [4], VI, VI, 694 pp.
4. Vasianina E.L. Obiazatel'stva v finansovom prave. M. : OOO "KnoRus", 2020. 130 pp.
5. Vinnitskii D.V. Rossiiskoe nalogovoe pravo: problemy teorii i praktiki. SPb. : Iuridicheskii tsentr Press, 2003. 397 pp.
6. Godeme E. Obshchaia teoriia obiazatel'stv. Evgenii Godeme, professor grazhdanskogo prava Iuridicheskogo fakul'teta Strasburgskogo universiteta. Per. s frants. I.B. Novitskogo. M. : Iuridicheskoe izdatel'stvo Ministerstva iustitsii SSSR, 1948. 512 pp. (Vsesoiuznyi institut Iuridicheskikh nauk Ministerstva iustitsii SSSR. Uchenye trudy; Vypusk XIII).
7. Golubtsov V.G. Reforma obiazatel'stvennogo prava: teoreticheskii i prakticheskii effekt sostoiavshikhsia izmenenii. Vestnik Permskogo universiteta. Iuridicheskie nauki. 2018. No. 3. Pp. 396–419.
8. Grishchenko V., Ostapenko V., Tkachev V., Trunev V. Sovremennaiia denezhnaia teoriia (MMT): novaia paradigma ili nabor rekomendatsii dlia makroekonomicheskoi politiki. Ekonomicheskaiia politika. 2021. T. 16. No. 3. Pp. 8–43.
9. Zagorovskii A.I. Istoricheskii ocherk zaima po russkomu pravu do kontsa XIII stoletia. Koch. A. Zagorovskago. Kiev : v Universitetskoi tip., 1875. 78 pp.
10. Zapol'skii S.V. Pravovye voprosy samofinansirovaniia predpriatii v usloviakh polnogo khoziaistvennogo rascheta (finansovo-pravovoi aspekt) : avtoreferat dis. ... dokt. iurid. nauk: 12.00.02. VNII sov. gos. str-va i zakonodatel'stva. M., 1989. 45 pp.
11. Zapol'skii S.V. Emissiia kak element pravovogo regulirovaniia finansov. Finansovoe pravo. 2024. No. 10. Pp. 2–6.
12. Litovtseva Iu.V. Zashchita prav kontroliruiushchikh dolzhnika lits v nalogovykh sporakh. Nalogoved. 2022. No. 11. Pp. 43–49.
13. Novye gorizonty razvitiia sistemy informatsionnogo prava v usloviakh tsifrovoy transformatsii. T.A. Poliakova, Pepeliaev S.G. Aktsiz na reklamu. Nalogoved. 2025. No. 2. URL: <https://nalogoved.ru/art/15304.html>
14. Porokhov E.V. Nalogovoe pravo : uchebnik dlia vuzov (akademicheskii kurs). Almaty : Nauchno-issledovatel'skii institut finansovogo i nalogovogo prava, 2023. 1148 pp.
15. Predpriatie. Zakon. Upravlenie : prakt. posobie. S.V. Zapol'skii i dr.; pod red. M.K. Iukova. M. : Iurid. lit., 1989. 239 pp.

ПРАВОСУДИЕ И ВИРТУАЛЬНОЕ ПРОСТРАНСТВО

Белякова А.В.¹

Ключевые слова: судебная система, цифровые технологии, киберправосудие, робот-судья, парадигма современного правосудия, искусственный интеллект в правосудии.

Аннотация

Цель статьи: анализ реализации современных общественных отношений в условиях повсеместного распространения «цифровых инструментов», в том числе исследование их влияния на национальную судебную систему; выявление и постановка ряда вопросов и проблем в указанной области с целью дальнейшего развития судебного процесса.

Методы исследования: общенаучные методы анализа, синтеза, обобщения и диалектический метод, а также формально-логический, юридико-технический методы и метод сравнительного правоведения.

Результаты исследования: проведенный анализ позволил сформулировать авторскую точку зрения по вопросу «виртуализации» и «цифровизации» современного судебного процесса. Конкретизируется позиция автора относительно содержания искусственного интеллекта в правосудии и виртуального пространства. Проанализированные научные подходы в данной области позволяют выявить области для дальнейших исследований и позволяют автору сформировать и уточнить свою точку зрения.

DOI: 10.24412/1994-1404-2025-1-38-49

Введение

Современное общество в целом и национальное общество в частности находятся в уникальном моменте своего развития, который заключается в том, что исторически сложившийся путь обновляется за счет общей картины мира; трансформируется и эволюционирует в связи с тем, что за короткий промежуток времени одновременно произошли разноплановые события, позволяющие изменить укоренившийся уклад жизни не только человека, гражданина, больших и малых социальных групп, но и целых государств. В геополитическом контексте формируются и действуют новые альянсы, способствующие развитию и формированию актуальной повестки как в социально-экономической сфере, так и в других областях. Аналогично, внедрение и распространение цифровых сервисов и продуктов ускоряет технологическое развитие отдельных отраслей, однако вопросы смежных сфер остаются недостаточно проработанными, в то время как масштаб использования виртуального пространства продолжает расширяться.

При этом существуют и негативные аспекты, в частности, отсутствие поступательного и прогностического развития. Не менее важным является соотношение информатизации и медиатизации не только в социально-

экономической сфере, но и в других областях, поскольку эти взаимосвязанные процессы трансформируют как общую культуру, восприятие и сознание отдельных людей, так и правовую культуру, включая правосознание и мировоззрение отдельных граждан и различных социальных групп.

Вышеизложенные аспекты отражаются на государственном и муниципальном управлении, а также оказывают влияние на систему правосудия. Эти процессы взаимосвязаны: в одних случаях связь очевидна, в других она может быть неочевидной, но от этого не менее значимой. Анализ любых процессов невозможно проводить без учета причинно-следственных связей, а также влияния социальных, экономических и геополитических факторов. Игнорирование этих взаимосвязей и возможных последствий недопустимо, особенно в условиях нынешнего исторического этапа, который является уникальным. В настоящее время формируются задачи как на ближайшее будущее, так и на долгосрочную перспективу, что требует комплексного и стратегического подхода. Полагаю, что процессы, происходящие в настоящий момент, окажут влияние не только на отдельные группы людей, но и на человечество в целом. Важно отметить, что судебная система

¹ **Белякова Анна Владимировна**, кандидат юридических наук, ведущий научный сотрудник Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Российская Федерация. ORCID: 0000-0003-4241-4511.

E-mail: belyakova.av@gmail.com

и правосудие не остаются в стороне от модернизации современного общественного уклада и также претерпевают значительные изменения.

Виртуальное пространство традиционно ассоциировалось с игровым и мультимедийным контентом, но в последние несколько десятилетий его сфера действия начала расширяться. Например, профессором М.А. Федотовым в научной работе 1999 года «Киберпространство как сфера обитания права» [1] были высказаны актуальные идеи о последующем развитии «киберпространства», которые имеют место быть в настоящее время.

Виртуальное пространство — это онлайн-среда, где пользователи глобальной сети Интернет реализуют свои интересы, которые могут быть как правомочными, так и нарушающими национальный правовой порядок [2—4].

В данном контексте рассматриваются не только вопросы соотношения права и виртуального пространства [5—8], но и другие аспекты реализации социально-экономических отношений посредством использования информационно-коммуникационных технологий в глобальной сети Интернет (трансформация образовательной среды; музейного, архивного, библиотечного дела; медицины, строительства и т. п.).

Виртуальное пространство в настоящее время — это не только передача сведений и информации, но и осуществление достаточного количества функций, включая трудовые, а также реализация гражданско-правовых отношений посредством совершения сделок в онлайн-формате [9; 10] и, как следствие, возникновение правовых конфликтов, требующих разрешения и урегулирования. Таким образом, современная судебная система интегрируется с различного рода информационными технологиями (далее — ИТ-технологии), реализация которых осуществляется в «режиме реального времени» (онлайн), то есть в виртуальном пространстве.

Реализация тех или иных общественных отношений в виртуальном пространстве является многоаспектным процессом, который включает в себя наличие разного рода технологических устройств (например, персональный компьютер, имеющий доступ и подключение к глобальной сети Интернет) и программного обеспечения (далее — ПО), которое в отдельных случаях должно быть специализированным или узкоспециализированным. Это же, в свою очередь, обязывает заинтересованных лиц обладать знаниями и навыками в данной области, а также владеть информацией об особенностях осуществления и реализации своих прав и законных интересов.

В последние годы внедрение и популяризация информационных технологий во всех сферах жизнедеятельности привели к тому, что правовое регулирование не успевает адаптироваться к новым продуктам и сервисам. Правовые нормы в этой области остаются разрозненными и фрагментарными, что создает необходимость переосмысления действующего законодательства. Например, отсутствие единого логико-струк-

турированного современного понятийного и категориального аппарата не только затрудняет реализацию общественных отношений в данной сфере, но и вызывает серьезные проблемы в правоприменительной практике. Смысловая и терминологическая разобщенность между юридическими и техническими понятиями впоследствии осложняет разработку технических заданий, реализацию проектов и исполнение договорных обязательств. Это обусловлено в том числе и особенностью развития национального правового порядка, сменой политической и экономической формации и историческими этапами развития национального общества.

Вопросам развития информационно-коммуникационных систем уделялось внимание и в советский период развития правовой доктрины [11; 12]. В тот же период профессор Н.А. Чечина в статье «Актуальные проблемы науки гражданского процессуального права» (опубликованной в журнале «Правоведение» в 1975 г., № 6) отмечала, что «применение техники недопустимо тогда, когда это может отрицательно повлиять на воспитание граждан, а также такое применение приведет к игнорированию системы нравственных ценностей» [13, с. 577], в этой же публикации она указывала на то, что необходимо определить (ограничить) сферу возможного применения машин в судопроизводстве, установить разумные пределы «нашествия» техники на устоявшиеся (действующие) правила судопроизводства [там же]. Данные научные воззрения в настоящее время не теряют актуальности и являются не только провидческими, но и требующими осмысления в условиях современных реалий.

Обсуждения по вопросу о необходимости кодификации и систематизации правовых норм данной сферы продолжают². Рассматриваются вопросы о «цифровом кодексе» [14; 15], «информационном кодексе» [16; 17, с. 7]. При этом единое мнение по данному аспекту среди ученых-правоведов до настоящего времени не сформировалось.

В продолжение ранее проведенных исследований хотелось бы уточнить и детализировать ряд авторских взглядов и позиций относительно трансформации и развития современной парадигмы национального правосудия в условиях растущего влияния технологических решений и цифровых инструментов на судебную систему.

Внедрение цифровых продуктов и алгоритмов в государственное управление, в том числе в органы судебной власти, а также в социально-экономические отношения набирает обороты, являясь объективной необходимостью поступательного развития на этапе совершенствования технологических и информационных процессов и их интеграции в жизнедеятельность индивидуумов.

² Например, актуальная дискуссия по данному вопросу развернулась на XII Петербургском международном юридическом форуме. Подробнее см.: URL: <https://legalforum.info/programme/business-programme/5371/> (дата обращения: 06.03.2025).

Юриспруденция, правовая система, право, государственное и муниципальное управление вынуждены адаптироваться к изменениям в обществе, экономике, науке, технике, политике и государственном устройстве. С одной стороны, цифровые и электронные продукты упрощают и оптимизируют процессы и выполнение задач, в том числе в условиях многозадачности, с другой стороны, существуют риски чрезмерного использования искусственного интеллекта (далее — ИИ) и минимизации человеческого фактора.

Существует ряд сфер профессиональной деятельности, где замена экспертов и специалистов роботами и информационными системами может привести к фатальным ошибкам. Общеизвестным фактом является то, что в настоящее время технический прогресс способствует росту мошеннических и иных преступных схем с использованием информационных технологий, что позволяет злоупотреблять правом, нарушать личные границы, вторгаться в частную жизнь граждан, тем самым нарушая конституционно-правовые гарантии.

Правосудие глубоко интегрировано в нашу жизнь и остро реагирует на происходящие изменения, поскольку, с одной стороны, вынуждено адаптироваться к растущей автоматизации и технологическому развитию судебного процесса и его организационно-технического сопровождения, а с другой — разрешать споры, осложненные влиянием внедряемого ПО на социально-экономические отношения.

Автор уже отмечала, что разобщенность в правовом регулировании, отсутствие единого логико-структурированного современного понятийного и категориального аппарата приводит не только к проблемам в реализации общественных отношений в изучаемой области [18; 19], но и формирует правовую неопределенность при рассмотрении и разрешении правовых конфликтов. Например, смысловая и терминологическая разобщенность в понятиях и терминах, используемых в юридической практике и применяемых техническими специалистами, приводит впоследствии к проблемам в реализации технических заданий, проектов и исполнении договорных обязательств, а как следствие — формирует необходимость для заинтересованных лиц обращаться в судебные органы, проводить сложные технические и технологические экспертизы. В свою очередь, это приводит к тому, что экономические и производственные процессы либо приостанавливаются, либо уменьшается их интенсивность.

Трансформация общественных отношений в условиях повсеместной «виртуализации»

Право в традиционном восприятии — это регулятор общественных отношений, призванный осуществлять их упорядочивание вне зависимости от условий, временного периода, а также механизмов, способов и технологий их осуществления.

Действующая правовая система и система законодательства вынуждены адаптироваться к внедре-

нию сложных технических программных объектов и устройств как способов, механизмов и технологий реализации тех или иных общественных отношений.

Виртуализация общественных отношений охватывает множество аспектов, включая объединение пользователей и компьютерных устройств в глобальной сети Интернет. Это позволяет им не только взаимодействовать посредством специального ПО, но и выполнять различные задачи, такие как работа, обучение и другие виды деятельности. Таким образом, виртуальное пространство открывает новые возможности, но одновременно создает определенные риски, которые могут иметь как позитивные, так и негативные последствия, затрагивающие не только отдельные сферы права, но и общественные процессы в целом.

Например, внедрение и повсеместное использование IT-технологий меняет не только гражданско-правовые, но и уголовно-правовые отношения, а именно: использование и применение специального ПО и специальных устройств, оснащённых специализированным ПО, при проведении оперативно-разыскных мероприятий (или оперативно-разыскной деятельности) позволяет отслеживать передвижение того или индивидуума или группы лиц. Этот наглядный пример призван проиллюстрировать, что осуществление и проведение тех или иных мероприятий и действий в правовой сфере, с одной стороны, может быть упрощено, а с другой — предоставляет достаточно возможностей для совершения злонамеренных действий. В частности, в последнее время сформировался феномен «киберпреследования» или «киберсталкерства» — отслеживание действий и преследование с использованием информационных технологий [20—23].

С одной стороны, современные ИКТ позволяют совершать большое количество действий, выполнять несколько задач и осуществлять различные функции одновременно, но при этом формируются отдельные риски как для граждан, так и для юридических лиц. Например, сбор, обработка, анализ и хранение персональных данных приводят к распространению преступлений, совершенных с использованием современных технических средств [24], которые затрагивают как уголовно-правовые, так и гражданско-правовые нормы [25, 26].

Отдельные научные подходы к трансформации судебной системы в современных условиях

Ряд ученых-правоведов видят позитивные перспективы повсеместного внедрения «цифровых инструментов» в государственное и муниципальное управление, включая систему национального правосудия. В частности, поднимается вопрос о «цифровой дееспособности» [27] в области защиты нарушенных прав, свобод и законных интересов, а также о соотношении «цифрового профиля» с «цифровой дееспособностью». Однако автор полагает, что в данном контексте ситуация не столь однозначна, поскольку достоверность «цифровых профилей» должна быть

подтверждена не только на техническом уровне, но и фактически. В противном случае, учитывая возможность подделки и манипуляции цифровыми данными, возникает вопрос о достоверности предоставляемых доказательств [28, 29].

Данные аспекты затрагивают интересы неограниченного круга лиц, поэтому требуют не только тщательной проработки, но и должны рассматриваться с учетом возможных правовых и фактических последствий, и не только в одностороннем порядке или с одной из позиций, а в комплексе, с точки зрения многоаспектности, поскольку все эти аспекты формируют современную и последующую действительность. На эти и многие другие особенности трансформации процессуальной формы в цивилистическом процессе в связи с внедрением ИКТ обращают современные представители процессуальной научной школы [30, с. 40; 31, с. 62—63; 32].

Справедливым и актуальным является научное воззрение о том, что «возможность замены судьи на определенных этапах отправления правосудия не только требует комплексной оценки соответствующих рисков, но и может быть признана нежелательной для общества» [33].

Ученые-правоведы, участвующие в научной дискуссии по вопросу внедрения положительного опыта «цифровых инструментов» иностранных государств [34—36] в систему национального правосудия и расширения границ его применения, не учитывают ряд факторов, имеющих, по мнению автора, особое значение.

К ним относятся, во-первых, национальные особенности реализации тех или иных программных и стратегических планов и мероприятий; во-вторых, технологическое и техническое оснащение в настоящее время в России; в-третьих, не только проблемы кадрового потенциала в данной сфере, но и уровень как узкопрофильного образования, так и междисциплинарной подготовки. Стоит отметить, что в отличие от России, иностранные государства, имеют длительный период поступательного развития в данном вопросе.

Немаловажно оценивать уровень социально-экономической составляющей в данной сфере. В частности, необходимо оснащать технически не только органы судебной власти, но и неограниченный круг лиц, так как судебная защита может понадобиться любому заинтересованному лицу в любой момент времени. Право на судебную защиту и на доступ к правосудию не должно зависеть от технической оснащенности судов или заинтересованного лица, а также иных объективных или субъективных причин или условий. Судебная система и отправление правосудия должны осуществляться в любых условиях и при любых обстоятельствах; ни внешние, ни какие-либо еще факторы не должны влиять на ход судебного процесса.

Например, об этом свидетельствует произошедший в недавнем времени технический сбой в системе

ГАС «Правосудие»³ (в период с 7 октября по 11 ноября 2024 года), который создал необходимость возвращения к письменным началам в судопроизводстве, а также дестабилизировал отправление правосудия и привел к ряду проблем накопительного характера в судопроизводстве.

При этом существуют и иные примеры, которые демонстрируют, что идеализация высокотехнологичных продуктов в системе правосудия может повлечь за собой негативные последствия, а также создать дополнительные трудности. Например, использование отдельного ПО привело к тому, что федеральный суд Южного округа Нью-Йорка в США рассматривал дело о наложении штрафа на практикующего юриста за использование технологий ИИ при поиске судебных актов прецедентного значения и создании краткого изложения иска⁴. В отечественной практике применение высокотехнологичного ПО, обладающего элементами ИИ, в беспилотном транспорте привело к тому, что происходят аварии с причинением вреда⁵.

Вышеизложенное тесно связано с судебной системой и правосудием. Так, посредством происходящей повсеместной цифровизации во всех сферах трансформируется форма и модель отправления правосудия, меняется организационно-техническая составляющая сопровождения судебной деятельности, а также появляются новые вызовы для судебной системы. Возникают особенности реализации профессиональной деятельности, не только позитивного, но и негативного характера, в том числе в области юриспруденции.

Произошедшая идеализация высокотехнологичных продуктов приводит к трем основным аспектам.

Первый аспект — это упрощение и ускорение отдельных процессов за счет качества и количества потребляемых ресурсов, в том числе специалистов и профессионалов, что приводит к перераспределению не только трудовых, но и производственных ресурсов.

Второй аспект — изменение социально-экономических отношений, а также трансформация государственной и судебной политики. В частности, нивелируется принцип «соблюдения частных и публичных интересов», защиты и учета основополагающих конституционных и общечеловеческих ценностей при разработке и внедрении высокотехнологичной продукции в различные отрасли, а также поддержки и развития смежных и междисциплинарных областей.

Третий аспект — не развиваются высокотехнологичные, многокомпонентные программные решения,

³ Кучушев С., Суринская Я., Арялина М. Как самый масштабный сбой ГАС «Правосудие» повлиял на работу судебной системы // Ведомости. 2024. 11 ноября.

⁴ Адвокат из США ответил в суде за ошибки искусственного интеллекта // Российское агентство правовой и судебной информации. 2023. 31 мая.

⁵ Минэк назвал число ДТП с участием экспериментальных беспилотных авто. Сколько инцидентов случилось по вине самих машин // РБК. 2025. 6 февраля.

которые могли бы повысить производственные показатели, с одной стороны, а с другой — сформировать высокотехнологичный, а также самостоятельный экономический и технологический базис национального общества [37].

Современная парадигма правосудия и виртуальное пространство

Автор рассматривает «парадигму российского правосудия» с традиционных, консервативных начал, а именно как «традиционную модель (тип) отправления правосудия», на которую в настоящее время влияет современная объективная реальность, в том числе многочисленные цифровые инструменты, внедряемые в судопроизводство и организационно-техническое сопровождение судебной деятельности.

Виртуальное пространство в правосудии включает в себя проведение не только онлайн-заседаний, но и использование других современных технологических решений, которые могут, с одной стороны, оптимизировать судебную деятельность, а с другой — привести к формированию отдельных рисков.

Например, узкоспециализированное ПО позволяет осуществлять трехмерное моделирование или реконструкцию событий [37], произошедших в прошлом, а также создавать трехмерные модели объектов материального мира в будущем [38].

Продолжающаяся тенденция трансформации правосудия в пользу «цифровых» и «программных» сервисов проявляется не только в научных исследованиях, но и на практике. Это приводит к размыванию содержания и сути национальной судебной системы. В частности, активно обсуждаются вопросы создания цифровых сервисов, способных самостоятельно генерировать судебные акты [39], а также внедрения ПО в формате «робота-судьи» [40]. Такой подход сводит осуществление правосудия к механистическому процессу, основанному лишь на программных алгоритмах и цифровых кодах.

В связи с этим хотелось бы обратить внимание на точку зрения выдающегося государственного деятеля своего времени Б.Н. Чичерина, который в своем фундаментальной работе «Курс государственной науки» отмечал, что «правосудие — это воздаяние каждому должного на основании закона» [41, с. 319], что не теряет своей актуальности в настоящее время.

Несмотря на происходящее поступательное развитие общества в условиях внедрения высокотехнологичных сервисов и программных решений, не следует отходить от традиционных канонов восприятия «суда как беспристрастного посредника в споре между двумя заинтересованными лицами (сторонами)», как было отмечено профессором И.Я. Фойницким [42, с. 7], а также от понимания того, что «суд служит не частным интересам отдельных лиц, отдельных общественных кружков или отдельных ведомств, а общим государственным интересам правосудия; все судебные реше-

ния постановляются именем государства; суд — есть функция государственной власти» [там же].

Таким образом, возникают не только риторические, но и философские вопросы, требующие анализа содержания современного национального правосудия, а также морально-нравственные аспекты в понимании справедливости и доступности правосудия, установления объективной истины, установления границ в делегировании информационным технологиям осуществления деятельности, отягощенной правообразующими аспектами.

В настоящее время исследования применения ИКТ в правосудии чаще всего рассматривают эту проблематику с одного или двух аспектов. Подходы, объединяющие различные аспекты или рассматривающие вопрос с позиции многоаспектности, встречаются реже и представлены небольшим числом авторов.

Например, специалисты в области уголовного судопроизводства и уголовного процесса отмечают, что «создание электронного уголовного дела — важный шаг по демократизации и открытости уголовного судопроизводства, защиты его от фальсификации, злоупотреблений и коррупционных рисков» [43—45]. Безусловно, данные аспекты важны и требуют развития, но при этом вопросы сохранения тайны и неприкосновенности личной жизни, а также сохранения репутации в подобного рода исследованиях не ставятся.

Для гражданского судопроизводства также характерна идеализация ИКТ с точки зрения доступности, беспристрастности, объективности, обеспечения прозрачности отправления судебного процесса по гражданским делам [46, 47].

Автору хотелось бы обратить внимание на важность разделения организационно-технических решений и непосредственной сути при отправлении правосудия. Иными словами, следует разграничивать судопроизводственные и судоустройственные начала при внедрении и использовании высокотехнологичных продуктов в судебной системе.

В связи с происходящим расширением границ цифровых технологий в области отправления правосудия возникают вопросы, требующие не только ответа, но и переосмысления. Кем будет выноситься судебное решение? «Именем Российской Федерации», «цифровым кодом» или «программным обеспечением с серийным номером»? В данном случае автор утрирует, но этот вопрос остается открытым: прежде чем ратовать за передачу принятия судебных решений ИТ-технологиям, необходимо обратиться к содержанию таких понятий, как «суд», «правосудие», «судебная власть», «отправление правосудия», «судопроизводство», «судоустройство», «судебная деятельность», «организационно-техническое обеспечение судебной деятельности».

Примеры, когда ПО или его комплексы дискредитировали себя, указывают на то, что идеализация ИТ-технологий и передача части юридической деятельности на их откуп являются преждевременными для национального правопорядка. Это касается не только

технической стороны вопроса, где такие технологии должны быть сертифицированы, а специалисты, использующие их, иметь соответствующую лицензию и аккредитацию. Важно также формирование нормативно-правовой базы, обеспечивающей соответствие охраны и безопасности как отдельным гражданам, так и неопределенному кругу лиц, включая окружающую среду, особенно в областях с повышенными рисками и угрозами, таких как космическая или военная сфера. Автор уже отмечала, что декодирование возможно во всех сферах деятельности, поэтому необходимо усилить не только нормативно-правовую базу, но и уровень подготовки специалистов в данной области.

Разработка IT-технологий должна осуществляться аккредитованными специалистами и компаниями, к которым должны предъявляться установленные законом требования повышенного уровня, так как необходимо учитывать вопросы защиты личной и национальной безопасности неограниченного круга лиц.

Искусственный интеллект в правосудии — способ, а не средство

Виртуальное пространство в правосудии включает в себя использование и применение ИИ — совокупности ПО, которое может позволить заменить профессиональные и экспертные области, которые ранее осуществлялись человеком.

В последние годы темпы внедрения ИИ увеличиваются, что, с одной стороны, свидетельствует о развитии технологического суверенитета, а с другой — ставит перед национальным обществом новые вопросы, цели и задачи, требующие решения. Авторская позиция по данному вопросу заключается в следующем. ИИ как наиболее часто используемая категория является продуктом профессиональной деятельности специалистов в области математики, информатики, информационных технологий, кибернетики и иных технических и точных наук. При этом ИИ — это совокупность ПО, которое разрабатывается группой лиц или рабочими группами, по заданным параметрам, под конкретные цели и задачи, которые формулируются и ставятся разработчиками заказчиками. Конкретизирую: под любое разрабатываемое ПО формируется (должно формироваться) техническое задание (далее — ТЗ), которое содержит (или должно содержать) не только технические и технологические условия по разработке данного ПО, параметры его функционирования, но и конкретные задачи, которые оно должно решать, а также цели и условия, в которых оно должно функционировать или которые должно создать при его внедрении в социально-экономические отношения, что является не менее актуальным. Поэтому аргументы о том, что ИИ является более объективным при выполнении поставленных задач, является спорным, так как так называемый человеческий фактор нельзя исключать из данного рода отношений.

В связи с этим возникает вопрос идентификации используемой и применяемой не только в научной

периодической литературе, но и на практике и в нормативно-правовой базе категории ИИ как технологии, системы или механизма, применяемого в профессиональной деятельности, так как засилие большого количества терминов и понятий в данной области может привести не только к сложности идентификации данного рода цифровых продуктов, но и к правовой неопределенности. Авторский поиск определения ИИ заключается в необходимости анализа устоявшихся терминов и понятий, которые могут позволить идентифицировать современный ИИ в правосудии.

Технология (от греч. τέχνη — искусство, мастерство, ремесло, наука) — это совокупность приемов и способов получения, добычи и обработки или переработки сырья, материалов и т. п., осуществляемых в различных отраслях промышленности, строительстве и т. д., при этом технология может охватывать методы производства товаров и услуг (технология в чистом виде), либо воплощенная технология, охватывающая машины, оборудование, сооружения, производственные системы и продукция с высокими технико-экономическими параметрами.

Данное понятие также включает в себя комплекс организационных мер, операций и приемов, направленных на изготовление чего-либо с заранее заданными параметрами (или номинальным качеством, которое должно быть реализовано в конечный продукт рынка)⁶.

Технологию также можно рассматривать и как научную дисциплину, базирующуюся на системном подходе по разработке и совершенствовании способов и инструментов производства, которые могут быть использованы для создания материальных и нематериальных ценностей.

На современном этапе развития общества в содержание понятия «технология» закладываются инновационные процессы по созданию и развитию «высоких технологий», а также сложные комплексы знаний или секреты производства, полученные на основе проведенных исследований⁷.

Система (от греч. σύστημα, в буквальном смысле — состав, а от лат. — составлять или ставить вместе) — совокупность элементов, находящихся во взаимосвязи между собой, которые образуют единое целое или определенную целостность⁸.

Автор данного исследования полагает, что категория ИИ наиболее близка по содержанию к термину «система», так как он также базируется на совокупности элементов не только ПО, но и сложных технических устройств (персональные компьютеры, серверы и не только), которые, в свою очередь, оснащены специализированным ПО, позволяющим разрабатывать

⁶Технология // Большая российская энциклопедия. Т. 32. Москва, 2016. С. 113—114.

⁷Там же.

⁸Садовский В.Н. Система // Большая российская энциклопедия: научно-образовательный портал. URL: <https://bigenc.ru/c/sistema-4284c7?v=9351238> (дата обращения: 06.03.2025).

совокупность ПО, которые в итоге будет образовывать ИИ (единое целостное ПО, сочетающее в себя ряд программных решений). А вот специализированное ПО, применяемое в тех или иных сферах, — это технология, то есть ИИ (как система) состоит из ПО (технологий).

Декодировать можно любую программу или иной цифровой сервис, или информационную систему, или иной инструмент и продукт, функционирующий на основе того или ПО. Таким образом, возникает вопрос: стоит ли формировать настолько сильную взаимосвязь между осуществлением защиты прав, свобод и законных интересов в судебных органах и внедрением повсеместного ИИ в судебной деятельности?

Целесообразно было бы обратиться, во-первых, к качеству ПО, используемого в данной деятельности, а во-вторых, развивать узкопрофильное, специализированное ПО, которое может быть применимо и быть использовано в судебной системе не только в судопроизводстве, но и в судоустройственной деятельности и организационно-техническом сопровождении судов.

Заключение

Руководствуясь положениями ст. 46 Конституции Российской Федерации (далее — Конституция РФ), можно заключить, что реализация конституционно-правовой гарантии права на судебную защиту включает в себя в том числе и доступность, эффективность правосудия с позиции не только своевременного восстановления нарушенных прав, свобод и законных интересов, но и своевременного и фактического их исполнения. Поэтому развитие цифровых инструментов в правосудии и органах ФССП должно способствовать оптимизации совершения отдельных процессуальных действий, а также формированию эффективного ведомственного и внутриведомственного взаимодействия, необходимого для оптимизации отдельных организационно-технических действий, совершаемых для реализации права на судебную защиту в полном объеме.

Особо хотелось бы отметить, что в условиях усиливающейся роли технологических решений и их применения и внедрения во всё большее количество сфер и областей, в том числе с учетом происходящей информатизации правосудия, необходимо, во-первых, учитывать соблюдение баланса частных и публичных интересов, а во-вторых — опираться на необходимость соблюдения основополагающих прав, свобод и законных интересов неограниченного круга лиц, в первую очередь, граждан и отдельных индивидуумов, так как при осуществлении судебной деятельности право должно быть восстановлено либо защищено, а не наоборот.

В связи с этим автор обращает внимание на то, что цифровые инструменты в правосудии в частности и в правовой системе в целом являются способом достижения поставленных целей и задач, а не средством их осуществления.

Иными словами, применяемые IT-технологии должны соответствовать своему назначению, отвечая современным запросам и потребностям общества, а не изменять процессуальную форму и содержание правосудия. Это касается не только проведения судебных заседаний с использованием IT-технологий (например, онлайн-заседания), но и трансформации многовекового опыта человечества в восприятии судебных органов, что отражается в популяризации терминов «виртуальные суды», «киберправосудие», «электронные весы правосудия» и др.

Отдельно следует остановиться на последствиях для заинтересованных лиц в случаях отказа от традиционных начал в национальном правосудии в угоду «виртуализации», а именно:

1. Обезличивание судебного процесса посредством внедрения всё большего количества цифровых инструментов; это не только создание шаблонного, унифицированного судопроизводства, но и уход (отход или отказ) от конституционно-правовых ценностей по защите основных прав, свобод и законных интересов.
2. Ситуативный отказ от целей, задач и принципов правосудия, а именно от поиска объективной истины, восстановления полной картины произошедших событий (реконструкция фактических обстоятельств дела по представленным материалам в суд), необходимых для защиты нарушенных прав, свобод и законных интересов, ведет к утрате справедливости при принятии судебных актов. Из этого следует, что конституционно-правовая гарантия «право на судебную защиту» (ст. 46 Конституции РФ) приобретает новые, не устоявшиеся формы.
3. Нивелирование значения судебного процесса как такового (а в отдельных случаях и судебных заседаний), его автоматизация и сведение до автоматического, системно-математического анализа представленных доказательств с целью принятия (вынесения) судебного акта низводит всю многовековую суть правосудия, которая заключается в поиске объективной истины по делу, установлении фактических обстоятельств, восстановлении справедливости для заинтересованных лиц, формировании и создании новых правоотношений или изменении имеющихся, то есть связана с правообразующими или распорядительными функциями, до выдачи судебного акта, как получения «бланкетных» документов.
4. Стремление к автоматизации судебных функций может привести и к другим неоднозначным последствиям, а именно: расширить получение сведений и информации об участниках процесса, либо привести к разглашению информации, подлежащей охране и т. п. Это порождает и другие вопросы, требующие ответа, например: как найти баланс между традиционными началами отправления правосудия и современными про-

цессами автоматизации и информатизации судебной деятельности? Принципы гласности, открытости, доступности и добросовестности приобретают новые формы реализации, однако возникает проблема достоверности фактов и фактических обстоятельств, поскольку цифровые инструменты открывают широкие возможности для искажения информации и даже фальсификаций.

Полагаю, что технологизация судебной деятельности сопряжена с рядом рисков, не только касающихся особой охраны персональных данных, но и непосредственно реализации конституционно-правовой гарантии права на судебную защиту, которое распространяет свое действие на всех заинтересованных лиц, т. е. не только на физические, юридические лица, но и публично-правовые образования. Реализация ст. 46 Конституции Российской Федерации приобретает все новые очертания, и последние события ушедшего года — тому пример.

Есть области правоотношений, где технический сбой «смерти подобен», и это — судебная система. Поэтому автор и предлагает обратиться к концептуальным аспектам развития правосудия и судебной системы с позиции «судебного права» [48].

Выводы

Автор полагает, что обозначенные проблемы связаны в первую очередь с тем, что отсутствует междисциплинарный подход к развитию данной отрасли. Обновление правовой составляющей в ней возможно с учетом синтеза знаний в области права, цифровых инструментов и информационной безопасности [49, 50].

Было бы целесообразно для начала рассмотреть возможность создания обновленного словаря тер-

минов изучаемой сферы как один из первых этапов формирования унифицированного понятийного аппарата, с привлечением специалистов в области как юриспруденции, так и информационных технологий. Для этого необходимо повысить уровень материального поощрения специалистов, обладающих междисциплинарными знаниями в области права, информационных технологий и информационной безопасности; усилить роль междисциплинарного взаимодействия при реализации проектов, технических заданий для преодоления возникающих проблем при достижении поставленных целей, а впоследствии — в правоприменении; преодолеть разобщенность правового регулирования, являющуюся следствием вышеизложенных пунктов; провести централизованный правовой мониторинг рассматриваемой отрасли и смежных отраслей, что позволит преодолеть последствия ускоренного развития информационных технологий, приводящие к тому, что базовое законодательство стремительно устаревает и требует систематического обновления и конкретизации.

Таким образом, проведение «ревизии» нормативных актов в данной области с использованием методик правового мониторинга позволило бы выявить противоречия в законодательном массиве, а также привести к упорядочиванию цифровизации социально-экономических отношений, так как происходящее увеличение разного рода информационных систем в различных отраслях, сферах и областях жизнедеятельности не способствует упрощению в отдельных случаях отношений, а иногда наоборот — приводит к тому, что традиционные способы осуществления тех или иных задач видоизменяются, трансформируются, в том числе возникают негативные тенденции, приводящие к нарушению прав, свобод и законных интересов как частных лиц, так и неограниченного их круга.

Литература

1. Федотов М.А. Киберпространство как сфера обитания права // Бюллетень ЮНЕСКО по авторскому праву. 1999. Т. XXXII. № 1. С. 21.
2. Васильев А. Даркнет как ускользящая сфера правового регулирования / А. Васильев, Ж. Ибрагимов, О. Васильева // Юрислингвистика. 2019. № 12 (23). С. 10—12.
3. Кодзоков Б.В. Скрытая сеть «даркнет»: криминологический аспект // Пробелы в российском законодательстве. 2021. Т. 14. № 3. С. 114—117.
4. Федорович М.А. «Даркнет» как угроза экономической безопасности Российской Федерации // Евразийский юридический журнал. 2022. № 7 (170). С. 391—393.
5. Право и виртуальное пространство : монография / Отв. ред. Ю.А. Тихомиров. М. : Проспект, 2025. 176 с.
6. Правовой статус субъектов в виртуальном пространстве / М.Е. Черемисинова. М. : Изд. дом «Юриспруденция», 2020. 208 с.
7. Черемисинова М.Е. Правовая культура в виртуальном пространстве // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2024. Т. 28. № 3. С. 477—493.
8. Залоило М.В. Метаморфозы юридического языка в виртуальном пространстве // Журнал российского права. 2024. Т. 28. № 12. С. 30—48.
9. Гутников О.В., Чагина Е.М. Защита интересов потребителей при регулировании электронной торговли // Право и бизнес. 2023. № 4. С. 8—15.
10. Защита прав потребителей: в поисках оптимальной модели / П.Д. Багрянская, М.О. Дьяконова, П.П. Кабытов [и др.]. М. : Юридическая фирма «Контракт», 2021. 268 с.

11. Куль И.Г., Нигол Р.П., Сильдмяз И.Я., Ээремаа К.А. Информационно-поисковая система для законодательного материала // Правоведение. 1970. № 4. С. 102—105.
12. Москвин С.С. Информационно-поисковая система нормативных материалов // Советское государство и право. 1972. № 2. С. 121—126.
13. Чечина Н.А. Избранные труды по гражданскому процессу / Сост. Е.Ю. Новиков, Н.С. Лосев; предисл. Н.М. Кропачев, С.А. Белов, Т.И. Яковлева, И.А. Тур, М.И. Горлачева. 2-е изд. СПб. : Изд-во С.-Петерб. ун-та, 2021. С. 577.
14. Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1. С. 3—29.
15. Жарич А.В. Национальные и международные предпосылки создания Цифрового кодекса РФ // Цивилист. 2023. № 4. С. 5—9.
16. Нестеров А.В. Цифровое право против информационного кодекса // Юрист. 2021. № 11. С. 8—12.
17. Рожкова М.А. Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса? // Хозяйство и право. 2020. № 4 (519). С. 3—12.
18. Белякова А.В. Особенности правового регулирования в сфере информационной безопасности // Цифровые технологии и право: сборник научных трудов III Международной научно-практической конференции (г. Казань, 20 сентября 2024 г.) / Под ред. И.Р. Бегишева, Е.А. Громовой, М.В. Залоило, И.А. Филиповой, А.А. Шутовой. В 6 т. Т. 5. Казань : Изд-во «Познание» Казанского инновационного университета, 2024. С. 146—147.
19. Белякова А.В. Проблемы правового регулирования в области кибернетики и информационной безопасности // Кибернетика и информационная безопасность «КИБ-2024» : сборник научных трудов II Всероссийской научно-технической конференции, Москва, 22—23 октября 2024 года. М. : Национальный исследовательский ядерный университет «МИФИ», 2024. С. 142—143.
20. Никитина Е.М. Международно-правовое сотрудничество государств в области борьбы с киберпреследованием женщин // Журнал правовых и экономических исследований. 2016. № 1. С. 52—58.
21. Юрченко И.А. Сталкер как субъект уголовной ответственности // Вестник Университета им. О.Е. Кутафина (МГЮА). 2018. № 12 (52). С. 53—61.
22. Абазова Е.Х. Противодействие киберпреступности в современных условиях // Право и управление. 2023. № 8. С. 224—227.
23. Куркин П.Г., Примакова С.В. К вопросу необходимости криминализации stalking и киберstalking // Право и управление. 2025. № 1. С. 174—178.
24. Кучина Я.О. Проблема экстраполяции элементов криминологической характеристики отдельных видов преступности в киберпространстве: общая характеристика киберstalking // Расследование преступлений: проблемы и пути их решения. 2020. № 3 (29). С. 47—51.
25. Зайцев И.А. Административная ответственность за оскорбление, совершенное публично с использованием информационно-телекоммуникационных сетей, включая сеть Интернет // Административное право и процесс. 2023. № 8. С. 54—60.
26. Белозерова Ю.Г. К слову о составе гражданского правонарушения в сети Интернет // Экономика. Право. Общество. 2020. Т. 5. № 3 (23). С. 23—26.
27. Фетисов А.К. Цифровая дееспособность // Арбитражный и гражданский процесс. 2021. № 5. С. 3—7.
28. Лукьянова И.Н. Достоверность электронных доказательств в судебном разбирательстве онлайн (некоторые рассуждения о проблемах электронного правосудия в эпоху «COVID-19» и после) // Законы России: опыт, анализ, практика. 2020. № 7. С. 44—50.
29. Лаптев В.А., Чуча С.Ю. Нотариально удостоверенные доказательства в судебном процессе: теория и правоприменительная практика // Вестник гражданского процесса. 2023. № 1. С. 79—99.
30. Брановицкий К.Л. Цифровая доступность правосудия: трансграничное измерение // Арбитражный и гражданский процесс. 2020. № 6. С. 39—44.
31. Брановицкий К.Л., Ренц И.Г., Незнамов Ал.В., Незнамов Ан.В., Ярков В.В. Цифровые технологии в цивилистическом процессе: некоторые проблемы и перспективы // Вестник гражданского процесса. 2019. № 4. С. 56—63.
32. Трезубов Е.С. Тенденции цифровизации цивилистического процесса // Вестник гражданского процесса. 2022. № 5. С. 204—227.
33. Незнамов А.В. К вопросу о применении технологий искусственного интеллекта в правосудии: терминологический аспект // Арбитражный и гражданский процесс. 2019. № 10. С. 14—18.
34. Бурдина Е.В., Чижов М.В. Организационно-правовые модели судебной деятельности в условиях платформизации правосудия: опыт России и других стран БРИКС // Журнал российского права. 2023. № 10. С. 116—129.
35. Харитонов Ю.С. Платформизация правосудия: опыт Китая и будущее судебных систем мира // Вестник арбитражной практики. 2020. № 3. С. 3—11.
36. Харитонов Ю.С., Ян Т. Правовые проблемы трансформации основных начал правосудия в условиях цифровизации цивилистического процесса в России и Китае // Вестник гражданского процесса. 2023. № 1. С. 203—235.
37. Белякова А.В. Современное правосудие «сквозь призму цифровизации»: отдельные аспекты // Правовая информатика. 2024. № 3. С. 156—167.
38. Березина Е.А. Опыт внедрения машиночитаемого формата юридических документов в Российской Федерации // Правовое государство: теория и практика. 2024. № 3 (77). С. 62—73.

39. Пашенцев Д.А., Новикова К.С. Искусственный интеллект как субъект судебного толкования права // Образование и право. 2020. № 7. С. 198—202.
40. Незнамов А.В. Перспективы внедрения технологий искусственного интеллекта в правосудие // Информационное право. 2022. № 1. С. 26—30.
41. Чичерин Б.Н. Курс государственной науки. Ч. 1: Общее государственное право. М. : Типо-лит. Выс. утв. т-ва И.Н. Кушнерев и К°, 1894. 481 с.
42. Фойницкий И.Я. Курс уголовного судопроизводства. Т. 1. СПб. : Типография т-ва «Общественная Польза», 1912. 577 с.
43. Халиков А.Н. Соотношение современной информационной сферы с государственной монополией на расследование уголовных дел при использовании цифровых технологий в уголовном судопроизводстве // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 101—105.
44. Макарова О.В. Совершенствование судопроизводства путем внедрения электронной формы уголовного дела // Журнал российского права. 2019. № 2. С. 159—168.
45. Шереметьев И.И. Использование цифровых технологий при рассмотрении уголовных дел в суде: реальность и перспективы // Lex russica. 2019. № 5. С. 117—131.
46. Фомин А.А. Цифровая трансформация судебной деятельности в современной России // Администратор суда. 2024. № 3. С. 2—6.
47. Цифровые технологии в гражданском и административном судопроизводстве: практика, аналитика, перспективы / М.В. Самсонова, Е.Г. Стрельцова, А.В. Чайкина и др.; отв. ред. Е.Г. Стрельцова. М. : Инфотропик Медиа, 2022. 336 с.
48. Belyakova A.V. Artificial Intelligence in the Judiciary: Issues and Outlooks // Legal Issues in the Digital Age. 2024. № 3. Pp. 68—87.
49. Карцхия А.А. Правовой формат искусственного интеллекта // Правовая информатика. 2024. № 2. С. 125—133.
50. Карцхия А.А., Макаренко Г.И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. 2024. № 1 (59). С. 2—14.

SECTION:
CONSTITUTIONAL LAW

ADMINISTRATION OF JUSTICE AND VIRTUAL SPACE

Anna Belyakova, Ph.D. (Law), Leading Researcher at the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russian Federation. ORCID: 0000-0003-4241-4511.

E-mail: belyakova.av@gmail.com

Keywords: *judicial system, digital technologies, cyberjustice, robot judge, paradigm of modern administration of justice, artificial intelligence in administration of justice.*

Abstract

Purpose of the paper: analysing the implementation of modern social relations in the context of ubiquitousness of digital tools; including studying their impact on the national judicial system, and identifying and raising a number of questions and problems in this field so as to facilitate further development of the judicial process.

Methods used in the study: general scientific methods of analysis, synthesis, generalisation, and the dialectical method, as well as the methods of formal logic, legal technique, and comparative law.

Study findings: the analysis carried out allowed to word the author's stand on virtualisation' and digitalisation' of today's judicial process. The author's standpoint regarding the content of artificial intelligence in administration of justice and virtual space is specified. The analysed research approaches in this area make it possible to identify fields for further research and allow the author to form and detail her standpoint.

References

1. Fedotov M.A. Kiberprostranstvo kak sfera obitaniia prava. Biulleten' IuNESKO po avtorskomu pravu. 1999. T. XXXII. No. 1. P. 21.
2. Vasil'ev A. Darknet kak uskol'zaiushchaia sfera pravovogo regulirovaniia. A. Vasil'ev, Zh. Ibragimov, O. Vasil'eva. Iurilingvistika. 2019. No. 12 (23). Pp. 10—12.

3. Kodzokov B.V. Skrytaia set' "darknet": kriminologicheskii aspekt. Probely v rossiiskom zakonodatel'stve. 2021. T. 14. No. 3. Pp. 114–117.
4. Fedorovich M.A. "Darknet" kak ugroza ekonomicheskoi bezopasnosti Rossiiskoi Federatsii. Evraziiskii iuridicheskii zhurnal. 2022. No. 7 (170). Pp. 391–393.
5. Pravo i virtual'noe prostranstvo : monografiia. Otv. red. Iu.A. Tikhomirov. M. : Prospekt, 2025. 176 pp.
6. Pravovoi status sub'ektov v virtual'nom prostranstve. M.E. Cheremisinova. M. : Izd. dom "Iurisprudentsiia", 2020. 208 s.
7. Cheremisinova M.E. Pravovaia kul'tura v virtual'nom prostranstve. Vestnik Rossiiskogo universiteta družby narodov. Seriia: iuridicheskie nauki. 2024. T. 28. No. 3. Pp. 477–493.
8. Zaloilo M.V. Metamorfozy iuridicheskogo iazyka v virtual'nom prostranstve. Zhurnal rossiiskogo prava. 2024. T. 28. No. 12. Pp. 30–48.
9. Gutnikov O.V., Chagina E.M. Zashchita interesov potrebiteli pri regulirovanii elektronnoi torgovli. Pravo i biznes. 2023. No. 4. Pp. 8–15.
10. Zashchita prav potrebiteli: v poiskakh optimal'noi modeli. P.D. Bagrianskaia, M.O. D'iakonova, P.P. Kabytov [i dr.]. M. : Iuridicheskaiia firma "Kontrakt", 2021. 268 pp.
11. Kull' I.G., Nigol R.P., Sil'dmiae I.Ia., Eeremaa K.A. Informatsionno-poiskovaia sistema dlia zakonodatel'nogo materiala. Pravovedenie. 1970. No. 4. Pp. 102–105.
12. Moskvina S.S. Informatsionno-poiskovaia sistema normativnykh materialov. Sovetskoe gosudarstvo i pravo. 1972. No. 2. Pp. 121–126.
13. Chechina N.A. Izbrannye trudy po grazhdanskomu protsessu. Sost. E.Iu. Novikov, N.S. Losev; predisl. N.M. Kropachev, S.A. Belov, T.I. Iakovleva, I.A. Tur, M.I. Gorlacheva. 2-e izd. SPb. : Izd-vo S.-Peterb. un-ta, 2021. P. 577.
14. Vaipan V.A. Istochniki tsifrovogo prava. Vestnik arbitrazhnoi praktiki. 2024. No. 1. Pp. 3–29.
15. Zharich A.V. Natsional'nye i mezhdunarodnye predposylki sozdaniia Tsifrovogo kodeksa RF. Tsivilist. 2023. No. 4. Pp. 5–9.
16. Nesterov A.V. Tsifrovoe pravo protiv informatsionnogo kodeksa. Iurist. 2021. No. 11. Pp. 8–12.
17. Rozhkova M.A. Iavliaetsia li tsifrovoe pravo otrasl'iu prava i ozhdat' li poiavleniia tsifrovogo kodeksa?. Khoziaistvo i pravo. 2020. No. 4 (519). Pp. 3–12.
18. Beliakova A.V. Osobennosti pravovogo regulirovaniia v sfere informatsionnoi bezopasnosti. Tsifrovye tekhnologii i pravo: sbornik nauchnykh trudov III Mezhdunarodnoi nauchno-prakticheskoi konferentsii (g. Kazan', 20 sentiabria 2024 g.). Pod red. I.R. Begisheva, E.A. Gromovoi, M.V. Zaloilo, I.A. Filipovoi, A.A. Shutovoi. V 6 t. T. 5. Kazan' : Izd-vo "Poznanie" Kazanskogo innovatsionnogo universiteta, 2024. Pp. 146–147.
19. Beliakova A.V. Problemy pravovogo regulirovaniia v oblasti kibernetiki i informatsionnoi bezopasnosti. Kibernetika i informatsionnaia bezopasnost' "KIB-2024": sbornik nauchnykh trudov II Vserossiiskoi nauchno-tekhnicheskoi konferentsii, Moskva, 22–23 oktiabria 2024 goda. M. : Natsional'nyi issledovatel'skii iadernyi universitet "MIFI", 2024. Pp. 142–143.
20. Nikitina E.M. Mezhdunarodno-pravovoe sotrudnichestvo gosudarstv v oblasti bor'by s kiberpresledovaniem zhen-shchin. Zhurnal pravovykh i ekonomicheskikh issledovani. 2016. No. 1. Pp. 52–58.
21. Iurchenko I.A. Stalker kak sub'ekt ugovnoi otvetstvennosti. Vestnik Universiteta im. O.E. Kutafina (MGlUa). 2018. No. 12 (52). Pp. 53–61.
22. Abazova E.Kh. Protivodeistvie kiberprestupnosti v sovremennykh usloviakh. Pravo i upravlenie. 2023. No. 8. Pp. 224–227.
23. Kurkin P.G., Primakova S.V. K voprosu neobkhodimosti kriminalizatsii stalkinga i kiberstalkinga. Pravo i upravlenie. 2025. No. 1. Pp. 174–178.
24. Kuchina I.A.O. Problema ekstrapoliatsii elementov kriminologicheskoi kharakteristiki ot del'nykh vidov prestupnosti v kiberprostranstve: obshchaia kharakteristika kiberstalkinga. Rassledovanie prestuplenii: problemy i puti ikh resheniia. 2020. No. 3 (29). Pp. 47–51.
25. Zaitsev I.A. Administrativnaia otvetstvennost' za oskorblenie, sovershennoe publichno s ispol'zovaniem informat-sionno-telekommunikatsionnykh setei, vkluchaia set' Internet. Administrativnoe pravo i protsess. 2023. No. 8. Pp. 54–60.
26. Belozerova Iu.G. K slovu o sostave grazhdanskogo pravonarusheniia v seti Internet. Ekonomika. Pravo. Obshchestvo. 2020. T. 5. No. 3 (23). Pp. 23–26.
27. Fetisov A.K. Tsifrovaia deеспособnost'. Arbitrazhnyi i grazhdanskii protsess. 2021. No. 5. Pp. 3–7.
28. Luk'ianova I.N. Dostovernost' elektronnykh dokazatel'stv v sudebnom razbiratel'stve onlain (nekotorye rassuzh-deniiia o problemakh elektronnoho pravosudiia v epokhu "COVID-19" i posle). Zakony Rossii: opyt, analiz, praktika. 2020. No. 7. Pp. 44–50.
29. Laptev V.A., Chucha S.Iu. Notarial'no udostoverennye dokazatel'stva v sudebnom protsesse: teoriia i pra-voprimenitel'naia praktika. Vestnik grazhdanskogo protsessa. 2023. No. 1. Pp. 79–99.
30. Branovitskii K.L. Tsifrovaia dostupnost' pravosudiia: transgranichnoe izmerenie. Arbitrazhnyi i grazhdanskii protsess. 2020. No. 6. Pp. 39–44.
31. Branovitskii K.L., Rents I.G., Neznamov A.I., Neznamov A.V., Iarkov V.V. Tsifrovye tekhnologii v tsivilisticheskom protsesse: nekotorye problemy i perspektivy. Vestnik grazhdanskogo protsessa. 2019. No. 4. Pp. 56–63.

32. Trezubov E.S. Tendentsii tsifrovizatsii tsivilisticheskogo protsessa. Vestnik grazhdanskogo protsessa. 2022. No. 5. Pp. 204–227.
33. Neznamov A.V. K voprosu o primenении tekhnologii iskusstvennogo intellekta v pravosudii: terminologicheskii aspekt. Arbitrazhnyi i grazhdanskii protsess. 2019. No. 10. Pp. 14–18.
34. Burdina E.V., Chizhov M.V. Organizatsionno-pravovye modeli sudebnoi deiatel'nosti v usloviakh platformizatsii pravosudiia: opyt Rossii i drugikh stran BRIKS. Zhurnal rossiiskogo prava. 2023. No. 10. Pp. 116–129.
35. Kharitonova Iu.S. Platformizatsiia pravosudiia: opyt Kitaia i budushchee sudebnykh sistem mira. Vestnik arbitrazhnoi praktiki. 2020. No. 3. Pp. 3–11.
36. Kharitonova Iu.S., Ian T. Pravovye problemy transformatsii osnovnykh nachal pravosudiia v usloviakh tsifrovizatsii tsivilisticheskogo protsessa v Rossii i Kitae. Vestnik grazhdanskogo protsessa. 2023. No. 1. Pp. 203–235.
37. Beliakova A.V. Sovremennoe pravosudie "skvoz' prizmu tsifrovizatsii": otdel'nye aspekty. Pravovaia informatika. 2024. No. 3. Pp. 156–167.
38. Berezina E.A. Opyt vnedreniia mashinochitaemogo formata iuridicheskikh dokumentov v Rossiiskoi Federatsii. Pravovoe gosudarstvo: teoriia i praktika. 2024. No. 3 (77). Pp. 62–73.
39. Pashentsev D.A., Novikova K.S. Iskusstvennyi intellekt kak sub"ekt sudebnogo tolkovaniia prava. Obrazovanie i pravo. 2020. No. 7. Pp. 198–202.
40. Neznamov A.V. Perspektivy vnedreniia tekhnologii iskusstvennogo intellekta v pravosudie. Informatsionnoe pravo. 2022. No. 1. Pp. 26–30.
41. Chicherin B.N. Kurs gosudarstvennoi nauki. Ch. 1: Obshchee gosudarstvennoe pravo. M. : Tipo-lit. Vys. utv. t-va I.N. Kushnerev i K°, 1894. 481 pp.
42. Foinitskii I.Ia. Kurs ugovnogo sudoproizvodstva. T. 1. SPb. : Tipografiia t-va "Obshchestvennaia Pol'za", 1912. 577 pp.
43. Khalikov A.N. Sootnoshenie sovremennoi informatsionnoi sfery s gosudarstvennoi monopoliei na rassledovanie ugovnykh del pri ispol'zovanii tsifrovnykh tekhnologii v ugovnom sudoproizvodstve. Biblioteka kriminalista. Nauchnyi zhurnal. 2018. No. 3 (38). Pp. 101–105.
44. Makarova O.V. Sovershenstvovanie sudoproizvodstva putem vnedreniia elektronnoi formy ugovnogo dela. Zhurnal rossiiskogo prava. 2019. No. 2. Pp. 159–168.
45. Sheremet'ev I.I. Ispol'zovanie tsifrovnykh tekhnologii pri rassmotrenii ugovnykh del v sude: real'nost' i perspektivy. Lex russica. 2019. No. 5. Pp. 117–131.
46. Fomin A.A. Tsifrovaia transformatsiia sudebnoi deiatel'nosti v sovremennoi Rossii. Administrator suda. 2024. No. 3. Pp. 2–6.
47. Tsifrovye tekhnologii v grazhdanskom i administrativnom sudoproizvodstve: praktika, analitika, perspektivy. M.V. Samsonova, E.G. Strel'tsova, A.V. Chaikina i dr.; otv. red. E.G. Strel'tsova. M. : Infotropik Media, 2022. 336 pp.
48. Belyakova A.V. Artificial Intelligence in the Judiciary: Issues and Outlooks. Legal Issues in the Digital Age. 2024. No. 3. Pp. 68–87.
49. Kartskhiia A.A. Pravovoi format iskusstvennogo intellekta. Pravovaia informatika. 2024. No. 2. Pp. 125–133.
50. Kartskhiia A.A., Makarenko G.I. Pravovye gorizonty tekhnologii iskusstvennogo intellekta: natsional'nyi i mezhdunarodnyi aspekt. Voprosy kiberbezopasnosti. 2024. No. 1 (59). Pp. 2–14.

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ В ЭПОХУ ГЛОБАЛЬНОГО ПРОТИВОСТОЯНИЯ

Баландин А.Ю.¹

Ключевые слова: киберугрозы, информационная безопасность, киберпространство, национальная безопасность, критическая информационная инфраструктура, цифровые технологии, юридические акты, хакерские группы, ИКТ-среда.

Аннотация

В статье рассматривается место правового обеспечения кибербезопасности в системе национальной безопасности Российской Федерации. При исследовании автором предложен системный подход, основанный на формулировании четких юридических определений, направленный на разработку международных и национальных юридических норм, а также интеграцию правовых, технических и организационных мер в целях формирования единого комплексного подхода. В статье уделено внимание необходимости соблюдения баланса между обеспечением безопасности и защитой прав человека в ИКТ-среде, формированию отвечающих общественному запросу правовых механизмов. Содержащиеся в статье предложения могут быть использованы для повышения эффективности правового регулирования, способного адаптироваться к вызовам цифровой эпохи, и необходимого для развития международного сотрудничества в области обеспечения информационной, в том числе кибербезопасности.

Цель работы: обосновать ключевые проблемы правового обеспечения информационной безопасности включая вопросы кибербезопасности.

Методы: системный анализ и сравнительное моделирование, позволяющее обеспечить точность юридических критериев, применяемых в моделях правового регулирования информационных правоотношений. Их применение обосновано необходимостью концептуальной оценки эффективности существующего правового регулирования в национальной и международной правовых системах.

Результаты: выявлены ключевые правовые и организационные проблемы обеспечения безопасности информационной инфраструктуры в условиях глобальных вызовов и угроз. Проанализированы принципы реализации основных типов угроз в киберсреде, включая трансграничные атаки и информационно-психологическое воздействие, что позволило определить их стратегическое значение для национальной безопасности. Обоснована необходимость развития инструментов правового регулирования сферы обеспечения кибербезопасности на национальном и наднациональном уровнях, включая унификацию подхода к регулированию трансграничных аспектов. На основе системного анализа и сравнительного моделирования выработаны предложения, связанные с формированием правовой базы, включая вопросы унификации юридических терминов и правовых категорий, взаимную интеграцию правовых, технических и организационных мер.

Кроме того, обосновано, что правовое обеспечение кибербезопасности является в условиях реализации национального проекта экономики данных и цифровой трансформации государства в Российской Федерации одним из приоритетных направлений реализации государственной политики и разработки международных юридически закрепленных стандартов. Указанные выводы свидетельствуют о том, что системный подход к правовому регулированию необходим для повышения устойчивости критической информационной инфраструктуры и укрепления международного сотрудничества в данной области. Практическая значимость работы заключается в формировании предложений для разработки адаптивных правовых механизмов, способных минимизировать риски в условиях появления новых киберугроз.

DOI: 10.24412/1994-1404-2025-1-50-56

¹ Баландин Артур Юрьевич, аспирант кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), г. Москва, Российская Федерация.
E-mail: 365inttech@gmail.com

Введение и постановка задачи

Высокая интенсивность развития цифровых технологий в сочетании с нарастающими геополитическими угрозами придают особую значимость вопросу обеспечения безопасности национальной информационной инфраструктуры. На государственном уровне поставлены стратегические задачи на достижение доминирования в таких высокотехнологичных областях, как искусственный интеллект и квантовые вычисления, потенциал которых способен радикально трансформировать киберпространство [1]. Повсеместное применение инновационных технологий ознаменовало зарождение так называемой цифровой цивилизации [2], а противостояние в ИКТ-среде становится одним из ключевых элементов современной геополитики, оказывающих существенное влияние как на развитие международных отношений, так и на проведение внутренней политики государств. При таких обстоятельствах представляется необходимым определить область правового регулирования вопросов безопасности информационной инфраструктуры, сформировать критерии для разработки и совершенствования соответствующих правовых механизмов, отвечающих вызовам сегодняшнего дня и тенденциям общественного развития.

Информационная безопасность и кибербезопасность: соотношение правовых категорий и норм правового регулирования

Использование информационных технологий в качестве инструмента распространения деструктивной информации [3, с. 286], оказывающей негативное информационно-психологическое воздействие на человеческое сознание, приводит к компрометации информационных систем и отдельных объектов информатизации, причинению ущерба объектам критической информационной инфраструктуры, репутационного ущерба органам публичной власти, имущественного вреда физическим и юридическим лицам. По мнению экспертов, отдельной категорией подобного рода субъектов являются привлеченные специализированными структурами недружественных государств проправительственные хакерские группы, специализирующиеся на совершении таргетированных продолжительных кибератак, характеризующихся высокой степенью технологичности и скрытности протекающих процессов [4].

Повсеместность применения инновационных сервисов и средств информационного обмена ставит в качестве приоритетной задачу обеспечения персональных данных и иной информации конфиденциального характера, обрабатываемой в информационных системах. Учитывая, что кибератаки могут быть компонентом гибридных войн, направленных на подрыв доверия к государственным институтам и дестабилизацию функционирования системы органов публичной власти,

кибербезопасность является важным направлением обеспечения информационной безопасности, в соответствии со Стратегией национальной безопасности, утвержденной Указом Президента Российской Федерации от 29.10.2024 № 920 в качестве стратегического национального приоритета государственной политики.

Несмотря на актуальность рассматриваемого вопроса, сегодня отмечается острый дефицит эффективных правовых норм, регулирующих деятельность субъектов информационных правовых отношений на государственном и международном уровнях, включая закрепленные на законодательном уровне и обязательные к исполнению меры обеспечения кибербезопасности. Возрастающая агрессивность интернет-пространства, недооценка значения необходимости реализации эффективных мер обеспечения индивидуальной и коллективной безопасности, а также отсутствие консолидированного правового противодействия делают как государственные структуры, так и бизнес, а также отдельных граждан максимально уязвимыми перед организованным целенаправленным вмешательством.

В связи с этим очевидна необходимость формирования информационно-правового пространства, реализующего применение информационных технологий на основании объективно сформулированных правовых норм, защищающих права граждан и общественные интересы, отвечающие требованиям обеспечения государственной безопасности в цифровой среде. Важен комплексный подход к решению поставленных проблем, связанных с формированием правовых инструментов обеспечения кибербезопасности как на международном, так и на национальном уровне, что требует интеграции правовых, технических, технологических и организационных мер для создания эффективных механизмов защиты информационных систем и данных.

Ключевым вопросом достижения консенсуса представляется разработка и унификация применяемых в национальных правовых системах юридических терминов. Киберугрозы все чаще носят трансграничный характер, что требует от субъектов международных правовых отношений в области применения информационных технологий конструктивного сотрудничества. Унификация межотраслевого понятийно-категориального аппарата видится отправной точкой для последующего успешного сотрудничества в сфере обеспечения кибербезопасности информационных систем на международном уровне и формирования перспективы применения международных правовых стандартов в данной области в целях обеспечения государственного суверенитета.

Достаточно острую дискуссию вызывает применение самого термина «кибербезопасность», до настоящего времени не нашедшего закрепления в российской правовой системе. Вместе с тем исследование позволяет выделить несколько подходов к формулированию данной юридической дефиниции.

Так, кибербезопасность рассматривается в контексте обеспечения защищенности от деструктивной

информации, распространяемой при помощи информационных технологий. При этом объектом деструктивного воздействия является человек, в сознании которого под влиянием транслируемой информации возникают когнитивные процессы, а результатом непосредственного воздействия — когнитивные процессы, порождаемые в человеческом сознании в результате восприятия вредоносного контента [5, с. 157].

В качестве альтернативы предлагается рассматривать ограничение сферы обеспечения кибербезопасности ИКТ-средой, при этом объектом деструктивного воздействия остается исключительно компьютерная инфраструктура, а недопустимые события в виде материального вреда либо репутационного ущерба, возникающие в реальном мире в результате подобного воздействия, выходят за рамки предметной области вопросов правового обеспечения кибербезопасности и подлежат рассмотрению в парадигме иных отраслей права [6]. Данный подход, на наш взгляд, достаточно радикален по отношению к первому и характеризуется строго определенными предметной областью, объектом правового регулирования и специфическими субъектами правовых отношений. При этом пресечение попыток распространения деструктивной информации в ИКТ-среде предлагается рассматривать в рамках необходимости обеспечения информационно-психологической безопасности с учетом специфики применяемых инструментов.

Вместе с тем, несомненно, кибербезопасность сегодня должна найти свое место в структуре российского информационного и, соответственно, публично-правового (государственного) регулирования, поскольку в приведенных позициях данное направление рассматривается как специализированный сегмент информационной безопасности в системе информационного права Российской Федерации.

Представляется, что юридическое закрепление данной категории будет способствовать достижению урегулирования спорных ситуаций, структурированию и совершенствованию действующих правовых норм и институционализации этих вопросов в системе информационного права и правового обеспечения информационной безопасности. Отсутствие общепринятых и юридически закрепленных на национальном и международном уровнях терминов в области обеспечения кибербезопасности является сегодня одной из ключевых проблем не только информационного права, но и смежных отраслей, а разработка новых юридических дефиниций необходима для развития доктрины информационного права.

Для обеспечения принципа преемственности вопрос унификации понятийно-категориального аппарата целесообразно рассматривать в общей концепции кодификации информационного законодательства, а необходимость разработки отдельного раздела, посвященного вопросам кибербезопасности, объясняется особой значимостью данного направления как приоритетного направления государственной безо-

пасности. Отсутствие единства юридических терминов и в связи с этим вынужденно субъективное толкование новых правовых категорий, а также потенциально возможные пробелы в соотношении новых юридических норм с уже существующими могут создать предпосылки для снижения уровня правовой определенности в развитии общественных отношений, что для сферы обеспечения национальной безопасности является недопустимым [7, с. 42].

Процесс кодификации нормативных правовых актов в определенной степени основывается как на переоценке существующих юридических норм, так и на формировании новых правовых конструкций, их объединении в единый структурированный документ. Особое значение процесс кодификации приобретает для развития информационного права, поскольку позволяет систематизировать и интегрировать в существующую нормативную базу российского законодательства нормативные правовые акты в области обеспечения кибербезопасности, имеющие комплексный характер и воплощающие межотраслевой подход, подлежащий применению при их формировании.

Упорядоченность правовых норм позволит сформировать единую систему, объективно оптимизирующую законотворческие и правоприменительные процессы, информационно-правовую деятельность. Таким образом, в рамках научной дискуссии о развитии национальной правовой системы внедрение кодификации видится не просто желательным, но и вполне закономерным шагом, отвечающим общественному вызову и продиктованном стремлением к повышению эффективности правового регулирования в области развития информационных технологий и обеспечения кибербезопасности национальной информационной инфраструктуры.

Не менее важной задачей правового обеспечения кибербезопасности является решение проблем юридической атрибуции. Установление субъектов, совершивших правонарушение или готовящихся к его совершению, включая подтверждение их принадлежности национальным юрисдикциям, представляется одним из наиболее эффективных правовых механизмов предотвращения и пресечения деструктивной хакерской деятельности. В контексте возможности эксплуатации уязвимостей как элементов тактик, применяемых при совершении кибератак, вместе с вопросами субъектной идентификации непосредственных исполнителей несанкционированного вмешательства в защищаемую инфраструктуру отмечается целесообразность репутационной оценки производителей программного обеспечения и программно-аппаратных платформ, ранее уличенных в производстве технических решений с большим количеством уязвимостей, содержащих скомпрометированные элементы, и не принимающих должных мер по их устранению.

Вопрос необходимости преодоления различий и восполнения правовых лагун в национальных правовых актах заслуживает особого внимания. Подходы

к регулированию рассматриваемых правовых отношений могут иметь существенные различия в зависимости от национальных приоритетов, что усложняет процесс достижения унифицированной международной правовой структуры. Следует согласиться, что при таких обстоятельствах, с учетом специфики и трансграничного характера киберпространства унификация правовых норм должна основываться на общности интересов субъектов международных правовых отношений, исключая приоритет интересов и технологическую гегемонию отдельных государств [8]. Ещё одной критически важной задачей является нахождение баланса между обеспечением безопасности и защитой прав человека. Правовое регулирование должно учитывать фундаментальные права и свободы, такие как право на неприкосновенность личной жизни и свободу слова, и при разрешении противоречий подход к применяемым ограничениям должен быть сбалансированным, а пределы вмешательства государства в частную жизнь — обоснованными. Это свидетельствует о сложности правового регулирования кибербезопасности и необходимости применения комплексного подхода к решению возникающих проблем.

В условиях современности стремительное развитие цифровых технологий требует от правового регулирования гибкости и адаптивности. Правовое регулирование закономерно не успевает за технологическими инновациями (наукоёмкими технологиями) и новыми формами киберугроз, что ведет к возникновению правовых лакун. В современном мире компьютерные технологии все чаще используются как инструмент геополитического влияния и даже агрессивных действий между государствами. В связи с этим следует признать справедливость позиции относительно того, что «правовые рамки, регулирующие вопросы кибероружия и стратегий предотвращения кибервойны, остаются недоработанными и требуют дальнейшего совершенствования» [9]. Это подчеркивает необходимость динамичного правового подхода, способного оперативно реагировать на изменяющуюся цифровую среду и обеспечивать надлежащую защиту от возникающих киберугроз и совершенствующихся тактик их реализации. Такие особенности подчеркивают необходимость комплексного и согласованного подхода к правовому регулированию кибербезопасности, а также постоянного диалога между государствами, технологическими компаниями и гражданским обществом.

Основные приоритеты и направления государственной политики в области информационной безопасности определены в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400, и Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646, в которых к числу основных угроз информационной безопасности в системе обеспечения национальной безопасности Российской Федерации относятся распространение ложной инфор-

мации и деструктивное информационно-техническое воздействие, нарушения защищенности информационно-коммуникационной инфраструктуры и утечки конфиденциальной информации и персональных данных. В связи с этим нормативные правовые акты, вопросы защищенности информации направлены в том числе и на защиту данных в цифровом виде. Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203, определяет информационную безопасность как одно из стратегических направлений для обеспечения национальной безопасности. В связи с этим правовые аспекты информационной безопасности являются приоритетными, поскольку правовые механизмы способны формировать устойчивую правовую основу для защиты от киберугроз и предотвращения их влияния на экономическую и политическую стабильность.

Как отмечают исследователи, в настоящее время правовое обеспечение цифровизации общества осуществляется через развитие базовых информационно-правовых норм, регулирующих ключевые аспекты цифровых отношений. Эти нормы включают принципы регулирования цифровых взаимодействий, режим управления цифровыми данными и другими объектами цифровой среды, определение правового статуса субъектов, функционирующих в цифровой среде, а также другие правовые элементы, отражающие сущность цифровой формы; нормы обладают универсальным характером и могут быть интегрированы в систему права в целом. Кроме того, правовое обеспечение цифровизации связано с появлением отраслевых цифровых норм. Указанные нормы разрабатываются и принимаются в различных отраслях права и отражают специфику реализации цифровых процессов в разных сферах общественных отношений, регулируемых соответствующими отраслями права, что позволяет учитывать уникальные особенности каждой сферы и эффективнее адаптировать правовое регулирование к потребностям цифровой эпохи [10].

В качестве предмета правового обеспечения информационной безопасности научную обоснованность получило представление о нем как об области правового воздействия на поведение людей в целях недопущения проявления угроз объектам национальных интересов в информационной сфере или минимизация негативных последствий проявления этих угроз [11]. Иная формулировка раскрывает данную дефиницию через влияние информации и информационной инфраструктуры на обеспечение национальных интересов [12].

В российской юридической науке предмет правового обеспечения информационной безопасности определен как *область правового воздействия на поведение людей в целях недопущения проявления угроз объектам национальных интересов в информационной сфере или минимизации негативных последствий проявления этих угроз* [11].

Требование защиты информационных и коммуникационных технологий приводит к необходимости

формирования специализированного понятия. Принимая во внимание специфику развития общественных отношений, темпы развития информационных технологий, а также общественный запрос на трансформацию информационных правовых отношений, представляется обоснованным определить предметную область правового регулирования кибербезопасности как **область нормативного правового воздействия, направленного на исключение вредоносного воздействия на информационно-технические ресурсы, реализуемого при помощи программно-аппаратных средств в информационно-коммуникационных системах либо посредством таковых, и/или ликвидации последствий проявления этих угроз.**

Вывод

На современном этапе информационное законодательство, находясь под влиянием цифровой

трансформации, выступает в качестве формирующей правовой системы и комплексной правовой отрасли, требующей современных теоретических подходов к урегулированию законодательства в России на основе научного анализа [13—16]. Создание и закрепление новых терминов в юридическом дискурсе позволит не только повысить точность правового регулирования, но и обеспечить соответствие норм права требованиям современного информационного общества. В этой связи для достижения высокоэффективного правового обеспечения безопасности национальной информационной инфраструктуры Российской Федерации необходимо определение кибербезопасности как одного из приоритетных векторов информационной безопасности сегодня в системе информационного права с четко определенной предметной областью, объектом правового регулирования и характеристиками субъектного состава.

Литература

1. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Развитие доктрины российского информационного права в условиях перехода к экономике данных // Государство и право. 2023. № 9. С. 158—171.
2. Троян Н.А. Современные подходы к эффективному правовому регулированию в целях обеспечения цифрового суверенитета России // Мониторинг правоприменения. 2024. № 1. С. 63—72.
3. Смирнов А.А. Формирование системы правового обеспечения информационно психологической безопасности в Российской Федерации : дисс. ... д-ра юрид. наук. М., 2022. С. 286.
4. Шарикив П.А. Военные аспекты кибербезопасности в контексте специальной военной операции ФПР на территории Украины // Аналитические записки Института Европы РАН. 2022. № 2. С. 5—12.
5. Саликов М.С., Несмеянова С.Э., Колобаева Н.Е., Кузнецова С.С., Мочалов А.Н. Государственное регулирование Интернета и права человека / Под ред. д-ра юрид. наук, профессора М.С. Саликова. Екатеринбург : изд-во УМЦ УПИ, 2022. 220 с.
6. Козлова Н.Ш., Довгаль В.А. Кибербезопасность и информационная безопасность: сходства и отличия // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2021. № 3 (286). С. 88—97.
7. Полякова Т.А. Развитие понятийного аппарата в области обеспечения информационной безопасности в Российской Федерации // Понятийный аппарат в информационном праве: сборник научных работ / ИГП РАН, отв. ред. И.Л. Бачило, Т.А. Полякова, В.Б. Наумов. М. : Канон-Плюс, 2017. 264 с.
8. Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16. № 3. С. 7—33.
9. Макаров В.А., Коротков В.Г. Подходы к обеспечению безопасности энергетических систем в условиях возможного применения кибероружия // Вестник НИЦ ВА РВСН. 2020. № 1. С. 47—55.
10. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166—179.
11. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России: дисс. ... д-ра юрид. наук. М., 2008. С. 111.
12. Стрельцов А.А. Предмет правового обеспечения информационной безопасности // Российский юридический журнал. 2003. № 2 (38). С. 24—35.
13. Полякова Т.А., Минбалеев А.В., Наумов В.Б. К вопросу о кодификации информационного законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81—91.
14. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 58—74. DOI: 10.21681/2311-3456-2023-1-58-74.
15. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23. DOI: 10.21681/2311-3456-2019-3-18-23.

SPECIFIC FEATURES OF LEGAL REGULATION OF CYBERSECURITY IN THE TIMES OF GLOBAL CONFRONTATION

Artur Balandin, Ph.D. student at the Department of Information Technology Law and Digital Technologies of the Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation.
E-mail: 365inttech@gmail.com

Keywords: cyber threats, information security, cyberspace, national security, critical information infrastructure, digital technologies, legal acts, hacker groups, ICT environment.

Abstract

The paper examines the place of legal provision of cybersecurity in the national security system of the Russian Federation. In the study, the author proposed a systematic approach based on the formulation of clear legal definitions aimed at the development of international and national legal norms, as well as the integration of legal, technical and organizational measures in order to form a single integrated approach. The article focuses on the need to maintain a balance between ensuring security and protecting human rights in the ICT environment, and the formation of legal mechanisms that meet public demand. The proposals contained in the article can be used to improve the effectiveness of legal regulation that can adapt to the challenges of the digital age and is necessary for the development of international cooperation in the field of information security, including cybersecurity.

Purpose of the study: identifying key problems of legal provision of information security, including cybersecurity issues.

Methods used in the study: system analysis and comparative modeling, which allows to ensure the accuracy of legal criteria used in models of legal regulation of information legal relations. Their application is justified by the need for a conceptual assessment of the effectiveness of existing legal regulation in national and international legal systems.

Study findings: within the framework of the conducted research, the key legal and organizational problems of ensuring the security of information infrastructure in the context of global challenges and threats have been identified. The principles of the implementation of the main types of threats in the cyber environment, including cross-border attacks and information and psychological impact, have been analyzed, which made it possible to determine their strategic importance for national security. As a result of the study, the need for the development of legal regulation tools for cybersecurity at the national and supranational levels, including the unification of the approach to regulating cross-border aspects, is substantiated. Based on system analysis and comparative modeling, proposals related to the formation of a legal framework have been developed, including issues of unification of legal terms and legal categories, mutual integration of legal, technical and organizational measures.

In addition, the study substantiates that the legal provision of cybersecurity is one of the priorities for the implementation of state policy and the development of international legally established standards in the context of the implementation of the national project of data economy and digital transformation of the state in the Russian Federation. These conclusions indicate that a systematic approach to legal regulation is necessary to increase the stability of critical information infrastructure and strengthen international cooperation in this area. The practical significance of the work lies in the formation of proposals for the development of adaptive legal mechanisms that can minimize risks in the face of new cyber threats.

References

1. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Razvitie doktriny rossiiskogo informatsionnogo prava v usloviakh perekhoda k ekonomike dannykh. Gosudarstvo i pravo. 2023. No. 9. Pp. 158–171.
2. Troian N.A. Sovremennye podkhody k effektivnomu pravovomu regulirovaniu v tselakh obespecheniya tsifrovogo suvereniteta Rossii. Monitoring pravoprimeneniia. 2024. No. 1. Pp. 63–72.
3. Smirnov A.A. Formirovanie sistemy pravovogo obespecheniya informatsionno psikhologicheskoi bezopasnosti v Rossiiskoi Federatsii : diss. ... d-ra iurid. nauk. M., 2022. P. 286.

4. Sharikov P.A. Voennye aspekty kiberbezopasnosti v kontekste spetsial'noi voennoi operatsii FPR na territorii Ukrainy. Analiticheskie zapiski Instituta Evropy RAN. 2022. No. 2. Pp. 5–12.
5. Salikov M.S., Nesmeianova S.E., Kolobaeva N.E., Kuznetsova S.S., Mochalov A.N. Gosudarstvennoe regulirovanie Interneta i prava cheloveka. Pod red. d-ra iurid. nauk, professora M.S. Salikova. Ekaterinburg : izd-vo UMTs UPI, 2022. 220 pp.
6. Kozlova N.Sh., Dovgal' V.A. Kiberbezopasnost' i informatsionnaia bezopasnost': skhodstva i otlichii. Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya: Estestvenno-matematicheskie i tekhnicheskie nauki. 2021. No. 3 (286). Pp. 88–97.
7. Poliakova T.A. Razvitie poniatiinogo apparata v oblasti obespecheniia informatsionnoi bezopasnosti v Rossiiskoi Federatsii. Poniatiinyi apparat v informatsionnom prave: sbornik nauchnykh rabot. IGP RAN, otv. red. I.L. Bachilo, T.A. Poliakova, V.B. Naumov. M. : Kanon-Plus, 2017. 264 pp.
8. Degterev D.A., Ramich M.S., Piskunov D.A. Podkhody SSHA i KNR k global'nomu upravleniiu kiberprostranstvom: "novaia bipoliarnost'" v "setevom obshchestve". Vestnik mezhdunarodnykh organizatsii: obrazovanie, nauka, novaia ekonomika. 2021. T. 16. No. 3. Pp. 7–33.
9. Makarov V.A., Korotkov V.G. Podkhody k obespecheniiu bezopasnosti energeticheskikh sistem v usloviakh vozmozhnogo primeneniia kiberoruzhiia. Vestnik NITs VA RVSN. 2020. No. 1. Pp. 47–55.
10. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Transformatsiia nauki informatsionnogo prava i informatsionnogo zakonodatel'stva: novyi etap v usloviakh nauchno-tekhnologicheskogo razvitiia Rossii. Gosudarstvo i pravo. 2024. No. 9. Pp. 166–179.
11. Poliakova T.A. Pravovoe obespechenie informatsionnoi bezopasnosti pri postroenii informatsionnogo obshchestva v Rossii: diss. ... d-ra iurid. nauk. M., 2008. P. 111.
12. Strel'tsov A.A. Predmet pravovogo obespecheniia informatsionnoi bezopasnosti. Rossiiskii iuridicheskii zhurnal. 2003. No. 2 (38). Pp. 24–35.
13. Poliakova T.A., Minbaleev A.V., Naumov V.B. K voprosu o kodifikatsii informatsionnogo zakonodatel'stva v usloviakh tsifrovoi transformatsii. Gosudarstvo i pravo. 2024. No. 1. Pp. 81–91.
14. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberpresupnosti. Voprosy kiberbezopasnosti. 2023. No. 1 (53). Pp. 58–74. DOI: 10.21681/2311-3456-2023-1-58-74 .
15. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiia kiberbezopasnosti v usloviakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti. 2019. No. 3 (31). Pp. 18–23. DOI: 10.21681/2311-3456-2019-3-18-23 .
16. Kartskhiia A.A., Makarenko G.I. Pravovye problemy iskusstvennogo intellekta v Rossii. Pravovaia informatika. 2024. No. 1. Pp. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19 .

ОТ ПОРОКОВ ДИСКРИМИНАЦИИ К РАЗВИТИЮ ОСНОВ НЕДИСКРИМИНАЦИИ

Оролов В.А.¹

Ключевые слова: принцип, права, свободы, защита, гарантии, неравенство, международные договоры.

Аннотация

Цель исследования: выявить социально-правовое и международно-правовое значение принципа недискриминации.

Методы исследования: при подготовке статьи использовались аналитический метод, историко-правовой и диалектический метод познания, позволяющие раскрыть особенности, сущность, внутренние связи отношений, возникающих при нарушении норм права (дискриминации), а также общественные отношения, основанные на нормах международных договоров о недискриминации. Выводы и предложения основаны на логическом, аналитическом, сравнительно-правовом, диалектическом, философско-правовом и иных методах.

Результаты: представлено действие принципа недискриминации в российском праве, в том числе в актах Конституционного суда РФ и Верховного суда РФ. Рассматриваются вопросы (истoki) возникновения дискриминации. Подчеркивается, что дискриминация вытекает из понятия неравенство. Там, где права и свободы человека не защищены должным образом, возникает опасность дискриминации личности. В ходе исследования установлено, что акты судов высших инстанций — Конституционного суда Российской Федерации, Верховного суда Российской Федерации — являются важным инструментом в борьбе с дискриминацией и способствуют формированию правоприменительной практики, направленной на защиту прав человека.

Научная новизна: получены знания о сущности, содержании понятий «дискриминация» и «недискриминация», их соотношении, об исторических истоках формирования данных понятий, пороке термина — «дискриминация» и значении принципа — «недискриминация» в международно-правовых актах (договорах) и национальном законодательстве. Исследование позволило сделать выводы о том, что принцип недискриминации — это основополагающий элемент правовой системы, который направлен на защиту прав и свобод человека. Его суть заключается в равенстве всех людей, независимо от их расы, пола, возраста, религии или других характеристик. Ратифицируя международные договоры, правительства принимают на себя обязательства обеспечить равные права и свободы гражданам и гарантируют их реализацию.

DOI: 10.24412/1994-1404-2025-1-57-62

Введение и постановка задачи

Дискриминация — негативное явление, которое на протяжении веков оказывало разрушительное влияние на общество, создавая барьеры между людьми. Дискриминация проявляется в сознательном, волевом нарушении прав человека, когда отдельные группы людей подвергаются неравному обращению на основании их расы, пола, возраста, религии, сексуальной ориентации или других признаков [1].

Дискриминация может принимать различные формы: от открытого насилия и преследования до более тонких проявлений, таких как предвзятость в отношении отдельного человека или определённых групп, народов. Дискриминация не только создает ограничения в реализации человеком своих прав и свобод, напри-

мер, в сфере труда, но порой и влияет на принятие неблагоприятных политических решений, подрывает основы социальной справедливости и гармонии в обществе [2].

В научной литературе дискриминацию зачастую связывают с отсутствием равноправия и/или равенства [8]. Весьма убедительным выглядит тезис видного ученого конституционалиста С.А. Авакьяна, который пишет: государство стремится обеспечить равные права и свободы своим гражданам. Но равные права не следует отождествлять с физическим равенством людей, каждый человек индивидуален и способности у всех разные. В основе международных отношений лежит принцип равноправия [5].

¹ **Оролов Вячеслав Александрович**, кандидат юридических наук, федеральный судья Арбитражного суда г. Москвы, Российская Федерация.

E-mail: glotozop2@yandex.ru

Его соратник, известный российский теоретик-государствовед В.Е. Чиркин подчеркивал, что дискриминация может иметь место только в тех условиях, когда она легализована, то есть когда законодательно закреплено неравенство прав граждан [6]. Это утверждение находит яркое подтверждение в истории человечества, особенно в контексте довоенной Германии. В тот период власти объявили о превосходстве арийской расы, что стало основой для систематического притеснения и дискриминации других групп населения. Законодательные акты, направленные на ограничение прав евреев и других меньшинств, создали правовую основу для их изоляции и преследования. В результате этого легитимизованного неравенства началась волна насилия, которая в итоге привела к массовому истреблению миллионов людей [6]. Таким образом, примеры из истории показывают, как закон может быть использован как инструмент для оправдания дискриминации и нарушения прав человека. Это подчеркивает актуальность защиты прав и свобод граждан на уровне законодательства, чтобы предотвратить повторение трагических событий прошлого. Закон должен служить гарантией равных прав, возможностей и справедливости, а не инструментом угнетения человека человеком и притеснения его прав.

В современных условиях международной нестабильности и нарушения международных норм вопросы равноправия и вытекающего из него принципа недискриминации становятся все более актуальными.

Исторические корни дискриминации

Важно понимать, что дискриминация — это системная проблема, к сожалению, имеющая глубоко уходящие в историю развития человеческой цивилизации корни. Обзор юридических источников античного мира свидетельствует о том, что, например, в Кодексе Хаммурапи (1750 г. до н.э.) было узаконено неравенство между полноправными гражданами Месопотамии, вольнонаемным населением (не гражданами) и рабами^{2,3}. Аналогично закреплялось неравенство и в Законах XII таблиц⁴. Да и первый свод законов Киевской Руси, Русская Правда, без сомнения свидетельствует об имевшемся социальном неравенстве: бесправии несвободной челяди и холопов. В Русской

Правде и раздел имеется: «Разделение Членов Общества на Повелевающих и Повинующихся»⁵.

И Судебник Ивана IV (Грозного) (1550 г.), и указы других великих реформаторов Руси — Алексея Михайловича (1629—1676), Петра Алексеевича (Петра I) и более либеральных царей — Екатерины II (1729-1796) и Александра II (1818—1881) устанавливали неравные права или прямо закрепляли неравенство между господами и их подданными — крестьянами. И даже упразднение крепостного права не освободило полностью крестьян от зависимости. Они обязаны были уплачивать барщину на землю, на которой они проживали^{6,7,8}.

До середины XIX века практически во всем мире господствовало неравенство. Либеральные течения в Европе начали широко развиваться лишь в конце XVIII — начале XIX века. Великая французская революция впервые подняла проблему неравенства граждан, но, к сожалению, не добилась поставленных задач. Позитивистская концепция, согласно которой права и свободы даруются человеку государством, а государство определяет их объем и содержание, одержали тогда верх. Вместе с тем в европейских странах начали формироваться взгляды, направленные на равенство и свободы. Лишь Февральская, а затем Октябрьская революция в России перевернули данную ситуацию.

Защита прав и свобод человека на международном уровне. Введение принципа недискриминации

После Второй мировой войны мировое сообщество столкнулось с необходимостью переосмысления основ человеческого существования и защиты прав личности. Ужасы войны, геноцид и массовые нарушения прав человека стали катализаторами для создания международных механизмов, направленных на предотвращение подобных трагедий в будущем. В этом контексте в 1948 году была принята Всеобщая декларация прав человека⁹, которая стала знаковым событием в истории международного права.

Декларация закрепила универсальные права и свободы, принадлежащие каждому человеку, независимо от его расы, пола, национальности, религии или других признаков. Принцип недискриминации был провозглашен как основополагающее начало, подчеркивающее, что все люди имеют равные права и должны пользоваться ими без каких-либо исключений. Этот документ

² Социальное неравенство в Законах Хаммурапи. URL: https://vuzlit.com/1398981/sotsialnoe_neravenstvo_zakonah_hammurapi_polozhenie_rabov

³ Постановление Конституционного Суда РФ от 16 июня 2006 г. № 7-П «По делу о проверке конституционности ряда положений статей 48, 51, 52, 54, 58 и 59 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» в связи с запросом Государственной Думы Астраханской области» // СПС «КонсультантПлюс».

⁴ Стейнберг С. Двенадцать таблиц и их происхождение: дебаты XVIII века (пер. с англ.) // Журнал истории идей. 1982. Т. 43. № 3. С. 379—396.

⁵ Пестель П.И. Русская правда или Заповедная Государственная Грамота Великого Народа Российского, URL: http://vivovoco.rsl.ru/vv/law/vv_pes_w.htm

⁶ Лаппо-Данилевский А.С. Очерк внутренней политики Екатерины II // СПб. : типогр. Стасюлевича, 1898. С. 61.

⁷ Моряков В.И. Екатерина II — просветитель или консерватор? // Вестник Московского университета. Сер. История. 2010. № 3. С. 9—26.

⁸ Отмена крепостного права (Манифест 1861 года). Владимирская областная научная библиотека. URL: <https://library.vladimir.ru/news/otmena-krepostnogo-prava-manifest-1861-goda.html>

⁹ Всеобщая декларация прав человека. Принята Генеральной Ассамблеей ООН 10.12.1948 // СПС «КонсультантПлюс».

стал основой для дальнейшего развития международного права в области прав человека и вдохновил множество стран на принятие собственных законов и конституций, направленных на защиту прав граждан.

Всеобщая декларация прав человека не только обозначила стандарты, к которым должны стремиться государства, но и стала символом надежды для миллионов людей, стремящихся к свободе и справедливости. Она подтолкнула к созданию различных международных и региональных механизмов защиты прав человека, таких как Международный пакт о гражданских и политических правах и Европейская конвенция о защите прав человека^{10,11}. Таким образом, Декларация стала важным шагом на пути к формированию глобального правопорядка, основанного на уважении к достоинству каждого человека.

Устав Организации Объединенных Наций¹², принятый в 1945 году, стал важнейшим документом, который заложил основы международного права и сотрудничества между государствами. В своей изначальной сути он утверждает принципы равноправия и уважения к правам человека как краеугольные камни всех правоотношений между людьми и народами. Эти принципы не только формируют основу для мирного сосуществования, но и служат гарантией справедливости и равенства в международных отношениях.

Одним из ключевых положений устава является статья 55, в которой подчеркивается, что стабильность и благополучие между нациями напрямую зависят от признания принципа равноправия и самоопределения народов. Это утверждение акцентирует внимание на том, что каждое государство несет ответственность за обеспечение уважения и соблюдения прав человека и основных свобод для всех своих граждан. Важно отметить, что это должно происходить без каких-либо различий по признакам происхождения, расы, пола, языка, религии и другим характеристикам.

Отдельные исследователи пишут о том, что Устав ООН не только провозглашает идеалы равенства и справедливости, но и обязывает государства активно работать над их реализацией. Конвенция о защите прав человека и основных свобод, известная также как Европейская конвенция по правам человека — ЕКПЧ¹³, была принята в 1950 году Советом Европы и стала основополагающим актом в области защиты прав человека в Европе. Этот документ был разработан в ответ на ужасы Второй мировой войны и стремление предотвратить повторение подобных трагедий в будущем. Цель Конвенции — установлении гарантий неотъемлемых прав и свобод каждого человека, независимо от его

расы, пола, языка, религии или любых других признаков. Европейская конвенция по правам человека не только закрепляет основные права и свободы, но и создает правовую основу для их защиты, способствуя укреплению демократии и верховенства права на континенте¹⁴.

В 1963 году была принята Международная конвенция ООН о ликвидации всех форм расовой дискриминации¹⁵, которая стала важным шагом на пути к обеспечению равенства и прав человека для всех людей, независимо от их расы или этнической принадлежности. Эта конвенция основывается на принципах, закрепленных в Уставе ООН и Всеобщей декларации прав человека, которые провозглашают равноправие и свободы как неотъемлемые права каждого человека.

С правовых позиций конвенция представляет собой важный документ, который не только осуждает расовую дискриминацию, но и определяет ее понятие. В соответствии с текстом конвенции дискриминация определяется как любое различие, исключение, ограничение или предпочтение, основанное на расе, цвете кожи, национальном или этническом происхождении, которое имеет целью или следствием уничтожение или ограничение признания, пользования или осуществление прав и свобод человека на равной основе.

Таким образом, Международная конвенция о ликвидации всех форм расовой дискриминации не только закрепляет правовые нормы, направленные на защиту прав человека, но и служит основой для борьбы с предрассудками и стереотипами, которые приводят к дискриминации. Принятие этой конвенции стало важным шагом в международном праве, подчеркивающим необходимость уважения к многообразию и достоинству каждого человека. Уважение прав человека становится неотъемлемой частью международного порядка, способствующего миру и безопасности. В условиях глобализации и межкультурного взаимодействия принципы равноправия и справедливости приобретают особую значимость, подчеркивая необходимость сотрудничества и взаимопонимания между народами для достижения мира и общего блага.

Реализация международных норм в актах Конституционного и Верховного судов Российской Федерации

Государства, подписавшие и ратифицировавшие международные договоры, в том числе по правам человека и недискриминации личности, берут на себя

¹⁰ Международный пакт о гражданских и политических правах. Принят резолюцией 2200 А Генеральной Ассамблеи ООН 16 декабря 1966 г.

¹¹ Конвенция о защите прав человека и основных свобод (заключена в г. Риме 04.11.1950, с изм. от 24.06.2013) // СПС «Консультант-Плюс».

¹² Устав ООН. URL: <https://www.un.org/ru/about-us/un-charter/full-text>

¹³ Европейская конвенция по правам человека // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>

¹⁴ Российская Федерация 05.09.2022 перестала быть стороной данного договора. Информация Европейского Суда по правам человека от 16 сентября 2022 г. «Российская Федерация перестает быть участником Европейской конвенции о правах человека» // ИПП «Гарант.ру».

¹⁵ Международная конвенция ООН о ликвидации всех форм расовой дискриминации. URL: <https://www.humanium.org/en/wp-content/uploads/2013/10/International-Convention-on-the-Elimination-of-All-Forms-of-Racial-Discrimination1.pdf>

обязательства не только уважать и защищать права, закрепленные в этих актах, но и активно создавать условия для их реализации на своей территории. Это подразумевает необходимость принятия соответствующего национального законодательства, которое должно соответствовать международным стандартам и обеспечивать защиту прав человека.

Кроме того, государства обязаны разрабатывать и внедрять эффективные механизмы защиты прав человека на национальном уровне. Это может включать создание специализированных органов, таких как омбудсмены или комиссии по правам человека, а также обеспечение доступа к правосудию для всех граждан. Важным аспектом является также обучение государственных служащих и правоохранительных органов принципам и нормам прав человека, что способствует более эффективному соблюдению и защите этих прав [7, 8].

Таким образом, выполнение международных обязательств требует от государств не только декларативного подхода, но и реальных действий, направленных на создание правовой и институциональной базы, способствующей защите прав человека и обеспечению их реализации в повседневной жизни граждан. Это подтверждается нормами российской Конституции, например, статьями 6, 15 и другими¹⁶.

В Российской Федерации решающая роль в защите прав граждан и обеспечении соблюдения конституционных норм отводится правосудию, которое выступает гарантом справедливости и законности в обществе. Конституционный Суд Российской Федерации, рассматривая дела, связанные с нарушением прав и свобод, принимает решения, которые не только разрешают конкретные споры, но и формируют правоприменительную практику, способствуя развитию законодательства о недискриминации.

В своих актах Конституционный Суд акцентирует внимание на принципах равенства и недопустимости дискриминации, подчеркивая, что каждый гражданин имеет право на защиту своих прав, вне зависимости от расы, пола, национальности, языка, происхождения, имущественного и должностного положения, а также других обстоятельств.

Эти принципы становятся основой для формирования правовой среды, в которой каждый человек может рассчитывать на справедливое отношение со стороны государства и общества^{17,18}.

¹⁶ Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 04.07.2020.

¹⁷ Постановление Конституционного Суда РФ от 16 июня 2006 г. № 7-П «По делу о проверке конституционности ряда положений статей 48, 51, 52, 54, 58 и 59 Федерального закона «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» в связи с запросом Государственной Думы Астраханской области» // СПС «КонсультантПлюс».

¹⁸ Постановление Конституционного Суда РФ от 6 июня 2017 г. № 15-П «По делу о проверке конституционности пункта 1 части тре-

Позиция Конституционного Суда служит важным ориентиром для нижестоящих судов и органов власти, побуждая их учитывать эти принципы в своей деятельности. Таким образом, решения Конституционного Суда не только способствуют защите индивидуальных прав, но и формируют правосознание общества, способствуя созданию более справедливой и равноправной правовой системы. Важно, чтобы все ветви власти и граждане осознавали значимость этих норм и стремились к их соблюдению, что в конечном итоге будет способствовать укреплению демократии и правового государства в России.

Формирование правоприменительной практики в области недискриминации в России во многом зависит от решений Верховного Суда РФ. Эти акты играют ключевую роль в определении и уточнении норм законодательства, касающихся различных аспектов жизни общества, включая трудовые отношения, доступ к образованию и медицинским услугам, а также защиту прав уязвимых групп населения.

Решения Верховного Суда не только фиксируют факты дискриминации, но и служат основой для разработки эффективных механизмов защиты прав граждан. Например, в сфере трудовых отношений суд может рассмотреть случаи дискриминации по признакам пола, возраста или инвалидности, что способствует созданию более справедливых условий труда. Важно, чтобы такие решения не ограничивались лишь констатацией нарушений, но и устанавливали четкие рекомендации для работодателей и государственных органов, направленные на предотвращение дискриминации¹⁹.

В области образования и медицинских услуг решения Верховного Суда могут способствовать улучшению доступа к этим важным сферам для всех граждан, независимо от их социального статуса, этнической принадлежности или других характеристик^{20,21,22}. Судебные акты могут устанавливать обязательства для образовательных учреждений и медицинских организаций по обеспечению равного доступа и качественного обслуживания для всех.

Кроме того, Верховный Суд может играть важную роль в защите прав уязвимых групп населения, таких как люди с инвалидностью, представители националь-

тей статьи 31 Уголовно-процессуального кодекса Российской Федерации в связи с запросом Ленинградского областного суда» // СПС «КонсультантПлюс».

¹⁹ Постановление Пленума Верховного Суда РФ от 17 марта 2004 г. № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации» // СПС «КонсультантПлюс».

²⁰ Обзор практики межгосударственных органов по защите прав и основных свобод человека № 6 (2024) (подготовлен Верховным Судом РФ). URL: <http://vsrf.ru>, 28.12.2024.

²¹ Обзор практики Верховного суда Российской Федерации по делам о реализации Федерального закона «Об образовании в Российской Федерации» и принятых в соответствии с ним подзаконных нормативных актах». URL: <https://lawbulletin.mgpru.ru/wp-content/uploads/sites/4/2021/08/740.pdf>

²² Обзор судебной практики Верховного Суда Российской Федерации № 2 (2020)» (утв. Президиумом Верховного Суда РФ 22.07.2020) // СПС «КонсультантПлюс».

ных меньшинств и другие категории, подверженные дискриминации²³. Установление прецедентов в этой области способствует формированию более инклюзивного общества, где права каждого гражданина защищены и уважаемы.

Вышеизложенное позволяет сделать заключение о том, что решения Верховного Суда РФ являются важным инструментом в борьбе с дискриминацией и способствуют формированию правоприменительной практики, направленной на защиту прав человека.

Несмотря на выход Российской Федерации из ряда европейских соглашений и прекращение членства в Совете Европы, законодательство страны продолжает содержать нормы, направленные на запрещение дискриминации. Это обстоятельство подчеркивает, что даже в условиях изменяющейся международной политической обстановки внутренние правовые механизмы могут оставаться важным инструментом для защиты прав граждан. Принцип недискриминации не теряет своей актуальности, даже когда международные обязательства становятся менее значимыми. Российское законодательство, включая Конституцию и различные федеральные законы, продолжает гарантировать права и свободы граждан, обеспечивая защиту граждан от дискриминации.

Таким образом, внутренние правовые механизмы могут служить основой для защиты прав человека, даже если международные институты и соглашения теряют свой авторитет. Ратифицируя международные договоры, правительства принимают на себя обязательства обеспечить равные права и свободы гражданам и гарантируют их реализацию. Это способствует

укреплению правового государства и защите прав личности внутри страны.

Несмотря на изменения в международной политике, внутренние правовые нормы остаются важным инструментом для обеспечения справедливости и защиты прав граждан в Российской Федерации.

Вывод

Из изложенного следует, что принцип недискриминации — это основополагающий элемент правовой системы, который направлен на защиту прав и свобод человека. Его суть заключается в обеспечении гарантий на равные права и возможности для всех людей, независимо от их расы, пола, возраста, религии или других характеристик. Этот принцип направлен не только на защиту прав отдельных индивидов, но и способствует созданию более справедливого и гармоничного общества.

В условиях, когда пороки дискриминации все еще имеют место в различных уголках мира, необходимо выявить социально-правовой потенциал принципа недискриминации. Для этого требуется комплексный подход, включающий образование, просвещение и активное участие общества в борьбе с дискриминацией. Важно не только осуждать проявления дискриминации, но и активно работать над созданием инклюзивной среды, где каждый сможет реализовать свои возможности. Это требует усилий со стороны российского правительства, общественных организаций и каждого из неравнодушных граждан.

В итоге принцип недискриминации — это не просто юридическая норма, а мощный международно-правовой инструмент, способный изменить общественные отношения в каждом государстве и повлиять на укрепление международного климата. Игнорирование принципа недискриминации подрывает основы демократических процессов в обществе, где каждый человек имеет право на уважение и равные права.

²³ Обзор практики рассмотрения судами дел по спорам, связанным с реализацией мер социальной поддержки отдельных категорий граждан. Утв. Президиумом Верховного Суда РФ 17 июня 2020 г. // СПС «КонсультантПлюс».

Литература

1. Кобзарь-Фролова М.Н. Запрет дискриминации в международном и национальном праве (историографические и юридические аспекты) // Право и управление. 2024. № 8. С. 20—27.
2. Гаврюшкин С.Н. Проблемы дискриминации в сфере трудовых отношений // Современное право. 2020. № 1. С. 60—65.
3. Шуралева С.В. Регулирование труда уязвимых групп работников: вызовы и пути их преодоления в эру искусственного интеллекта // Трудовое право в России и за рубежом. 2024. № 1. С. 44—47.
4. Микрина В.Г. Международно-правовые механизмы защиты трудовых прав наиболее уязвимых групп населения : дис. ... канд. юрид. наук. М., 2018. С. 12—13, 16.
5. Авакьян С.А. Конституционное право России : учебный курс : в 2-х т. Т. 1. М. : Норма, 2021. С. 182—187.
6. Чиркин В.Е. Конституционное право зарубежных стран : учебник. 9-е изд., перераб. и доп. М. : Норма : Инфра-М, 2020. С. 532.
7. Гришковец А.А., Кобзарь-Фролова М.Н., Сморгочкова Л.Н. Этнический анклав: юридические проблемы новой угрозы национальной безопасности // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2023. № 11. С. 147—152.
8. Виноградова Е.В., Кобзарь-Фролова М.Н., Сморгочкова Л.Н. К вопросу о правовом регулировании общественных отношений в сфере противодействия формированию этнических анклавов // Правовая политика и правовая жизнь. 2024. № 1. С. 161—174.

FROM THE VICES OF DISCRIMINATION TO DEVELOPING THE FOUNDATIONS OF NON-DISCRIMINATION

Viacheslav Frolov, Ph.D. (Law), Federal Judge at the Moscow Commercial Court, Moscow, Russian Federation.

E-mail: glotozop2@yandex.ru

Keywords: principle, rights, freedoms, protection, guarantees, inequality, international treaties.

Abstract

Purpose of the study: to identify the socio-legal and international legal significance of the principle of non-discrimination.

Methods used in the study: when preparing the article, the analytical method, historical-legal and dialectical method of cognition were used, allowing to reveal the features, essence, internal connections of relations arising from violation of legal norms, as well as social relations based on the norms of international treaties on non-discrimination. Conclusions and proposals are based on logical, analytical, comparative legal, dialectical, philosophical-legal and other methods.

Study findings: the effect of the principle of non-discrimination in Russian law is presented, including in the acts of the Constitutional Court of the Russian Federation and the Supreme Court of the Russian Federation. The issues (sources) of the emergence of discrimination are considered. It is emphasized that discrimination follows from the concept of inequality. Where human rights and freedoms are not properly protected, there is a risk of discrimination against individuals. The study found that acts of higher courts, i.e. the Constitutional Court of the Russian Federation, the Supreme Court of the Russian Federation, are an important tool in the fight against discrimination and contribute to the formation of law enforcement practice aimed at protecting human rights.

Research novelty: knowledge was obtained about the essence, content of the concepts of “discrimination” and “non-discrimination”, their relationship, the historical origins of the formation of these concepts, the flaw in the term “discrimination” and the meaning of the principle of “non-discrimination” in international legal acts (treaties) and national legislation. The study allowed us to conclude that the principle of non-discrimination is a fundamental element of the legal system, which is aimed at protecting human rights and freedoms. Its essence lies in the equality of all people, regardless of their race, gender, age, religion or other characteristics. By ratifying international treaties, governments undertake to ensure equal rights and freedoms for citizens and guarantee their implementation.

References

1. Kobzar'-Frolova M.N. Zapret diskriminatsii v mezhdunarodnom i natsional'nom prave (istoriograficheskie i iuridicheskie aspekty). Pravo i upravlenie. 2024. No. 8. Pp. 20–27.
2. Gavriushkin S.N. Problemy diskriminatsii v sfere trudovykh otnoshenii. Sovremennoe pravo. 2020. No. 1. Pp. 60–65.
3. Shuraleva S.V. Regulirovanie truda uiazvimykh grupp rabotnikov: vyzovy i puti ikh preodoleniia v eru iskusstvennogo intellekta. Trudovoe pravo v Rossii i za rubezhom. 2024. No. 1. Pp. 44–47.
4. Mikrina V.G. Mezhdunarodno-pravovye mekhanizmy zashchity trudovykh prav naibolee uiazvimykh grupp naseleniia : dis. ... kand. iurid. nauk. M., 2018. Pp. 12–13, 16.
5. Avak'ian S.A. Konstitutsionnoe pravo Rossii : uchebnyi kurs : v 2-kh t. T. 1. M. : Norma, 2021. Pp. 182–187.
6. Chirkin V.E. Konstitutsionnoe pravo zarubezhnykh stran : uchebnik. 9-e izd., pererab. i dop. M. : Norma : Infra-M, 2020. P. 532.
7. Grishkovets A.A., Kobzar'-Frolova M.N., Smorchkova L.N. Etnicheskii anklav: iuridicheskie problemy novoi ugrozy natsional'noi bezopasnosti. Sovremennaiia nauka: aktual'nye problemy teorii i praktiki. Seriia: Ekonomika i pravo. 2023. No. 11. Pp. 147–152.
8. Vinogradova E.V., Kobzar'-Frolova M.N., Smorchkova L.N. K voprosu o pravovom regulirovanii obshchestvennykh otnoshenii v sfere protivodeistviia formirovaniu etnicheskikh anklavov. Pravovaia politika i pravovaia zhizn'. 2024. No. 1. Pp. 161–174.

ПЕРСПЕКТИВЫ И ПРОБЛЕМАТИКА МОДЕРНИЗАЦИИ ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ¹

Чудесенко А.В.²

Ключевые слова: информационное общество, недостоверная информация, цифровизация, цифровая трансформация, Legal Tech, технологическое развитие, модернизация юридической деятельности.

Аннотация

Цель исследования: статья посвящена актуальным вопросам развития модернизации юридической деятельности и использования технических и технологических решений в юридической профессии. Исследовались вопросы изменения цифровой среды и необходимости повышения уровня технологической адаптации юридической деятельности в условиях цифровой трансформации.

Методы исследования: работа основана на системном анализе, это способствовало комплексно исследовать процессы модернизации юридической деятельности в условиях цифровой трансформации.

Результаты исследования: проведенное исследование позволило сделать вывод, что улучшение и структурирование процесса управления информационными ресурсами и технологиями в юридической профессии могут улучшить качества предоставляемых услуги и повысить уровень защищенности общества в условиях нового времени. В исследовании представлено научное осмысление концептуального подхода к формированию и развитию Legal Tech решений, которые существенно могут улучшить порядок оказания юридической помощи и повысить качество и скорость обработки информации, что в свою очередь может обеспечить защищенность данных и безопасность государства в условиях новых вызовов и угроз.

Научная новизна: установлена необходимость разработки в условиях цифровой трансформации новых образовательных и научных программ, посвященных развитию модернизации юридической деятельности, необходимость обеспечения общественного диалога между представителями государственного регулирования и общества, а также необходимость улучшения законодательного регулирования внедрения технологических решений в юридическую деятельность и разработки критериев оценки эффективности их апробации в условиях цифровой трансформации.

DOI: 10.24412/1994-1404-2025-1-63-69

Введение

В современном мире цифровизация становится неотъемлемой частью жизни общества. Новые технологии выступают в роли катализатора экономического роста и повышения качества жизни. Цифровая трансформация государства и общества порождает множество вопросов, включая необходимость расширения применения информационных технологий. В последнее время особое внимание уделяется сквозным технологиям — межатраслевым направлениям, которые способны создавать инновационные продукты и сервисы. Эти технологии способны значительно изменить экономику и рынки, влияя на различные сферы. Поэтому важно следить за их развитием и интеграцией в повседневную жизнь, чтобы максимально использовать

их потенциал для создания устойчивого и динамичного информационного общества³. В современном обществе необходимо признать, что роль информации очень велика. Поэтому общество, ориентированное на прогрессивное движение, не может не быть информационным. Наряду с информационными и коммуникационными технологиями, находящимися в основании современного общества, особая роль отведена праву, которое в данной миссии присутствует весьма многопланово.

³ Распоряжение Правительства РФ от 16 марта 2024 г. № 637-р «Стратегическое направление в области цифровой трансформации государственного управления» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 15.02.2025.

¹ Статья написана в рамках Государственного задания FMUZ-2024-0035 «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами».

² Чудесенко Антон Вадимович, аспирант ИГП РАН, младший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук, г. Москва, Российская Федерация.

E-mail: a.chudesenko@mail.ru

Проблематика развития применения информационных технологий в юридической деятельности в условиях цифровой трансформации

Можно констатировать, что сегодня происходит «цифровая трансформация», связанная с новыми вызовами, обусловленными возникновением, возрастающей агрессивностью распространения ложной («фейковой», недостоверной) информации, включая и правовую. Не случайно данная тенденция уже получила определение «инфодемия», которая представляет собой серьезную угрозу информационной безопасности [1, с. 53]. В этой связи понятие «информация», занимая ключевое место в ряде естественно-научных отраслей знания, продолжает тем не менее оставаться одним из наиболее спорных и противоречивых [2, с. 133].

Бесконтрольное распространение информации, ее непоступательная обработка, невозможность отличить достоверные сведения и их обработать — это лишь часть постоянных проблем, возникающих в процессе развития юридической деятельности. Повышение объема данных ставит перед современными юристами целый ряд сложных задач, которые могут быть решены путем внедрения новых технологий в постоянные процессы ведения дел в юридической деятельности. Современные цифровые технологии создают уникальную технологическую среду для правового регулирования. Это, в свою очередь, поднимает важные вопросы адаптации правовых норм к новым возможностям, которые предлагают эти технологии. Цифровизация значительно влияет на традиционные отрасли экономики, изменяя подходы к управлению в бизнесе, государственном управлении, а также в сферах обороны и обеспечения безопасности [3, с. 47; 4]. Стремительное развитие цифровых решений требует от правовой системы гибкости и способности быстро реагировать на изменения, чтобы эффективно регулировать новые реалии и защищать права граждан. Таким образом, актуальность данной проблемы очевидна, и её решение будет способствовать более эффективному использованию цифровых технологий в различных сферах жизни общества [6, с. 59—60; 7]. При реализации государственной политики в сфере цифровой трансформации необходимо повышать уровень доверия граждан к цифровым инициативам государства, так как цифровая трансформация жизненно необходима России для устойчивости развития [11, с. 14].

Надо признать, что цифровая трансформация в обществе образовала и новые средства и способы обработки информации, например, с помощью технологий искусственного интеллекта, виртуальной и дополненной реальности, нейронных сетей, что в свою очередь способствует росту недостоверной информации, распространению киберугроз, информационных угроз и фальсификаций [9, с. 99; 14, с. 4].

Перспективы модернизации юридической деятельности и применения Legal Tech как направления развития

В настоящее время наблюдается заметный рост интереса к использованию информационных технологий в юридической деятельности, что приводит к появлению нового направления модернизации юридической деятельности с применением новых технологических решений — Legal Tech. Это направление объединяет различные технологические решения, направленные на улучшение работы юристов, судей, адвокатов и других специалистов сферы права.

Legal Tech представляет собой инновационный подход к обработке, хранению и передаче юридической информации. Он может включать в себя различные виды программного обеспечения, онлайн-платформы для юридических консультаций, а также использование искусственного интеллекта для автоматизации процессов юридической работы.

Одним из главных преимуществ данного направления является повышение эффективности и скорости юридической работы. Благодаря автоматизации рутинных операций юристы могут сосредоточиться на более сложных задачах и принятии стратегических решений. Кроме того, использование технологий позволяет уменьшить вероятность ошибок и повысить качество предоставляемых правовых услуг.

Термин Legal Tech используется для обозначения всех технологических достижений в юридической сфере. С точки зрения возможностей, внедрение технологических решений сможет предложить населению точные юридические консультации, снизив их стоимость, и, с другой стороны, проанализировать большие объемы данных, которые юридические фирмы будут использовать для повышения эффективности работы.

Говоря о понятийном определении трактовки такой деятельности, следует обратить внимание, что они связаны с категориями «информационное право», «машиночитаемое право», «право цифровой трансформации». Необходимо признать, что ключевыми направлениями научно-технологического развития являются переход к передовым технологиям и создание высокотехнологической продукции, роботизированных и высокопроизводительных вычислительных систем, обработка больших данных, технологий машинного обучения и искусственного интеллекта, и потому такая деятельность как нельзя кстати подходит под концепцию, презентованную в законодательном регулировании⁴.

С.Г. Еремеев и его соавторы рассматривают Legal Tech как научное юридическое направление — «право цифровой трансформации», как подотрасль информа-

⁴ Указ Президента РФ от 28 февраля 2024 г. № 145 «Стратегия научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 10.02.2025.

ционного права. В качестве юридического концепта авторы указывают информационное право, а также связь человека с техникой и объективную неизбежную реакцию системы права на технологические изменения. Соглашаясь с ними, следует отметить, что развитие и трансформация институтов непременно нуждается в осмыслении с точки зрения юриспруденции. С научной точки зрения «машиночитаемое право» как явление, основанное на информации в цифровой форме, как направление имеет несомненные перспективы. Более того, перспективы опосредованы неоднозначностью содержательного наполнения самого явления. Все это создает благодатную почву для научных размышлений [5, с. 124].

А. Пронин, говоря о перспективах Legal Tech, выдвигает смелые прогнозы: «с внедрением технологий автоматизации на блокчейн-платформах можно будет разрабатывать смарт-законы, или самоисполняемые законы (по аналогии со смарт-контрактами)». В качестве примера преобразования закона в цифровой код он приводит сферу «автоматической выписки штрафов с камер видеонаблюдения». Однако полагаем, что данный пример не является «смарт-законом» в смысле цифрового (электронного) законодательства [Савченко]. Это, скорее всего, «смарт-правоприменение» — автоматическое применение нормы права в целях реализации мер ответственности за нарушение установленных правил. Также указывается на довольно эффективную меру использования искусственного интеллекта в сфере законотворчества — обнаружение коллизий в законах. Такое применение вполне оправдано, поскольку полностью соответствует критериям эффективности цифровой экономики. Важно, что разработана Концепция развития технологий машиночитаемого права⁵ (далее — Концепция), в которой обосновывается актуальность развития машиночитаемого права: повышение удобства его правоприменения государством, предпринимательским сообществом и гражданами. В Концепции отмечается российский опыт применения машиночитаемого права⁶ в различных бизнес-проектах в качестве таких сервисов, как «робот-юрист» (департамент Сбербанка), «цифровой юрист» (компания «Мегафон»); платформа «Нормотворчество» для реализации взаимодействия участников нормотворческого процесса в рамках федерального проекта «Цифровое государственное управление» программы «Цифровая экономика». В Концепции также обозначены сферы применения: стандартизация и сертификация, сделки в машиночитаемом формате, контрольная

(надзорная) деятельность, отчетность, судопроизводство и производство по административным делам, нормотворчество, взаимодействие государственных информационных систем с цифровыми платформами.

В качестве основного риска использования технологий в модернизации юридической деятельности выделяется масштабное использование больших данных, которое провоцирует вторжение в частную сферу граждан и несанкционированное использование данных. Незащищенность в цифровой среде снижает активность использования ресурсов [10, с. 6]. Из исследования ресурсов, применяемых в различных сферах экономической деятельности как частного, так и публичного характера, следует вывод: модернизация юридической деятельности — это элемент цифровой экономики, служащий широкому кругу субъектов экономических отношений. Это современное цифровое инструментальное средство правового регулирования экономической деятельности, в том числе экономической деятельности граждан, опосредованное отношениями субъектов и государственных (муниципальных) органов [12, с. 87].

В данном аспекте на основе классического понимания правовых средств в механизме правового регулирования, с точки зрения инструментально-правового подхода по отношению к субъектам экономической деятельности Legal Tech выступает в таких аспектах, как:

- ресурс повышения правовой и информационной грамотности;
- фактор информационно-правового воздействия, оказывающего влияние на выбор правового режима экономической деятельности;
- стимулятор исполнения договорных обязательств, налоговых обязанностей и в целом правомерного поведения;
- средство государственного контроля за деятельностью субъектов экономической деятельности.

По одной из теорий, Legal Tech можно рассматривать как подотрасль информационного права, поскольку оно углубленно изучает вызовы права в XXI веке с учетом российских традиций, основываясь на закономерностях нормативного регулирования процессов и результатов цифровой трансформации. Информационное право, следуя российским традициям кодификации, фокусируется на более широких понятиях и процессах, акцентируя важность методологии взаимодействия информации с человеком. Отсюда Legal Tech может быть воспринято как развитие информационного права для решения актуальных задач цифровой эпохи в контексте российской правовой системы [8, с. 52].

По мнению И.Л. Бачило, предметом, формирующим специальную отрасль отношений, условно называемых информационными, является совокупность реально существующих материализованных результатов творчества и труда, воплощенных в:

- 1) информации при разнообразии форм ее проявления и формируемых на этой основе информационных ресурсах;

⁵ Распоряжение Правительства РФ от 31.12.2020 № 3684-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021—2030 годы)» // Собрание законодательства РФ. 2021. № 3. Ст. 609.

⁶ Концепция развития технологий машиночитаемого права (утверждена Правительственной комиссией по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 15.09.2021 № 31) // СПС «КонсультантПлюс».

2) средствах и технологиях работы с информацией (информационных технологиях — потенциал ИКТ);

3) средствах и технологиях коммуникации информации по сетям связи.

На базе этой триады предметов формируется новая область общественных отношений, которая в системе права выделяется как самостоятельная сфера правового регулирования⁷.

Legal Tech играет важную роль в цифровой трансформации правового регулирования экономической деятельности, особенно в отношении упрощенной регистрации субъектов экономики. Применение современных технологий позволяет ускорить и упростить процедуры регистрации, что способствует развитию предпринимательства и содействует развитию экономики в целом.

Кроме того, такой технологический подход и модернизация используется в качестве инструмента государственного контроля в правовом регулировании экономической деятельности. Автоматизированные механизмы, основанные на искусственном интеллекте и анализе больших данных, позволяют эффективнее осуществлять мониторинг и контроль за деятельностью субъектов экономики, включая физических лиц, и обеспечить соблюдение ими правовых норм и требований.

Таким образом, использование Legal Tech в правовом регулировании экономической деятельности способствует улучшению процессов регистрации предприятий, повышению эффективности государственного контроля и стимулированию правомерного поведения участников экономики. Это важное направление развития правовой сферы, нацеленное на обеспечение прозрачности и соблюдения законности в экономике.

Технологическое развитие юридической профессии играет ключевую роль в цифровой трансформации процессов правового регулирования экономической деятельности. Электронный документооборот, автоматизированные механизмы регистрации и обработки отчетности позволяют существенно улучшить качество государственных и муниципальных услуг, обеспечивая более эффективное выявление нарушений и применение мер контроля.

С точки зрения частных и публичных интересов важно отметить, что Legal Tech способствует развитию институтов, которые служат интересам всех субъектов права, участвующих в экономических процессах. Например, для частных интересов технологии предоставляют возможность повышения информированности субъектов, снижают материальные и трудовые издержки, обеспечивают более эффективные мотивационные механизмы для исполнения обязанностей и упрощают цифровые формы взаимодействия. Для публичных

интересов модернизация юридических процессов обеспечивает автоматизированную государственную регистрацию субъектов экономической деятельности, упрощает процессы сдачи отчетности и обеспечивает прозрачность контроля [10, с. 5; 14, с. 4].

Таким образом, правовая модернизация играет важную роль в обеспечении эффективности, прозрачности и соблюдения правовых норм в экономической сфере, способствуя развитию как частных, так и публичных интересов в правовом регулировании экономической деятельности. Учитывая современные условия развития юридической деятельности, можно выделить следующие основные характеристики использования Legal Tech на современных этапах.

1. Продвинутый уровень обеспечения доступности юристов для клиентов: IT-технологии в ближайшем будущем обеспечат режим круглосуточного удаленного доступа к юридическим услугам, без привязки к географическим точкам.
2. Цифровизация юридического документооборота позволит значительно ускорить совершение юридически значимых действий (электронное правительство, электронный нотариат, электронное правосудие).
3. Существенный толчок в развитии бизнес-процессов может дать широкое внедрение чат-ботов в контексте развития удаленного юридического консалтинга.
4. Перспективным является использование программных методов анализа юридических документов (англ. predictive coding). В зарубежной практике уже делаются попытки использования программного анализа в антимонопольных разбирательствах, где хорошие результаты дает машинный анализ электронных данных о содержании государственных и муниципальных контрактов.
5. В ближайшие годы перед ведущими международными юридическими фирмами встанет задача создания крупных IT-интеграторов с конкурентоспособными программно-аппаратными решениями в области юридического сопровождения бизнес-процессов.

Из исследований видно, что это неотъемлемый элемент цифровой экономики, который обеспечивает эффективное правовое регулирование экономической деятельности как в частном, так и в публичном секторе. Legal Tech является современным цифровым инструментом, который служит широкому кругу участников экономических отношений.

Используя классическое понимание правовых средств в механизме правового регулирования, цифровая модернизация юридической деятельности выступает важным инструментом для субъектов экономической деятельности. Она выступает в следующих ролях.

1. Ресурс повышения правовой и информационной грамотности: модернизация способствует улучшению знаний и понимания субъектов по право-

⁷ Бачило И.Л. Современные задачи информационного права // Право на доступ к информации: возможности ограничения в электронной среде : сб. материалов Междунар. науч.-практ. конф. СПб., 2011. С. 32.

вым вопросам, обеспечивая им доступ к актуальной информации.

2. Фактор информационно-правового воздействия: влияет на выбор правового режима в экономической деятельности, обеспечивая субъектам необходимую информацию для принятия обоснованных решений.
3. Стимулятор исполнения обязательств: помогает стимулировать исполнение договорных обязательств, налоговых обязанностей и общее правомерное поведение со стороны участников экономических отношений.
4. Средство государственного контроля за деятельностью субъектов экономической деятельности: обеспечивает более эффективное и прозрачное наблюдение за соблюдением законодательства.

Таким образом, Legal Tech играет ключевую роль в различных аспектах правового регулирования экономической деятельности, обеспечивая эффективное функционирование рыночных отношений и соблюдение правовых норм со стороны как частных, так и публичных участников.

Заключение

Подводя итог анализа явления, следует выделить некоторые направления дальнейшего исследования, а также следующие предложения.

- Для обеспечения разработки и апробирования технологических решений на базе вузов и грантовых проектов необходимо создавать специализированные программы и исследовательские центры, которые будут заниматься разработкой и тестированием инновационных технологий в области права. Эти вузы и проекты могут стать площадками для проведения научных исследований, обучения студентов и молодых специалистов, а также для создания прототипов и пилотных проектов в исследуемой области [6, с. 37].
- Для обеспечения взаимодействия представителей органов государственной власти и представителей бизнес-сообщества в целях организации эффективного сотрудничества в разработке новых решений в Legal Tech необходимо создавать платформы для диалога и обмена опытом между разными заинтересованными сторонами. Это могут быть конференции, форумы, рабочие группы и другие мероприятия, на которых можно обсуж-

дать актуальные вопросы и находить общие решения.

- Для анализа примеров успешных внедрений Legal Tech решений в зарубежной практике с целью адаптации в рамках российской практики необходимо проводить исследования, анализировать отчеты и публикации, привлекать экспертов и специалистов из других стран для обмена опытом и передачи знаний. Это позволит выявить лучшие практики и технологии, которые можно успешно адаптировать и использовать в России.
- Для обеспечения разработки и усовершенствования курсов технической подготовки юристов, приобретающих характер массовости, необходимо создавать образовательные программы, которые будут соответствовать современным требованиям и потребностям рынка. Важно также учитывать динамичное развитие технологий и внедрять инновационные методики обучения, чтобы обеспечить высокий уровень компетенций у будущих специалистов в области Legal Tech.

Ключевые направления научно-технологического развития действительно ставят перед собой задачи, связанные с переходом на передовые технологии и созданием высокотехнологичной продукции. В условиях глобальной трансформации, которая затрагивает финансовые, логистические и производственные системы, необходимо уделять внимание новым вызовам.

Необходимо отметить, что рост геополитической и экономической нестабильности, а также системного неравенства подчеркивает важность стабильных национальных институтов. В условиях цифровой трансформации особенно актуальными становятся вопросы кибербезопасности и защиты персональных данных. Для повышения грамотности населения в области информационной безопасности необходимо разрабатывать комплексные подходы и проводить информационные кампании. Это не только повысит доверие к цифровым сервисам, но и поможет защитить граждан от преступлений с использованием информационно-коммуникационных технологий. Таким образом, будет возможно создать безопасное и надежное цифровое пространство, что приведет к дальнейшей цифровизации экономики и повышению качества жизни граждан. Модернизация юридической деятельности позволит обеспечить более качественную защиту интересов общества, а развитие технологий позволит укрепить технологический суверенитет в условиях цифровой трансформации.

Литература

1. Полякова Т.А. Влияние цифровой трансформации на развитие информационного права: тенденции, проблемы, перспективы // Мониторинг правоприменения. 2020. № 2 (35). С. 53—58. DOI: 10.21681/2226-0692-2020-2-53-58. EDN: KTRBVM.
2. Троян Н.А. Правовая информация как условие трансформации информационного общества в эпоху цифровизации // Право и государство: теория и практика. 2020. № 10 (190). С. 133—137.

3. Полякова Т.А. Трансформация системы информационного права в условиях цифровизации // Человек, общество, право в условиях цифровой реальности : сб. ст. / Под ред. О.Ю. Рыбакова. М., 2020. С. 45—56.
4. Минбалеев А.В. и др. Информационно-технологическое обеспечение юридической деятельности (Legal Tech). М. : Проспект, 2022. 368 с.
5. Новые горизонты развития системы информационного права в условиях цифровой трансформации : монография / Отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : ИГП РАН, 2022. 368 с.
6. Карцхия А.А., Макаренко Г.И. Правовые горизонты искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. 2024. № 1 (59). С. 2—14. DOI: 10.681/2311-3456-2024-1-2-14.
7. Карцхия А.А. Цифровая трансформация права // Мониторинг правоприменения. 2019. № 1 (30). С. 25—29.
8. Карцхия А.А., Макаренко Г.И. Правовые аспекты современной кибербезопасности и противодействия киберпреступности // Вопросы кибербезопасности. 2023. № 1 (53). С. 58—74. DOI: 10.21681/2311-3456-2023-1-58-74.
9. Савенко Н.Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. № 1. С. 145—171. DOI: 10.17323/2072-8166.2023.1.145.171. EDN: AVJYME.
10. Губин Е.П. Экономическая деятельность, экономические права и их защита в контексте соотношения права и экономики // Предпринимательское право. 2021. № 31. С. 3—10.
11. Рожкова М.А., Исаева О.В. и др. Legaltech, Fintech, Regtech etc.: правовые аспекты использования цифровых технологий в коммерческой деятельности. М. : Статут, 2021. 310 с.
12. Степанов О.А. Правовое воздействие на развитие цифровой среды в обществе. М. : Проспект, 2021. 88 с.
13. Тихомиров Ю.А., Талапина Э.В. Право как фактор экономического развития // Право. Журнал Высшей школы экономики. 2020. № 1. С. 4—26.
14. Карцхия А.А., Макаренко Г.И. Правовые проблемы искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4—19. DOI: 10.21681/1994-1404-2024-1-4-19.

SECTION:
CONSTITUTIONAL LAW

PROSPECTS AND PROBLEMS OF MODERNISING LAWYERS' ACTIVITIES IN THE CONTEXT OF DIGITAL TRANSFORMATION

Anton Chudesenko, Ph.D. student, Junior Researcher at the Sector of Information Technology Law and International Information Security of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.
E-mail: a.chudesenko@mail.ru

Keywords: information society, unreliable information, digitalisation, digital transformation, Legal Tech, technological development, lawyers' activities modernisation.

Abstract

Purpose of the study: the paper is devoted to topical issues of the development of the modernization of legal activity and the use of technical and technological solutions in the legal profession. The issues of changing the digital environment and the need to increase the level of technological adaptation of legal activity in the context of digital transformation were investigated. In his work, the author explored the current issues of the possibility of implementing various solutions in legal activities, the problems of their implementation and possible prospects for the modernization of jurisprudence in the context of changing the rule of law.

Methods used in the study: the work is based on a systematic analysis, which contributed to a comprehensive study of the processes of modernization of legal activity in the context of digital transformation.

Study findings: the conducted research led to the conclusion that improving and structuring the management process of information resources and technologies in the legal profession can improve the quality of services provided and increase the level of security of society in modern times. The study presents a scientific understanding of the conceptual approach to the formation and development of Legal Tech solutions that can significantly improve the procedure for providing legal assistance and improve the quality and speed of information processing, which in turn can ensure data security and the security of the state in the face of new challenges and threats.

Research novelty: it was found that it is needed to develop, in the context of digital transformation, new educational and research programmes for modernisation of lawyers' activities, to organise a social dialogue between the representatives of government regulation and the society, to improve legislative regulation for introducing technological solutions into lawyers' activities and to develop criteria for evaluating the efficiency of using them in the context of digital transformation.

References

1. Poliakova T.A. Vliianie tsifrovoi transformatsii na razvitie informatsionnogo prava: tendentsii, problemy, perspektivy. Monitoring pravoprimeneniia. 2020. No. 2 (35). Pp. 53–58. DOI: 10.21681/2226-0692-2020-2-53-58 . EDN: KTRBVM.
2. Troian N.A. Pravovaia informatsiia kak uslovie transformatsii informatsionnogo obshchestva v epokhu tsifrovizatsii. Pravo i gosudarstvo: teoriia i praktika. 2020. No. 10 (190). Pp. 133–137.
3. Poliakova T.A. Transformatsiia sistemy informatsionnogo prava v usloviakh tsifrovizatsii. Chelovek, obshchestvo, pravo v usloviakh tsifrovoi real'nosti : sb. st. Pod red. O.Iu. Rybakova. M., 2020. Pp. 45–56.
4. Minbaleev A.V. i dr. Informatsionno-tekhnologicheskoe obespechenie iuridicheskoi deiatel'nosti (Legal Tech). M. : Prospekt, 2022. 368 pp.
5. Novye gorizonty razvitiia sistemy informatsionnogo prava v usloviakh tsifrovoi transformatsii : monografiia. Otv. red. T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : IGP RAN, 2022. 368 pp.
6. Kartskhiia A.A., Makarenko G.I. Pravovye gorizonty iskusstvennogo intellekta: natsional'nyi i mezhdunarodnyi aspekt. Voprosy kiberbezopasnosti. 2024. No. 1 (59). Pp. 2–14. DOI: 10.681/2311-3456-2024-1-2-14 .
7. Kartskhiia A.A. Tsifrovaia transformatsiia prava. Monitoring pravoprimeneniia. 2019. No. 1 (30). Pp. 25–29.
8. Kartskhiia A.A., Makarenko G.I. Pravovye aspekty sovremennoi kiberbezopasnosti i protivodeistviia kiberprestupnosti. Voprosy kiberbezopasnosti. 2023. No. 1 (53). Pp. 58–74. DOI: 10.21681/2311-3456-2023-1-58-74 .
9. Savenko N.E. Legaltech v tsifrovoi ekonomike i pravovom regulirovanii ekonomicheskoi deiatel'nosti grazhdan. Pravo. Zhurnal Vyshei shkoly ekonomiki. 2023. No. 1. Pp. 145–171. DOI: 10.17323/2072-8166.2023.1.145.171 . EDN: AVJYME.
10. Gubin E.P. Ekonomicheskai deiatel'nost', ekonomicheskie prava i ikh zashchita v kontekste sootnosheniia prava i ekonomiki. Predprinimatel'skoe pravo. 2021. No. 31. Pp. 3–10.
11. Rozhkova M.A., Isaeva O.V. i dr. Legaltech, Fintech, Regtech etc.: pravovye aspekty ispol'zovaniia tsifrovyykh tekhnologii v kommercheskoi deiatel'nosti. M. : Statut, 2021. 310 pp.
12. Stepanov O.A. Pravovoe vozdeistvie na razvitie tsifrovoi sredy v obshchestve. M. : Prospekt, 2021. 88 pp.
13. Tikhomirov Iu.A., Talapina E.V. Pravo kak faktor ekonomicheskogo razvitiia. Pravo. Zhurnal Vyshei shkoly ekonomiki. 2020. No. 1. Pp. 4–26.
14. Kartskhiia A.A., Makarenko G.I. Pravovye problemy iskusstvennogo intellekta v Rossii. Pravovaia informatika. 2024. No. 1. Pp. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19 .

СТРАТЕГИЧЕСКИЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОГО И ЦИФРОВОГО СУВЕРЕНИТЕТА: ПРАВОВЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ НОВОЙ ИНФОРМАЦИОННОЙ СРЕДЫ¹

Полякова Т.А.², Троян Н.А.³

Ключевые слова: информационный суверенитет, цифровой суверенитет, достоверная информация, цифровая трансформация, государственное управление, вызовы, угрозы, правовое регулирование, искусственный интеллект, наукоемкие технологии, цифровые платформы.

Аннотация

Цель исследования: изучить актуальные информационно-правовые вопросы, касающиеся возрастающего значения задач достижения национального суверенитета России в информационной сфере под влиянием цифровой трансформации.

Методы исследования: общенаучные методы анализа и синтеза, а также системный метод, который позволяет анализировать состояние и проблемы развития информационного законодательства России в сферах с использованием цифровых технологий.

Результаты исследования: авторы обращали внимание на важные проблемы, связанные с обеспечением технологического и цифрового суверенитета в условиях реализации стратегических задач научно-технологического развития Российской Федерации. В связи с принятием новых национальных проектов, направленных на развитие экономики данных и цифровой трансформации управления, возрастает роль информационного права не только как нового научного направления, но и публично-правовой (государственно-правовой) науки, перед которой стоят задачи развития ее теории в условиях формирования экономики данных, а также решения стратегических задач по обеспечению национальных приоритетов научно-технологического развития и информационной безопасности, включая вопросы кибербезопасности. Проведенное исследование позволило обосновать вывод о том, что реализация новых стратегических задач научно-технологического развития и достижение национального суверенитета в информационной сфере — технологического и цифрового — требует развития национальной государственной политики, направленной на правовое обеспечение информационной безопасности, в том числе защиты кибербезопасности. Представляется, что данные меры позволят обеспечить защиту информационного суверенитета России, охрану субъектов и объектов наукоемких технологий, инновационной инфраструктуры.

Научная новизна: переход современного общества на цифровые технологии и достижение цифрового технологического суверенитета в современных условиях, на наш взгляд, возможен посредством развития организационно-правовых механизмов на основе анализа защищенности цифровых данных, формирования безопасной цифровой среды, обладающей необходимым уровнем цифровой зрелости. Установлено, что достижение технологического и цифрового суверенитета России, несомненно, связано с развитием публично-правовой науки, междисциплинарными подходами к поиску правовых, фундаментальных решений в целях обеспечения национальной безопасности страны. Авторы отмечают, что приоритетными должны стать: разработка доктрины информационного права, включая правовое обеспечение информационной (национальной и международной), безопасности, в том числе кибербезопасности и достижение киберстабильности, в свете принятия универсальных международных документов по противодействию киберпреступности; доктринальная модель развития системы информационного законодательства (включая цифровое), направленное на научное обоснование, упорядочение правового регулирования информационных отношений.

DOI: 10.24412/1994-1404-2025-1-70-78

¹ Статья написана в рамках Государственного задания FMUZ-2024-0035 «Обеспечение цифрового суверенитета и информационной безопасности правовыми средствами».

² **Полякова Татьяна Анатольевна**, доктор юридических наук, профессор, заслуженный юрист РФ, главный научный сотрудник, и о. зав. сектором информационного права и международной информационной безопасности Института государства и права Российской академии наук, г. Москва, Российская Федерация.

E-mail: polyakova_ta@mail.ru

³ **Троян Наталья Анатольевна**, кандидат юридических наук, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук, г. Москва, Российская Федерация.

E-mail: n-fadeeva@ya.ru

Сегодня развитие экономики и государственного управления в значительной степени определяется цифровой трансформацией, что отражено и в новых национальных проектах России, которые начинают действовать с января 2025 года. Новые задачи научно-технологического развития, определенные в новой редакции Стратегии, утвержденной Президентом РФ⁴, оказывают существенное влияние на развитие информационного общества, находящегося в постоянной динамике, способствуют выделению нового вектора развития права и современных правоотношений. Это детерминирует необходимость совершенствования законодательства, обеспечения высокого уровня защищенности прав и свобод граждан, модернизации и повышения эффективности государственного управления, деятельности органов публичной власти, правовой информатизации, защиты национальных интересов от внешних и внутренних угроз в правовой сфере и создание безопасной единой информационно-правовой среды [1, с. 50]. Необходимо признать, что сегодня право служит своеобразным отражением всех проявлений суверенитета, поскольку право не «привязано» лишь к обществу или государству и способствует обеспечению жизнедеятельности социальных субъектов права — людей, социальных общностей и объединений [2, с. 7]. Однако новизна этих вопросов вызывает множество дискуссий о роли государства как главного регулятора общественных отношений, о существенных признаках, в частности, о государственном суверенитете. Необходимо признать, что конституционно-правовое пространство формируется под влиянием многих аспектов, ключевым из которых является суверенитет. Следовательно, сегодня укрепление суверенитета государства является одним из ключевых условий обеспечения состояния защищенности национальных интересов государства в процессе цифровой трансформации.

Следует отметить, что суверенитет как явление и понятие имеет достаточно длительную историю. В словаре Д.Н. Ушакова суверенитет охарактеризован как независимость государства в его внутренних делах и внешней политике⁵. Под суверенитетом нередко понимают самостоятельность, независимость. Тем не менее отмечается дискуссионность вопросов, связанных с суверенитетом и государственной властью, а также различия между понятиями суверенитета и совокупностью суверенных прав или отдельных полномочий государства. В этой связи особенно тревожит несоблюдение (нарушение) одного из ключевых принципов международного права — уважения и соблюдения суверенитета государства, что, в свою очередь, значи-

тельно затрагивает и сферу информационно-коммуникационных технологий. Изложенная выше позиция была сформулирована еще в 1990-х годах Ю.М. Батуриным. В своих исследованиях он отмечал, что «парад суверенитетов» 1988—1990 гг. естественным образом вел к «войне законов» и «параличу» хозяйственной жизни и далее по принципу нарастающей обратной связи к растаскиванию «суверенных» территорий⁶. Вместе с тем по поводу государственного суверенитета он отметил, что «в пределах государства, по праву, нет власти выше, чем власть государственная: ее правовой авторитет выше, чем всякой другой власти, ее веления имеют высшую правовую силу — это верховная власть, иначе называемая суверенною (от латинского слова *superanus, superior*, перешедшего в старофранцузское слово *sovrains*, что означает — «верховный»). Суверенитет, т. е. верховенство, считается обязательным признаком верховной государственной власти»⁷, полновластия и политической свободы государственной власти.

В современных реалиях информационного общества необходимо формирование новых инструментов в области цифровой трансформации. В этой связи суверенитет отражает общественный характер публичной власти как один из важных признаков государства. Безусловно, сегодня на суверенитет существенно влияют процессы цифровизации, новые условия глобализации и масштабные интеграционные процессы. Тем не менее значение суверенитета сохраняется, но он наполняется новым содержанием.

Сформировавшаяся как основа укрепления государства, его независимости и самостоятельности парадигма суверенной государственности сегодня получает новые прочтения. Более того, современные интерпретации делают актуальным изучение новых элементов системы суверенной государственности, включая информационный, технологический, демографический, экологический и другие виды суверенитета [3, с. 121]. Так, членом-корреспондентом РАН, доктором юридических наук, профессором А.Н. Савенковым обоснована такая трансформация, и он отмечает «парадигмы государственного суверенитета на основе тенденций правовой интерпретации как в форме «мягкого права», так и развития экстерриториального действия законодательства ряда стран»⁸. Им также справедливо замечено, что в последнее время вопросы цифрового суверенитета стали основой политического дискурса⁹. Это связано с вызовами цифровой трансформации к традиционному понятию суверенитета.

⁶ Батурин Ю.М. Парад суверенитетов в СССР (Декларации независимости 1988—1990 гг.). М. : РАН, 2020. 54 с.

⁷ Там же.

⁸ Савенков А.Н. Философия права, правовое мышление и глобальные проблемы современной цивилизации // Трансформация парадигмы права в цивилизационном развитии человечества : доклады членов РАН / Под. общ. ред. А.Н. Савенкова. М., 2019. С.67—69.

⁹ Научно-технический центр ФГУП «ГРЧЦ». Цифровой суверенитет. Обзор подходов. URL: https://rdc.grfc.ru/2022/10/digital_sovereignty_approach_review (дата обращения: 30.01.2025).

⁴ Указ Президента Российской Федерации от 28 февраля 2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 12.01.2025.

⁵ Ушаков Д.Н. Большой толковый словарь русского языка. Новая современная редакция. 2020. 816 с.

На наш взгляд, в рамках обсуждения данных вопросов необходимо признать, что в фокусе внимания ученых в настоящее время находится решение проблем, связанных с развитием информационных систем, а также цифровых отношений. Это касается появления новых субъектов и объектов информационного права, развития наукоемких технологий, формирования новых информационных пространств, а также необходимости обеспечения состояния защищенности интересов государства, общества и граждан от новых вызовов и угроз [4, с. 163]. Безусловно, эти проблемы требуют не только пристального внимания со стороны государства, но и выработки подходов к их решению в среде научного сообщества, теоретиков и практиков. В этой связи современные научные исследования требуют обоснованных предложений по развитию доктрины информационного права, развитию информационного законодательства, а также науки международного информационного права, направленных на регулирование в цифровой среде. Важно признать, что информационное общество и цифровая экономика сегодня во многом определили позиции информационного права не только как нового научного направления, но и инновационной отрасли, которая продолжает активно развиваться в условиях цифровой трансформации государства и права, формирования экономики данных, а также решения стратегических задач по обеспечению национального суверенитета в информационной сфере и информационной безопасности, в том числе вопросов кибербезопасности в цифровой среде [4, с. 162].

Особое внимание уделяется вопросам информационной безопасности как на международном, так и на национальном уровнях в связи с возросшими вызовами, рисками и угрозами в области цифровых технологий. Следует согласиться с А.К. Дубенем, что формирование и развитие национальной государственной политики, направленной на обеспечение информационной безопасности, будет способствовать дальнейшему совершенствованию защиты информационных технологий и систем, недопущению уязвимости данных и снижению возникновения информационных угроз. Это позволит обеспечить защиту информационного суверенитета России, охрану субъектов и объектов наукоемких технологий и инновационной инфраструктуры¹⁰.

Очевидно, что остается достаточно много острых проблем. Необходимо признать, что действие права не ограничивается только территориальными аспектами и границами государств; оно проникает во все сферы жизни общества. В связи с этим исследование границ правового регулирования показывает как их устойчивость, так и изменчивость и динамичность внутри самой правовой системы¹¹. По мнению Председа-

теля Конституционного Суда РФ В.Д. Зорькина, «идеальные правовые модели едва ли существуют. Для каждого исторического этапа, для каждого государства в разные исторические периоды их существования нужны особенные модели такого регулирования, нужна тонкая настройка механизмов правового регулирования. С этой точки зрения право будущего — недостижимый идеальный концепт, который по мере приближения к нему будет снова меняться и отдаляться... Поэтому мы можем говорить о смене парадигмы понимания права с устаревшего постмодернистского восприятия на новое, признающее фундаментальные ценности метамодернистского права, которое серьезно относится и к индивидуальной свободе, и к ценности сильного государства»¹².

В дискуссиях последнего времени вопросы цифрового суверенитета стали основой и политического дискурса. Это связано с вызовами цифровой трансформации традиционному понятию суверенитета. Перспективность права понималась преимущественно через призму новых явлений общественной жизни, таких как искусственный интеллект, большие данные (Big Data), технологии блокчейна, изменения передачи и хранения больших данных. В этой связи в условиях трансформации и цифровизации сформировалась необходимость в определении понятий «цифровой суверенитет», «технологический суверенитет». Следует признать, что, несмотря на актуальное значение в области обеспечения информационной безопасности, данные дефиниции на сегодняшний день не имеют правовой определенности [5, с. 169; 6, с. 170]. Между тем, как показывает исследование, термин «цифровой суверенитет» становится все более популярным не только в публичных выступлениях, но также в стратегических документах и научных публикациях. Однако на сегодняшний день имеется довольно много весьма противоречивых суждений относительно того, что представляет собой цифровой суверенитет и может ли он или должен быть суверенным¹³. Причем в рамках исследования проблем особенно важной представляется тема, касающаяся цифровой инфраструктуры и ИТ-технологий. Для обеспечения цифрового суверенитета следует сформировать информационно-техническую систему, защищающую информацию от утечки при использовании информационных технологий. При этом представляется важным, что в условиях цифровизации сформировалась необходимость в определении не только понятия «технологический суверенитет», но и термина «цифровой суверенитет». Несомненно, в этом контексте вопрос определения терминологии представляет собой важную составляющую государственного суверенитета в современных условиях, когда наблюдается

¹⁰ Дубень А.К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации : дис. ... канд. юрид. наук. М., 2023. С. 88—89.

¹¹ Границы правового регулирования : научно-практическое пособие / Отв. ред. И.В. Плюгина, Е.В. Черепанова. М. : Институт закон-ва и сравнит. правовед. при Правительстве РФ, 2011. 184 с.

¹² Валерий Зорькин. Право будущего в эпоху цифр // НАМИБ. URL: <https://namib.online/2020/04/valerij-zorkin-pravo-budushhego-v-jerohu-cifr> (дата обращения: 13.02.2025).

¹³ Границы правового регулирования : научно-практическое пособие / Отв. ред. И.В. Плюгина, Е.В. Черепанова. М. : Институт закон-ва и сравнит. правовед. при Правительстве РФ, 2011. 184 с.

рост мирового кризиса, преодоление усиливающихся санкций и переход к многополярности. В связи с этим появилась необходимость сосредоточиться на вопросах технологического суверенитета, которые касаются прежде всего обеспечения реализации политики импортозамещения [7, с. 284]. Безусловно, данные проблемы решить непросто, и пока нет четких ответов в отношении конкретных задач. В свете растущего влияния наукоемких технологий и цифровых технологий одним из ключевых аспектов цифрового суверенитета становится поддержка и развитие национальных технологий и цифровых платформ. Это выражается в возможностях внедрения правовых мер, таких как финансовая поддержка разработчиков, а также обязательные требования по использованию отечественных программных решений в государственных структурах. Кроме того, важно создать благоприятное правовое поле для стартапов и инновационных компаний. Эти шаги помогут избежать зависимости от иностранных технологий, которые могут быть уязвимы к внешним угрозам и вмешательству. Тем не менее и в этих условиях возникло множество дискурсов, касающихся обеспечения цифрового суверенитета, сетевого, научно-технологического и других видов суверенитета. Таким образом, имеется целый ряд вопросов, каким образом эти проблемы соотносятся с правовым обеспечением информационной безопасности и как между собой соотносятся используемые сегодня понятия, которые определяют различные виды суверенитета, с общепризнанным государственным (национальным) суверенитетом при наличии большого количества кибератак и отдельных угроз. Цифровой суверенитет является возможностью независимого суверенного государства самостоятельно определять степень и способ участия в информационной деятельности при применении цифровых технологий для реализации собственных интересов и противодействия противоправным действиям в национальном информационном пространстве¹⁴. В условиях цифровой трансформации особенно важным является принятие четких и обоснованных правовых решений на государственном уровне. В связи с этим целесообразно изучение и разработка вопросов о внесении изменений в нормативные правовые акты Российской Федерации. Приоритетом должны стать современные научные исследования, тематика которых непосредственно связана с реализацией стратегических задач в научно-технологической сфере, имеющих приоритетное значение для обеспечения технологического суверенитета России. Это между тем не отменяет необходимости сохранения исторически сложившегося государственного единства и традиционных российских духовно-нравственных ценностей, а также культуры и исторической памяти.

¹⁴ Дубень А.К. Правовое обеспечение информационной безопасности в системе информационного права в Российской Федерации : дис. ... канд. юрид. наук. М., 2023. С. 89.

Сегодня многие вызовы и угрозы имеют глобальный и трансграничный характер, поэтому нельзя отрицать значение правовых норм и общепризнанных принципов международного права в ИКТ-среде [4]. В этой связи представляется важным осуществлять обмен знаниями и опытом в рамках Содружества Независимых Государств (СНГ), а также с государствами, входящими в такие международные организации, как Шанхайская организация сотрудничества (ШОС) и БРИКС, а также с другими дружественными странами. Безусловно, это будет способствовать не только укреплению взаимных связей, но и обеспечит устойчивое развитие правовой системы и государства в целом. Важно также учитывать, что в условиях глобализованного мира, где информация и технологии играют ключевую роль, такие инициативы будут способствовать большему взаимопониманию и сотрудничеству, что позволит создать стабильную политическую и правовую обстановку¹⁵. Следует признать, что в условиях современных глобальных политических и экономических реалий, когда санкционное давление со стороны различных стран становится всё более ощутимым, вопрос технологического суверенитета имеет особую актуальность и ставит перед государственным сектором приобретает большие задачи — самостоятельно разрабатывать, производить и использовать ключевые технологии. Это, в свою очередь, значительно укрепляет его позицию на международной арене и обеспечивает национальную безопасность. В свете растущего влияния современных технологий и цифровой трансформации планирование развития нормативного правового регулирования в области цифровой среды в контексте экономики данных определяет необходимость решения задач на уровне федерального законодательства. Это включает как общие аспекты, касающиеся всех цифровых технологий: экспериментальные правовые режимы, «цифровые песочницы», вопросы идентификации и аутентификации в цифровой среде, а также отдельные технологии, в том числе искусственный интеллект. Необходимо отметить, что на смену национальной программе «Цифровая экономика» приходит выполнение мероприятий нового национального проекта «Экономика данных и цифровая трансформация государства»¹⁶. Одной из ключевых задач нового национального проекта является внедрение современных платформенных решений и сервисов. Кроме того, в рам-

¹⁵ Семагин И.О. Правовое преобразование системы образования Российской Федерации на современном этапе развития // Современное право. 2024. № 3. С. 60—63.

¹⁶ «Экономика данных»: что будет в новом национальном проекте в России // Коммерсант. URL: <https://www.kommersant.ru/doc/6380045?ysclid=m4igh6h2i9279658719> (дата обращения: 10.09.2024). Продолжается работа по нацпроекту «Экономика данных». URL: <https://ac.gov.ru/news/page/novyy-nacproekt-ekonomika-dannyh-budet-realizovan-v-ramkah-8-federalnyh-proektov-27883?ysclid=m4iv8ws6wm207759537> (дата обращения: 12.02.2025); Новый национальный проект «Экономика данных» будет реализован в рамках 8 федеральных проектов. URL: <https://ac.gov.ru/news/page/novyy-nacproekt-ekonomika-dannyh-budet-realizovan-v-ramkah-8-federalnyh-proektov-27883?ysclid=m4iwhqhkj3102426462> (дата обращения: 14.01.2025).

ках нацпроекта предусмотрена поддержка ИТ-компаний и стартапов, которые разрабатывают как оборудование, так и программное обеспечение (ПО). Это будет способствовать увеличению доступности качественных современных телекоммуникационных сервисов и высокоскоростного Интернета для граждан, а также развитию инфраструктуры, включая сети спутниковой и мобильной связи¹⁷. В рамках нового национального проекта необходимо выделить вопросы, связанные с обеспечением информационной безопасности, устойчивости работы инфраструктуры Интернета; также сформирована новая задача, связанная с уменьшением преступлений, которые совершаются с использованием цифровых технологий. Кроме того, необходимо, на наш взгляд, отметить еще ряд задач, связанных с формированием больших данных, а также обеспечением защиты персональных данных¹⁸. Требуется реализации задачи обеспечения цифровой зрелости ключевых отраслей экономики, которая, в свою очередь, дополнена тем, что цифровая зрелость должна достигаться за счет массового внедрения цифровых платформ [8, с. 145; 9], перехода к использованию больших данных, искусственного интеллекта (ИИ) и машинного обучения¹⁹.

Распоряжением Правительства РФ от 28 декабря 2024 года № 4146-р утверждена «Стратегия пространственного развития Российской Федерации на период до 2030 года с прогнозом до 2036 года»²⁰, представляющая собой документ стратегического планирования, разработанный в рамках целеполагания по территориальному принципу²¹. Стратегия направлена на достижение национальных целей и учитывает текущие тенденции, новые вызовы и возможности развития регионов России. В рамках реализации Стратегии появилась возможность не только справиться с негативными тенденциями, но и использовать новые перспективы, а также своевременно реагировать на вызовы. Это, в свою очередь, будет способствовать достижению национальных целей. Также проводится комплексная работа по исполнению Основных направлений реализации положений Договора о создании Союзного государства на 2024—2026 гг. между Российской Федерацией и Республикой Беларусь, предусматривающие развитие совместных производств, защиту технологического суверенитета, создание новых промышленных мощностей

для обеспечения экономической стабильности Союзного государства²², создания объединенной транспортной и энергетической системы, проведения согласованной политики в социальной и культурной областях²³.

В целях обеспечения технологической независимости России Указом Президента РФ от 28 февраля 2024 г. № 145 утверждена Стратегия научно-технологического развития Российской Федерации²⁴, являющаяся основой для разработки отраслевых документов стратегического планирования в области научно-технического развития. В рамках реализации Стратегии сформировано нормативно-правовое регулирование системы управления в области науки и современных технологий. Производится запуск крупных научно-технических программ и проектов, направленных на реализацию стратегических инициатив Президента РФ в научно-технологической сфере. Кроме того, в целях обеспечения развития в основных социально значимых сферах (здравоохранение, жилищно-коммунальный комплекс, энергетика, сферы безопасности, культуры, образования, социальная сфера) проводится ускоренная разработка импортонезависимых технологий, локализация известных иностранных технологий, замещение устаревших технологий и увеличение экспорта отечественных наукоемких технологий и продукции²⁵. Правительством РФ также утверждена «Стратегия развития системы государственной статистики и Росстата»²⁶, способствующая выявлению потребностей пользователей в официальной статистической информации, достоверной, научно-обоснованной, прозрачной и достаточной для принятия управленческих решений и планирования статистической деятельности²⁷.

Следует отметить, что основные процессы, происходящие в сфере государственного управления в рамках эксперимента по переводу информационных систем и информационных ресурсов органов государственной власти Российской Федерации, государственных учреждений, в государственную единую облачную платформу, требуют обеспечить органы публичной власти РФ автоматизированными рабочими местами и отечественным программным обеспечением, использовать модель «общественное облако», обеспечить соответствие инфраструктуры требованиям информационной

²² Там же.

²³ ВГС утвердил Основные направления реализации положений Договора о создании СГ на 2024—2026 годы // Парламентское Собрание. URL: <https://belrus.ru/info/vgs-utverdil-osnovnye-napravleniya-realizacii-polozhenij-dogovora-o-sozdanii-sg-na-2024-2026-gody> (дата опубликования: 15.02.2025).

²⁴ Указ Президента РФ от 28.02.2024 № 145 «О Стратегии научно-технологического развития Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата опубликования: 12.02.2025).

²⁵ Там же.

²⁶ Распоряжение Правительства РФ от 30 декабря 2024 года № 4159-р «Стратегия развития системы государственной статистики и Росстата до 2030 года» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата опубликования: 12.02.2025).

²⁷ Там же.

¹⁷ Названы главные задачи нацпроекта «Экономика данных и цифровая трансформация государства». URL: https://www.cnews.ru/news/top/2024-06-26_mishustin_nazval_osnovnye_ysclid=m74si1zdud280760161 (дата обращения: 14.02.2025). Нормативное регулирование цифровой среды / Министерство экономического развития РФ. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/?ysclid=m4iksi1j5o859876740 (дата обращения: 12.02.2025).

¹⁸ Там же.

¹⁹ Там же.

²⁰ Стратегия пространственного развития Российской Федерации на период до 2030 года с прогнозом до 2036 года // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата опубликования: 15.02.2025).

²¹ Там же.

безопасности объектов критической информационной инфраструктуры, а также обеспечить промышленный суверенитет. Распоряжением Правительства РФ от 16 марта 2024 года № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления»²⁸ проводится корректировка стратегического направления в сфере государственного управления с учетом новых угроз национальной безопасности и существенного сокращения ресурсов развития. Посредством применения современных сервисов появилась возможность заменить мессенджеры на компьютерные программы для работы с документами, а также на сервисы видеоконференцсвязи. Внедряются также отечественные программы, соответствующие политике импортозамещения и направленные на укрепление технологического суверенитета Российской Федерации. Необходимо укрепление и поддержка в России информационных технологий и инфраструктуры, обеспечивающих независимость от иностранных технологий. Для реализации столь масштабных задач предусмотрены решения государственной политики в информационной сфере.

Так, Правительством РФ утвержден «Единый план по достижению национальных целей развития Российской Федерации до 2030 года и на перспективу до 2036 года»²⁹. В соответствии с поручением Президента РФ сформированы также стратегические приоритеты Правительства РФ по достижению национальных целей и характеризующих их показателей³⁰, направленные на достижение национальных целей, а также соответствующих показателей. Ключевыми факторами и инструментами, способствующими достижению показателей национальных целей, являются сокращение технологической зависимости отечественной экономики от иностранной продукции и технологий. В этой связи реализация мероприятий будет сосредоточена на разработке новых технологий, освоении производства на их основе и увеличении объемов производства отечественной продукции. Еще одним важным направ-

лением становится обеспечение сетевого суверенитета в области информационной безопасности в информационно-коммуникационной сети Интернет³¹.

В Послании Президента РФ Федеральному Собранию Российской Федерации были отмечены принципиально важные стратегические задачи для долгосрочного развития страны, связанные с защитой и укреплением суверенитета и безопасности. Изучение документа стратегического планирования, разработанного в рамках целеполагания в Стратегии научно-технологического развития России³², утверждённой Указом Президента РФ от 28 февраля 2024 года № 145, показывает, что он направлен на научно-технологическое обеспечение реализации задач и национальных приоритетов Российской Федерации. Его целью является необходимость достижения технологического суверенитета в разных сферах: средства производства и станки, робототехника, все виды транспорта, беспилотные авиационные, морские и другие системы, экономика данных, новые материалы и химия, способствующие устойчивости всей экономики страны. Представляется необходимым создание конкурентных продуктов, опирающиеся на уникальные отечественные разработки, в том числе в области космических, атомных и новых энергетических технологий. Особый интерес представляют элементы цифровых платформ, являющиеся алгоритмами искусственного интеллекта. На наш взгляд, необходимы новые обновления редакции Национальной стратегии развития искусственного интеллекта, должны быть поставлены новые цели и задачи, в режиме реального времени способствующие обеспечению технологического суверенитета по таким революционным направлениям, как генеративный искусственный интеллект и большие языковые модели [19, с. 18]. Для решения приоритетных задач требуется развитие всей инфраструктуры экономики данных³³. Сегодня важен переход цифровой среды к стратегии «цифрового глобального лидерства»³⁴. Необходимо понимать, что государство обладает полным контролем над технологиями, разрабатываемыми и используемыми в его пределах, может регулировать, контролировать и определять использование технологий в интересах национальной безопасности, экономики и социального развития. В этой связи технологический суверенитет может включать в себя различные аспекты, такие как контроль над ключевыми технологиями, включая генеративный искусственный интеллект, биотехнологии, нанотехнологии и космические технологии, а также

²⁸ Распоряжение Правительства РФ от 16 марта 2024 года № 637-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 12.02.2025; Постановление Правительства РФ от 15.04.2023 № 603 «Об утверждении приоритетных направлений проектов технологического суверенитета и проектов структурной адаптации экономики Российской Федерации и Положения об условиях отнесения проектов к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации, о представлении сведений о проектах технологического суверенитета и проектах структурной адаптации экономики Российской Федерации и ведении реестра указанных проектов, а также о требованиях к организациям, уполномоченным представлять заключения о соответствии проектов требованиям к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 12.02.2025.

²⁹ Единый план по достижению национальных целей развития Российской Федерации до 2030 года и на перспективу до 2036 года. URL: <http://static.government.ru>, 09.01.2025.

³⁰ Там же.

³¹ Там же.

³² Указ Президента РФ от 28 февраля 2024 г. № 145 «О Стратегии научно-технологического развития Российской Федерации // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 12.02.2025.

³³ Там же.

³⁴ Государство должно быть незаметным / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/events/39010> (дата обращения: 16.02.2025).

контроль над инфраструктурой цифрового общества, в том числе Интернетом, сетями связи и криптографией. Безусловно, технологический суверенитет является важным фактором обеспечения национальной безопасности, экономической конкурентоспособности и социального развития государства. Однако он также может вызывать определенные вопросы и ограничения, связанные с глобализацией и международным сотрудничеством в области технологий [10, с. 44; 11, с. 12; 12]. «Сегодня важны меры государственной поддержки разработчиков отечественного программного обеспечения...», как отмечалось в ходе дискуссии на сессии «Цифровой суверенитет»³⁵. Прежде всего, требуется масштабная государственная поддержка отечественных ИТ-производителей на глобальном рынке. Россия — одна из немногих стран, которая обладает конкурентоспособными ИТ-решениями и при масштабном экспорте ИТ-технологий может потенциально создать свой глобальный цифровой кластер. Только создание собственной глобальной цифровой повестки сможет обеспечить России не только цифровой суверенитет, но и глобальное цифровое лидерство³⁶.

Вывод

Таким образом, исследование показывает, что обеспечение цифрового суверенитета правовыми средствами требует комплексного подхода, включающего как международное, так и национальное законода-

тельство. Следует отметить, что приоритетными также являются: разработка доктрины информационного права, включая правовое обеспечение информационной (национальной и международной) безопасности, в том числе кибербезопасности, и достижение киберстабильности в свете принятия универсальной международной конвенции по противодействию киберпреступности, доктринальной модели развития системы информационного законодательства (включая цифровое), направленной на научное обоснование и упорядочение правового регулирования информационных отношений [4, с. 170].

Возрастает роль правовых инструментов, которые могут создать основу для защиты интересов государства и его граждан в постоянно меняющемся цифровом мире. Необходимо признать, что на современном этапе в условиях ускорения технологического прогресса и растущих угроз киберпространства вопросы, связанные с цифровым суверенитетом и правами граждан, приобретают приоритетное значение для решения стратегических задач, в том числе и правовых, имеющих ключевое значение для обеспечения национальной безопасности государства, включая информационную безопасность. Полагаем, что рассмотренные изменения в системе актов стратегического планирования в Российской Федерации имеют определяющее значение для развития государственной политики в рассматриваемой сфере. Однако очевидно также, что особое значение для формирования и реализации государственной политики имеет разработка и скорейшее принятие обновленной Доктрины информационной безопасности с учетом новых целей и задач, включая обеспечение кибербезопасности.

³⁵ Цифровой суверенитет: инструмент национальной кибербезопасности. URL: <https://roscongress.org/materials/tsifrovoy-suverenitet-kak-instrument-natsionalnoy-kiberbezopasnosti/?ysclid=m73djp64bh297539443> (дата обращения: 23.02.2025).

³⁶ Там же.

Литература

1. Троян Н.А., Петровская О.В. Систематизация законодательства Российской Федерации как одна из базовых задач в информационно-правовой среде // Шестые Бачиловские чтения : сборник статей участников международной научно-практической конференции / Отв. ред. Т.А. Полякова. М. : Институт государства и права РАН, 2023. 256 с.
2. Трансформация информационного права : монография / Отв. ред. Т.А. Полякова, А.В. Минбалева, В.Б. Наумов. М. : Институт государства и права РАН, 2023. 256 с.
3. Виноградова Е.В. Информационный суверенитет как основа единства конституционного-правового пространства современной России // Правовое обеспечение суверенитета и кодификация информационного законодательства : монография / Отв. ред. Т.А. Полякова, А.В. Минбалева, В.Б. Наумов. М. : Институт государства и права РАН, 2024. 237 с.
4. Полякова Т.А., Минбалева А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. № 1. 2025. С. 160—173.
5. Троян Н.А. Правовое обеспечение цифрового суверенитета России: актуальные проблемы и перспективные направления // Право и государство: теория и практика. 2024. № 6 (234). С. 169—172.

6. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Трансформация науки информационного права и информационного законодательства: новый этап в условиях научно-технологического развития России // Государство и право. 2024. № 9. С. 166—179.
7. Полякова Т.А., Троян Н.А., Петровская О.В. Правовое обеспечение укрепления технологического суверенитета Российской Федерации на основе реализации модели импортозамещения // Правовая политика и правовая жизнь. 2024. № 3. С. 281—293.
8. Полякова Т.А., Троян Н.А. Публично-правовые подходы к обеспечению государственного суверенитета в информационной сфере // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2024. Т. 10 (76). № 2. С. 143—151.
9. Карцхия А.А., Макаренко Г.И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4—19. DOI: 10.21681/1994-1404-2024-1-4-19.
10. Карцхия А.А. Технологический суверенитет и энергетическая безопасность // Предпринимательское право. 2024. № 1. С. 39—44.
11. Карцхия А.А., Макаренко Г.И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. 2024. № 1 (59). С. 2—14. DOI: 10.21681/2311-3456-2024-1-2-14.
12. Рыбаков О.Ю. Правовая информационная культура в условиях цифровой трансформации общества и государства // Правосудие. 2024. Т. 6. № 3. С. 59—74.

SECTION:
PRIVATE LAW

STRATEGIC TASKS OF SECURING TECHNOLOGICAL AND DIGITAL SOVEREIGNTY: THE LEGAL ASPECTS OF FORMATION OF A NEW INFORMATION ENVIRONMENT

Tat'iana Poliakova, Dr.Sc. (Law), Professor, Honoured Lawyer of the Russian Federation, Principal Researcher, Acting Head of the Sector of Information Technology Law and International Information Security of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.

E-mail: polyakova_ta@mail.ru

Natal'ia Troian, Ph.D. (Law), Senior Researcher at the Sector of Information Technology Law and International Information Security of the Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation.

E-mail: n-fadeeva@ya.ru

Keywords: *information sovereignty, digital sovereignty, reliable information, digital transformation, public administration, challenges, threats, legal regulation, artificial intelligence, high-tech technologies, digital platforms.*

Abstract

Purpose of the work: to study topical information and legal issues related to the increasing importance of the tasks of achieving Russia's national sovereignty in the information sphere under the influence of digital transformation.

Methods used in the study: the author uses general scientific methods of analysis and synthesis, as well as a system method that allows analyzing the state and problems of the development of information legislation in Russia in areas using digital technologies.

Study findings: the authors drew attention to important problems related to ensuring technological and digital sovereignty in the context of the implementation of strategic objectives of the scientific and technological development of the Russian Federation. In connection with the adoption of new national projects aimed at the development of the data economy and the digital transformation of management, the role of information law is increasing not only as a new scientific direction, but also as a public law (state-legal) science, which is faced with the task of developing its theory in the context of the formation of the data economy, as well as solving strategic tasks to ensure national priorities for scientific and technological development and information security, including cybersecurity issues. The study substantiates the conclusion that the implementation of new strategic tasks of scientific and technological development and the achievement of national technological and digital sovereignty in the information sphere requires the development of national state policy aimed at the legal support

of information security, including the protection of cybersecurity. It seems that these measures will ensure the protection of information security. sovereignty of Russia, protection of subjects and objects of high-tech technologies, innovative infrastructure.

Research novelty: the transition of modern society to digital technologies and the achievement of digital technological sovereignty in modern conditions, in our opinion, is possible through the development of organizational and legal mechanisms based on the analysis of the security of digital data, the formation of a safe digital environment with the necessary level of digital maturity. It is established that the achievement of technological and digital sovereignty of Russia is undoubtedly associated with the development of public law science, interdisciplinary approaches to the search for legal, fundamental solutions in order to ensure the national security of the country. The authors note that the priority should be: the development of the doctrine of information law, including the legal support of information (national and international), security, including cybersecurity and the achievement of cyber stability, in the light of the adoption of universal international documents on combating cybercrime; doctrinal model of development of the system of information legislation (including digital), aimed at scientific substantiation, streamlining of legal regulation of information relations.

References

1. Troian N.A., Petrovskaia O.V. Sistematizatsiia zakonodatel'stva Rossiiskoi Federatsii kak odna iz bazovykh zadach v informatsionno-pravovoi srede. Shestye Bachilovskie chteniia : sbornik statei uchastnikov mezhdunarodnoi nauchno-prakticheskoi konferentsii. Otv. red. T.A. Poliakova. M. : Institut gosudarstva i prava RAN, 2023. 256 pp.
2. Transformatsiia informatsionnogo prava : monografiia. Otv. red. T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava RAN, 2023. 256 pp.
3. Vinogradova E.V. Informatsionnyi suverenitet kak osnova edinstva konstitutsionnogo-pravovogo prostranstva sovremennoi Rossii. Pravovoe obespechenie suvereniteta i kodifikatsiia informatsionnogo zakonodatel'stva : monografiia. Otv. red. T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava RAN, 2024. 237 pp.
4. Poliakova T.A., Minbaleev A.V., Naumov V.B. Sovremennye priority razvitiia informatsionnogo prava: pravovoe obespechenie gosudarstvennogo suvereniteta i informatsionnoi bezopasnosti v informatsionnom prostranstve Rossii. Gosudarstvo i pravo. No. 1. 2025. Pp. 160–173.
5. Troian N.A. Pravovoe obespechenie tsifrovogo suvereniteta Rossii: aktual'nye problemy i perspektivnye napravleniia. Pravo i gosudarstvo: teoriia i praktika. 2024. No. 6 (234). Pp. 169–172.
6. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Transformatsiia nauki informatsionnogo prava i informatsionnogo zakonodatel'stva: novyi etap v usloviakh nauchno-tekhnologicheskogo razvitiia Rossii. Gosudarstvo i pravo. 2024. No. 9. Pp. 166–179.
7. Poliakova T.A., Troian N.A., Petrovskaia O.V. Pravovoe obespechenie ukrepleniia tekhnologicheskogo suvereniteta Rossiiskoi Federatsii na osnove realizatsii modeli importozameshcheniia. Pravovaia politika i pravovaia zhizn'. 2024. No. 3. Pp. 281–293.
8. Poliakova T.A., Troian N.A. Publichno-pravovye podkhody k obespecheniiu gosudarstvennogo suvereniteta v informatsionnoi sfere. Uchenye zapiski Krymskogo federal'nogo universiteta imeni V.I. Vernadskogo. Iuridicheskie nauki. 2024. T. 10 (76). No. 2. Pp. 143–151.
9. Kartskhiia A.A., Makarenko G.I. Pravovye problemy primeneniia iskusstvennogo intellekta v Rossii. Pravovaia informatika. 2024. No. 1. Pp. 4–19. DOI: 10.21681/1994-1404-2024-1-4-19.
10. Kartskhiia A.A. Tekhnologicheskii suverenitet i energeticheskaiia bezopasnost'. Predprinimatel'skoe pravo. 2024. No. 1. Pp. 39–44.
11. Kartskhiia A.A., Makarenko G.I. Pravovye gorizonty tekhnologii iskusstvennogo intellekta: natsional'nyi i mezhdunarodnyi aspekt. Voprosy kiberbezopasnosti. 2024. No. 1 (59). Pp. 2–14. DOI: 10.21681/2311-3456-2024-1-2-14.
12. Rybakov O.Iu. Pravovaia informatsionnaia kul'tura v usloviakh tsifrovoy transformatsii obshchestva i gosudarstva. Pravosudie. 2024. T. 6. No. 3. Pp. 59–74.

ТОВАРНЫЕ ЗНАКИ В МЕТАВСЕЛЕННОЙ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Коданева С.И.¹

Ключевые слова: средства индивидуализации, невзаимозаменяемые токены, NFT, торговая марка, метавселенная, виртуальные товары, социальные сети, цифровые сервисы, цифровые права, имущественные права.

Аннотация

Цель работы: анализ трансформации концепции товарных знаков в условиях развития виртуальных пространств — метавселенных, определении того, подлежат ли правовой охране исключительные права на товарные знаки в отношении виртуальных «товаров» и если да, то требуют ли они дополнительного законодательного закрепления.

Методы исследования: общенаучные и специальные методы научного познания — методы логического анализа, анализа законодательства, научной и деловой литературы, сравнительного анализа, систематизации и обобщения.

Результаты: исследование позволило сделать следующие выводы. Во-первых, обоснована необходимость законодательного закрепления правового режима невзаимозаменяемых токенов в качестве правоудостоверяющих документов. Во-вторых, сделан вывод о том, что исключительные права на товарные знаки, зарегистрированные в отношении физических товаров, не могут распространяться на виртуальные «товары», а в случае использования соответствующих обозначений в виртуальном пространстве третьими лицами с целью извлечения прибыли подлежит применению законодательство о защите конкуренции.

DOI: 10.24412/1994-1404-2025-1-79-85

Введение и постановка задачи

В последние годы ускорилось развитие метавселенной — концепции онлайн-мира в виртуальном пространстве, объединяющего криптовалюту, финансы, работу и социальные сети и позволяющего людям взаимодействовать через своих аватаров, испытывая при этом ощущения, близкие к обычной реальности. Единого общепризнанного определения метавселенной на настоящий момент не существует. Одни авторы обращают внимание на характеристики метавселенной как новой виртуальной среды, именуя ее следующим поколением Интернета или даже новым общественным пространством, другие акцентируются на технологической составляющей [1]. Часть авторов ограничивается общими словами о том, что метавселенная является точкой пересечения реального и виртуального миров. Например, К. Бхугаонкар с соавторами подчеркивают, что метавселенная включает в себя интеграцию и наложение цифрового и физического мира, интеграцию цифровой и реальной экономики, цифровой и социальной жизни, цифровой и реальной идентичности и цифровых и физических активов [5, с. 2]. Другие стараются дать как можно более подробное определение. Например, согласно И.В. Понкину, «кибер-мета-вселенная — это формируемое

и поддерживаемое посредством интероперабельных динамических цифровых моделирований и синтеза сложное виртуально-реальное (гибридное) гомеостатическое и персистентное цифровое многопользовательское мета-пространство, включающее множество децентрализованных и/или интерсекциональных реально-виртуальных мультимасштабных (и масштабируемых) трёхмерных пространственных миров (эко-систем, универсумов) сложно-когнитивного и голографически-визуального порядков (дополненной или воспроизведённой реальности — согласованно и сообразно с естественными законами физического бытия и человеческого восприятия, понимания и преобразования мира), с обеспечением интерактивности вовлечения (участия, взаимодействия, активного преобразования) пользователя через его аватар и с обеспечением иммерсивности погружения пользователя в онтологию этих миров» [4, с. 119].

Общепризнанным является то, что метавселенная базируется на восьми фундаментальных технологиях — это расширенная реальность (синтез виртуальной, дополненной и смешанной реальности), человеко-компьютерное взаимодействие, искусственный интеллект, блокчейн, компьютерное зрение, Интернет

¹ **Коданева Светлана Игоревна**, кандидат юридических наук, доцент, ведущий научный сотрудник отдела правоведения ИНИОН РАН, доцент РГУ нефти и газа им. И.М. Губкина, г. Москва, Российская Федерация. ORCID: 0000-0002-8232-9533.

E-mail: kodanevas@gmail.com

вещей и робототехника, пограничные и облачные вычисления, а также мобильные сети будущего [12, с. 4]. Сочетание этих технологий придает метавселенной ее уникальные характеристики — иммерсивность² и персистентность³.

Изначально метавселенная использовалась исключительно в игровых целях, затем она стала рассматриваться как более продвинутая версия социальных сетей [1]. Однако технические возможности метавселенной делают ее привлекательной не только для игр и общения, но также для создания виртуальных миров и новых видов бизнеса в них, использования в добывающей и перерабатывающей промышленности, государственном управлении, образовании и здравоохранении.

Поэтому многие компании экспериментируют с такими виртуальными пространствами, в том числе в целях продвижения с их помощью своих товаров и расширения клиентской базы. Это, в свою очередь, порождает юридические вопросы, связанные с регистрацией и защитой средств индивидуализации, используемых как самими правообладателями в отношении реальных товаров и услуг, так и компаниями, ведущими свой бизнес исключительно в виртуальном пространстве.

Таким образом, как законодательство, так и сама концепция средств индивидуализации, в частности, товарных знаков, требуют переосмысления и актуализации с учетом новых видов общественных отношений, складывающихся в метавселенной.

Трансформация концептуальных основ правового режима товарных знаков в метавселенной

Права на товарные знаки служат важнейшими правовыми механизмами защиты коммерческих интересов их правообладателей и потребителей товаров. С одной стороны, они позволяют идентифицировать происхождение товара, что облегчает потребителям выбор. С другой стороны, исключительное право на товарный знак позволяет правообладателю защититься от несанкционированного использования его репутации и недобросовестной конкуренции. Таким образом, обращаясь к природе товарных знаков, следует обратить внимание на два ключевых момента. Во-первых,

исключительное право на товарный знак не означает абсолютного права на соответствующее обозначение, поскольку это исключительное право не абстрактно, а существует только применительно к конкретному физическому товару, в отношении которого оно зарегистрировано. Поэтому, во-вторых, товарный знак — это не просто узнаваемое изображение. Он существует во взаимосвязи с товаром, передавая потребителю информацию о нем. Именно поэтому права на товарный знак действуют только при маркировке товаров и могут быть досрочно прекращены при длительном неиспользовании. Эта взаимосвязь между обозначением и маркируемым им физическим товаром традиционно была концептуальной основой правового статуса товарных знаков. Поэтому, например, упоминание зарегистрированного словесного обозначения в литературном произведении рассматривалось не как нарушение прав на товарный знак, а как проявление художественного творчества автора.

Однако с развитием технологий, в частности, появлением Интернета, этот концептуальный фундамент стал давать трещины, поскольку зарегистрированные обозначения стали использоваться уже не только для маркировки, но и в целях рекламы. Соответственно, ст. 1484 Гражданского кодекса РФ относит к использованию исключительного права на товарный знак размещение его в предложениях о продаже товаров, о выполнении работ, об оказании услуг, а также в объявлениях, на вывесках и в рекламе, а также в сети Интернет, в том числе в доменном имени и при других способах адресации.

Развитие метавселенной с ее уникальными характеристиками еще больше подрывает традиционный взгляд на сущность товарных знаков, поскольку она по своей природе стирает границы между физической и цифровой сферами. В частности, возникает вопрос: распространяется ли исключительное право на товарный знак, зарегистрированный в отношении одежды, обуви или аксессуаров, на цифровые представления соответствующих предметов? Вопрос этот не праздный, поскольку в метавселенной складывается рынок подобных товаров для аватаров и даже цифровых двойников пользователей. Например, один мужчина купил цифровое платье за 9500 долларов для подарка жене, чтобы она могла «надеть» его в социальных сетях [9, р. 87].

Другой вопрос связан с тем, где заканчиваются границы правовой охраны товарного знака и начинается защита прав авторов на свободу художественного творчества. Примером может служить дело “ESS Entertainment 2000, Inc. vs Rock Star Videos, Inc.”, в котором рассматривался вопрос о том, нарушало ли виртуальное изображение реального стриптиз-клуба в популярной игре “Grand Theft Auto: San Andreas” права на логотип стрип-клуба и товарный знак. В конечном счете суд постановил: нарушения не было, поскольку игра была произведением искусства, защищенным свободой слова и самовыражения в соответствии с Первой поправ-

² Иммерсивность среды — это ее свойство обеспечивать возможности и способности субъективно реалистичного или близкого к реалистичному ощущения присутствия пользователя в этой среде за счет гибридной мультисенсорной перцептивной обратной связи (в том числе тактильной, т. е. осязательной), проживания и переживания (полным спектром ощущений) им в режиме реального времени бытия внутри этой среды (универсума) как вполне реально [4, с. 119].

³ Персистентность среды — свойство сохранять все свои предыдущие состояния и доступ к этим состояниям при внесении в них каких-то изменений (в том числе на основе блокчейн-технологий), в том смысле, что в условиях неподключенности ни одного пользователя, система продолжает работать, а достигнутые позиции пользователей по состоянию при закрытии их сеансов сохраняются, загружаясь в момент следующего подключения [4, с. 119].

кой к Конституции США, и потребители вряд ли были введены в заблуждение, полагая, что эта сложная виде-игра была создана стриптиз-клубом [9].

И если данное дело вполне вписывается в традиционные концепции авторского права и прав на средства индивидуализации, то использование последних в NFT-токенах заставляет по-новому взглянуть на границы между этими двумя типами объектов интеллектуальной собственности. Связано это с тем, что складывающаяся судебная практика определяет NFT-токены в качестве объектов авторского права как сами по себе (поскольку они являются программами для ЭВМ), так и во взаимосвязи с теми произведениями, права на которые они удостоверяют. Однако в метавселенных, особенно децентрализованных, основанных на блокчейне, гражданский оборот различных активов осуществляется посредством оборота NFT-токенов, выполняющих функцию цифровых сертификатов, удостоверяющих права на соответствующий актив. Возникает вопрос: следует ли относить защищенные обозначения, используемые в таком токене, в качестве средства индивидуализации или объекта авторского права?

Если исходить из традиционной концепции товарных знаков, то, вероятно, верным должно быть второе, поскольку обозначение не маркирует физический товар, а становится самоценным само по себе, чего быть не должно. С этой точки зрения регистрация исключительного права на товарный знак в отношении такого класса товаров, как NFT-токены, не должна допускаться. Однако практика, отвечая на потребности трансформирующегося гражданского оборота, пошла по иному пути, расширяя и видоизменяя традиционные подходы к пониманию концептуального содержания института средств индивидуализации.

Практика охраны товарных знаков в метавселенной

В РФ пока что использование товарных знаков в метавселенной и, соответственно, споры об их защите не получили широкого распространения. Тем не менее в зарубежных странах, и прежде всего в США, такая практика уже начала складываться.

Многие крупные компании стремятся защитить свои права и репутацию, регистрируя товарные знаки в таких классах, как компьютерные программы (класс 9), услуги розничных магазинов с виртуальными «товарами» (класс 35), развлекательные услуги (класс 41), онлайн-овые не загружаемые виртуальные «товары» и невзаимозаменяемые токены (NFT) (класс 42), а также финансовые услуги, включая цифровые токены (класс 36). Так, в США заявки на регистрацию подали такие марки одежды, как Nike, New Balance, Skechers, Forever, Victoria's Secret, Kiehl's, Burberry, Dolce & Gabbana, Ralph Lauren, Tommy Hilfiger и др.; кафе, например, McDonald's, журналы, такие как Bon Appetit, Wired, Vanity Fair, Vogue и GQ [13]. Регистрируют товарные знаки в этих классах и другие компании. Например, Miracle-

gro в отношении товаров для виртуального сада, Tomcat & Design — в отношении ловушек для виртуальных мышей, Johnson & Johnson — в отношении пластырей для аватаров. Эстафету подхватили и некоторые спортсмены, например, Shaquille O'Neal, Kobe Bryant и Luka Doncic [9].

При этом многие из этих компаний указывают на то, что планируют использовать зарегистрированное обозначение в будущем. То есть даже те из них, кто пока не готовы развивать свой бизнес в виртуальном пространстве, стремятся себя обезопасить от рисков использования их марок третьими лицами. Связано это с участвовавшими в последние годы судебными спорами о незаконном использовании товарных знаков в метавселенной. Наибольшую известность получили дела "Hermès International v. Rothschild", "Yuga Labs v. Ryder Ripps" и "Nike v. StockX" в США, а также дело "Juventus v. Blokeras", рассмотренное судом Рима.

Каждое из этих дел интересно по-своему, поскольку отражает различные способы использования средств индивидуализации в метавселенной.

Так, спор "Hermès International v. Rothschild" был связан с тем, что М. Ротшильд выпустил серию NFT-токенов, содержащих созданные им изображения знаменитых сумок Birkins от Hermès, назвав их «MetaBirkins». Важно отметить, что не все эти изображения полностью воспроизводили пресловутые сумки. Некоторые из них просто были выполнены в стиле Birkins. Тем не менее автор развернул широкую кампанию в метавселенной и социальных сетях, предлагая свои MetaBirkins к продаже по цене, близкой к стоимости оригинальных сумок Hermès. Он открыто заявлял, что это «дань уважения» знаменитым сумочкам. Еще одной важной деталью было то, что не только пользователи социальных сетей были введены в заблуждение, но даже известные модные журналы Elle и The New York Post опубликовали новость о том, что Hermès реализует этот виртуальный проект совместно с М. Ротшильдом [7]. Когда Hermès подала в суд, ответчик защищался, ссылаясь на свободу художественного творчества, Первую поправку к Конституции США и так называемый тест Роджерса, сформулированный в деле "Rogers v. Grimaldi". Второй окружной суд в своем прецедентном решении исходил из рассмотренной выше традиционной концепции товарного знака, поэтому полагал, что использование соответствующих обозначений в художественном творчестве не может нарушать исключительного права на средство индивидуализации, если только это использование имеет хотя бы минимальный художественный смысл и не вводит в заблуждение [6]. Иными словами, порог признания правомерности использования крайне низкий, на что и рассчитывал М. Ротшильд. Однако суд присяжных принял решение в пользу Hermès, сославшись на то, что ответчик использовал те же каналы продвижения для своих NFT-токенов, что и истец (Интернет и социальные сети) и что его рекламная компания ввела в заблуждение не только рядовых потребителей, но даже и модные журналы.

Во втором деле Yuga Labs создала NFT-токены под названием «Клуб „Яхта скучающей обезьяны“» (Bored Ape Yacht Club или BAYC) — изображения обезьян с различным выражением лица и одеждой. Коллекция BAYC стала одной из самых известных и успешных коллекций NFT-токенов в мире, привлекла значительное внимание средств массовой информации и была представлена в журналах Rolling Stone и Forbes. В мае 2022 г. художник-концептуалист Р. Риппс выпустил свою собственную коллекцию NFT-токенов под названием Ryder Ripps Bored Ape Yacht Club (RR/BAYC), в которой были представлены те же цифровые иллюстрации, что и в коллекции BAYC NFT. Соответственно, Yuga Labs подала в суд, ссылаясь на то, что коллекция Р. Риппса продавалась как «ложно эквивалентная» их коллекции, что привело к падению цен на оригинальные NFT-токены и нарушила права истца на товарный знак. Ответчик, также как и в предыдущем деле, пытался сослаться на первую поправку к Конституции США. Однако суд вынес решение в пользу истца, в целом повторив аргументацию из дела “Hermès International v. Rothschild”. Однако он также сформулировал еще один важный вывод о том, что тест Роджерса неприменим к создателям NFT-токенов, если они преследовали исключительно коммерческую цель, а не цель самовыражения, защищаемую Первой поправкой [10].

Дело “Nike v. StockX”, начавшееся также в 2022 г. и по сей день находящееся на рассмотрении суда, интересно тем, что NFT-токены содержали изображения реальной обуви, что позволяет ответчику утверждать, что они выполняют функцию квитанции, подтверждающей покупку конкретной пары обуви, и сослаться на принцип исчерпания права. В свою очередь, Nike обращает внимание на явно и чрезмерно завышенную цену, которую покупатели платят за эти NFT-токены, что свидетельствует о том, что они выполняют инвестиционную функцию, а также на якобы обнаруженные ею не менее 77 пар поддельных кроссовок. Кроме того, компания уже купила участок земли в Roblox для создания Nikeland, где посетители могут не только поиграть в «классические игры на новый лад», но и заглянуть в онлайн-салон виртуальной обуви, одежды и аксессуаров Nike, а также приобрести «бесплатные эксклюзивные кепку и рюкзак Nike», которые можно взять с собой в любую точку Roblox. Соответственно, Nike подала заявку на регистрацию своих товарных знаков для этих виртуальных «товаров» и утверждает, что NFT-токены StockX нарушают ее исключительные права. Исход этого спора будет иметь важное значение для определения правового статуса NFT-токенов [8]. Если суд встанет на сторону Nike, это подтвердит ранее сложившуюся практику признания единства токена и содержащегося в нем объекта. В этом случае NFT-токены будут рассматриваться как товар, который подпадает под действие законодательства о средствах индивидуализации, то есть создателям токенов понадобятся лицензии на использование соответствующих обозначений в своих NFT. В случае же победы StockX NFT-токены

будут признаны сертификатами, удостоверяющими права на реальные или виртуальные товары, а следовательно, судебные споры должны будут касаться не самих токенов, а таких товаров. К слову, данный подход будет соответствовать новой редакции МКТУ, вступившей в силу 1 января 2023 г., согласно которой NFT рассматриваются как уникальные цифровые сертификаты, зарегистрированные в блокчейне, которые аутентифицируют цифровые элементы, но отличаются от них.

Наконец, в деле “Juventus v. Bokeras” ответчик создал коллекционные NFT-токены с изображением футболиста К. Вьери, одетого в официальную форму Ювентуса. Суд постановил, что товарные знаки Ювентуса широко известны общественности и активно продвигаются по маркетинговым каналам, что делает их широко известными и имеющими право на более широкую защиту. Суд пришел к выводу, что создание и чеканка NFT-токенов с изображением известных товарных знаков создают риск возникновения путаницы среди потребителей, которые могут поверить, что Ювентус каким-либо образом участвовал в создании спорной коллекции [6].

Научная дискуссия о правовом регулировании товарных знаков в метавселенной

Как можно видеть из приведенной судебной практики, использование защищенных средств индивидуализации в метавселенной поднимает концептуальные вопросы о том, подлежат ли товарные знаки охране применительно к цифровым объектам и если да, то каким образом.

Как показывает анализ научной литературы, подходы к ответам на эти вопросы довольно сильно различаются. Так, если следовать традиционному пониманию природы товарных знаков как обозначений, предназначенных исключительно для маркировки физически существующих товаров и не имеющих самостоятельной ценности, то можно прийти к выводу, что регистрация прав на них в отношении виртуальных предметов недопустима, поскольку превращает права на товарный знак в абстрактную защиту брендов, т. е. компаний, а не товаров. Как отмечает Марк Маккена, цифровая обувь не обладает ни одной из характеристик реальной обуви. Знаки, используемые в отношении этих «товаров», не несут никакой информации, которую законодательство о товарных знаках и доктрина всегда рассматривали как основополагающую для возникновения права. Это информация о происхождении и характеристиках маркируемых товаров, поскольку компания-производитель, обладающая товарным знаком, контролирует качество и не допускает появления контрафактных товаров. Поэтому автор предлагает с осторожностью подходить к регистрации прав на товарные знаки в метавселенной [7].

Впрочем, большинство авторов сходятся в том, что товарные знаки на виртуальные товары должны защищаться, хотя и признают, что распространить охрану,

предоставленную реальным товарам, на метавселенную, скорее всего, не удастся. И если крупные бренды, университеты и спортивные клубы еще имеют шанс выиграть суды, ссылаясь на свою широкую известность и вероятность путаницы, как в случае с Hermès и Juventus, менее знаменитым компаниям лучше зарегистрировать свои знаки специально для метавселенной в 9, 35, 36, 41, 42 и 45 классах МКТУ (см., например, [8—10, 12, 13]). А. Кхан дополнительно предлагает пересмотреть традиционный подход к ограничению охраны товарных знаков и праве использовать их в авторских произведениях применительно к NFT. Она утверждает, что ключевым в этом вопросе должно быть установление цели создания токена. И если эта цель сугубо коммерческая, то такой объект не должен охраняться правом автора на самовыражение. Его следует квалифицировать как подделку, нарушающую права на товарный знак [6].

Ч. Соу и Ж. Чан обратили внимание на проблему юрисдикции споров о нарушении товарных знаков. По общему правилу, правообладатель должен обращаться в суд той страны, где его права зарегистрированы и нарушены. Однако в случае метавселенной это правило реализовать практически невозможно. Поэтому авторы, опираясь на доктрину *"forum non conveniens"*, предлагают рассматривать такие дела в стране, где проживают потребители соответствующих виртуальных «товаров» и рекламы, при том условии, что в этой стране зарегистрированы права на товарный знак. Они также предлагают ряд подходов к определению местонахождения пользователей, начиная от требований к авторизации при входе в метавселенную и заканчивая различными техническими средствами отслеживания интернет-трафика [11].

Выводы

Представленное исследование научной литературы и практики защиты товарных знаков позволяет сделать следующие выводы.

Во-первых, до сих пор в российском законодательстве прямо не урегулирован статус невзаимозаменяемых токенов (NFT), что является существенным пробелом, особенно в условиях развития метавселенных. Представляется необходимым законодательное закрепление статуса данного объекта. При этом, определяя его правовую природу, следует согласиться с Д.С. Емельяновым [2] в том, что такие токены не являются самостоятельными объектами права, а только подтвержда-

ют права на другие объекты. Однако вызывает вопросы вывод автора о необходимости распространения на NFT действия Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Более обоснованной выглядит позиция П.И. Петкилёва [3], который доказывает, что невзаимозаменяемый токен не может быть признан цифровым активом, поскольку он схож с *"traditio longa manu"*. В связи с этим представляется, что данный вид токенов следует признавать в качестве правоподтверждающего документа, удостоверяющего право собственности на записанное в нем имущество.

Во-вторых, следует признать, что исключительные права на товарные знаки, зарегистрированные в отношении физических товаров (одежда, обувь и т. д.), не могут распространяться на виртуальные «товары», поэтому правообладатели, желающие защитить свои обозначения в метавселенной, должны регистрировать права в отношении соответствующих классов товаров и услуг. Однако следует учитывать, что в соответствии с Гражданским кодексом РФ неиспользование товарного знака в течение трех лет может служить основанием для досрочного прекращения его охраны. Соответственно, для компаний возникает дилемма, если они, с одной стороны, не готовы расширять свой бизнес в виртуальном пространстве, но, с другой стороны, опасаются, что их товарными знаками в метавселенной могут воспользоваться третьи лица, что, скорее всего, не будет признано нарушением в силу того, что такое использование явно не подпадает ни под охраняемые, ни под смежные классы товаров и услуг. В данной ситуации наиболее эффективным может быть применение статьи 14.6 Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции», «Запрет на недобросовестную конкуренцию, связанную с созданием смешения», при этом ключевым критерием для применения данной статьи антимонопольными органами должна быть цель создания виртуальных объектов с использованием зарегистрированного средства индивидуализации. Если такие объекты являются всего лишь визуальной частью пространства метавселенной и имеют чисто художественное значение, то такое деяние не должно признаваться нарушением. Напротив, если единственной целью создания соответствующих виртуальных объектов является их коммерческое использование, т. е. извлечение прибыли, то это, очевидно, образует состав правонарушения.

Литература

1. Батурин Ю.М., Полубинская С.В. Реальный мир как дополнение метавселенной (грядущие трансформации права) // Государство и право. 2023. № 11. С. 155—169.
2. Емельянов Д.С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования / Д.С. Емельянов, И.С. Емельянов // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 71—76.

3. Петкилёв П.И. Невзаимозаменяемый токен (NFT) как объект гражданского права // Законодательство. 2022. № 7. С. 15—21.
4. Понкин И.В. Кибер-мета-вселенная: правовой взгляд // International Journal of Open Information Technologies. 2023. Т. 11. № 1. С. 119.
5. Bhugaonkar K., Bhugaonkar R., Masne N. The Trend of Metaverse and Augmented and Virtual Reality Extending to the Healthcare System. Cureus. 2022. Vol. 14. No. 9. P. 2.
6. Khan A. The Ultimate Metaverse Match: An Analysis of First Amendment Protections and Unauthorized Trademark Use in Non-Fungible Tokens. SMU Law Review. 2023. Vol. 76. No. 4. P. 975–998.
7. McKenna M.P. Trademarks in the Metaverse. IPSC Conference at Stanford. 2022. URL: [https://www.law.nyu.edu/sites/default/files/Mark McKenna - Trademarks in the Metaverse.pdf](https://www.law.nyu.edu/sites/default/files/Mark%20McKenna%20-%20Trademarks%20in%20the%20Metaverse.pdf)
8. Roibu A.N. Protection in a Virtual Reality: The Dire Need for Trademark and Copyright Law Expansion to Encompass Digital Content Within the Metaverse. Touro Law Review. 2024. Vol. 39. No. 4. P. 1455–1518.
9. Ryan H.S. Trademarking Virtual Goods in the Metaverse: Just Because You Can't Touch Them Doesn't Mean They Aren't Real. Florida Entertainment and Sports Law Review. 2022. Vol. 1. No. 2. P. 81–97.
10. Santiago M.L. The Legal Challenges of the Metaverse: Business Trademarks. 8th International Scientific-Business Conference LIMEN 2022 – Conference Proceedings. 2023. P. 357–370.
11. Saw C.L., Chan Zh.W.S. The Subsistence and Enforcement of Copyright and Trademark Rights in the Metaverse // Journal of Intellectual Property Law & Practice. 2024. Vol 19. No. 4. P. 371–384.
12. Wang Yue, Zhu Mengying, Chen Xi, Liu Ruibin, Ge Jinnian, Song Yuxuan, Yu Guilin. The Application of Metaverse in Healthcare. Frontiers in Public Health. 2024. Vol. 12. P. 1–9.
13. Vaughan-Jones J. Fashion Forward: How Luxury Brands, Handbags, and NFTs are Shaping the Future of Trademark Law in the Metaverse and Beyond. North Carolina Journal of Law & Technology. 2022. Vol. 24. No. 2. P. 134–170.

SECTION:
PRIVATE LAW

TRADEMARKS IN THE METAVERSE: PROBLEMS OF LEGAL REGULATION

Svetlana Kodaneva, Ph.D. (Law), Leading Researcher at the Department of Legal Studies of the Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences, Associate Professor at the Gubkin National Research University of Oil and Gas, Moscow, Russian Federation. ORCID: 0000-0002-8232-9533.

E-mail: kodanevas@gmail.com

Keywords: means of individualization, non-fungible tokens, NFT, trademark, metaverse, virtual goods, social networks, digital services, digital rights, property rights.

Abstract

Purpose of the work: analysing the transformation of the concept of trademarks in the context of the development of virtual spaces, metaverses; to determine whether exclusive rights to trademarks in relation to virtual goods are subject to legal protection and, if so, whether they require additional legislative consolidation.

Methods used in the study: both general scientific and special methods of scientific cognition, such as methods of logical analysis, analysis of legislation, scientific and business literature, comparative analysis, systematization and generalization.

Study findings: the study allowed to make the following conclusions. Firstly, the need for legislative consolidation of the legal regime of non-fungible tokens as documents of title is substantiated. Secondly, it is concluded that the exclusive rights to trademarks registered in relation to physical goods cannot apply to virtual goods; and in the case of the use of the relevant designations in the virtual space third parties are subject to the application of competition law for the purpose of making a profit.

References

1. Baturin Iu.M., Polubinskaia S.V. Real'nyi mir kak dopolnenie metavselennoi (griadushchie transformatsii prava). Gosudarstvo i pravo. 2023. No. 11. Pp. 155–169.
2. Emel'ianov D.S. Nevzaimozameniaemye tokeny (NFT) kak samostoiatel'nyi ob'ekt pravovogo regulirovaniia. D.S. Emel'ianov, I.S. Emel'ianov. Imushchestvennye otnosheniia v Rossiiskoi Federatsii. 2021. No. 10 (241). Pp. 71–76.

3. Petkilev P.I. Nevzaimozameniaemyi token (NFT) kak ob"ekt grazhdanskogo prava. *Zakonodatel'stvo*. 2022. No. 7. Pp. 15–21.
4. Ponkin I.V. Kiber-meta-vselennaia: pravovoi vzgliad. *International Journal of Open Information Technologies*. 2023. T. 11. No. 1. P. 119.
5. Bhugaonkar K., Bhugaonkar R., Masne N. The Trend of Metaverse and Augmented and Virtual Reality Extending to the Healthcare System. *Cureus*. 2022. Vol. 14. No. 9. P. 2.
6. Khan A. The Ultimate Metaverse Match: An Analysis of First Amendment Protections and Unauthorized Trademark Use in Non-Fungible Tokens. *SMU Law Review*. 2023. Vol. 76. No. 4. P. 975–998.
7. McKenna M.P. Trademarks in the Metaverse. IPSC Conference at Stanford. 2022. URL: [https://www.law.nyu.edu/sites/default/files/Mark McKenna - Trademarks in the Metaverse.pdf](https://www.law.nyu.edu/sites/default/files/Mark%20McKenna%20-%20Trademarks%20in%20the%20Metaverse.pdf)
8. Roibu A.N. Protection in a Virtual Reality: The Dire Need for Trademark and Copyright Law Expansion to Encompass Digital Content Within the Metaverse. *Touro Law Review*. 2024. Vol. 39. No. 4. P. 1455–1518.
9. Ryan H.S. Trademarking Virtual Goods in the Metaverse: Just Because You Can't Touch Them Doesn't Mean They Aren't Real. *Florida Entertainment and Sports Law Review*. 2022. Vol. 1. No. 2. P. 81–97.
10. Santiago M.L. The Legal Challenges of the Metaverse: Business Trademarks. 8th International Scientific-Business Conference LIMEN 2022 – Conference Proceedings. 2023. P. 357–370.
11. Saw C.L., Chan Zh.W.S. The Subsistence and Enforcement of Copyright and Trademark Rights in the Metaverse. *Journal of Intellectual Property Law & Practice*. 2024. Vol 19. No. 4. R. 371–384.
12. Wang Yue, Zhu Mengying, Chen Xi, Liu Ruibin, Ge Jinnian, Song Yuxuan, Yu Guilin. The Application of Metaverse in Healthcare. *Frontiers in Public Health*. 2024. Vol. 12. P. 1–9.
13. Vaughan-Jones J. Fashion Forward: How Luxury Brands, Handbags, and NFTs are Shaping the Future of Trademark Law in the Metaverse and Beyond. *North Carolina Journal of Law & Technology*. 2022. Vol. 24. No. 2. P. 134–170.

О НАЛОГОВОЙ ПРАВОСУБЪЕКТНОСТИ ОРГАНИЗАЦИЙ-РЕЗИДЕНТОВ, ОСУЩЕСТВЛЯЮЩИХ СВОЮ ДЕЯТЕЛЬНОСТЬ НА ТЕРРИТОРИЯХ ОСОБЫХ ЭКОНОМИЧЕСКИХ ЗОН

Пименов С.Д.¹

Ключевые слова: налоговое резидентство организаций, особые экономические зоны, зоны опережающего развития, резиденты ОЭЗ/ОР, налоговые льготы.

Аннотация

Цель работы: в статье исследуются особенности налогообложения организаций, функционирующих в особых экономических зонах, зонах опережающего развития и промышленных кластерах в России.

Метод исследования: сравнительно-правовой анализ российского законодательства и судебной практики особых экономических зон.

Результат исследования: анализируются налоговые льготы и преференции, доступные резидентам этих зон, и выявляются проблемы, возникающие при их применении, включая нечеткое законодательное регулирование, непоследовательную практику налоговых органов и отсутствие четких критериев определения принадлежности к ОЭЗ, ОР и ПК. Общие принципы налогового регулирования ОЭЗ иллюстрируются конкретными примерами из законодательства и судебной практики. Анализируются изменения в законодательстве и их влияние на резидентов ОЭЗ, подчеркиваются различия между старой и новой практикой.

Практическая ценность: предлагаются меры для совершенствования законодательства, обеспечения единообразного применения льгот, установления четких критериев и разработки механизмов досудебного урегулирования споров. Особое внимание уделяется необходимости уточнения законодательства, разработке разъяснений Минфина, усилению взаимодействия между налоговыми органами и резидентами, а также созданию механизма внесудебного разрешения споров.

DOI: 10.24412/1994-1404-2025-1-86-94

Введение и постановка задачи

В современных условиях развития экономики Российской Федерации создание благоприятных условий для бизнеса является важной задачей. Особые экономические зоны (ОЭЗ) играют ключевую роль в привлечении инвестиций и стимулировании экономического роста в регионах.

В статье И.В. Тюрина рассматривается проблема неоднозначного понимания термина «особая экономическая зона» (ОЭЗ) в российском законодательстве. Автор отмечает, что, несмотря на длительный период развития института правового регулирования ОЭЗ, подход законодателя к их определению остается противоречивым и не всегда четким [8].

Чистякова Ю.В. отмечает в своей работе, что «Государства, которые фактически теряли капитал вследствие популярности офшорных зон, старались предпринимать попытки по созданию альтернативных, но при этом подконтрольных аналогов офшоров» [10]. Поэтому начали создаваться ОЭЗ.

Особые экономические зоны — это территории Российской Федерации, которые государство наделяет специальным юридическим статусом, в отличие от иных, которые создаются с целью привлечения инвестиций, развития предпринимательства и повышения экономической активности в определённых регионах. Для организаций, осуществляющих свою деятельность на территориях ОЭЗ, предусматривается ряд налоговых льгот и преференций, которые позволяют им снизить налоговую нагрузку и повысить свою конкурентоспособность².

Как указывает в своей работе Гуляева В.Б., «В современных социально-экономических условиях для достижения устойчивого социально-экономического развития необходимо создание условий, максимально благоприятствующих предпринимательской деятель-

² Федеральный закон от 22.07.2005 № 116-ФЗ «Об особых экономических зонах в Российской Федерации» // СПС «КонсультантПлюс».

¹ Пименов Сергей Дмитриевич, юрисконсульт АО «Концерн «Гранит-Электрон», г. Санкт-Петербург, Российская Федерация.
E-mail: mr.pimenov91@mail.ru

ности и содействующих решению государством стратегически важных задач. Необходимость нахождения баланса частных и государственных интересов обуславливает развитие различных механизмов взаимодействия государства и бизнеса»³.

Налоговая правосубъектность резидентов (далее по тексту — ОЭЗ), территорий опережающего развития (далее по тексту — ОР) и предприятий промышленного комплекса (ПК) имеет свои особенности.

Резиденты ОЭЗ и ОР имеют право на налоговые льготы и преференции, установленные соответствующим законодательством. На территории Российской Федерации существуют также ОР, на которых могут создаваться и осуществлять предпринимательскую деятельность организации и оптимизировать на этих территориях свой режим налогообложения, статус таких земель определяется Федеральным законом от 22.07.2005 № 116-ФЗ «Об особых экономических зонах в Российской Федерации» и Федеральным законом от 29.12.2014 № 473-ФЗ (ред. от 10.07.2023) «О территориях опережающего развития в Российской Федерации»⁴. Такие территории отличаются льготными режимами и разными условиями для ведения бизнеса. Например, к таким условиям ведения бизнеса можно отнести сниженные ставки по налогу на прибыль, налогу на имущество организаций и земельному налогу. Для резидентов ОЭЗ и ОР также предусмотрены льготные тарифы страховых взносов, что снижает общую налоговую нагрузку и стимулирует инвестиции в создание новых рабочих мест.

Однако на практике возникают проблемы с реализацией этих льгот. Например, налоговые органы часто отказывают в предоставлении льгот резидентам ОЭЗ и ОР, ссылаясь на несоответствие их деятельности требованиям законодательства.

Необходимо провести анализ особенностей налоговой правосубъектности организаций, осуществляющих деятельность на территориях ОЭЗ, а также выявить основные преимущества и недостатки такого режима. Необходимо изучить налоговые льготы и преференции, доступные резидентам ОЭЗ, а также проблемы, возникающие при их реализации. Анализ должен включать в себя обзор нормативно-правовой базы, регулирующей деятельность ОЭЗ, и практику применения налогового законодательства в отношении резидентов ОЭЗ.

Организации, осуществляющие деятельность в ОЭЗ, обладают специфической налоговой правосубъектностью, определяемой Федеральным законом № 116-ФЗ. Они вправе добровольно выбирать специальные налоговые режимы, такие как упрощённая система налогообложения (далее — УСН) или патентная система

налогообложения (далее — ПСН). Резидентам ОЭЗ предоставляются значительные налоговые льготы, включая освобождение от налога на прибыль и имущество на первые 5 лет, снижение ставки налога на прибыль и возможное снижение НДС. Предусмотрены инвестиционные налоговые вычеты, позволяющие уменьшить налогооблагаемую базу на сумму инвестиций в развитие производства и инфраструктуры ОЭЗ.

В статье В.В. Самойловой рассматриваются налоговые льготы для резидентов ОЭЗ, включающие пониженные ставки налога на прибыль и нулевые ставки на имущество, транспорт и землю на определенный период. Для получения льгот имущество должно использоваться в деятельности резидента на территории ОЭЗ. Автор отмечает отсутствие единого налогового режима для резидентов ОЭЗ в российском законодательстве, что затрудняет налогообложение и препятствует привлечению инвесторов [6].

Резиденты могут участвовать в системе налогового мониторинга, что обеспечивает взаимодействие с налоговыми органами в режиме реального времени. Они обязаны предоставлять специализированную налоговую отчетность в электронном виде. Налоговый контроль осуществляется в соответствии с законодательством РФ, включая выездные и камеральные проверки. Нарушения налогового законодательства влекут ответственность в виде штрафов, пени и взыскания недоимки. Преимущества налогового режима в ОЭЗ направлены на снижение налоговой нагрузки, повышение инвестиционной привлекательности и конкурентоспособности резидентов.

Особенности налоговой правосубъектности организаций, осуществляющих свою деятельность на территориях ОЭЗ

1. Применение специальных налоговых режимов.

Резидент ОЭЗ может выбрать один из специальных налоговых режимов, предоставляемых на территории ОЭЗ, например, УСН (позволяет заменить уплату нескольких налогов одним: НК РФ⁵, глава 26.2), ПСН (для индивидуальных предпринимателей, осуществляющих определенные виды деятельности: НК РФ, глава 26.5) или единый налог на вменённый доход. Выбор специального налогового режима осуществляется на добровольной основе и действует в течение всего срока нахождения организации в ОЭЗ.

2. Резиденты ОЭЗ пользуются значительными налоговыми льготами. В течение первых 5 лет они освобождены от уплаты налога на прибыль и налога на имущество. После этого периода им предоставляется снижение ставки налога на прибыль. Кроме того, предусмотрено снижение ставки налога на добавленную стоимость (НДС) на период до 5 лет. Важным преимуществом является освобождение от уплаты таможен-

³ Гуляева В.В. Функционирование особых экономических зон в контексте их интеграции в социально-экономическое пространство региона : автореф. дис. ... канд. экон. наук. Ин-т проблем регион. экономики РАН. Санкт-Петербург, 2017.

⁴ Федеральный закон от 29.12.2014 № 473-З «О территориях опережающего развития в Российской Федерации» // СПС «КонсультантПлюс».

⁵ Налоговый кодекс Российской Федерации. Федеральный закон № 117-ФЗ от 05.08.2000 // СПС «КонсультантПлюс».

ных пошлин на ввозимое технологическое оборудование и сырье. Конкретные условия и сроки действия льгот определяются действующим законодательством, регулирующим деятельность ОЭЗ. Для получения подробной информации необходимо обратиться к соответствующим нормативным правовым актам.

3. Инвестиционный налоговый вычет, предусмотренный НК РФ, ст. 286⁶:

- Резиденты ОЭЗ имеют право на получение инвестиционных налоговых вычетов, которые позволяют им уменьшить налогооблагаемую базу по налогу на прибыль на сумму инвестиций, вложенных в развитие производства и инфраструктуры ОЭЗ.
- Инвестиционный налоговый вычет предоставляется в течение 10 лет с момента ввода основных средств в эксплуатацию.

4. Резиденты ОЭЗ могут участвовать в системе налогового мониторинга, которая позволяет им осуществлять взаимодействие с налоговыми органами в режиме реального времени и получать оперативную информацию о состоянии своих налоговых обязательств. Участие в налоговом мониторинге даёт возможность организациям минимизировать налоговые риски и повысить уровень прозрачности своей финансово-хозяйственной деятельности. Особенности налоговой правосубъектности организаций, осуществляющих свою деятельность на территориях ОЭЗ, направлены на создание благоприятных условий для инвестиционной и предпринимательской деятельности, привлечение новых инвестиций и повышение экономической активности в регионах, где создаются ОЭЗ (ст. 105.26 НК РФ).

5. Резиденты ОЭЗ обязаны представлять в налоговые органы отчётность по специальным формам, установленным для резидентов ОЭЗ. Налоговая отчётность представляется в электронном виде через оператора электронного документооборота.

6. Налоговый контроль в отношении резидентов ОЭЗ осуществляется налоговыми органами в соответствии с законодательством Российской Федерации о налогах и сборах. Налоговые органы имеют право проводить выездные налоговые проверки у резидентов ОЭЗ, осуществлять камеральные проверки налоговых деклараций, требовать от налогоплательщиков представления документов и информации, необходимых для осуществления налогового контроля.

Выездные и камеральные налоговые проверки регулируются статьями 82, 87—89 НК РФ. Налоговый орган вправе проверить правильность исчисления и своевременность уплаты налогов. Льготы, предусмотренные для резидентов ОЭЗ, устанавливаются федеральными законами об ОЭЗ и региональным законодательством (если применимо). Примером может служить пониженная ставка налога на прибыль организаций, установленная для резидентов технико-внедренческих

ОЭЗ (ст. 284 НК РФ). Обоснованность применения этих льгот также подлежит контролю.

7. Ответственность за нарушение налогового законодательства.

- Резиденты ОЭЗ несут ответственность за нарушение налогового законодательства в соответствии с законодательством Российской Федерации о налогах и сборах (статья 106 НК РФ).
- За совершение налоговых правонарушений резиденты ОЭЗ могут быть привлечены к ответственности в виде штрафов, пени, взыскания недоимки по налогам и сборам.

Таким образом, налоговый режим в ОЭЗ предоставляет организациям ряд следующих преимуществ, которые повышают инвестиционную привлекательность и конкурентоспособность резидентов ОЭЗ.

- Снижение налоговой нагрузки за счёт освобождения от уплаты налогов или снижения их ставок.
- Возможность получения инвестиционных налоговых вычетов, что позволяет снизить налогооблагаемую базу и уменьшить налоговые платежи.
- Упрощённая отчётность, которая снижает административные издержки и упрощает взаимодействие с налоговыми органами.
- Гарантии стабильности налогового режима в течение срока нахождения организации в ОЭЗ, что обеспечивает предсказуемость условий ведения бизнеса.

Благодаря этим преимуществам налоговый режим в ОЭЗ является привлекательным для организаций, планирующих инвестировать в развитие бизнеса и повышать свою конкурентоспособность.

Современная правовая модель налоговых отношений характеризуется дроблением правовых режимов под конкретные категории налогоплательщиков; для полноценного изучения налоговой правосубъектности организаций необходимо провести анализ таких субъектов налоговых отношений как организаций — резидентов ОЭЗ, ОР и т. д., а также организаций, имеющих правовой статус промышленных предприятий.

В статье Е.В. Безиковой рассматривается правовое регулирование финансовых отношений в особых экономических зонах (ОЭЗ) дружественных стран (Китай, Иран, Турция, Египет, Марокко, ОАЭ) в условиях цифровизации. Автор приходит к выводу, что законодательство этих стран содержит специфические финансово-правовые стимулы для резидентов ОЭЗ, обусловленные различиями в видах деятельности, экономическом и научном потенциале стран. Геополитические изменения и санкции стимулируют конкуренцию между ОЭЗ, предлагающими широкий спектр механизмов для инвесторов. Анализ преференциальных режимов показывает, что наличие развитой инфраструктуры, административных преференций, удобное географическое положение и строгое соблюдение стратегий развития ОЭЗ являются приоритетными условиями для резидентов при выборе направления инвестиций [1].

⁶ НК РФ, часть вторая.

Организации, являющиеся резидентами ОЭЗ, могут пользоваться льготными налоговыми ставками, освобождением от некоторых налогов и уменьшением административных сборов. Налоговый режим для таких резидентов регламентируется Федеральным законом от 22 июля 2005 года № 116-ФЗ «Об особых экономических зонах в Российской Федерации» в редакции, действовавшей до января 2025 года.

В письме Минфина России от 03.10.2024 № 03-07-11/95799 дано разъяснение о применении НДС при получении ИП, применяющим УСН: «Согласно пункту 3 статьи 346.11 Налогового кодекса Российской Федерации в редакции, действующей до 1 января 2025 года (далее — Кодекс), индивидуальные предприниматели, применяющие упрощенную систему налогообложения, не признаются налогоплательщиками НДС, за исключением НДС, подлежащего уплате в соответствии с Кодексом при ввозе товаров на территорию Российской Федерации и иные территории, находящиеся под ее юрисдикцией (включая суммы НДС, подлежащие уплате при завершении действия таможенной процедуры свободной таможенной зоны на территории Особой экономической зоны в Калининградской области), а также НДС, уплачиваемого в соответствии со статьями 161 и 174.1 Кодекса. Поэтому операции по реализации товаров (работ, услуг), имущественных прав, осуществляемые указанным индивидуальным предпринимателем до 1 января 2025 года, НДС не облагаются».

Таким образом, индивидуальный предприниматель, применяющий УСН и являющийся резидентом ОЭЗ, в общем случае освобождается от уплаты НДС по операциям реализации товаров, работ и услуг до 1 января 2025 года, если эти операции не подпадают под исключения, указанные в пункте 3 статьи 346.11 НК РФ.

Особенности торгово-экономических зон

Торгово-экономические зоны (территории опережающего развития, ОР) также предоставляют зарегистрированным в них организациям определённые налоговые привилегии. К ним относятся пониженные ставки налога на прибыль и налога на имущество, а также освобождение от уплаты земельного и транспортного налогов на период до пяти лет. Правовые условия для резидентов ОР определяются Федеральным законом от 29 декабря 2014 года № 473-ФЗ «О территориях опережающего развития в Российской Федерации».

Отдельной категорией являются промышленные предприятия, имеющие специальный налоговый статус. Они могут получать инвестиционный налоговый вычет, позволяющий сокращать налогооблагаемую базу за счёт затрат на приобретение основных средств для производства. Правовой статус этих предприятий регулируется Федеральным законом от 31.12.2014 № 488-ФЗ «О промышленной политике в Российской

Федерации»⁷. Анализ правового статуса резидентов ОЭЗ, ОР и промышленных предприятий выявляет как общие черты, так и отличия в их налоговой правосубъектности⁸.

Правовой статус промышленного комплекса в Москве определяется рядом нормативных актов, включая Федеральный закон № 488 «О промышленной политике в Российской Федерации», касающийся промышленной политики в России, и закон г. Москвы от 19 декабря 2007 г. № 49 «Об основах управления собственностью города Москвы»⁹, который регулирует управление объектами промышленного комплекса в столице.

В своём докладе заместитель начальника управления промышленной политики Департамента инвестиционного развития города Москвы Путилин А.Р. указал, что «промышленные комплексы Москвы получают ряд налоговых льгот, включая пониженные ставки на прибыль (13,5%) и имущество (1,1%), а также значительное снижение земельного налога и арендной платы. Статус промышленного комплекса присваивается имущественному комплексу, состоящему из производственных компаний, соответствующих определенным критериям. Для получения этого статуса организации должны соблюдать два из трех требований: фонд оплаты труда на уровне не менее 133,9 млн руб. на гектар; выручка минимум 404,6 млн руб. на гектар; или объем инвестиций за последние пять лет не менее 110,4 млн руб. на гектар. Средняя заработная плата сотрудников должна составлять не менее 76,5 тыс. руб. Таким образом, статус промышленного комплекса важен для стимулирования инвестиционной привлекательности и поддержки производственного сектора в Москве»¹⁰.

Компании, входящие в реестр московского промышленного комплекса, получают определённые налоговые льготы, включая освобождение от налога на имущество для объектов, используемых в производстве, а также снижение земельного налога для земельных участков с промышленными зданиями и льготные ставки транспортного налога для нужд производства: см. пункт 2 статьи 4 закона г. Москвы от 09.07.2008 № 33 (ред. от 14.12.2022) «О транспортном налоге» — «резиденты особых экономических зон технико-внедренческого типа, созданных на территории города Москвы (далее — особые экономические зоны), — в отношении транспортных средств, зарегистрированных на указанных резидентов, с момента включения в реестр резидентов особой экономической зоны. Льгота предоставляется сроком на 10 лет, начиная с месяца регистрации транспортного средства. Право на льготу подтверждается выпиской из реестра резидентов осо-

⁷ Федеральный закон № 488 от 31.12.2014 «О промышленной политике в Российской Федерации» // СПС «КонсультантПлюс».

⁸ Вакуленко И.И. Об определении правового статуса промышленных предприятий // Молодой ученый. 2021. № 20 (362). С. 323—325.

⁹ Закон г. Москвы от 19 декабря 2007 года № 49 «Об основах управления собственностью города Москвы» // СПС «Гарант».

¹⁰ URL: <http://old.prommoscow.info/publication/bussines/2490#>

бой экономической зоны, выданной органом управления особой экономической зоной»¹¹.

На практике возникают затруднения в определении характера деятельности предприятий, которые могут при определенных обстоятельствах быть не признаны промышленными с вытекающими юридическими последствиями. Для того чтобы данный статус был подтвержден, необходимо, чтобы предприятие занималось промышленным производством или научными исследованиями, находилось на территории Москвы и использовало объекты промышленного назначения, а также показывало положительные финансовые результаты.

Законодательство также предусматривает, что компании с долей доходов от промышленной деятельности свыше 70% могут получить налоговые льготы. Признание статуса промышленного комплекса осуществляется соответствующими администрациями города.

Все три типа организаций имеют возможность воспользоваться особыми налоговыми режимами. Эти льготы направлены на привлечение инвестиций и содействие экономическому развитию. Правовой статус каждой из категорий определяется отдельными федеральными законами.

Статья Е.В. Гриценко посвящена анализу и систематизации особых режимов и моделей управления территориями в России, подчеркивая тенденцию углубления асимметрии федеративного и муниципального устройства. Отмечается дальнейшая дифференциация режимов и статусов территорий, усложняющаяся из-за сочетания нескольких особых режимов на одной территории, для которых отсутствует четкая концепция сосуществования [4].

ОЭЗ и ОР могут находиться в различных регионах, в то время как промышленные предприятия могут быть зарегистрированы в любой части России. Условия для получения и сохранения статуса резидента для ОЭЗ, ОР и промышленных предприятий различны. Объем и виды налоговых льгот зависят от типа организации.

Правосубъектность организаций в области налогообложения обозначается дифференциацией на конкретные категории налогоплательщиков. Организации с особыми правовыми статусами, такие как резиденты ОЭЗ, ОР и промышленные предприятия, обладают особыми налоговыми преимуществами.

Анализ правового статуса этих организаций помогает выявить как общие черты, так и различия в их налоговых правах, что подчеркивает необходимый дифференцированный подход к налогообложению для стимуляции инвестиций, экономического роста и развития промышленности.

В отличие от НК РФ, который определяет налоговых резидентов, Федеральный закон от 22.07.2005 № 116-ФЗ «Об особых экономических зонах Российской Федерации» вводит другое понятие резидента, который полу-

чает определённые преимущества при ведении бизнеса в этих зонах.

Выделяются четыре основных типа зон с особыми условиями: промышленные, технико-внедренческие, портовые и туристско-рекреационные. Соглашение о проведении деятельности в этих зонах заключается между резидентом ОЭЗ и уполномоченным федеральным или региональным органом власти (статья 12 Федерального закона от 22.07.2005 № 116-ФЗ).

Если организация хочет работать на территории такой зоны и удовлетворяет её требованиям, она получает статус резидента и может воспользоваться налоговыми льготами, такими как снижение налогов на прибыль, имущество, транспорт и землю. Эти льготы могут устанавливаться на разных уровнях — федеральном, местном или региональном.

Законодательством субъектов Российской Федерации могут устанавливаться пониженные налоговые ставки на определенной территории, как, например, в Свердловской области, где резиденты ОЭЗ на 10 лет освобождаются от налога на имущество.

Государство создаёт ОЭЗ для стимулирования развития ключевых отраслей экономики. Научно-технологическое развитие этих зон критично, а эффективное применение льгот поможет разрабатывать предпринимательские проекты в необходимых направлениях.

Субъекты не имеют права открывать филиалы за пределами ОЭЗ, что подтверждает принцип территориального резидентства. По положению Налогового кодекса РФ, для резидентов ОЭЗ возможно установление сниженной ставки налога на прибыль для бюджетов субъектов.

В ст. 12 НК РФ Федеральным законом от 04.08.2023 № 415-ФЗ¹² введен п. 8, который позволяет устанавливать налоги разового характера, установленные федеральными законами, принятыми в соответствии с НК РФ.

Ранее этот нормативный акт содержал положение о налогообложении резидентов, однако актуальная редакция позволяет устанавливать иные налоговые преференции, не внося изменения в Налоговый кодекс, включая возможный налог на сверхприбыль.

Федеральный закон от 04.08.2023 № 414-ФЗ «О налоге на сверхприбыль»¹³, который начал действовать с 1 января 2024 года, устанавливает налог на сверхприбыль, являющийся налогом разового характера.

Вместе с тем, на основании пункта 27 статьи 1 и пункта 2 статьи 7 Федерального закона от 04.08.2023 № 448-ФЗ «О внесении изменений в Федеральный закон «Об особых экономических зонах в Российской Федерации» и отдельные законодательные акты Российской Федерации», «Акты законодательства Россий-

¹¹ URL: [https://www.mos.ru/upload/documents/files/1632/ZakongMoskviot09072008N33\(redot14122022\).pdf](https://www.mos.ru/upload/documents/files/1632/ZakongMoskviot09072008N33(redot14122022).pdf)

¹² Федеральный закон от 04.08.2023 № 415-ФЗ «О внесении изменений в часть первую и статью 270 части второй Налогового кодекса Российской Федерации» // СПС «КонсультантПлюс».

¹³ Федеральный закон от 04.08.2023 № 414-ФЗ «О налоге на сверхприбыль» // СПС «КонсультантПлюс».

ской Федерации о налогах и сборах, законы субъектов Российской Федерации о налогах и сборах, нормативные правовые акты органов местного самоуправления о налогах и сборах, ухудшающие положение налогоплательщиков — резидентов ОЭЗ, за исключением актов законодательства Российской Федерации о налогах и сборах, касающихся налогообложения подакцизных товаров, не применяются в отношении резидентов особых экономических зон в течение срока действия соглашения о ведении промышленно-производственной, технико-внедренческой, туристско-рекреационной деятельности или о деятельности в портовой особой экономической зоне»¹⁴, — статья 38 Федерального закона № 116-ФЗ с 01.01.2024 признается утратившей силу. Это считалось своего рода стабилизационной оговоркой для резидентов ОЭЗ, защищающей их от ухудшения налоговых условий.

Отсутствие в статье 5 НК РФ положений «о стабилизационной оговорке», которая в литературе рассматривается в качестве налогового стимула [5] для резидентов ОЭЗ; положения Федерального закона № 414-ФЗ «О налоге на сверхприбыль» будут действовать с 01.01.2024 также для резидентов ОЭЗ, что ранее было невозможным и подтверждается письмом Министерства финансов Российской Федерации от 11.08.2023 № 03-03-05/75723¹⁵.

Таким образом, отношения по установлению, ведению и взиманию налогов и сборов в Российской Федерации на территории ОЭЗ и ОР начинают приобретать диспозитивный характер в ряде императивных норм, а именно: организации могут получать преференции по налогам и сборам по собственному желанию.

Упоминание о том, что организации могут получать преференции «по собственному желанию», подразумевает, что некоторые императивные нормы, обычно обязательные для всех, в этих зонах становятся более гибкими. Это может означать возможность применения пониженных ставок, освобождение от уплаты определенных налогов или особый порядок их уплаты, если организация соответствует определенным критериям и принимает решение воспользоваться этими льготами.

Указом Президента РФ 8 августа 2023 г. были приостановлены договора «об отмене двойной уплаты налогов»¹⁶ с недружественными странами до устранения иностранными государствами допущенных ими нарушениями законных экономических и иных интересов Российской Федерации, среди которых 38 госу-

дарств, в число которых входят: Польша, США, Корея, Болгария, Великое Герцогство Люксембург и т. д.

Этот документ отменяет соглашение не полностью, а, в частности, по следующим направлениям: порядок налогообложения прибыли от дивидендов, процентов доходов от облигаций и других ценных бумаг, доходов от недвижимости и земельных участков.

Особенности налоговой правосубъектности организаций, осуществляющих свою деятельность на территориях ОЭЗ, направлены на создание благоприятных условий для инвестиционной и предпринимательской деятельности, привлечение новых инвестиций и повышение экономической активности в регионах, где создаются ОЭЗ.

Особенности налоговой правосубъектности резидентов ОЭЗ, ОР и ПК в судебных решениях

В определении Верховного Суда РФ от 26.06.2017 № 310-КГ17-5116 по делу № А14-350/2016¹⁷ налоговая инспекция доначислила государственному унитарному предприятию налог на имущество, посчитав, что у предприятия нет оснований для применения льготы, предусмотренной п. 15 ст. 381 НК РФ, поскольку ему не присвоен статус государственного научного центра. Три судебные инстанции признали решение налоговой инспекции недействительным, ссылаясь на то, что льгота распространяется на федеральные научно-производственные центры, к которым относится предприятие, основываясь на разъяснениях ВАС РФ. Верховный Суд РФ указал, что новая редакция п. 15 ст. 381 НК РФ, действующая с 2015 года, предполагает освобождение от налога только для организаций, которым присвоен статус государственного научного центра. Ранее данные разъяснения ВАС РФ больше не применимы. Поскольку предприятию не присвоен данный статус, оно не имеет права на льготу, и доначисления налогового органа правомерны.

Постановлением Арбитражного суда Поволжского округа от 21.06.2023 № Ф06-3605/2023 по делу № А65-8284/2022¹⁸ Министерство экономики Республики Татарстан обратилось в арбитражный суд с иском к ООО «Комбинат энергосберегающих материалов „Уоллсейвинг“» о расторжении соглашения об осуществлении деятельности в особой экономической зоне и взыскании 5 млн руб. штрафа. Иск был мотивирован неосуществлением Обществом деятельности, его банкротством и неисполнением обязанности по уплате штрафа. Общество возражало, указывая на отсутствие доказательств досудебного урегулирования спора, пропуск срока исковой давности и отсутствие полномочий у Министерства. Арбитражный суд Республики

¹⁴ Федеральный закон от 04.08.2023 № 448-ФЗ «О внесении изменений в Федеральный закон «Об особых экономических зонах в Российской Федерации» и отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».

¹⁵ Письмо Минфина России от 11.08.2023 № 03-03-05/75723 // «Ж-Бухгалтер» (Бухгалтерское приложение). 2023. № 34.

¹⁶ Указ Президента РФ от 08.08.2023 № 585 «О приостановлении Российской Федерацией действия отдельных положений международных договоров Российской Федерации по вопросам налогообложения» // СПС «КонсультантПлюс».

¹⁷ Определение Верховного Суда РФ от 26.06.2017 № 310-КГ17-5116 по делу № А14-350/2016 // СПС «КонсультантПлюс».

¹⁸ Постановление Арбитражного суда Поволжского округа от 21.06.2023 № Ф06-3605/2023 по делу № А65-8284/2022 // СПС «КонсультантПлюс».

Татарстан удовлетворил иск, расторгнув соглашение и взыскав штраф. Одиннадцатый арбитражный апелляционный суд оставил решение без изменения. Общество в лице конкурсного управляющего подало кассационную жалобу в Арбитражный суд Поволжского округа, прося отменить судебные акты и отказать во взыскании штрафа, ссылаясь на банкротство как обстоятельство непреодолимой силы и несоблюдение претензионного порядка. Постановлением суда жалоба оставлена без удовлетворения, так как основания для расторжения соглашения были подтверждены.

Другой аналогичный пример: постановление Арбитражного суда Поволжского округа от 27.11.2024 № Ф06-8535/2024¹⁹ по делу № А72-153/2024. Арбитражный суд Поволжского округа рассмотрел кассационную жалобу АО «Портовая особая экономическая зона „Ульяновск“» (ПОЭЗ) на решения нижестоящих судов по делу № А72-153/2024. Дело касалось иска Правительства Ульяновской области к ООО «Завод ИнжеТех» о расторжении соглашения об осуществлении деятельности в ПОЭЗ из-за неисполнения обязательств. ПОЭЗ также заявило самостоятельные требования к ООО «Завод ИнжеТех» о взыскании неустойки в связи с досрочным прекращением соглашения. Основное требование удовлетворено, требования третьего лица удовлетворены в части, поскольку факт нарушения резидентом обязательств по соглашению подтвержден, основания для расторжения соглашения установлены, размер штрафа снижен на основании ст. 333 ГК РФ.

Арбитражный суд Ульяновской области удовлетворил иск правительства области о расторжении соглашения и частично удовлетворил требования ПОЭЗ, взыскав часть штрафа. Одиннадцатый арбитражный апелляционный суд оставил решение без изменений. ПОЭЗ не согласилось с уменьшением размера штрафа и обратилось в кассационный суд, утверждая об отсутствии оснований для снижения ответственности ООО «Завод ИнжеТех».

По делу № А20-5035/2020 Арбитражный суд Северо-Кавказского округа рассмотрел кассационную жалобу АО «Кавказ.РФ» на решения суда Кабардино-Балкарской Республики и апелляционного суда по делу о признании недействительными решений налоговой инспекции об отказе АО «Курорты Северного Кавказа» в применении льготы по налогу на имущество организаций в отношении горнолыжной трассы и гаража за 2016—2019 годы²⁰.

Суд первой инстанции ранее удовлетворял требования общества, однако кассационный суд отменил решение и направил дело на новое рассмотрение.

При повторном рассмотрении суд отказал в удовлетворении требований, указав, что объекты отвечали признакам основных средств на момент приобретения обществом и общество не подтвердило создание объектов за счет инвестиций.

АО «Кавказ.РФ» в кассационной жалобе настаивает, что ремонтные работы и модернизация объектов проводились за счет средств общества, полученных из федерального бюджета, и его инвестиционных вложений, в том числе при достройке канатной дороги и доведении гаража до пригодного состояния.

В удовлетворении требования отказано, поскольку спорные объекты к моменту их приобретения обществом отвечали признакам основных средств, созданных и поставленных на кадастровый учет в соответствии с требованиями действующего законодательства. Создание объектов за счет инвестиционных вложений документально не подтверждено, в связи с чем право на применение льготы в виде освобождения от уплаты налога на имущество у общества отсутствовало.

Заключение

Таким образом, в ходе анализа судебной практики арбитражных судов выявилась тенденция к отказам со стороны налоговых органов в предоставлении льгот резидентам ОЭЗ, ОР и ПК. Основной причиной таких отказов является несоответствие деятельности резидентов требованиям законодательства.

Резиденты ОЭЗ, ОР и ПК вправе обжаловать действия налоговых органов в судебном порядке. В случае вынесения решения в пользу налогоплательщика суд может обязать налоговый орган предоставить соответствующую льготу.

В статье Челпановой М.М. и Понежина Л.Ю. анализируется проблема неэффективности функционирования ОЭЗ в России, констатируемая на официальном уровне. Авторы подчеркивают необходимость разработки четкой системы мер для решения накопившихся экономических проблем, препятствующих полноценному развитию ОЭЗ [9].

Основными проблемами, связанными с реализацией статуса резидентов ОЭЗ, ОР и ПК, являются:

- нечеткое законодательное регулирование налоговой правосубъектности этих субъектов (резидентов);
- непоследовательная практика применения налоговых льгот и преференций налоговыми органами;
- отсутствие четких критериев определения принадлежности субъектов к ОЭЗ, ОР и ПК.

Эти проблемы приводят к судебным спорам, нестабильности налогового режима и трудностям в планировании деятельности для резидентов ОЭЗ, ОР и ПК.

Для решения обозначенных проблем необходимо:

- совершенствовать законодательное регулирование налоговой правосубъектности резидентов ОЭЗ, ОР и ПК;

¹⁹ Постановление Арбитражного суда Поволжского округа от 27.11.2024 № Ф06-8535/2024 по делу № А72-153/2024 // СПС «КонсультантПлюс».

²⁰ Постановление Арбитражного суда Северо-Кавказского округа от 31.08.2023 № Ф08-7309/2023 по делу № А20-5035/2020 // СПС «КонсультантПлюс».

- обеспечить единообразное применение налоговых льгот и преференций налоговыми органами;
- установить чёткие критерии определения принадлежности субъектов к ОЭЗ, ОР и ПК;
- разработать механизмы досудебного урегулирования налоговых споров, связанных с реализацией статуса резидентов ОЭЗ, ОР и ПК.

Для улучшения правоприменительной практики и обеспечения эффективной защиты прав резидентов ОЭЗ, ОР и ПК целесообразно предпринять следующие меры:

- уточнение законодательства в части предоставления налоговых льгот и преференций для резидентов;

- разработка чётких и понятных разъяснений Минфина РФ по вопросам применения налогового законодательства (в данной сфере);
- усиление взаимодействия между налоговыми органами и резидентами;
- создание механизма внесудебного разрешения споров.

Налоговая правосубъектность резидентов ОЭЗ, ОР и ПК имеет свои особенности, которые находят отражение в судебной практике арбитражных судов. Для обеспечения эффективной защиты прав налогоплательщиков и надлежащего применения законодательства необходимы комплексные меры, направленные на устранение выявленных нарушений и создание благоприятных условий для деятельности резидентов ОЭЗ, ОР и ПК.

Литература

1. Безикова Е.В. Правовое регулирование отношений в сфере организации финансов свободных (особых) экономических зон дружественных стран в условиях цифровизации (на примере Китая, Ирана, Турции, Египта, Марокко, ОАЭ) // Безопасность бизнеса. 2024. № 3. С. 2—6.
2. Вакуленко И.И. Об определении правового статуса промышленных предприятий // Молодой ученый. 2021. № 20 (362). С. 323—325.
3. Гриценко Е.В. Конституционная география России: как не заблудиться в лабиринтах особых режимов и статусов территорий? // Сравнительное конституционное обозрение. 2024. № 3. С. 4—42.
4. Коновалов Д. «Проблемные» документы, штрафы, прощение долга работнику: узкие места налогового учета // Налогообложение, учет и отчетность в коммерческом банке. 2024. № 6. С. 58—69.
5. Леднева Ю.В. «Стабилизационная оговорка» в налоговом праве // Финансовое право. 2020. № 6. С. 18—22.
6. Самойлова В.В. Триумфальное возвращение особых экономических зон: развитие экономики или пустые надежды? // Финансовое право. 2021. № 12. С. 35—38.
7. Терехова В.В. Оценка эффективности правового регулирования применения финансовых инструментов в российских особых экономических зонах // Финансовое право. 2021. № 2. С. 21—23.
8. Тюрин И.В. К вопросу о сохраняющейся неоднозначности понимания термина «особая экономическая зона» по российскому законодательству // Журнал российского права. 2023. № 8. С. 136—149.
9. Челпанова М.М., Понежина Л.Ю. Основные проблемы функционирования особых экономических зон и пути их решения // Финансовое право. 2022. № 3. С. 31—34.
10. Чистякова Ю.В. Правовое регулирование редомициляции: современные тенденции и зарубежный опыт // Актуальные проблемы российского права. 2024. № 11. С. 84—95.

SECTION:
PRIVATE LAW

ON TAX LEGAL PERSONALITY OF RESIDENT ORGANIZATIONS OPERATING IN THE TERRITORIES OF SPECIAL ECONOMIC ZONES

Sergei Pimenov, legal advisor at AO (JSC) "Kontsern Granit-Elektron", Saint Petersburg, Russian Federation.

E-mail: mr.pimenov91@mail.ru

Keywords: *tax residency of organizations, special economic zones, advanced development zones, SEZ/ADZ residents, tax benefits.*

Abstract

Purpose of the work: studying features of taxation of organizations operating in special economic zones (SEZ), advanced development zones (ADZ) and industrial clusters (IC) in Russia.

Methods used in the study: comparative legal analysis of Russian legislation and judicial practice of special economic zones.

Study findings: the paper analyzes the tax benefits and preferences available to residents of these zones and identifies the problems that arise in their application, including unclear legislative regulation, inconsistent practice of tax authorities and the lack of clear criteria for determining belonging to SEZs, ADZs and ICs residents, the differences between the old and new practices are emphasized.

Practical value: measures are proposed to improve legislation, ensure the uniform application of benefits, establish clear criteria and develop mechanisms for pre-trial settlement of disputes. Particular attention is paid to the need to clarify legislation, develop clarifications from the Ministry of Finance, strengthen interaction between tax authorities and residents, as well as create a mechanism for out-of-court dispute resolution.

References

1. Bezikova E.V. Pravovoe regulirovanie otnoshenii v sfere organizatsii finansov svobodnykh (osobykh) ekonomicheskikh zon družestvennykh stran v usloviakh tsifrovizatsii (na primere Kitaia, Irana, Turtsii, Egipta, Marokko, OAE). Bezo-pasnost' biznesa. 2024. No. 3. Pp. 2–6.
2. Vakulenko I.I. Ob opredelenii pravovogo statusa promyshlennykh predpriatii. Molodoi uchenyi. 2021. No. 20 (362). Pp. 323–325.
3. Gritsenko E.V. Konstitutsionnaia geografiia Rossii: kak ne zabludit'sia v labirintakh osobykh rezhimov i statusov ter-ritorii? Sravnitel'noe konstitutsionnoe obozrenie. 2024. No. 3. Pp. 4–42.
4. Konovalov D. "Problemnye" dokumenty, shtrafy, proshchenie dolga rabotniku: uzkie mesta nalogovogo ucheta. Na-логообложение, учет и отчетность в коммерческом банке. 2024. No. 6. Pp. 58–69.
5. Ledneva Iu.V. "Stabilizatsionnaia ogovorka" v nalogovom prave. Finansovoe pravo. 2020. No. 6. Pp. 18–22.
6. Samoilova V.V. Triumfal'noe vozvrashchenie osobykh ekonomicheskikh zon: razvitie ekonomiki ili pustye nadezhdy? Finansovoe pravo. 2021. No. 12. Pp. 35–38.
7. Terekhova V.V. Otsenka effektivnosti pravovogo regulirovaniia primeneniia finansovykh instrumentov v rossiiskikh osobykh ekonomicheskikh zonakh. Finansovoe pravo. 2021. No. 2. Pp. 21–23.
8. Tiurin I.V. K voprosu o sokhraniiaushcheisia neodnoznachnosti ponimaniia termina "osobaia ekonomicheskaia zona" po rossiiskomu zakonodatel'stvu. Zhurnal rossiiskogo prava. 2023. No. 8. Pp. 136–149.
9. Chelpanova M.M., Ponezhina L.Iu. Osnovnye problemy funktsionirovaniia osobykh ekonomicheskikh zon i puti ikh resheniia. Finansovoe pravo. 2022. No. 3. Pp. 31–34.
10. Chistiakova Iu.V. Pravovoe regulirovanie redomitsiliatsii: sovremennye tendentsii i zarubezhnyi opyt. Aktual'nye problemy rossiiskogo prava. 2024. No. 11. Pp. 84–95.

К ВОПРОСУ О СИСТЕМЕ ЗАКОНОДАТЕЛЬСТВА, РЕГУЛИРУЮЩЕГО ВОЗВРАТ СБЕРЕЖЕНИЙ ГРАЖДАН АГЕНТСТВОМ ПО СТРАХОВАНИЮ ВКЛАДОВ

Паршукова А.П.¹

Ключевые слова: система гарантирования, единообразие регулирования, негосударственное пенсионное обеспечение, программа долгосрочных сбережений, договор страхования жизни, участники финансового рынка, вклад, инструмент долгосрочного инвестирования.

Аннотация

Цель исследования: анализ правового регулирования процедур возврата сбережений граждан Агентством по страхованию вкладов (в том числе страхование вкладов, гарантирование прав участников негосударственных пенсионных фондов, гарантирование по договорам страхования жизни).

Методы исследования: системный, сравнительно-правовой метод и метод синергетики.

Результаты исследования: системы гарантирования рассмотрены в сравнении и взаимосвязи с системой страхования вкладов. Установлено наличие генетического родства указанных систем, единой финансово-правовой основы их функционирования, выражающейся в выплате возмещения гражданам за счет специальных публичных фондов денежных средств, аккумулируемых Агентством по страхованию вкладов. Обоснован тезис о расширении предмета обязательного публичного страхования денежных средств граждан ввиду появления нового вида общественных отношений — гарантирования по договорам страхования жизни. Выработаны предложения по совершенствованию регулятивной базы посредством создания единого кодифицированного акта, который будет определять общие принципы и механизмы обязательного публичного страхования (гарантирования) сбережений и устанавливать нормы, отражающие специфику отдельных видов отношений.

Научная новизна: обосновывается вывод о необходимости унификации законодательства и перспективах принятия единого регулятивного акта для данных видов общественных отношений.

DOI: 10.24412/1994-1404-2025-1-95-100

Памяти моего наставника А.В. Турбанова²

Введение и постановка задачи

Приведение норм к единообразию является одним из острых вопросов правотворческой деятельности, актуальность которого возрастает с появлением новых видов общественных отношений. Особенно важно обеспечить непротиворечивость, сбалансированность регулирования в случаях, когда одному лицу предоставляются правомочия в рамках функционирования нескольких сходных механизмов.

Ярким примером изложенного является правовой статус государственной корпорации «Агентство по страхованию вкладов» (далее — Агентство), которая

изначально была создана на основании Федерального закона от 23.12.2003 № 177-ФЗ «О страховании вкладов в банках Российской Федерации» (далее — Закон № 177-ФЗ, Закон о страховании вкладов) как специальный субъект, обеспечивающий функционирование системы страхования вкладов (далее — ССВ). Однако с течением времени, развитием финансово-экономических отношений и актуализацией запросов и потребностей общества на Агентство были последовательно возложены функции гарантирования прав застрахованных лиц в системе обязательного пенсионного стра-

¹ Паршукова Анастасия Павловна, начальник отдела аудита деятельности Агентства по страхованию вкладов, гарантированию пенсионных накоплений и внутрихозяйственной деятельности службы внутреннего аудита государственной корпорации «Агентство по страхованию вкладов», г. Москва, Российская Федерация.

E-mail: anastasia.p2018@mail.ru

² Александр Владимирович Турбанов (31 января 1950 г., Челябинск — 25 января 2025 г., Москва) — российский государственный и общественный деятель, доктор юридических наук.

В 1993—1995 годах был депутатом Государственной Думы. В 1996 году перешёл на работу в Банк России, отвечал за банковский надзор. С 1999 года возглавлял ГК «Агентство по реструктуризации кредитных организаций», созданную для преодоления последствий кризиса в банковской системе. С 2004 по 2012 год был первым генеральным директором ГК «Агентство по страхованию вкладов». Один из инициаторов и авторов закона об обязательном страховании вкладов.

После выхода на пенсию занялся научной и преподавательской деятельностью. Руководил кафедрой «Регулирование финансово-кредитной деятельности» РАНХиГС при Президенте Российской Федерации, был научным руководителем Института финансового и банковского права МГЮА имени О.Е. Кутафина.

хования³, гарантирования прав участников негосударственных пенсионных фондов (далее — СГПУ) по договорам негосударственного пенсионного обеспечения и программы долгосрочных сбережений⁴. С 01.01.2027 Агентство также будет обеспечивать и функционирование системы гарантирования прав по договорам страхования жизни⁵.

Отметим, что все упомянутые системы методологически и сущностно не являются обособленными элементами, находящимися в вакууме и развивающимися в отрыве друг от друга. Напротив, они связаны генетически, имеют общие цели, принципы и модели функционирования. В частности, СГПУ построена «по образу и подобию» страхования вкладов и гарантирования в рамках обязательного пенсионного обеспечения, а гарантирование по договорам страхования жизни, в свою очередь, базируется на модели СГПУ [1].

Примечательно, что о расширении круга публичных страховых отношений еще в 2004 году высказывался А.В. Турбанов, отмечая сходство банковских вкладов и вкладов в страховые, пенсионные, инвестиционные компании. Он отмечал, что поскольку «основными целями введения системы страхования вкладов являются формирование общих условий конкуренции для финансовых институтов разных видов, защита наиболее широких слоев вкладчиков, создание условий для привлечения сбережений населения и использования их в качестве долгосрочных ресурсов для кредитования экономики, можно сделать вывод, что включение страховых организаций, пенсионных и инвестиционных фондов в систему страхования вкладов полностью отвечает названным целям» [2, с. 269]. Как видно из реалий современного правового регулирования, гипотеза А.В. Турбанова о сближении ССВ, пенсионных и страховых отношений, оказалась верной.

Общая проблематика регулирования систем гарантирования и страхования

Даже на уровне простого перечисления заметно терминологическое сходство систем гарантирования и страхования. Очевидна и ведущая роль Агентства в создании условий для достижения их общей цели — обеспечения возврата сбережений граждан. Вместе с тем даже беглый взгляд на совокупность законов, регулирующих деятельность Агентства, обнаруживает следующие вопросы:

³ Федеральный закон от 28.12.2013 № 422-ФЗ «О гарантировании прав застрахованных лиц в системе обязательного пенсионного страхования Российской Федерации при формировании и инвестировании средств пенсионных накоплений, установлении и осуществлении выплат за счет средств пенсионных накоплений».

⁴ Федеральный закон от 28.12.2022 № 555-ФЗ «О гарантировании прав участников негосударственных пенсионных фондов в рамках деятельности по негосударственному пенсионному обеспечению и формированию долгосрочных сбережений».

⁵ Федеральный закон от 26.12.2024 № 477-ФЗ «О гарантировании прав по договорам страхования жизни».

- Обеспечено ли единство правового регулирования систем, управляемых Агентством?
- Является ли необходимым и целесообразным их дифференцированное регулирование?

Ответ на них требует не только комплексного анализа моделей возврата сбережений граждан, но и определения родовых признаков указанных систем и мотивов законодателя.

Банк России неоднократно отмечал, что тенденции развития современной российской экономики обуславливают необходимость создания условий для усиления роли финансового рынка в финансировании ее трансформации при сохранении устойчивости финансового сектора. В указанных целях принципиально важным становится повышение роли рынка капитала и небанковских финансовых посредников⁶. Ограничение доступа к внешнему капиталу обуславливает возрастание роли внутренних источников финансирования экономики, в том числе сбережений граждан, которые могут быть направлены в инструменты долгосрочного инвестирования.

Анализируя механизмы долгосрочного инвестирования, Банк России указывает на необходимость повышения уровня доверия к инвестиционным продуктам⁷. К числу стимулов развития внутреннего финансового рынка относятся создание и поддержка государством механизмов коллективного страхования (гарантирования) накоплений граждан как в банковском секторе, так и на рынке страхования и в негосударственных пенсионных фондах. Таким образом, потребность в страховании риска неисполнения обязательств финансовыми организациями обуславливает расширение круга общественных отношений гарантирования и указывает на намечающуюся тенденцию к обособлению системы страхования сбережений в рамках обязательного государственного (публичного) страхования как в теоретическом, так и в нормативно-правовом аспектах.

В свою очередь, признание необходимости построения на базе СГПУ новой системы гарантирования по договорам страхования жизни позволяет говорить о расширении предмета обязательного публичного страхования денежных средств граждан. Установление императивных норм, определяющих формы и способы финансового обеспечения в рамках гарантирования, расширение компетенции Агентства как особого субъекта, реализующего социально-значимую функцию, установление нового вида парafискалитетов (обязательных неналоговых платежей, устанавливаемых и взимаемых для достижения публично-значимых целей), к числу которых относятся гарантийные взносы, являющиеся источником формирования фонда

⁶ Основные направления единой государственной денежно-кредитной политики на 2024 год и период 2025 и 2026 годов. Одобрены Советом директоров Банка России 01.11.2023 // Официальный сайт Банка России.

⁷ Проект Основных направлений развития финансового рынка Российской Федерации на 2025 год и период 2026 и 2027 годов // Официальный сайт Банка России.

гарантирования, — всё это указывает на повышение приоритетности публично-правового способа регулирования. Функционирование же четырех самостоятельных систем обязательного публичного страхования денежных средств под управлением единого специального субъекта свидетельствует о возрастании социальной роли Агентства. Таким образом, наличие целевых предпосылок унификации систем гарантирования (страхования), по нашему мнению, является объективно подтвержденным фактом.

С точки зрения теории права и юридической техники привести к единообразию возможно только схожие (аналогичные) общественные отношения, в связи с чем принципиально важным является определение их периметра. Представляется очевидным, что СГПУ, равно как ССВ и иные системы, носит комплексный характер и включает не только финансово-правовые, но и иные виды отношений, которые обуславливают их функционирование, но не нуждаются в приведении к единообразию в рамках нормативного регулирования и предмета финансового права (например, административные отношения лицензирования, возникающие между Банком России и финансовыми организациями).

Проиллюстрируем данный тезис на примере СГПУ. Из содержания Федерального закона от 28.12.2022 № 555-ФЗ⁸ (далее — Закон о гарантировании прав участников НПФ) следует, что гарантированием является публично-правовое обязательство государства в лице специально уполномоченного субъекта (государственной корпорации «Агентство по страхованию вкладов») по выплате возмещения участникам негосударственного пенсионного фонда (далее — НПФ) или по переводу обязательств фонда, в отношении которого наступил гарантийный случай, в иной НПФ, за счет средств целевого публичного фонда денежных средств (фонда гарантирования пенсионных резервов). Содержанием гарантирования является право требования участника НПФ к специально уполномоченному субъекту (Агентству) о выплате гарантийного возмещения (переводу обязательств фонда);

Финансово-правовую природу в рамках гарантирования имеют следующие виды отношений:

- по формированию фонда гарантирования пенсионных резервов (включая вопросы взимания гарантийных взносов и применения мер ответственности за их неполную и несвоевременную уплату) [3];
- по осуществлению Агентством обязательств по выплате гарантийного возмещения и переводу обязательств в иной фонд-участник (включая связанные с указанной процедурой вопросы применения мер ответственности; учета обязательств фондов; раскрытия информации о наступлении гарантийного случая).

Единство и дифференциация нормативных актов в сфере страхования и гарантирования сбережений

Поскольку основой функционирования ССВ, СГПУ, гарантирования прав застрахованных лиц в системе обязательного пенсионного страхования и гарантирования по договорам страхования жизни являются соответствующие целевые публичные фонды денежных средств, аккумулируемые Агентством и управляемые им, обратимся к вопросу о единообразии соответствующих регулятивных норм.

Первое, что обращает на себя внимание — это терминологическая рассинхронизация Закона о страховании вкладов, Закона о гарантировании прав застрахованных лиц⁹, Закона о гарантировании прав участников НПФ, а также Федерального закона от 26.12.2024 № 477-ФЗ «О гарантировании прав по договорам страхования жизни» (далее — Закон № 477-ФЗ). При этом смысл, заложенный в базовые дефиниции гарантирования (гарантийный случай, гарантийный взнос, гарантийное возмещение), аналогичен терминам «страховой случай», «страховой взнос», «страховое возмещение». Следует признать, что отказ от единых дефиниций, присущих обязательному государственному страхованию в целом, затрудняет уяснение содержания указанных законов, равно как и понимание сути системы гарантирования и ее взаимосвязи с системой страхования вкладов.

С учетом системного подхода, общими являются также и следующие недостатки регулирования:

- отсутствие установленных пределов полномочий Агентства при рассмотрении заявлений о восстановлении срока подачи требований о выплате гарантийного возмещения (в частности, не урегулированы вопросы о том, правомочно ли Агентство запрашивать у заявителя дополнительные документы и является ли их непредоставление основанием отказа в восстановлении срока; имеет ли Агентство право самостоятельного получения необходимых для рассмотрения заявления документов, например, в порядке направления запросов в государственные органы);
- отсутствие в дефиниции гарантийных взносов признаков парафискалитета (за исключением указания на определение порядка их уплаты в соответствии со специальным законом).

Применительно к системе гарантирования по договорам страхования жизни существенными, на наш взгляд, являются вопросы:

- неопределенности правовой природы процентов за несвоевременную или неполную уплату гарантийных взносов. Закон № 477-ФЗ устанавливает,

⁸ Федеральный закон от 28.12.2022 № 555-ФЗ «О гарантировании прав участников негосударственных пенсионных фондов в рамках деятельности по негосударственному пенсионному обеспечению и формированию долгосрочных сбережений».

⁹ Федеральный закон от 28.12.2013 № 422-ФЗ «О гарантировании прав застрахованных лиц в системе обязательного пенсионного страхования Российской Федерации при формировании и инвестировании средств пенсионных накоплений, установлении и осуществлении выплат за счет средств пенсионных накоплений».

что проценты уплачиваются в порядке, предусмотренном статьей 395 ГК РФ; вместе с тем по своей сути обязанность по уплате гарантийных взносов является финансово-правовой, следовательно, механизм ответственности за неисполнение указанного обязательства не может регулироваться нормами гражданского законодательства;

- превалирования диспозитивного (разрешительного) метода при определении источников формирования целевого фонда в составе имущества Агентства, обеспечивающего функционирование новой системы гарантирования. В сравнении с источниками фонда обязательного страхования вкладов, фонда гарантирования пенсионных накоплений и фонда гарантирования пенсионных резервов отмечается установление трех источников финансово-правовой природы (гарантийные взносы, доходы от инвестирования средств фонда, процентов за несвоевременную или неполную уплату гарантийных взносов) одного источника гражданско-правового характера (денежные средства, полученные от реализации права требования к страховщику в размере уплаченной гарантийной выплаты). Иные источники не поименованы и носят открытый характер.

Отметим, что, в отличие от системы гарантирования прав участников, ведущая роль в регулировании системы гарантирования по договорам страхования жизни предоставлена Агентству, а не Банку России. Указанное следует из процедуры установления ставок гарантийных взносов решением Совета директоров Агентства, а не решением Совета директоров Банка России.

Заключение

Сравнительный анализ базовых регулятивных актов, определяющих вопросы функционирования систем страхования и гарантирования, указывает перспективную потребность в значительной переработке сложной системы норм, регулирующих вопросы выплаты возмещения гражданам. По нашему мнению, целесообразным является формирование единого кодифицированного документа, который будет определять как общие принципы и механизмы систем страхования (гарантирования), так и специальные нормы, отражающие специфику отдельных видов отношений, в том числе по договорам страхования жизни, негосударственному пенсионному обеспечению, в рамках программы долгосрочных сбережений.

Видится, что одновременно с приведением к единообразию систем гарантирования и страхования целесообразно рассмотреть вопрос конкретизации функционала Агентства в части:

- регламентации сроков и процедур досудебного урегулирования вопросов, связанных с пополнением целевых фондов денежных средств. Указанная потребность проистекает в том числе из отсутствия в Законе о гарантировании прав

участников НПФ норм, устанавливающих необходимость соблюдения претензионного порядка в виде направления Агентством в адрес НПФ требования об уплате гарантийного взноса до обращения в суд с иском о взыскании сумм неисполненных обязательств и пени. По нашему мнению, императивный характер обязанности НПФ по уплате гарантийных взносов и публичный характер обязанности Агентства по обеспечению функционирования СГПУ обуславливают необходимость квалификации направления требования об уплате и информирования Банка России как обязательных процедур, а не как субъективного права Агентства. Иное понимание нормы статьи 21 Закона № 555-ФЗ порождает ситуацию, в которой Агентство может не предпринимать активных действий для пополнения фонда гарантирования пенсионных резервов и по реагированию на нарушение обязательных требований закона со стороны НПФ.

- определения унифицированных механизмов восполнения дефицита целевых фондов денежных средств за счет средств федерального бюджета и кредитных средств Банка России.

Закон № 555-ФЗ не содержит специальной нормы, определяющей процедуры обеспечения финансовой устойчивости системы гарантирования, а имеет отсылку к Закону № 177-ФЗ, из которой следует, что для СГПУ применяются те же механизмы и процедуры, что и для ССВ (статья 22 Закона № 555-ФЗ). При этом формулировка статьи 19 Закона № 555-ФЗ о том, что источником фонда гарантирования пенсионных резервов являются «средства федерального бюджета в случаях и порядке, которые предусмотрены законодательством Российской Федерации», предполагает возможность выбора способа финансирования в рамках процедур, определенных Бюджетным кодексом РФ (БК РФ). В частности, формой привлечения федеральных средств является не только предоставление бюджетного кредита (статья 93.2 БК РФ), но также субсидии государственной корпорации (специальная статья 78.3 БК РФ введена в 2017 году).

Кроме того, развитие форм коллективной ответственности участников финансового рынка обуславливает перспективную потребность и в дальнейшем расширении круга полномочий Агентства, включении в систему страхования (гарантирования) и иных видов отношений.

Отмечаем, что вопросы кодификации и в целом переработки законодательства для обеспечения его актуального состояния и соответствия потребностям общества являются одними из самых острых в теории и практике. Например, до сих пор обсуждается необходимость разработки единого закона о финансах [4], кодификации предпринимательского законодательства [5] и ряд других. С учетом изложенного полагаем, что проблематика настоящего исследования послу-

жит движущей силой для дальнейшего осмысления правовой природы и роли системы обязательного государственного (публичного) страхования, а также подтолкнет широкий круг исследователей к дис-

куссии о системе законодательства, регулирующего процедуры возврата сбережений граждан Агентством по страхованию вкладов.

Литература

1. Паршукова А.П. К вопросу о правовой природе гарантирования прав и законных интересов участников негосударственных пенсионных фондов // Финансовое право. 2024. № 7. С. 23—27.
2. Турбанов А.В. Финансово-правовые основы создания и функционирования системы страхования банковских вкладов в Российской Федерации : дис. ... докт. юрид. наук: 12.00.14 // МГИМО (У) МИД России. М., 2004. 368 с.
3. Паршукова А.П. О правовой природе фонда гарантирования пенсионных резервов // Финансовое право. 2024. № 9. С. 2—5.
4. Горбунова О.Н., Поветкина Н.А., Леднева Ю.В. Направления совершенствования системы финансового законодательства Российской Федерации // Финансовое право. 2023. № 11. С. 3—11.
5. Ячменев Ю.В. О системе и систематизации предпринимательского законодательства: теоретические и правоприменительные аспекты // Третейский суд. 2022. № 2/3. С. 288—295.

SECTION:
PRIVATE LAW

ON THE QUESTION OF THE SYSTEM OF LAWS REGULATING THE REPAYMENT OF CITIZENS' SAVINGS BY THE DEPOSIT INSURANCE AGENCY

Anastasiia Parshukova, Head of the Division for Auditing the Activities of the Deposit Insurance Agency, Guaranteeing Retirement Savings and In-House Activities of the Internal Auditing Service of the Public Corporation "Deposit Insurance Agency", Moscow, Russian Federation.
E-mail: anastasia.p2018@mail.ru

Keywords: guarantee system, uniformity of regulation, non-government pension provision, long-term savings program, life insurance contract, financial market participants, deposit, long-term investment tool.

Abstract

Purpose of the study: analysis of the legal regulation of the procedures for the return of citizens' savings by the Deposit Insurance Agency (including deposit insurance, guaranteeing the rights of participants in non-state pension funds, guaranteeing under life insurance contracts).

Methods used in the study: systemic, comparative-legal method and synergetics method.

Study findings: the guarantee systems are considered in comparison and interrelation with the deposit insurance system. It is established that there is a genetic relationship between these systems, a single financial and legal basis for their functioning, expressed in the payment of compensation to citizens at the expense of special public funds of funds accumulated by the Deposit Insurance Agency. A justification is given for the position on expanding the subject of mandatory public insurance of citizens' monies due to the emergence of a new type of social relations, i.e. guarantees under life insurance contracts. Proposals have been developed to improve the regulatory framework through the creation of a single codified act that will determine both the general principles and mechanisms of compulsory public insurance (guarantee) of savings, and establish norms that reflect the specifics of certain types of relations.

Research novelty: the conclusion about the need for unification of legislation and the prospects for the adoption of a single regulatory act for these types of social relations is substantiated.

References

1. Parshukova A.P. K voprosu o pravovoi prirode garantirovaniia prav i zakonnykh interesov uchastnikov negosudarstvennykh pensionnykh fondov. Finansovoe pravo. 2024. No. 7. Pp. 23–27.

2. Turbanov A.V. Finansovo-pravovye osnovy sozdaniia i funktsionirovaniia sistemy strakhovaniia bankovskikh vkladov v Rossiiskoi Federatsii : dis. ... dokt. iurid. nauk: 12.00.14. MGIMO (U) MID Rossii. M., 2004. 368 pp.
3. Parshukova A.P. O pravovoi prirode fonda garantirovaniia pensionnykh rezervov. Finansovoe pravo. 2024. No. 9. Pp. 2–5.
4. Gorbunova O.N., Povetkina N.A., Ledneva Iu.V. Napravleniia sovershenstvovaniia sistemy finansovogo zakonodatel'stva Rossiiskoi Federatsii. Finansovoe pravo. 2023. No. 11. Pp. 3–11.
5. Iachmenev Iu.V. O sisteme i sistematizatsii predprinimatel'skogo zakonodatel'stva: teoreticheskie i pravoprimenitel'nye aspekty. Treteiskii sud. 2022. No. 2/3. Pp. 288–295.

АГЕНТНЫЕ МОДЕЛИ ПРИНЯТИЯ РЕШЕНИЙ НА ОСНОВЕ ГЕНЕРАТИВНОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бурий А.С.¹, Цаплина О.С.²

Ключевые слова: информационные технологии, системы поддержки принятия решений, большие языковые модели, мультиагентные технологии, агентное моделирование.

Аннотация

Цель работы: развитие концептуальных основ применения моделей адаптивных агентов для задач поддержки принятия решений на базе интеллектуальных многоагентных систем в формате виртуального помощника.

Методы исследования: системный и структурный анализ, концептуально-логическое моделирование, формально-логическая разработка и обоснование структур построения гибридных систем поддержки принятия решений на основе многоагентного подхода.

Результаты: получена формально-логическая трактовка концептуальной структуры построения междисциплинарной имитационной модели гибридной системы поддержки принятия решений на основе многоагентного представления вычислительного процесса. Дополнительные преимущества рассматриваемого подхода заключаются в возможности применения адаптивных агентов, реализованных на основе больших языковых моделей в развитии направления генеративного искусственного интеллекта, обеспечивающего повышение обоснованности принятия решений в системах информационного управления.

DOI: 10.24412/1994-1404-2025-1-101-109

Введение

Применение моделей искусственного интеллекта (ИИ) в различных системах мониторинга, анализа, оптимизации, оценки и прогнозирования комплексных процессов постоянно растет. Однако решение сложных задач в контурах управления в социально-технических предметных областях (ПрО) часто требует глубоких знаний технологических и информационно-коммуникационных процессов. Эти знания необходимы для получения данных и основанных на моделировании идей, которые обеспечивают обоснованность принятия решений.

Современные системы поддержки принятия решений (СППР) требуют постоянного совершенствования методов интеграции человеческого мышления с новейшими разработками в области методологии информационно-логического представления процессов управления, а также их модельно-алгоритмической реализации в вычислительных и эргатических структурах [16]. Комплексы моделирования и информационно-вычислительной техники [1], обеспечивая решение оптимизационных задач и совершенствование процессов интеллектуальной обработки информации, всё чаще работают в условиях многомерности данных,

роста их объема и адаптивности к процессам [6, 12], необходимости своевременного принятия эффективного для конкретной ситуации решения [2], в условиях ограничений [17] (временных, технических, технологических и др.) на принятие решений.

Инструменты ИИ открывают новую страницу современной эпохи цифровизации, включая:

- расширенный анализ больших данных в реальном масштабе времени [6, 19];
- междисциплинарный подход при решении многих задач управления и принятия решений [8, 9], включая этическую сторону (предвзятость, справедливость, конфиденциальность, прозрачность и др. факторы), что связывают в конечном счете с морализацией технологий [21];
- обеспечение доступными, быстро адаптируемыми, оперативными, целенаправленными, многовариантными методами совместной командной работы [20] на принципах коллективного интеллекта [8];
- имитационные модели на основе ИИ и интеллектуальных агентов [25], включая особенности ПрО проектирования (бортовые системы воздушных

¹ **Бурий Алексей Сергеевич**, доктор технических наук, заместитель начальника отдела Российского института стандартизации, ведущий научный сотрудник Института проблем управления им. В. А. Трапезникова Российской академии наук, г. Москва, Российская Федерация.

E-mail: a.s.burij@gostinfo.ru

² **Цаплина Ольга Сергеевна**, аспирант Российского института стандартизации, г. Москва, Российская Федерация.

E-mail: tsaplinaolga@inbox.ru

судов [3], концептуальное представление цифровых двойников [7], системы управления на основе многоагентных технологий [17]);

- СППР на основе интеллектуальных методов и алгоритмов ассистирования лицам, принимающим решения, в задачах визуализации³, экспертного оценивания [14], в составе рекомендательных систем [10, 14], систем проектирования [18], в системах семантического поиска информации на базе онтологии знаний [4].

Перспективным направлением развития интеллектуальных СППР выступает генеративный ИИ [11], реализованный на базе больших языковых моделей (LLM — Large Language Models) [5, 13], которые находят приложения в производственной [13] и научной сфере [5], в задачах поиска и раннего обнаружения киберугроз [15] в системах управления обучением [23]. Однако предполагаемые перспективы использования методов генеративного ИИ, по нашему мнению, еще полностью не раскрыты, и развитие инновационных приложений, включая системы подготовки и принятия решений, является актуальной научной проблемой.

Целью настоящего исследования является развитие концептуальных основ применения моделей адаптивных агентов в системах поддержки принятия решений на базе интеллектуальных многоагентных систем в формате виртуального помощника.

В этом контексте мы исследуем потенциал использования предварительно обученных больших языковых моделей для создания и представления знаний, поддержки операционных исследований.

Исследование предпосылок моделирования

Агентно-ориентированный подход уже нашел применение в таких областях, как распределенное решение сложных задач, реинжиниринг предприятий, телекоммуникации, электронный бизнес, проектирование и т. п. Важной областью применения мультиагентных технологий является моделирование. В этой области основоположник ИИ в нашей стране Д.А. Поспелов⁴ выделяет два класса задач:

1) задачи распределенного управления и задачи планирования достижения целей, где усилия разных агентов направлены на решение общей проблемы и необходимое обеспечение эффективного способа кооперации их деятельности;

2) задачи, где агенты самостоятельно решают свои локальные задачи, используя общие, как правило, ограниченные ресурсы.

Термин «агент» происходит от латинского глагола *agere*, что означает «действовать», «двигать», «править»,

«управлять». Понятие *агент* соответствует аппаратно или программно реализованной сущности, которая способна действовать в интересах достижения целей. Обобщая, под агентами будем понимать метаобъекты или некоторые интеллектуальные сущности, способные манипулировать другими информационными объектами, формировать собственные программы действий в рамках установленных целей, автономии и уровня доступности данных [9].

Введем понятия «событие» и «действие» как ключевые в моделях агентов. Под простейшим *событием* (e^t) понимается момент времени, в который произошло изменение значения какого-либо атрибута модели [2]:

$$e^t = \langle t, atr, z_1^{atr}, z_2^{atr} \rangle; z_1^{atr} \neq z_2^{atr}, \quad (1)$$

где t — момент времени; atr — атрибут; z_1^{atr} — значение атрибута до события e^t ; z_2^{atr} — значение атрибута после события.

Под *действием* (Act) будем понимать изменение состояний объекта или модели, происходящее за конечный промежуток времени. Действие характеризуется событием и функцией действия, приводящей к изменению значения атрибута объектов:

$$Act = \langle e, F^{Act}, \{atr\} \rangle, \quad (2)$$

где e — событие; F^{Act} — функция действия; $\{atr\}$ — множество изменяемых атрибутов.

В формате агентного представления взаимодействия агентов формализуем в виде следующего кортежа [9]:

$$Int = \langle \mathcal{A}, T, Pr \rangle, \quad (3)$$

где Int — взаимодействие⁵ агентов из множества агентов $\mathcal{A}$; T — множество типов агентов; Pr — множество программ (стандартов, сценариев) взаимодействия между агентами.

Агенты могут выполнять следующие (типовые, а также уникальные) действия [2]:

- анализировать окружение (текущую ситуацию);
- диагностировать ситуацию, обращаться к базе данных и знаний; в случае определения некоторой исключительной ситуации агент обеспечивает поиск решения (сценарий действий) в базе знаний или запрашивает дополнительные ресурсы;
- вырабатывать (принимать) решение;
- определять (переопределять) цели;
- контролировать достижение целей;
- делегировать цели другим объектам процесса преобразования ресурсов, а также другим агентам;
- обмениваться сообщениями.

На рис. 1 представлены категории агентов, основное предназначение которых может быть описано, основываясь на (1), (2), отображением вида:

$$\mathcal{A}: \{e\} \xrightarrow{\varphi} \{Act\}, \quad (4)$$

³ Интеллектуальные системы поддержки принятия решений — краткий обзор. URL: <https://habr.com/ru/companies/ods/articles/359188> (дата обращения: 25.01.2025).

⁴ Поспелов Д.А. Многоагентные системы — настоящее и будущее // Информационные технологии и вычислительные системы. 1998. № 1. С. 14—21.

⁵ Сокр. от англ. *interaction* — взаимодействие.

связывающего пространство состояний $\{e\}$ с областью принятых действий — множество $\{Act\}$, причем суть отображения φ и определяет категорию агента.

Для реактивного агента (РА) (рис. 1а) это обычная система правил действий вида (2), для совещательных агентов (рис. 1б) решаемые задачи усложняются.

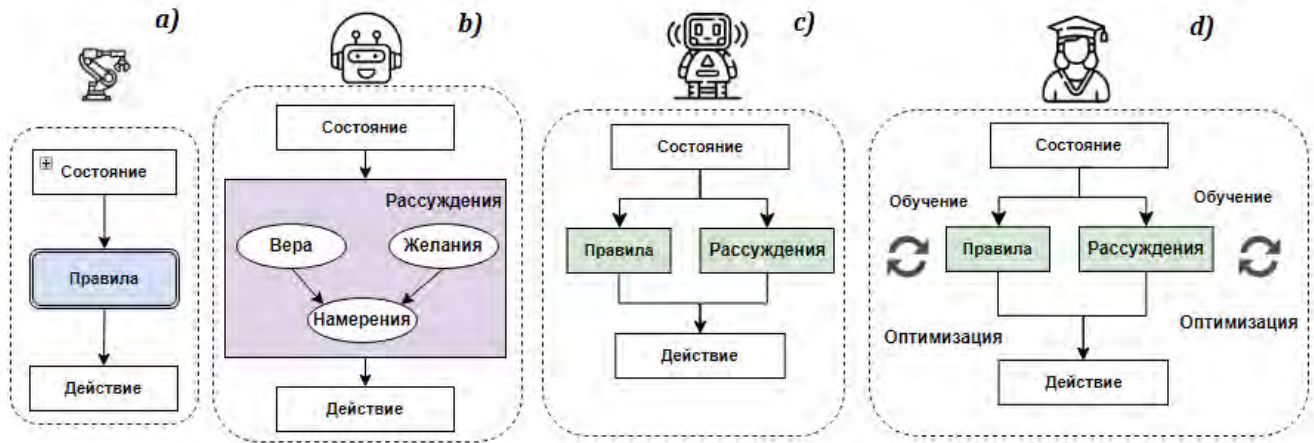


Рис. 1. Основные категории агентов:

а) — реактивный агент, б) — совещательный агент,
 в) — гибридный агент, г) — адаптивный агент

Совещательный агент (СА) обладает способностью описывать окружающую среду и логически рассуждать. Его поведение является результатом таких этапов переработки данных, как оценивание, моделирование и планирование [24]. Структура СА согласуется со структурой BDI-агентов: Убеждения (*Beliefs*) — Желания (*Desires*) — Намерения (*Intentions*), предложенной в работе A.S. Rao и M.P. Georgeff⁶. Иногда "*Beliefs*" переводится и как «представление», «убеждение», т. е. это восприятие агентом окружающей среды и своего собственного внутреннего состояния. Желание обозначает конкретную цель агента, а намерение символизирует пары «поведение — план», которым агент должен следовать и принять.

Выбор окончательных действий агентов осуществляется в соответствии с процедурой⁷ по аналогии с выражением (4):

$$select: Bel \times 2^G \xrightarrow{\varphi_{BDI}} \{Act\}, \quad (5)$$

где сформированные на основе представлений и намерений оперативные цели вида

$$(2^G): Bel \times Inten \rightarrow 2^G,$$

определяющие множество возможных действий агентов данной категории, где G — идентифицирует целевую принадлежность (от англ. *Goals*).

Гибридные агенты (ГА) (рис. 1в) применимы в многофункциональных подсистемах с вариативностью конфигураций (в том числе и в иерархических структу-

рах) [24]. ГА может справляться с реактивным поведением и поведением при долгосрочном планировании по отдельности, но плохо справляется со комплексными задачами и не может своевременно обновлять (менять) механизм принятия решений.

Адаптивный агент (АА) (рис. 1г) — доминирующая структура, используемая в настоящее время для моделирования виртуального общества в вычислительных экспериментах. Внутренний поток управления информацией связывает четыре модуля (восприятие, обучение, рассуждение и оптимизация) в единое целое. АА может собирать информацию из окружающей среды для выработки соответствующих планов, а затем корректировать свое поведение. После выполнения ряда действий АА может оптимизировать механизм принятия решений на основе результатов обратной связи.

ГА аккумулирует задачи вида (4) и (5). Для АА способен проводить некоторую диагностику ситуации: оценивать свои возможности (ресурсы), предлагать и осуществлять сценарии действий для достижения группы целей (в ходе, например, выполняемой стратегии).

Для многошаговых задач поиска оптимального решения с учетом моделируемых информационных объектов (ИО) — источников информации, преобразователей данных, процедур обработки и др. — на каждом шаге оценивают степень близости полученного результата к цели в виде [2]:

$$\Delta_{min} = \min(\Delta(IO_j^{i+1,i}) | IO_j^{i+1,i} \in MS), \quad (6)$$

где IO — модели ИО, j — номер модели ИО; i и $i+1$ — соседние шаги моделирования; MS — множество моделей ИО, используемых в моделирующем комплексе.

Таким образом, перебрав все решения, выбираем единственное. Решению должен соответствовать на-

⁶ Rao A.S., Georgeff M.P. BDI for agents: from theory to practice // In: Icmas. 1995. Vol. 95, pp. 312—319.

⁷ Бугайченко Д.Ю., Соловьев И.П. Абстрактная архитектура интеллектуального агента и методы её реализации // Системное программирование. 2005. Т. 1. № 1. С. 36—67.

бор действий как самого агента, так и элементов (процессов) информационного взаимодействия. Степень близости вида (б) может служить оценкой качества принимаемого решения.

Адаптивные агенты на основе искусственного интеллекта

В ходе анализа возможностей систем моделирования на основе инструментов ИИ ключевыми вопросами выступают: *автоматизация*, т. е. сокращение человеческого взаимодействия в операциях [25]; *когнитивность*, т. е. способность к обучению, рассуждению, извлечению знания из данных, имитация мыслительной деятельности человека; *интеллектуальные вычисления*, т. е. методы, направленные на усиление и поддержку естественного интеллекта (поддержку принятия решений экспертами)⁸.

Использование современных интеллектуальных технологий позволяет принимать более разумные и быстрые решения относительно бизнес-процессов, в итоге увеличивая производительность и эффективность всей операции, где ИИ выступает как ведущая технология в заданной ПрО.

Очевидно, что ИИ является чрезвычайно востребованной технологией для делового мира. Выделим следующие свойства ИИ, которые привлекают к нему как исследователей, так и потенциальных пользователей [22] (см. рис. 2):

- обучение: система ИИ обучается на данных для прогнозирования, анализа и принятия решений;
- восприятие: способность ИИ понимать и интерпретировать мир, имитируя человеческие чувства; эта способность включает в себя компьютерное зрение, обработку голоса и обработку естественного языка;
- предсказание: способность ИИ прогнозировать будущие результаты на основе прошлых данных и закономерностей, что выходит за рамки просто числовых или категориальных данных и включает в себя процедуры анализа разнотипных данных (текст, видео, аудио и др.) и регрессию, классификацию, прогнозирование временных рядов и обнаружение аномалий;

- взаимодействие: ИИ взаимодействует с окружающей средой и принимает решения, в том числе взаимодействуя с людьми;
- адаптивность: способность ИИ адаптироваться и совершенствоваться с течением времени на основе новых данных и меняющихся условий;
- рассуждение: способность ИИ рассуждать, планировать и принимать решения, которые имеют решающее значение для сложных задач. Эта способность включает в себя символическое мышление, планирование и принятие решений;
- креативность: способность генеративного ИИ влиять на человеческое творчество, предоставляя инструменты, расширяющие творческие возможности и оптимизирующие связанные рабочие процессы⁹.

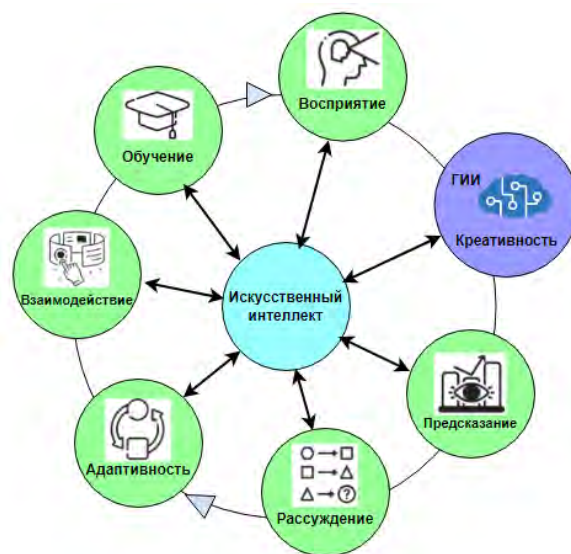


Рис. 2. Основные возможности систем искусственного интеллекта

Сравнение АА, реализующих интеллектуальные возможности LLM-моделей и обычных систем моделирования на основе агентов (ABM) представлено в таблице [24].

Таблица

Сравнение ABM и адаптивных агентов на основе LLM

Функции	ABM	АА на основе LLM
Гетерогенность	Большие данные расширяют функционал ABM, позволяя идентифицировать характеристики личности, реализовывать поведенческие модели и т. д., но это существенно усложняет модели агентов.	LLM позволяют разработать идеальные ролевые подсказки в соответствии с потребностями сценария и предоставить эти подсказки агенту на основе LLM, существенно расширяя возможности имитационных комплексов.

⁸ Массель Л.В., Массель А.Г. Интеллектуальные вычисления в исследованиях направлений развития энергетики // Известия Томского политехнического университета. 2012. Т. 321. № 5. С. 135—140.

⁹ Как генеративный ИИ меняет творческую работу. URL: <https://www.geeksforgeeks.org/> (дата обращения 29.01.2025).

Функции	АВМ	АА на основе LLM
Ограниченная рациональность	Встроенные психологические модели позволяют ограниченно реализовывать рациональность людей. Однако обобщенное моделирование весьма ограничено.	Избыточный для РА объем знаний грозит снизить доверие к модели. АА, управляемый подсказками, может выражать знания, которые не соответствуют объекту моделирования, вызывая галлюцинации в модели. Обычным решением является сбор актуальных событий {e}, связанных с персонажем, для формирования набора данных и точной настройки LLM, чтобы агент на основе LLM мог предсказывать способности персонажа.
Автономное принятие решений	Алгоритмы машинного обучения позволяют реализовывать агентами механизмы принятия решений на основе существующих данных, однако объем решаемых задач существенно ограничен.	Функционал СА, расширенный LLM, обеспечивает ИИ, подобным человеческому. Для агента, работающего на базе LLM, рассуждения являются ключом к достижению автономного принятия решений. Способность рассуждать является основой интеллекта и важна для принятия решений и критического анализа.
Обучение	Алгоритмы машинного обучения способны оптимизировать механизмы принятия решений на основе анализируемых данных во время работы агентов, но для этого обычно требуются четкие целевые функции и механизмы ее реализации.	LLM предоставляет агентам возможность автономного обучения во взаимодействии с оптимизацией механизмов принятия решений для адаптации к различным задачам и условиям. АА на базе LLM может принимать решения, обучаясь на аналогиях, а также реализуя непрерывное обучение.
Взаимодействие	Социальные сети помогают агентам определять взаимосвязь между различными объектами, но конкретные взаимодействия могут быть реализованы только путем передачи векторов состояний.	АА на базе LLM обладает способностью понимать язык и использовать естественный язык для взаимодействия и выполнения целевых задач. АА на базе LLM может использовать внешние инструменты (поиск, математические вычисления, перевод и т. д.) для значительного расширения своих функций.

Интеграция в многоагентных структурах

Представим концепцию многоагентных коллаборативных структур¹⁰ на основе LLM как развитие адаптивных агентов.

В обобщенном виде для многоагентной системы совместной работы раскроем множество агентов вида (4):

$$\mathcal{A} = \{a_i\}_{i=1}^n,$$

где n — количество агентов, которое предварительно определяется или динамически корректируется в зависимости от текущих требований системы; типы (T) агентов также могут учитываться, как $\sum_{k=1}^{|T|} n_k = n$, где $|T|$ — мощность множества типов агентов.

Будем описывать работу агента следующим кортежем [26]:

$$a_i = \langle m_i, o_i, \varepsilon_i, x_i, y_i \rangle, \quad (7)$$

где $m_i = \{St_i, zd_i, mem_i\}$ — модель i -го агента, состоящая из описания его структуры — St_i (для АА на LLM структуры представляют собой варианты язы-

ковых моделей), решаемых задач (zd_i) и реализованной в нем ситуативной памяти (mem_i), обеспечивающей необходимую коммутацию в зависимости от сложившейся ситуации; o_i — внутрисистемная цель i -го агента, например, типовые «ответ-вопрос» цифровых помощников [11], или минимизация перекрестной энтропии между сгенерированным ответом и истинным его значением (из базы данных) [26]; ε_i — среда или контекст, охватывающая состояние или условия (1), (2), в которых действует агент; x_i — входные данные агента, а atc_i — действие или выход, определяемый функцией

$$atc_i = \bar{m}(x_i, o_i, \varepsilon_i); atc_i \in \{Act\}. \quad (8)$$

Междисциплинарное пространство как совокупность в общем случае нескольких Про характеризуется:

- множеством целей $O = \{o_i\}$, формируемое за счет целевых задач отдельных агентов a_i вида (7), обеспечивая соответствие общей цели системы;
- общей информационной средой взаимодействия $E = \{\varepsilon_i\}$, из которой агенты получают контекстуальные данные; для интеллектуальных многоагентных систем среда может принимать различные формы, такие как базы данных, общие интерфейсы обмена сообщениями, среда принятия решений и др.;

¹⁰ Коллаборативные структуры — это формы совместной созидательной деятельности проектного характера в информационной среде, на междисциплинарной основе и особых нормах взаимодействия.

- множеством $\{Int\}$ интерфейсов (информационных каналов) вида (3) совместной работы, которые облегчают взаимодействие между агентами, позволяя обмениваться информацией на основе поставленных целей, окружающей среды и исходных данных, в качестве которых могут выступать результаты действия моделей ИО коллаборативных структур.

Агенты на основе LLM могут адаптивно взаимодействовать, способны реагировать на изменение требований задач, проходят предварительное обучение на различных наборах данных, чтобы обеспечить надежную базу знаний.

В ходе предварительного обучения каждый отдельный агент приобретает необходимые навыки и умения, гарантируя, что он сможет внести значимый вклад в среду совместной работы. Более того, каждый агент также может быть оснащен внешними инструментами, уникальными для его собственного типа.

Таким образом, междисциплинарная интегрированная модель может быть представлена кортежем следующего вида:

$$\overline{MS}: \langle \mathcal{A}; \{Int\}; O; E \rangle, \quad (9)$$

объединяющим множество разнотипных агентов, множество каналов взаимодействия, целевое множество (группы задействованных в проекте разнотипных агентов), множество состояний интегрированной информационной среды соответственно.

Процесс концептуальной реализации модели (9) включает следующие этапы:

- подготовительный этап, в ходе которого формируются все исходные множества в соответствии с выражениями (1) — (4);
- этап частных (однозадачных) экспериментов с агентами вида РА, СА, ГА, АА с оценкой эффективности принимаемых решений на примере выражения (6), а также в условиях вариативности

реализуемых сценариев управления принятием решений;

- этап интеллектуальной поддержки принятия решений на основе интеграции адаптивных агентов с привлечением возможностей генеративного ИИ в виде агентов на основе LLM для расширения области знаний лица, принимающего решение, в сложных условиях при анализе критических ситуаций, характеризующихся большей неопределенностью и временными ограничениями.

Заключение

Разработчики агентного моделирования часто предполагают, что их модели отражают некоторые общие закономерности и структуры, хотя они будут созданы с определенными параметрами для представления некоторых конкретных случаев.

Агенты — это особый тип ограниченного рационального программного агента, наделенного определенными ментальными установками (убеждениями, желаниями и намерениями), когда убеждения включают правила вывода, позволяющие строить цепочку к новым убеждениям.

Представленный подход к структурированию ПрО исследования для дальнейшей разработки имитационно-моделирующих комплексов позволяет с системных позиций рассмотреть состав элементов будущей системы, возможную ее структуру, а также выявить закономерности влияния изменения состава решаемых задач на требования к структуре, моделям, информационным объектам и в целом к информационной среде.

Предлагаемая структура характеризует сотрудничество по пяти ключевым параметрам: агентам, их типам, структурам, стратегиям и механизмам координации, обеспечивая систематический подход к анализу и разработке совместных взаимодействий в рамках многоагентного подхода с опорой на генеративный ИИ.

Литература

1. Агеева А.Ф. Обзор современных систем поддержки принятия решений, созданных при помощи агентного подхода // Электронные информационные системы. 2018. № 4 (19). С. 29—46.
2. Аксенов К.А., Гончарова Н.В. Гибридное моделирование мультиагентных процессов преобразования ресурсов: монография. М.: Издательский дом Академии Естествознания, 2019. 222 с.
3. Бельский А.Б., Чобан В.М., Дибичев А.К. Общие подходы и методы для внедрения технологий и элементов искусственного интеллекта в комплексы бортового оборудования вертолетной техники // Труды Академии наук авиации и воздухоплавания. 2024. № 2. С. 3—14.
4. Беляков С.Л., Боженюк А.В., Голова Н.А. [и др.] Интеллектуальная рекомендательная система для пространственного анализа // Известия ЮФУ. Технические науки. 2022. № 3 (227). С. 14—26. DOI: 10.18522/2311-3103-2022-3-14-26.
5. Брагин А.В., Бахтизин А.Р., Макаров В.Л. Большие языковые модели четвертого поколения как новый инструмент в научной работе // Искусственные общества. 2023. Т. 18. № 1. DOI: 10.18254/S207751800025046-9.
6. Бурый А.С. Облачные вычисления в цифровой трансформации информационных технологий // Правовая информатика. 2021. № 2. С. 4—14. DOI: 10.21681/1994-1404-2021-2-04-14.
7. Бурый А.С. Цифровые двойники как основа парадигмы развития прикладных информационных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2022. № 6 (70). С. 24—32.

8. Бурый А.С., Костылева К.В. Экспертное обоснование вариантов построения интеллектуальных систем на основе интеграции веб-технологий // Правовая информатика. 2024. № 4. С. 4—12. DOI: 10.24412/1994-1404-2024-4-4-12 .
9. Бурый А.С., Ловцов Д.А. Информационные структуры умного города на основе киберфизических систем // Правовая информатика. 2022. № 4. С. 15—26. DOI: 10.21681/1994-1404-2022-4-15-26 .
10. Бурый А.С., Ловцов Д.А. Архитектура экспертных рекомендательных систем принятия решений в формате умного города // Правовая информатика. 2023. № 3. С. 41—53.
11. Бурый А.С., Цаплина О.С. Генеративный искусственный интеллект цифрового университета // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 5 (80). С. 85—91.
12. Варламов О.О., Коценко А.А., Аладин Д.В. [и др.]. Миварные системы принятия решений роботов. РобоРазум : монография. М. : ООО «Научно-издательский центр ИНФРА-М», 2024. 549 с. ISBN: 978-5-16-020037-8.
13. Добренко Н.В., Добренко Д.А., Улизько М.В. Интеллектуальная поддержка принятия управленческих решений в mes-системах с использованием больших языковых моделей // Экономика. Право. Инновации. 2024. № 3. С. 47—59.
14. Калимуллина О.В., Ярцева К.А., Литун К.В. Роль экспертных и рекомендательных систем для интеллектуализации бизнеса: отраслевой анализ рынка // Вопросы инновационной экономики. 2022. Т. 12. № 3. С. 1613—1636. DOI: 10.18334/vinec.12.3.114969 .
15. Котенко И.В., Абраменко Г.Т. Использование больших языковых моделей для поиска угроз кибербезопасности на основе методов глубокого обучения: анализ современных исследований // Правовая информатика. 2024. № 3. С. 32—42. DOI: 10.24682/1994-1404-2024-3-32-42 .
16. Ловцов Д.А. Алгоритмизация в крупномасштабных иерархических эргасистемах // Правовая информатика. 2022. № 1. С. 4—14. DOI: 10.21681/1994-1404-2022-1-04-14 .
17. Маслобоев А.В. Принципы разработки прикладных мультиагентных систем управления жизнеспособностью критических инфраструктур // Труды Института системного анализа Российской академии наук. 2024. Т. 74. № 2. С. 62—81. DOI: 10.14357/20790279240208 .
18. Стешина Л.А., Петухов И.В. Концепция человеко-ориентированного проектирования сложных технических систем // Современные наукоемкие технологии. 2023. № 7. С. 92—96. DOI: 10.17513/snt.39700 .
19. Тимохин М.Ю., Шаранин В.Ю. Искусственный интеллект и теория принятия решений: современные тенденции // Инженерный вестник Дона. 2023. № 10 (106). С. 1—11.
20. Цаплина О.С. Думай и предпринимай. М. : Эксмо, 2024. 208 с. ISBN 978-5-9908890-1-9.
21. Шляпников В.В. Некоторые проблемы этики искусственного интеллекта // Идеи и идеалы. 2023. Т. 15. № 2-2. С. 365—376. DOI: 10.17212/2075-0862-2023-15.2.2-365-376 .
22. Jackson I., Ivanov D., Dolgui A., Namdar J. Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation. International Journal of Production Research. 2024. № 62 (17). С. 6120—6145. DOI: 10.1080/00207543.2024.2309309 .
23. Laeeq K., Memon Z.A. Scavenge: An intelligent multi-agent based voice-enabled virtual assistant for LMS. Interactive Learning Environments. 2021. Т. 29. № 6. С. 954—972.
24. Ma Q., Xue X., Zhou D., et al. Computational experiments meet large language model based agents: A survey and perspective. arXiv preprint, arXiv: 2402.00262, 2024.
25. Sarker I.H. AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Computer Science. 2022. № 3 (2). С. 158.
26. Tran K.T., Dao D., Nguyen M.D., et al. Multi-Agent Collaboration Mechanisms: A Survey of LLMs. arXiv preprint, arXiv: 2501.06322, 2025.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

AGENT-BASED MODELS FOR DECISION-MAKING USING GENERATIVE ARTIFICIAL INTELLIGENCE

Aleksei Buryi, Dr.Sc. (Technology), Deputy Head of Division of the Russian Standardisation Institute, Leading Researcher at the Trapeznikov Institute of Control Sciences of the Russian Academy of Sciences, Moscow, Russian Federation.
E-mail: a.s.burij@gostinfo.ru

Ol'ga Tsaplina, Ph.D. Student at the Russian Standardisation Institute, Moscow, Russian Federation.
E-mail: tsaplinaolga@inbox.ru

Keywords: *information technologies, decision support systems, large language models, multi-agent technologies, agent-based modelling.*

Abstract

Purpose of the paper: is to develop the conceptual foundations of the application of adaptive agent models for decision support tasks based on intelligent multi-agent systems in the digital assistant format.

Methods used in the study: system and structural analysis, conceptual and logical modeling, formal and logical development and improvement of structures for building hybrid decision support systems based on a multi-agent approach.

Study findings: a formal and logical interpretation of the conceptual structure of building an interdisciplinary simulation model of a hybrid decision support system based on a multi-agent representation of the computational process is obtained. Additional advantages of the considered approach are the possibility of using adaptive agents implemented on the basis of large language models in the development of the field of generative artificial intelligence, which provides increased validity of decision-making in information management systems.

References

1. Ageeva A.F. Obzor sovremennykh sistem podderzhki priniatiia reshenii, sozdannykh pri pomoshchi agentnogo podkhoda. Elektronnye informatsionnye sistemy. 2018. No. 4 (19). Pp. 29–46.
2. Aksenov K.A., Goncharova N.V. Gibridnoe modelirovanie mul'tiagentnykh protsessov preobrazovaniia resursov: monografiia. M. : Izdatel'skii dom Akademii Estestvoznaniia, 2019. 222 pp.
3. Bel'skii A.B., Choban V.M., Dibizhev A.K. Obshchie podkhody i metody dlia vnedreniia tekhnologii i elementov iskusstvennogo intellekta v kompleksty bortovogo oborudovaniia vertoletnoi tekhniki. Trudy Akademii nauk aviatsii i vozdukhoplavaniia. 2024. No. 2. Pp. 3–14.
4. Beliaikov S.L., Bozheniuk A.V., Golova N.A. [i dr.] Intellektual'naia rekomendatel'naia sistema dlia prostranstvennogo analiza. Izvestiia IuFU. Tekhnicheskie nauki. 2022. No. 3 (227). Pp. 14–26. DOI: 10.18522/2311-3103-2022-3-14-26 .
5. Bragin A.V., Bakhtizin A.R., Makarov V.L. Bol'shie iazykovye modeli chetvertogo pokoleniia kak novyi instrument v nauchnoi rabote. Iskusstvennye obshchestva. 2023. T. 18. No. 1. DOI: 10.18254/S207751800025046-9 .
6. Buryi A.S. Oblachnye vychisleniia v tsifrovoi transformatsii informatsionnykh tekhnologii. Pravovaia informatika. 2021. No. 2. Pp. 4–14. DOI: 10.21681/1994-1404-2021-2-04-14.
7. Buryi A.S. Tsifrovye dvoyniki kak osnova paradigmy razvitiia prikladnykh informatsionnykh sistem. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia. 2022. No. 6 (70). Pp. 24–32.
8. Buryi A.S., Kostyleva K.V. Ekspertnoe obosnovanie variantov postroeniia intellektual'nykh sistem na osnove integratsii veb-tekhnologii. Pravovaia informatika. 2024. No. 4. Pp. 4–12. DOI: 10.24412/1994-1404-2024-4-4-12 .
9. Buryi A.S., Lovtsov D.A. Informatsionnye struktury umnogo goroda na osnove kiberfizicheskikh sistem. Pravovaia informatika. 2022. No. 4. Pp. 15–26. DOI: 10.21681/1994-1404-2022-4-15-26 .
10. Buryi A.S., Lovtsov D.A. Arkhitektura ekspertnykh rekomendatel'nykh sistem priniatiia reshenii v formate umnogo goroda. Pravovaia informatika. 2023. No. 3. Pp. 41–53.
11. Buryi A.S., Tsaplina O.S. Generativnyi iskusstvennyi intellekt tsifrovogo universiteta. Informatsionno-ekonomicheskie aspekty standartizatsii i tekhnicheskogo regulirovaniia. 2024. No. 5 (80). Pp. 85–91.
12. Varlamov O.O., Kotsenko A.A., Aladin D.V. [i dr.]. Mivarnye sistemy priniatiia reshenii robotov. RoboRazum : monografiia. M. : OOO "Nauchno-izdatel'skii tsentr INFRA-M", 2024. 549 pp. ISBN: 978-5-16-020037-8.
13. Dobrenko N.V., Dobrenko D.A., Uliz'ko M.V. Intellektual'naia podderzhka priniatiia upravlencheskikh reshenii v mes-sistemakh s ispol'zovaniem bol'shikh iazykovykh modelei. Ekonomika. Pravo. Innovatsii. 2024. No. 3. Pp. 47–59.
14. Kalimullina O.V., Iartseva K.A., Litun K.V. Rol' ekspertnykh i rekomendatel'nykh sistem dlia intellektualizatsii biznesa: otraslevoi analiz rynka. Voprosy innovatsionnoi ekonomiki. 2022. T. 12. No. 3. Pp. 1613–1636. DOI: 10.18334/vinec.12.3.114969 .
15. Kotenko I.V., Abramenko G.T. Ispol'zovanie bol'shikh iazykovykh modelei dlia poiska ugroz kiberbezopasnosti na osnove metodov glubokogo obucheniia: analiz sovremennykh issledovani. Pravovaia informatika. 2024. No. 3. Pp. 32–42. DOI: 10.24682/1994-1404-2024-3-32-42 .
16. Lovtsov D.A. Algoritmizatsiia v krupnomasshtabnykh ierarkhicheskikh ergasistemakh. Pravovaia informatika. 2022. No. 1. Pp. 4–14. DOI: 10.21681/1994-1404-2022-1-04-14 .
17. Masloboev A.V. Printsipy razrabotki prikladnykh mul'tiagentnykh sistem upravleniia zhiznesposobnost'iu kriticheskikh infrastruktur. Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk. 2024. T. 74. No. 2. Pp. 62–81. DOI: 10.14357/20790279240208 .
18. Steshina L.A., Petukhov I.V. Kontseptsiiia cheloveko-orientirovannogo proektirovaniia slozhnykh tekhnicheskikh sistem. Sovremennye naukoemkie tekhnologii. 2023. No. 7. Pp. 92–96. DOI: 10.17513/snt.39700 .
19. Timokhin M.Iu., Sharanin V.Iu. Iskusstvennyi intellekt i teoriia priniatiia reshenii: sovremennye tendentsii. Inzhenernyi vestnik Dona. 2023. No. 10 (106). Pp. 1–11.
20. Tsaplina O.S. Dumai i predprinimai. M. : Eksmo, 2024. 208 pp. ISBN 978-5-9908890-1-9.

21. Shliapnikov V.V. Nekotorye problemy etiki iskusstvennogo intellekta. Idei i idealy. 2023. T. 15. No. 2-2. Pp. 365–376. DOI: 10.17212/2075-0862-2023-15.2.2-365-376 .
22. Jackson I., Ivanov D., Dolgui A., Namdar J. Generative artificial intelligence in supply chain and operations management: a capability-based framework for analysis and implementation. International Journal of Production Research. 2024. No. 62 (17). Pp. 6120–6145. DOI: 10.1080/00207543.2024.2309309 .
23. Laeeq K., Memon Z.A. Scavenge: An intelligent multi-agent based voice-enabled virtual assistant for LMS. Interactive Learning Environments. 2021. T. 29. No. 6. Pp. 954–972.
24. Ma Q., Xue X., Zhou D., et al. Computational experiments meet large language model based agents: A survey and perspective. arXiv preprint, arXiv: 2402.00262, 2024.
25. Sarker I.H. AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Computer Science. 2022. No. 3 (2). P. 158.
26. Tran K.T., Dao D., Nguyen M.D., et al. Multi-Agent Collaboration Mechanisms: A Survey of LLMs. arXiv preprint, arXiv: 2501.06322, 2025.

МЕТОДИКА ЗАЩИТЫ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ОТ СОСТЯЗАТЕЛЬНЫХ АТАК НА ОСНОВЕ ШУМОПОДАВЛЯЮЩИХ АВТОЭНКОДЕРОВ¹

Котенко И.В.², Ичетовкин Е.А.³

Ключевые слова: кибербезопасность, обнаружение вторжений, глубокое обучение, атаки на компоненты машинного обучения, автоэнкодер.

Аннотация

Цель работы: разработка методики защиты компонентов машинного обучения систем обнаружения вторжений от состязательных атак, таких как атака на основе метода быстрого знака градиента (Fast Gradient Sign Method), с использованием подсистемы защиты на основе автоэнкодеров.

Методы исследования: использование long short-term memory (LSTM) с добавлением гауссовского шума и регуляризации. Обучение модели производится на зашумленных данных, что позволяет игнорировать искажения и выделять ключевые признаки. В качестве метрик оценки для определения эффективности модели в условиях атак использовались F-мера, точность (precision) и полнота (recall). Эксперименты проводились на трех системах обнаружения вторжений (СОВ): системе обнаружения многошаговых вторжений, системе обнаружения вторжений на основе машинного обучения и системе обнаружения вторжений на основе глубокого обучения.

Результаты исследования: предложенный метод значительно повышает устойчивость СОВ к состязательным атакам. Для системы обнаружения многошаговых вторжений F-мера увеличилась с 0.67 до 0.97, для системы обнаружения вторжений на основе машинного обучения и системы обнаружения вторжений на основе глубокого обучения — с 0.57 до 0.92. Наилучшие результаты достигнуты при конфигурации количества нейронов входного слоя LSTM1=128, выходного слоя LSTM2=64 и уровне шума $\varepsilon=0.2$ —0.3. При этом точность и полнота также демонстрируют рост, что подтверждает эффективность метода. Использование LSTM с гауссовским шумом и регуляризацией приводит к повышению надежности классификации. Разработанная подсистема защиты позволяет использовать компоненты машинного обучения в различных системах обнаружения вторжений и позволяет обеспечить устойчивость к состязательным атакам.

DOI: 10.24412/1994-1404-2025-1-110-120

Введение

Информационные инфраструктуры критических приложений являются сложными гетерогенными системами. Они достаточно разнородны и могут состоять из совокупности различных объектов. К критическим могут быть отнесены системы, при компрометации которых будет поставлена под угрозу жизнь людей, нанесен экономический ущерб, создается угроза государству. Цифровизация таких инфраструктур сделала их подверженными не только физическим воздействиям, но и киберугрозам. Кибератаки чаще всего направлены на воздействие через вычислительные сети. Злоумышленники используют различ-

ные виды атакующих воздействий. Для защиты от такого рода атак применяют системы обнаружения вторжений (СОВ). В состав современных СОВ включаются компоненты машинного обучения (МО) для выявления ранее неизвестных типов атак и аномалий поведения сети. Такой подход характеризуется приемлемыми результатами детектирования без необходимости сложной настройки системы. Однако применяемые компоненты МО сами могут становиться потенциальными целями киберпреступников из-за подверженности особым видам атак — состязательным атакам, направленным на искажение и нарушение результатов работы

¹ Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

² **Котенко Игорь Витальевич**, заслуженный деятель науки РФ, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0001-6859-7120.

E-mail: ivkote@comsec.spb.ru

³ **Ичетовкин Егор Андреевич**, аспирант лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Российская Федерация.

E-mail: ichetovkin.e@iias.spb.su

компонентов МО. При атаках отравления данных злоумышленник компрометирует обучающий набор данных, а при атаках уклонения воздействует на систему МО с помощью специально сгенерированных входных данных. Такие атаки являются существенным препятствием для применения СОВ, основанных на МО [1].

Актуальность исследования заключается в нарастающем интересе в использовании компонентов МО в системах обнаружения вторжений. Так, например, в [2] предложен подход к синтезу модели МО для обнаружения сетевых атак. Такой подход позволяет эффективно выявлять аномалии в сетевом трафике. В [3] рассмотрена методика сбора обучающих данных, защищенных от атак отравлением. Этап сбора данных является ключевым этапом для повышения точности распознавания кибератак компонентами МО. В [4] проведено сравнение СОВ на основе МО с традиционными системами, основанными на сигнатурах. В [5] предложено применение глубокого обучения для анализа сетевого трафика, что позволяет повысить точность обнаружения атак, но также увеличивает сложность модели и ее уязвимость к атакам.

Полученные результаты показали, что методы МО обладают значительным преимуществом в обнаружении неизвестных ранее типов атак по сравнению с традиционными. Однако, как отмечают авторы рассмотренных работ, классификаторы, используемые в исследованиях, оказались уязвимы к состязательным атакам. Так, в [6] и [7] показано, как киберпреступники используют слабые места классификаторов на основе МО, применяя атаки на основе FGSM (Fast Gradient Sign Method, метод быстрого знака градиента). Это давно известный тип атаки, который обычно применяют для атак на классификаторы изображений. Атакующий создает некоторое количество незаметного для человека шума на входе, что приводит к неверному функционированию компонента МО. В [8] представлен анализ существующих средств защиты от состязательных атак. Выяснилось, что существующие методики защиты, например, такие, как «типичная тренировка противника» (typical enemy training), работают неэффективно. Подобные стратегии защиты часто игнорируют динамическую, многомерную природу сетевых данных [9]. Основная выявленная проблема, высвеченная в данной работе, — отсутствие работоспособной методики защиты компонентов МО систем обнаружения вторжений от состязательных атак [10].

В качестве базы для методики защиты в настоящей работе предложено использование нейронных сетей LSTM (long short-term memory, долгая краткосрочная память). Существующие исследования показывают эффективность применения данного подхода в СОВ, но только в качестве основы для обнаружения вторжений, так как LSTM хорошо справляется с последовательными шаблонами атак [11, 12]. В настоящей работе показана эффективность использования LSTM именно для защиты компонентов МО. Кроме того, отличительной чертой работы является ее практическая значи-

мость. Упор в исследовании делается на применение метрик, которые важны для корректной оценки работоспособности классификаторов систем обнаружения вторжений. Это такие метрики, как точность (precision), полнота (recall) и F-мера [13]. Указанный подход был использован также в работах [14] и [15], в которых решалась задача оценки применимости компонентов МО систем обнаружения вторжений при воздействии состязательных атак.

В настоящей работе представлено комплексное исследование различных моделей классификаторов компонентов МО систем обнаружения вторжений, например, ОС-SVM (One-Class Support Vector Machines, метод опорных векторов для одноклассовой классификации), RF (Random Forest, случайный лес) и другие. Для всех моделей было проведено моделирование атак и показана эффективность разработанной подсистемы защиты в условиях состязательных атак.

Метрики оценки воздействия и данные для моделирования

Для определения воздействия состязательных атак на компоненты МО систем обнаружения вторжений в работе используются классические метрики, применяемые для оценки эффективности классификаторов.

Точность, с которой система идентифицирует конкретную запись l из множества записей L как являющуюся частью атаки, определяется как:

$$Precision = \frac{TP}{TP+FP}. \quad (1)$$

Доля обнаруженных вредоносных событий от всех вредоносных событий в примере $l \in L$ описывается метрикой полноты системы:

$$Recall = \frac{TP}{TP+FN}. \quad (2)$$

F-мера гармонически объединяет полноту и точность:

$$F = 2 \frac{precision \times recall}{precision + recall}, \quad (3)$$

здесь TP, TN — количество правильно классифицированных положительных и отрицательных примеров, а FP, FN — количество ложноположительных и ложноотрицательных результатов [16].

Набор данных для экспериментальной части — это набор данных, разработанный Канадским институтом кибербезопасности (CICIDS). CICIDS содержит актуальный набор атак, позволяющих моделировать поведение вычислительной сети в различных состояниях. В наборе данных отдельные сетевые потоки размечены временными отрезками. CICIDS содержит данные о IP-адресах, портах, протоколах и атаках.

Набор данных использует систему В-профилей (behavioral profiles, поведенческих профилей) — моделей, которые описывают поведение в сети, для моделирования работы пользователей и генерации нейтрального фонового трафика.

Взаимодействие происходит на основе протоколов HTTP (HyperText Transfer Protocol, протокол передачи гипертекста), HTTPS (HyperText Transfer Protocol Secure, защищённый протокол передачи гипертекста), FTP (File Transfer Protocol, протокол передачи файлов), SSH (Secure Shell, безопасная оболочка), SSL (Secure Sockets Layer, уровень защищенных сокетов) и протоколов электронной почты SMTP (Simple Mail Transfer Protocol, простой протокол передачи почты), POP3 (Post Office Protocol, version 3, протокол почтового отделения, версия 3), IMAP (Internet Message Access Protocol, протокол доступа к электронной почте в Интернете).

В наборе данных присутствуют различные типы атак, такие как Heartbleed (уязвимость в SSL), веб-атаки, например, SQL-инъекции, XSS (Cross-Site Scripting, межсайтовый скриптинг), CSRF (Cross-Site Request Forgery, подделка межсайтовых запросов), ботнеты (сети заражённых компьютеров), DDoS (Distributed Denial of Service, распределённая атака на отказ в обслуживании) и другие [2, 17, 18].

Исследуемые COB применяют компоненты МО, основанные на различных моделях классификаторов для детектирования атак. Компоненты МО были обучены на наборе CICIDS [17].

Для эксперимента были отобраны семь различных моделей МО: Наивный Байес, DBN (Deep Belief Networks, глубокие сети доверия), QDA (Quadratic Discriminant Analysis, квадратичный дискриминантный анализ), Случайный лес, ID3 (Iterative Dichotomiser 3, итеративный дихотомизатор 3), AdaBoost (Adaptive Boosting, адаптивное бустирование), MLP (Multilayer Perceptron, многослойный перцептрон) и k-ближайших (k-Nearest Neighbors, k-ближайших соседей).

Эти модели характеризуются высокой точностью обнаружения кибератак [18—20]. Сравнительная характеристика моделей классификаторов в составе систем обнаружения вторжений с компонентами машинного обучения представлена в табл. 1.

Таблица 1

Сравнительная характеристика компонентов МО COB

Модель	COB	Показатели		
		F	Precision	Recall
OC-SVM / RF	COB-MB (Система обнаружения многошаговых вторжений) [18]	0.99	99.26	98.34
RF	COB-MO (Система обнаружения вторжений на основе МО) [19]	0.97	98.20	96.10
DBN	COB-ГО (Система обнаружения вторжений на основе глубокого обучения) [20]	0.94	88.70	99.70
MLP		0.87	81.70	99.50

Все модели COB с компонентами МО, представленные в табл. 1, реализованы на языке Python. COB-MB имеет архитектуру, включающую пять уровней: предварительная фильтрация, базовая классификация, углубленный анализ, принятие решений и обратная связь с обучением. На первом уровне происходит сбор и очистка сетевого трафика, на втором — начальная классификация с использованием простых алгоритмов МО, таких как деревья решений (Decision Trees). Для обработки аномалий применен третий уровень — глубокое обучение. На четвертом уровне модель осуществляет окончательную классификацию киберугрозы. Пятый уровень обеспечивает обновление модели через механизмы непрерывного обучения.

COB-MB разработана с использованием библиотек МО: Scikit-learn, TensorFlow и PyTorch. Для обработки больших объемов данных применяется Apache Spark, сбор сетевого трафика осуществляется через Wireshark и tcpdump. Данные хранятся в распределенных базах Apache Kafka и Elasticsearch. Система интегрирована с сетевыми устройствами через RESTful API и NETCONF. Разработчики COB-MB увеличили устойчивость, используя регуляризацию и адаптивное обучение. Одна-

ко авторы указывают на необходимость исследований в этой области для повышения надежности [18].

В [19] описана COB-MO. Она построена на моделях обучения с учителем. Использованы алгоритмы: RF, SVM и градиентное усиление (Gradient Boosting). Структура включает этапы предобработки данных, выделения признаков, обучения и тестирования. На этапе предобработки данные очищаются от шума и нормализуются для улучшения качества обучения. Для выделения признаков используются PCA (Principal Component Analysis, анализ главных компонент). Классификатор реализован с использованием библиотек Scikit-learn и XGBoost. Для ускорения применяются Pandas и NumPy. Разработчики COB-MO указывают на необходимость применения подсистемы защиты компонента МО [19].

COB-ГО использует многослойную архитектуру. Модель DBN реализована с использованием библиотек глубокого обучения TensorFlow и Keras. Система использует RBM (Restricted Boltzmann Machines, ограниченные машины Больцмана) в качестве скрытых слоев. Первый слой инициализируется входными данными, а последующие слои соединяются друг с другом. Входные данные для последующих уровней DBN также

обновляются, возвращая значение среднеквадратичной ошибки (MSE). Авторами всех вышеописанных систем обнаружения вторжений с компонентами МО высказано опасение, что они могут быть подвержены специфическим атакам на сам классификатор [18—20].

Состязательные атаки на компоненты МО

Исследование уязвимости компонентов МО проведено в рамках состязательных атак. Такие атаки представляют собой вмешательство в работу компонента МО. Злоумышленники изменяют входные данные с целью получения неверных результатов работы классификатора [21].

Атакующий, анализируя архитектуру и алгоритмы моделей, создает состязательный набор. Основная цель атакующего воздействия — добиться неверной

классификации или идентификации. В качестве состязательной атаки исследователями рассмотрен подход FGSM. Метод основан на вычислении градиентов функции потерь:

$$\eta = \varepsilon \text{sign} (\nabla \times J(w, x, y)), \quad (4)$$

где ε — это небольшая константа, определяющая величину возмущения, $\nabla \times J(w, x, y)$ — градиент функции потерь относительно входного образа x , а y — истинная метка [22]. В данной работе FGSM служит инструментом для исследования устойчивости моделей компонентов МО COB.

Ранее авторами уже было проведено исследование влияния состязательных атак на компоненты МО COB, представленных в таблице 1 [23, 24]. Для COB было проведено моделирование атак FGSM. Срезы результатов моделирования представлены в табл. 2.

Таблица 2

Воздействие FGSM-атаки на показатели классификаторов COB

Система обнаружения вторжений	ε	Показатели		
		F	Precision (%)	Recall (%)
COB-MB	0.00	0.98	99	98
	0.15	0.74	72	76
	0.30	0.57	52	64
COB-MO	0.00	0.97	98	96
	0.15	0.8	92	71
	0.30	0.67	84	56
COB-FO	0.00	0.94	88	99
	0.15	0.79	72	88
	0.30	0.65	60	72

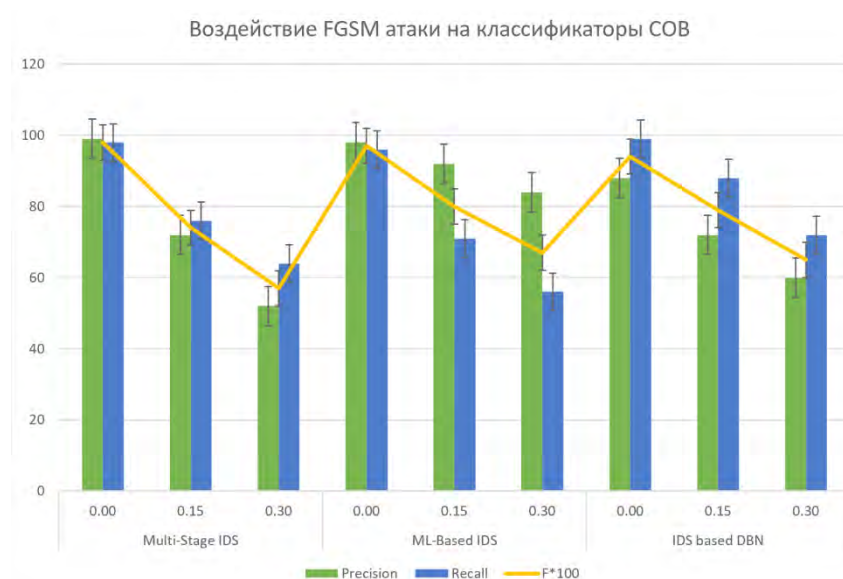


Рис. 1. Сравнительная диаграмма воздействия FGSM-атаки на показатели классификаторов COB

В таблице 2 сведены исследуемые показатели (1—3) ранее проведенных экспериментов по моделированию атак на компоненты МО COB [23]. На основе значений показателей в таблице 2 можно проанализировать тенденцию по снижению показателей классификаторов МО COB (рис. 1).

COB-MB демонстрирует высокую точность (0.99) и полноту (0.98) при отсутствии шума ($\varepsilon = 0.00$), однако с увеличением ε до 0.15 и 0.30 наблюдается значительное снижение всех метрик: точность падает до 0.74 и 0.57, а полнота — до 0.76 и 0.64 соответственно. Это указывает на низкую устойчивость системы к шуму и атакам.

COB-МО, напротив, показывает более сбалансированные результаты. При $\epsilon = 0.00$ точность (0.97) и полнота (0.96) близки к COB-MB, но F-мера выше (0.97), что свидетельствует о лучшем балансе между точностью и полнотой. С увеличением ϵ до 0.15 точность возрастает до 0.8, а полнота снижается до 0.71, что может говорить о более адекватной классификации. При $\epsilon = 0.30$ F-мера (0.67) остается выше, чем у COB-MB, что подтверждает лучшую устойчивость COB-МО к шуму.

COB-ГО при $\epsilon = 0.00$ демонстрирует максимальную полноту (0.99), но более низкую точность (0.94) по сравнению с другими системами. Это может указывать на склонность системы к ложным срабатываниям. С увеличением ϵ до 0.15 и 0.30 точность и полнота снижаются, но F-мера остается на приемлемом уровне (0.79 и 0.65 соответственно), что говорит о частичной устойчивости системы к шуму.

Вышеописанные COB уязвимы к шуму. Для их полноценной эксплуатации в критической инфраструктуре необходимо применение методики защиты от состязательных атак. Для этого далее будет представлена предлагаемая методика защиты компонентов МО COB.

Методика защиты

Существуют различные подходы к защите компонентов МО COB. Поскольку данные атаки так или иначе связаны с применением шума, то для защиты могут быть использованы шумоподавляющие автоэнкодеры (denoising autoencoders) [12, 25—27]. Шумоподавляющий автоэнкодер обучается на вредоносных наборах данных. В процессе обучения на вход подаются зашумленные данные, а на выходе получается значение без шума. Если x — оригинальный образ, а $\tilde{x}$ — зашумленный образ, то задача автоэнкодера заключается в минимизации разности между оригиналом и восстановленным образом:

$$L(x, \tilde{x}) = |x - \tilde{x}|^2, \quad (6)$$

где L — функция потерь (обычно используется среднеквадратичная ошибка) [25].

LSTM — это одна из архитектур шумоподавляющих автоэнкодеров. Для обучения LSTM на входные данные накладывается специально сгенерированный гауссовский шум, имитирующий атаку FGSM. Модели в таких условиях учатся отличать важные признаки исходного образа от случайного шума. После завершения обучения нейронные сети могут быть использованы для фильтрации входных состязательных образов. Такой подход позволяет повысить устойчивость компонентов МО COB. LSTM представляют из себя рекуррентные нейронные сети, которые способны запоминать состояния в течение длительных промежутков времени [12, 25—27].

Рассмотрим далее основные элементы LSTM: уровень (ворота) забывания (Forget Gate), вход (Input Gate),

предложенное значение (Candidate Values), выход (Output Gate).

Ворота забывания определяют информацию, которую необходимо забыть:

$$f_t = \sigma(W_f \cdot [h_t - 1, x_t] + b_f), \quad (7)$$

где f_t — вектор забывания в момент t , W_f — матрица весов для забывающего слоя, b_f — вектор смещения для забывающего слоя, σ — сигмоидная функция, возвращает от 0 до 1, $[h_t - 1, x_t]$ — конкатенация предыдущего состояния $h_t - 1$ и текущего входа x_t .

Вход добавляет информацию:

$$i_t = \sigma(W_i \cdot [h_t - 1, x_t] + b_i), \quad (8)$$

где i_t — вектор входа в момент t , W_i — матрица весов для входного слоя, b_i — вектор смещения для входного слоя, выходное состояние.

Предложенное значение:

$$C_t = \tanh(W_c \cdot [h_t - 1, x_t] + b_c), \quad (9)$$

где C_t — кандидатные значения в момент t , W_c — матрица весов для кандидатных значений, b_c — вектор смещения для кандидатных значений, $\tanh$ — гиперболический тангенс, значения от -1 до 1.

Обновление состояния:

$$C_t = f_t C_{t-1} + i_t \tilde{C}_t, \quad (10)$$

где C_t — новое состояние в момент t , C_{t-1} — предыдущее состояние на шаге $t - 1$, $\tilde{C}_t$ — вектор новых значений.

Выход:

$$o_t = \sigma(W_o \cdot [h_t - 1, x_t] + b_o), \quad (11)$$

где o_t — вектор выхода в момент t , W_o — матрица весов для выходного слоя, b_o — вектор смещения для выходного слоя.

Выходное состояние LSTM:

$$h_t = o_t \tanh(C_t), \quad (12)$$

где h_t — скрытое состояние (выход) в момент t .

Схема, описывающая реализацию подсистемы защиты на основе автоэнкодера с двумя LSTM слоями (входящий и выходящий), представлена на рис. 2.

Методика защиты компонентов МО COB с использованием подсистемы защиты включает в себя следующие блоки: загрузка и предобработка данных; создание модели LSTM; реализация атаки FGSM; обучение модели с защитой от атак; тестирование модели.

Обучение модели проводится с использованием средства оптимизации Adam. Для предлагаемой подсистемы защиты применяются следующие параметры: сгенерированный гауссовский уровень шума (Noise), количество нейронов входного (LSTM1) и выходного слоев (LSTM2). Такая настройка позволит оценить эффективность методики, реализованной в подсистеме защиты от атак уклонением на компоненты МО COB. Это нивелирует последствия FGSM-атаки.

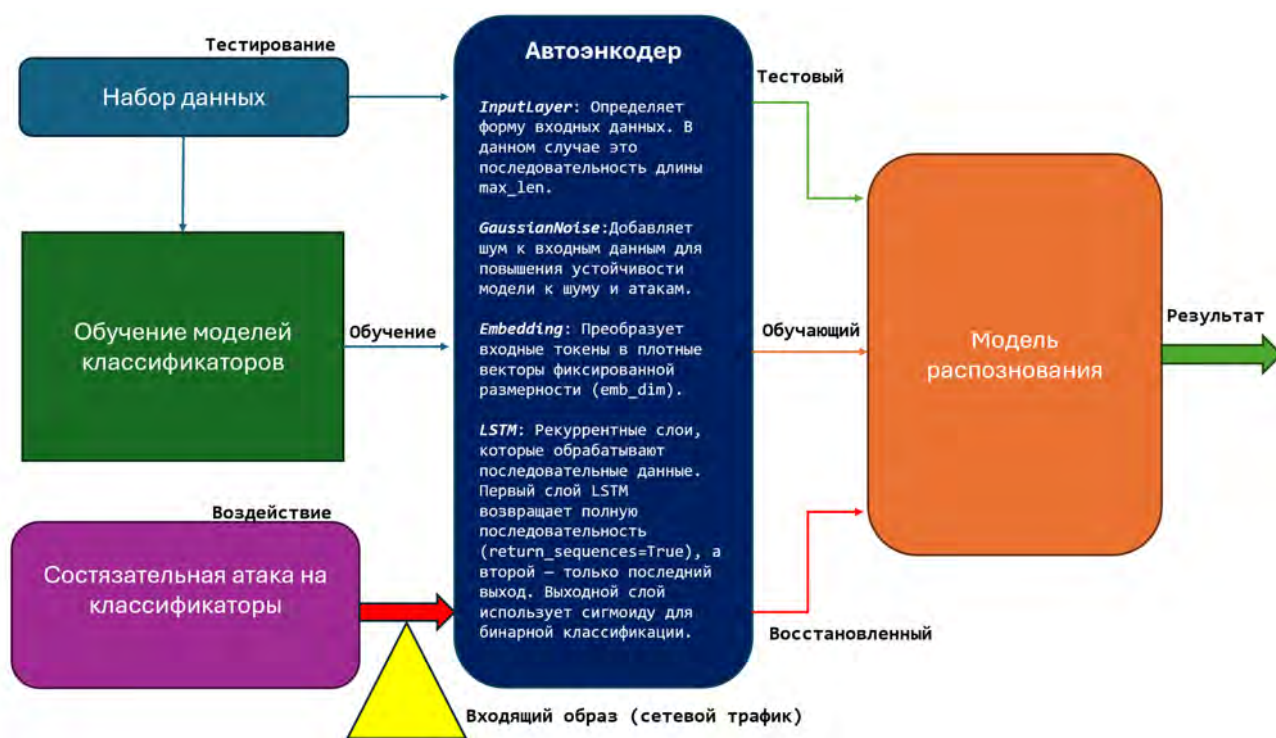


Рис. 2. Подсистема защиты компонентов МО COB

Анализ эффективности методики

Для оценки эффективности подсистемы защиты используем метрики (1—3). Модели классификаторов, которые исследованы, представлены в таблице 1. Сетевые атаки смоделированы проверочной выборкой из CICIDS. В качестве атак на компоненты МО COB применяется FGSM с параметром $\epsilon = 0.3$ (4). Подсистема защиты реализована на базе LSTM.

В эксперименте использования подсистемы защиты для COB-MB наблюдаются признаки линейной зависимости показателей (1—3) на тестируемом участке. Можно предположить, что локальное насыщение наступает в конце при количестве нейронов входного слоя $LSTM1 = 128$, выходного $LSTM2 = 64$, уровня гауссовского шума $Noise = 0,3$. Результаты восстановления параметров детектирования: $F = 0.92$, $Precision = 88$, $Recall = 96$.

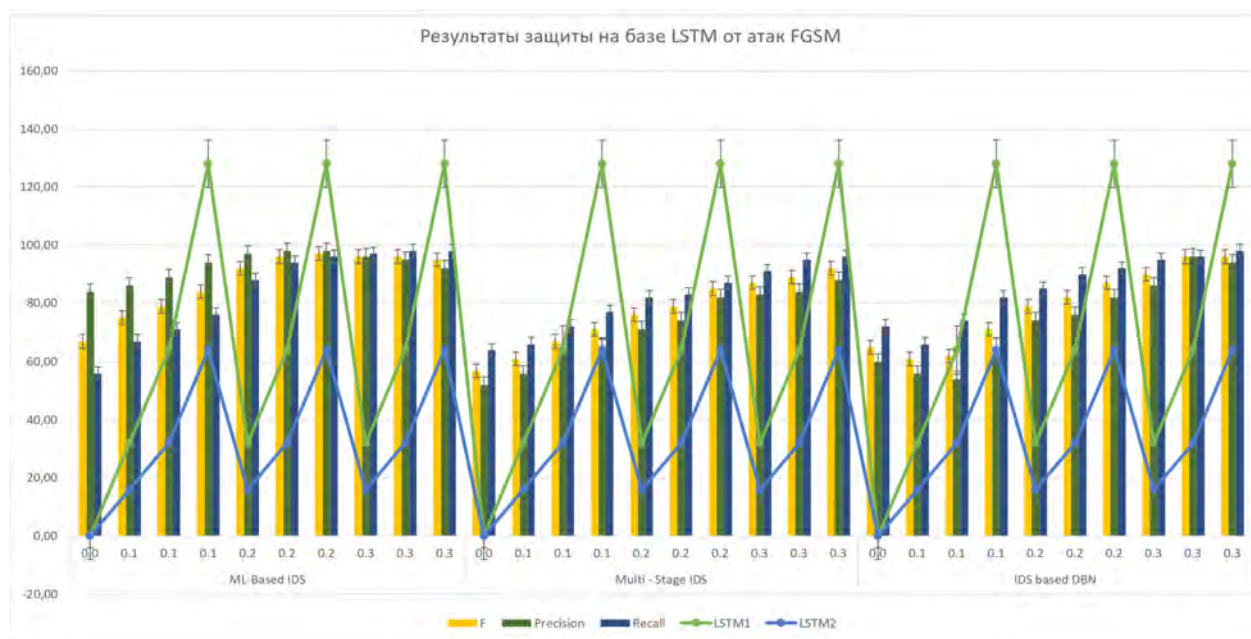


Рис. 3. Результаты работы подсистемы защиты

Воздействие FGSM-атаки на показатели классификаторов COB

COB	FGSM	Подсистема защиты			Показатели		
					F*100	Precision (%)	Recall (%)
	ε	Noise	LSTM1	LSTM2			
COB-MB	0.30	0.00	0	0	67,00	84,00	56,00
		0.10	32	16	75,00	86,00	67,00
		0.10	64	32	79,00	89,00	71,00
		0.10	128	64	84,00	94,00	76,00
		0.20	32	16	92,00	97,00	88,00
		0.20	64	32	96,00	98,00	94,00
		0.20	128	64	97,00	98,00	96,00
		0.30	32	16	96,00	96,00	97,00
		0.30	64	32	96,00	95,00	98,00
		0.30	128	64	95,00	92,00	98,00
COB-MO		0.00	0	0	57,00	52,00	64,00
		0.10	32	16	61,00	56,00	66,00
		0.10	64	32	67,00	63,00	72,00
		0.10	128	64	71,00	65,00	77,00
		0.20	32	16	76,00	71,00	82,00
		0.20	64	32	79,00	74,00	83,00
		0.20	128	64	85,00	82,00	87,00
		0.30	32	16	87,00	83,00	91,00
		0.30	64	32	89,00	84,00	95,00
		0.30	128	64	92,00	88,00	96,00
COB-ГО		0.00	0	0	57,00	52,00	64,00
		0.10	32	16	61,00	56,00	66,00
		0.10	64	32	67,00	63,00	72,00
		0.10	128	64	71,00	65,00	77,00
		0.20	32	16	76,00	71,00	82,00
		0.20	64	32	79,00	74,00	83,00
		0.20	128	64	85,00	82,00	87,00
		0.30	32	16	87,00	83,00	91,00
		0.30	64	32	89,00	84,00	95,00
		0.30	128	64	92,00	88,00	96,00

Для COB-MO удалось практически полностью восстановить работоспособность системы. Пределом восстановления стали параметры $LSTM1 = 32$, $LSTM2 = 16$, $Noise = 0,3$. При таких параметрах удалось добиться следующих результатов работы системы: $F = 0.96$,

$Precision = 96$, $Recall = 97$. Разница между исходными параметрами незначительная.

В эксперименте с COB-ГО наблюдаются потенциально интересные явления для гармонической метрики F , которая в конце сближается с $Recall$. Насыщение проис-

ходит при параметрах, близких к $LSTM1 = 64$, $LSTM2 = 32$, $Noise = 0.3$. Получены результаты $F = 0.96$, $Precision = 94$, $Recall = 98$. Параметры восстановлены до приемлемого уровня. Полученные параметры работы подсистемы защиты представлены в табл. 3 выше.

Таким образом, в экспериментах были исследованы системы обнаружения вторжений с компонентами МО, описанными в [18—20]. Результаты экспериментов показали, что применение предложенной методики защиты позволяет защитить компоненты МО СОВ от атак уклонением и восстановить метрики F , $Precision$, $Recall$ фактически до исходных параметров, что изображено на рис. 3 выше.

Предложенный подход демонстрирует достаточно высокую эффективность защиты компонентов машинного обучения систем обнаружения вторжений от состязательных атак, таких как FGSM. В отличие от традиционных методов, которые фокусируются на повышении точности классификации, данный подход решает проблему устойчивости моделей к атакам. Использование LSTM с добавлением гауссовского шума ($\epsilon = 0.1—0.3$) и регуляризации (Dropout, L2) позволяет модели эффективно классифицировать атаки и противостоять искажениям входных данных. Это подтверждается ростом F -меры с 0.67 до 0.97 для СОВ-МВ, с 0.57 до 0.92 для СОВ-МО и СОВ-ГО.

Заключение

В статье представлена методика защиты компонентов МО СОВ критических инфраструктур. В качестве основного инструмента защиты предлагается при-

менение подсистемы защиты на базе Long Short-Term Memory. Проведен обзор релевантных работ и описан математический аппарат защиты. Проведено моделирование атак уклонением Fast Gradient Sign Method с последующей защитой. Предложенная методика защиты реализована на языке Python. Методика показала возможность восстановления метрик детектирования F , $precision$, $recall$ к значениям, близким к исходным. Полученные показатели эффективности превосходят известные методы, такие как TIDCS (A Dynamic Intrusion Detection and Classification System Based on Feature Selection, динамическая система обнаружения и классификации вторжений на основе выбора признаков) [2], показатели которого для F -меры 0.85. В предложенной реализации удалось достичь значений 0.97 для СОВ-МВ и 0.92 для СОВ-МО и СОВ-ГО.

Следует отметить, что исследование применимости LSTM для сетевых данных еще не завершено, и полученные результаты являются базисом для последующих исследований. Существующие исследования, например, [13] и [21], рассматривают LSTM только в приложениях компьютерного зрения и промышленных системах. Обзорные работы, например, [28], дают только общее представление о методах защиты, без раскрытия конкретных решений. Новизна предложенной методики заключается в комбинировании LSTM, состязательного обучения и регуляризации. Полученные результаты направлены на повышение устойчивости СОВ к состязательным атакам.

Направление дальнейшего исследования видится в разработке методики защиты компонентов МО СОВ более широкого спектра классификаторов.

Рецензент: **Лаута Олег Сергеевич**, доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия.
E-mail: laos-82@yandex.ru

Литература

1. Ковцур М.М., Кириллов Д.И., Михайлова А.В., Потемкин П.А. Разработка методики внедрения машинного обучения для повышения информационной безопасности web-приложения // Техника средств связи. 2020. № 4 (152). С. 74—86.
2. Chkirbene Z., Erbad A., Hamila R., Mohamed A., Guizani M., Hamdi M. TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection. IEEE Access. 2020. Vol. 8. P. 95864—95877. DOI: 10.1109/ACCESS.2020.2994959.
3. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды ИСП РАН. 2021. Т. 33. Вып. 5. С. 83—104. DOI: 10.15514/ISPRAS-2021-33(5)-5.
4. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. 2022. Т. 34. Вып. 5. С. 111—126. DOI: 10.15514/ISPRAS-2022-34(5)-7.
5. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Никольская А.Г., Рыболовлев Д.А. Состязательные атаки против системы обнаружения вторжений, основанной на применении методов машинного обучения // Проблемы информационной безопасности. Компьютерные системы. 2023. № 4. С. 156—190. DOI: 10.48612/jisp/etr-5pxb-akt8.

6. Alhajjar E., Maxwell P., Bastian N. Adversarial Machine Learning in Network Intrusion Detection Systems. *Expert Systems with Applications*. 2021. Vol. 186. P. 115782. DOI: 10.1016/j.eswa.2021.115782 .
7. Alotaibi A., Rassam M.A. Adversarial Machine Learning Attacks Against Intrusion Detection Systems: A Survey on Strategies and Defense. *Future Internet*. 2023. Vol. 15. No. 2. P. 62. DOI: 10.3390/fi15020062 .
8. Apruzzese G., Andreolini M., Ferretti L., Marchetti M., Colajanni M. Modeling Realistic Adversarial Attacks Against Network Intrusion Detection Systems. *Digital Threats: Research and Practice*. 2022. Vol. 3. No. 3. P. 1–19. DOI: 10.1145/3530870 .
9. Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А., Никольская А.Г. Применение глубокого обучения для обнаружения компьютерных атак в сетевом трафике // *Труды ИСП РАН*. 2023. Т. 35. Вып. 4. С. 65—92. DOI: 10.15514/ISPRAS-2023-35(4)-3 .
10. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. Атаки и методы защиты в системах машинного обучения: анализ современных исследований // *Вопросы кибербезопасности*. 2024. № 1 (59). С. 24—37. DOI: 10.21681/2311-2024-1-24-37 .
11. Ravi V., Chaganti R., Alazab M. Recurrent Deep Learning-Based Feature Fusion Ensemble Meta-Classifer Approach for Intelligent Network Intrusion Detection System. *Computers and Electrical Engineering*. 2022. Vol. 102. P. 108156. DOI: 10.1016/j.compeleceng.2022.108156 .
12. Nazir A. et al. A Deep Learning-Based Novel Hybrid CNN-LSTM Architecture for Efficient Detection of Threats in the IoT Ecosystem // *Ain Shams Engineering Journal*. 2024. P. 102777. DOI: 10.1016/j.asej.2024.102777 .
13. Akhtar N., Mian A., Kardan N., Shah M. Advances in Adversarial Attacks and Defenses in Computer Vision: A Survey. *IEEE Access*. 2021. Vol. 9. P. 155161–155196. DOI: 10.1109/ACCESS.2021.3127960 .
14. Alahmed S., Alasad Q., Hammood M.M., Yuan J.-S., Alawad M. Mitigation of Black-Box Attacks on Intrusion Detection Systems-Based ML. *Computers*. 2022. Vol. 11. No. 7. P. 115. DOI: 10.3390/computers11070115 .
15. Mohammadian H., Ghorbani A.A., Lashkari A.H. A Gradient-Based Approach for Adversarial Attack on Deep Learning-Based Network Intrusion Detection Systems. *Applied Soft Computing*. 2023. Vol. 137. P. 110173. DOI: 10.1016/j.asoc.2023.110173 .
16. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches. *Transactions on Emerging Telecommunications Technologies*. 2021. Vol. 32. No. 1. P. e4150. DOI: 10.1002/ett.4150 .
17. Kurniabudi, Stiawan D., Darmawijoyo, Idris M.Y. Bin, Bamhdi A.M., Budiarto R. CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection. *IEEE Access*. 2020. Vol. 8. P. 132911–132921. DOI: 10.1109/ACCESS.2020.3009843 .
18. Verkerken M. et al. A Novel Multi-Stage Approach for Hierarchical Intrusion Detection. *IEEE Transactions on Network and Service Management*. 2023. Vol. 20. No. 3. P. 3915–3929. DOI: 10.1109/TNSM.2023.3259474 .
19. Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 // *Труды ИСП РАН*. 2020. Т. 32. Вып. 5. С. 81—94. DOI: 10.15514/ISPRAS-2020-32(5)-6 .
20. Belarbi O., Khan A., Carnelli P., Spyridopoulos T. An Intrusion Detection System Based on Deep Belief Networks // *The 4th International Conference on Science of Cyber Security (SciSec 2022)*. Springer International Publishing, Cham, 2022. P. 377–392. DOI: 10.48550/arXiv.2207.02117 .
21. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial Attacks on Machine Learning Cybersecurity Defences in Industrial Control Systems. *Journal of Information Security and Applications*. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2021.102717 .
22. Aldweesh A., Derhab A., Emam A.Z. Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues. *Knowledge-Based Systems*. 2020. Vol. 189. P. 105124. DOI: 10.1016/j.knsys.2019.105124 .
23. Ichetovkin E., Kotenko I. Modeling Poisoning Attacks Against Machine Learning Components of Intrusion Detection Systems. 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM). Altai, Russian Federation, 2024. P. 1850–1855. DOI: 10.1109/EDM61683.2024.10615198 .
24. Ichetovkin E., Kotenko I. Modeling Attacks on Machine Learning Components of Intrusion Detection Systems. 2024 International Russian Smart Industry Conference (SmartIndustryCon). Sochi, Russian Federation, 2024. P. 261–266. DOI: 10.1109/SmartIndustryCon61328.2024.10515506 .
25. Laghrissi F.E., Douzi S., Douzi K., Hssina B. Intrusion Detection Systems Using Long Short-Term Memory (LSTM) // *Journal of Big Data*. 2021. Vol. 8. No. 1. P. 65. DOI: 10.1186/s40537-021-00453-7 .
26. Ayub M.A., Johnson W.A., Talbert D.A., Siraj A. Model Evasion Attack on Intrusion Detection Systems Using Adversarial Machine Learning. 2020 54th Annual Conference on Information Sciences and Systems (CISS). 2020. P. 1–6. DOI: 10.1109/CISS48834.2020.1570617295 .
27. Chou D., Jiang M. A Survey on Data-Driven Network Intrusion Detection. *ACM Computing Surveys (CSUR)*. 2021. Vol. 54. No. 9. P. 1–36. DOI: 10.1145/3477132 .
28. Jmila H., Khedher M.I. Adversarial Machine Learning for Network Intrusion Detection: A Comparative Study. *Computer Networks*. 2022. Vol. 214. P. 109073. DOI: 10.1016/j.comnet.2022.109073 .

A TECHNIQUE FOR PROTECTING INTRUSION DETECTION SYSTEMS AGAINST ADVERSARIAL ATTACKS BASED ON DENOISING AUTOENCODERS

Igor' Kotenko, Honoured Figure of Science of the Russian Federation, Dr.Sc. (Technology), Professor, Principal Researcher and Head of the Laboratory for Computer Security Problems of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation. ORCID: 0000-0001-6859-7120.

E-mail: ivkote@comsec.spb.ru

Egor Ichetovkin, Ph.D. student at the Laboratory for Computer Security Problems of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation.

E-mail: ichetovkin.e@ias.spb.su

Keywords: cyber security, intrusion detection, deep learning, attacks against machine learning components, autoencoder.

Abstract

Purpose of the work: development of a technique to protect machine learning components of intrusion detection systems from adversarial attacks such as Fast Gradient Sign Method using an autoencoder based defense subsystem.

Methods used in the study: application of long short-term memory (LSTM) with the addition of Gaussian noise and regularisation. The model is trained on noisy data, which allows it to ignore distortions and highlight key features. F-measure, precision and recall were used as evaluation metrics to assess the performance of the model under attack. Experiments were conducted on three intrusion detection systems (IDS): Multi-Stage IDS, Machine Learning-Based IDS and Deep Learning-Based IDS.

Study findings: the technique significantly improves the robustness of IDSs to adversarial attacks. For Multi-Stage IDS, the F-measure increased from 0.67 to 0.97, for Machine Learning-Based IDS and Deep Learning-Based IDS from 0.57 to 0.92. The best results are achieved when the configuration of the number of neurons of the input layer $LSTM1=128$, the output layer $LSTM2=64$ and the noise level $\epsilon=0.2-0.3$. Precision and recall also show an increase, which confirms the effectiveness of the method. The use of LSNM with Gaussian noise and regularisation improves the reliability of classification. The technique provides robustness against adversarial attacks. The developed defense subsystem allows the use of machine learning components in different intrusion detection systems.

References

1. Kovtsur M.M., Kirillov D.I., Mikhailova A.V., Potemkin P.A. Razrabotka metodiki vnedreniia mashinnogo obucheniia dlia povysheniia informatsionnoi bezopasnosti web-prilozheniia. Tekhnika sredstv svyazi. 2020. No. 4 (152). Pp. 74–86.
2. Chkirbene Z., Erbad A., Hamila R., Mohamed A., Guizani M., Hamdi M. TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection. IEEE Access. 2020. Vol. 8. P. 95864–95877. DOI: 10.1109/ACCESS.2020.2994959.
3. Get'man A.I., Goriunov M.N., Matskevich A.G., Rybolovlev D.A. Metodika sbora obuchaiushchego nabora dannykh dlia modeli obnaruzheniia komp'iuternykh atak. Trudy ISP RAN. 2021. T. 33. Vyp. 5. Pp. 83–104. DOI: 10.15514/ISPRAS-2021-33(5)-5.
4. Get'man A.I., Goriunov M.N., Matskevich A.G., Rybolovlev D.A. Sravnenie sistemy obnaruzheniia vtorzhenii na osnove mashinnogo obucheniia s signaturnymi sredstvami zashchity informatsii. Trudy ISP RAN. 2022. T. 34. Vyp. 5. Pp. 111–126. DOI: 10.15514/ISPRAS-2022-34(5)-7.
5. Get'man A.I., Goriunov M.N., Matskevich A.G., Nikol'skaia A.G., Rybolovlev D.A. Sostizatel'nye ataki protiv sistemy obnaruzheniia vtorzhenii, osnovannoi na primenenii metodov mashinnogo obucheniia. Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy. 2023. No. 4. Pp. 156–190. DOI: 10.48612/jisp/etr-5pxb-akt8.
6. Alhajjar E., Maxwell P., Bastian N. Adversarial Machine Learning in Network Intrusion Detection Systems. Expert Systems with Applications. 2021. Vol. 186. P. 115782. DOI: 10.1016/j.eswa.2021.115782.
7. Alotaibi A., Rassam M.A. Adversarial Machine Learning Attacks Against Intrusion Detection Systems: A Survey on Strategies and Defense. Future Internet. 2023. Vol. 15. No. 2. P. 62. DOI: 10.3390/fi15020062.

8. Apruzzese G., Andreolini M., Ferretti L., Marchetti M., Colajanni M. Modeling Realistic Adversarial Attacks Against Network Intrusion Detection Systems. *Digital Threats: Research and Practice*. 2022. Vol. 3. No. 3. P. 1–19. DOI: 10.1145/3530870.
9. Get'man A.I., Goriunov M.N., Matskevich A.G., Rybolovlev D.A., Nikol'skaia A.G. Primenenie glubokogo obucheniia dlia obnaruzheniia komp'iuternykh atak v setevom trafike. *Trudy ISP RAN*. 2023. T. 35. Vyp. 4. Pp. 65–92. DOI: 10.15514/ISPRAS-2023-35(4)-3.
10. Kotenko I.V., Saenko I.B., Lauta O.S., Vasil'ev N.A., Sadovnikov V.E. Ataki i metody zashchity v sistemakh mashin-nogo obucheniia: analiz sovremennykh issledovani. *Voprosy kiberbezopasnosti*. 2024. No. 1 (59). Pp. 24–37. DOI: 10.21681/2311-2024-1-24-37.
11. Ravi V., Chaganti R., Alazab M. Recurrent Deep Learning-Based Feature Fusion Ensemble Meta-Classifer Approach for Intelligent Network Intrusion Detection System. *Computers and Electrical Engineering*. 2022. Vol. 102. P. 108156. DOI: 10.1016/j.compeleceng.2022.108156.
12. Nazir A. et al. A Deep Learning-Based Novel Hybrid CNN-LSTM Architecture for Efficient Detection of Threats in the IoT Ecosystem. *Ain Shams Engineering Journal*. 2024. P. 102777. DOI: 10.1016/j.asej.2024.102777.
13. Akhtar N., Mian A., Kardan N., Shah M. Advances in Adversarial Attacks and Defenses in Computer Vision: A Survey. *IEEE Access*. 2021. Vol. 9. P. 155161–155196. DOI: 10.1109/ACCESS.2021.3127960.
14. Alahmed S., Alasad Q., Hammood M.M., Yuan J.-S., Alawad M. Mitigation of Black-Box Attacks on Intrusion Detection Systems-Based ML. *Computers*. 2022. Vol. 11. No. 7. P. 115. DOI: 10.3390/computers11070115.
15. Mohammadian H., Ghorbani A.A., Lashkari A.H. A Gradient-Based Approach for Adversarial Attack on Deep Learning-Based Network Intrusion Detection Systems. *Applied Soft Computing*. 2023. Vol. 137. P. 110173. DOI: 10.1016/j.asoc.2023.110173.
16. Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches. *Transactions on Emerging Telecommunications Technologies*. 2021. Vol. 32. No. 1. P. e4150. DOI: 10.1002/ett.4150.
17. Kurniabudi, Stiawan D., Darmawijoyo, Idris M.Y. Bin, Bamhdi A.M., Budiarto R. CICIDS-2017 Dataset Feature Analysis With Information Gain for Anomaly Detection. *IEEE Access*. 2020. Vol. 8. P. 132911–132921. DOI: 10.1109/ACCESS.2020.3009843.
18. Verkerken M. et al. A Novel Multi-Stage Approach for Hierarchical Intrusion Detection. *IEEE Transactions on Network and Service Management*. 2023. Vol. 20. No. 3. P. 3915–3929. DOI: 10.1109/TNSM.2023.3259474.
19. Goriunov M.N., Matskevich A.G., Rybolovlev D.A. Sintez modeli mashinnogo obucheniia dlia obnaruzheniia komp'iuternykh atak na osnove nabora dannykh CICIDS2017. *Trudy ISP RAN*. 2020. T. 32. Vyp. 5. Pp. 81–94. DOI: 10.15514/ISPRAS-2020-32(5)-6.
20. Belarbi O., Khan A., Carnelli P., Spyridopoulos T. An Intrusion Detection System Based on Deep Belief Networks // *The 4th International Conference on Science of Cyber Security (SciSec 2022)*. Springer International Publishing, Cham, 2022. P. 377–392. DOI: 10.48550/arXiv.2207.02117.
21. Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A. Adversarial Attacks on Machine Learning Cybersecurity Defences in Industrial Control Systems. *Journal of Information Security and Applications*. 2021. Vol. 58. P. 102717. DOI: 10.1016/j.jisa.2021.102717.
22. Aldweesh A., Derhab A., Emam A.Z. Deep Learning Approaches for Anomaly-Based Intrusion Detection Systems: A Survey, Taxonomy, and Open Issues. *Knowledge-Based Systems*. 2020. Vol. 189. P. 105124. DOI: 10.1016/j.knosys.2019.105124.
23. Ichetovkin E., Kotenko I. Modeling Poisoning Attacks Against Machine Learning Components of Intrusion Detection Systems. 2024 IEEE 25th International Conference of Young Professionals in Electron Devices and Materials (EDM). Altai, Russian Federation, 2024. P. 1850–1855. DOI: 10.1109/EDM61683.2024.10615198.
24. Ichetovkin E., Kotenko I. Modeling Attacks on Machine Learning Components of Intrusion Detection Systems. 2024 International Russian Smart Industry Conference (SmartIndustryCon). Sochi, Russian Federation, 2024. P. 261–266. DOI: 10.1109/SmartIndustryCon61328.2024.10515506.
25. Laghrissi F.E., Douzi S., Douzi K., Hssina B. Intrusion Detection Systems Using Long Short-Term Memory (LSTM) // *Journal of Big Data*. 2021. Vol. 8. No. 1. P. 65. DOI: 10.1186/s40537-021-00453-7.
26. Ayub M.A., Johnson W.A., Talbert D.A., Siraj A. Model Evasion Attack on Intrusion Detection Systems Using Adversarial Machine Learning. 2020 54th Annual Conference on Information Sciences and Systems (CISS). 2020. P. 1–6. DOI: 10.1109/CISS48834.2020.1570617295.
27. Chou D., Jiang M. A Survey on Data-Driven Network Intrusion Detection. *ACM Computing Surveys (CSUR)*. 2021. Vol. 54. No. 9. P. 1–36. DOI: 10.1145/3477132.
28. Jmila H., Khedher M.I. Adversarial Machine Learning for Network Intrusion Detection: A Comparative Study. *Computer Networks*. 2022. Vol. 214. P. 109073. DOI: 10.1016/j.comnet.2022.109073.

ПОДХОДЫ К УПРАВЛЕНИЮ РАЗВИТИЕМ ОТЕЧЕСТВЕННЫХ СИСТЕМ ИНФОРМАЦИОННО- ТЕЛЕМЕТРИЧЕСКОГО ОБЕСПЕЧЕНИЯ

Воронцов В.Л.¹

Ключевые слова: информационно-телеметрическое обеспечение, программно-технические средства, отработка средств выведения, телеметрируемый объект, телеметрическая информация, телеметрический комплекс космодрома.

Аннотация

Цель работы: анализ первоочередных организационно-технических мер, направленных на развитие отечественных систем информационно-телеметрического обеспечения отработки средств выведения.

Методы исследования: системный и экспертный анализ, концептуальное моделирование, формализованное описание.

Результаты: систематизация и детализация имеющихся знаний в области телеметрических систем, направленная на существенное улучшение управления развитием отечественных систем информационно-телеметрического обеспечения средств управления испытаниями космической техники.

Практическая ценность: полученные результаты могут быть использованы при выработке мер по улучшению управления развитием отечественных систем информационно-телеметрического обеспечения отработки средств выведения.

DOI: 10.24412/1994-1404-2025-1-121-129

Введение

Рассмотрены [2—7] различные аспекты научно-методического обеспечения развития отечественных систем информационно-телеметрического обеспечения (СИТО) отработки средств выведения (СИТО_{св}), которые являются, по сути, информационными системами, причём ориентированными на телеметрическую информацию (ТМИ), получаемую, в частности, при отработке ракет-носителей, применяемых для выведения космических аппаратов. При этом рассматриваются научно-технические и организационно-технические аспекты развития СИТО_{св}.

С научно-техническими аспектами связаны [2] методы и алгоритмы, обеспечивающие сокращение потерь ТМИ (прежде всего, повышением помехоустойчивости в каналах «борт-Земля»), критерии, модели и методики, касающиеся оценивания обеспечиваемой разработанными методами (алгоритмами) помехоустойчивости.

Действия по развитию СИТО_{св} (сокращение потерь ТМИ или получение дополнительной ТМИ) являются операциями по усовершенствованию и применению по целевому назначению СИТО_{св} (в том числе по применению усовершенствованных СИТО_{св}; далее для краткости — по применению СИТО_{св}). На исходы операций существенно влияют неопределённые факторы различной природы [2].

Для оценивания результативности действий (операций) по развитию СИТО_{св} в условиях влияния неопределённых факторов разработан комплекс общих (обобщённых) показателей [2, 3], базирующийся на теории оценивания эффективности проведения операций с использованием технических систем [9, 10]. Показаны [2, 5] отношения этих общих (обобщённых) показателей и частных показателей, характеризующих, в частности, потери ТМИ.

Сущности стратегий операций усовершенствования и применения СИТО_{св}, осуществляемых в условиях «природной» [9, 10] неопределённости, описаны [2] относительно полно (они касаются научно-технических аспектов развития СИТО_{св}).

С организационно-техническими аспектами связаны официальная концепция развития СИТО_{св} [6] и соответствующая её требованиям система стандартов телеметрии, а также комплекс мер по их развитию и результативному практическому применению (включая меры по созданию рабочей группы, условно названной «СИТО_{св}», устава для регламентирования её деятельности и меры по созданию условий для её результативной работы [3, 4]).

В зависимости от изменений сущностей СИТО_{св} в процессе их развития изменяются производственные

¹ **Воронцов Валерий Леонидович**, кандидат технических наук, ведущий инженер-исследователь АО «Российские космические системы», г. Москва, Российская Федерация.

E-mail: a762642@yandex.ru

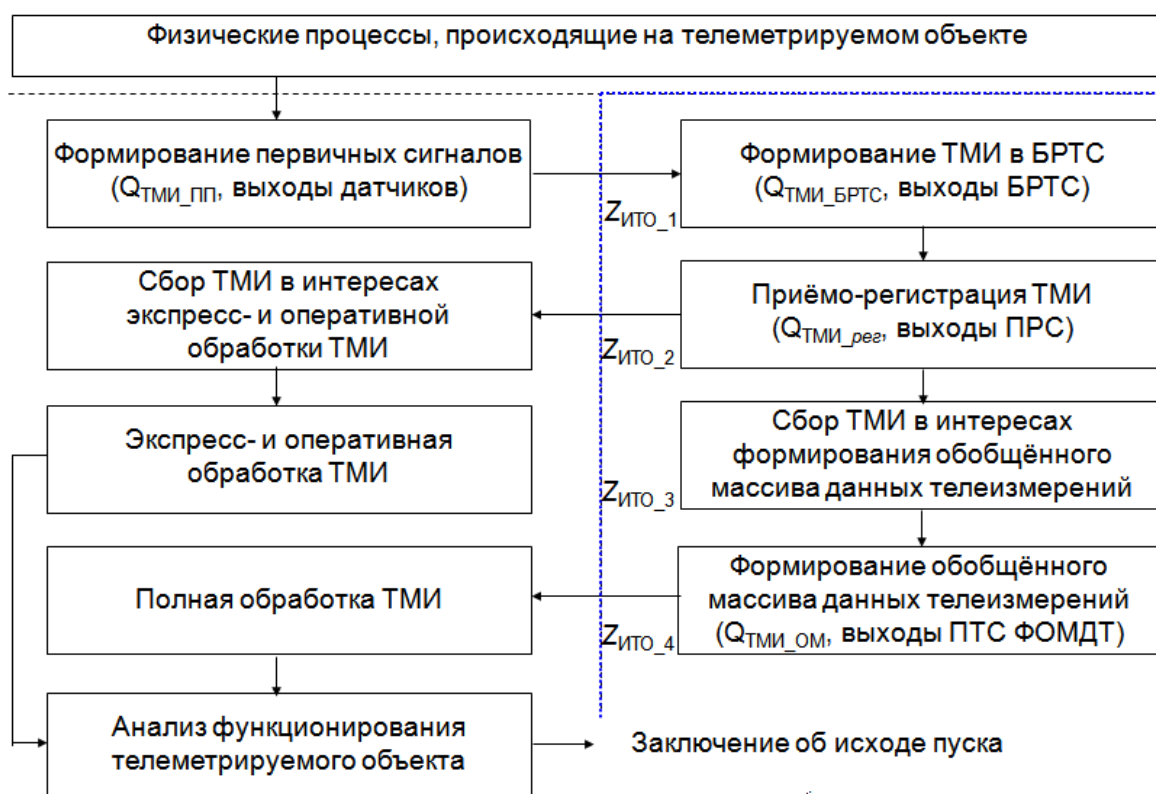


Рис. 1. Задачи ИТО

отношения предприятий/организаций ракетно-космической отрасли (РКО) [2, 5]. Важно, чтобы эти изменения не были связаны с неожиданным проявлением подрывных технологий, создающих экстремальные (форс-мажорные) ситуации вынужденного интенсивного подхода к развитию СИТО_{св}, причём в условиях ограниченных материальных ресурсов и времени [5]. Важно, чтобы осуществлялась эффективная работа по развитию СИТО_{св} на упреждение.

В настоящее время, когда научно-технические аспекты научно-методического обеспечения развития отечественных СИТО_{св} представлены достаточно полно, чтобы быть реализованными практически, «камнем преткновения» является осуществление его организационно-технических аспектов, прежде всего связанных с разработкой официальной концепции развития СИТО_{св} на основе предложенной [6], с построением соответствующей её требованиям системы стандартов телеметрии, с созданием полноценной рабочей группы «СИТО_{св}». Поэтому в настоящее время наиболее важны результаты исследований организационно-технических аспектов, касающихся максимального использования созидательных возможностей сотрудников предприятий/организаций РКО, обеспечиваемого эффективным управлением развитием отечественных СИТО_{св}.

Целью настоящей работы являются: анализ первоочередных организационно-технических мер, направленных на развитие отечественных СИТО_{св}.

Задачи информационно-телеметрического обеспечения отработки средств выведения и основные проблемные вопросы, связанные с их решением

Под СИТО_{св} понимаются [2] располагаемые материально-технические, стоимостные, временные, человеческие и другие ресурсы, которыми может воспользоваться оперирующая сторона (в том числе исследователь операции) для достижения цели операции, относящейся к решению задач информационно-телеметрического обеспечения отработки средств выведения (см. «Активные средства» в гл. 4 [9]).

Средствами выведения являются прежде всего ракеты-носители (РН) и разгонные блоки ракет космического назначения (РКН), являющиеся также телеметрируемыми объектами².

Показаны [2] (рис. 1) задачи информационно-телеметрического обеспечения (ИТО) отработки средств выведения (далее — задачи ИТО) и последовательность их выполнения.

Выделены (см. рис. 1) наиболее актуальные задачи ИТО, а именно:

²ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения. М. : Стандартинформ, 2005.

- формирование телеметрической информации в бортовой радиотелеметрической системе (БРТС)³;
- приёмо-регистрация ТМИ;
- сбор ТМИ в интересах формирования обобщённого массива данных телеизмерений (ФОМДТ);
- ФОМДТ.

Актуальность этих задач обусловлена тем, что с ними связаны значительные потери ТМИ вследствие действия неопределённых факторов разной природы.

Если эти выделенные задачи ИТО отнести к системе, то вход этой системы — *первичные сигналы* (т. е. выходные сигналы датчиков), а её выход — обобщённые данные телеизмерений. Обобщённые данные — это данные, полученные методами разнесённого приёма [2].

Атрибутами СИТО_{св} являются сигналы/данные заданной структуры, содержащие ТМИ, методы и алгоритмы действий над этими сигналами/данными, программно-технические средства (ПТС) для осуществления действий над вышеупомянутыми сигналами/данными и т. д.

Развитие СИТО_{св} стимулируют следующие факторы [2]:

- 1) новые задачи ИТО;
- 2) физическое старение ПТС СИТО_{св};
- 3) естественный ход развития современных ПТС и информационных технологий, их очевидные достоинства, проявляющиеся при успешном решении аналогичных задач в смежных областях;
- 4) производственные отношения, требующие постоянного повышения технического и технологического уровней предприятий/организаций РКО в целях сохранения конкурентоспособности.

Замечено [2], что в настоящее время развитие отечественных СИТО_{св} осуществляется в условиях доминирования факторов 1—3, что обрекает отечественные предприятия/организации на действия по устранению последствий проявления подрывных технологий [5], при том что усиление влияния фактора 4 позволило бы работать на упреждение.

Выявлены [2] следующие основные недостатки существующего ИТО:

- большие потери информации вследствие ошибок в выборе ожидаемого диапазона измерений телеметрируемых параметров (ТМП) (прежде всего вибропараметров), а также вследствие влияния помех каналов «борт-Земля» при пусках, которые сопоставимы с потерями времён 60—70-х годов XX века;
- ПТС телеметрического комплекса космодрома (ТК) избыточны, но не инвариантны к текущим задачам ИТО (обычно требуется их доработка при подготовке к очередному пуску);
- просматривается разобщённость в действиях предприятий/организаций РКО по развитию

отечественных средств ИТО. Зачастую от предприятий/организаций РКО поступают взаимоисключающие технические предложения по развитию средств ИТО. В таких условиях затруднительно в полной мере использовать созидательный потенциал сотрудников РКО в интересах результативного развития отечественных СИТО_{св}.

Для успешных действий по развитию отечественных СИТО_{св} необходимо выявить причины доминирования вышеупомянутых стимулов развития и неустранения перечисленных выше недостатков.

Краткая предыстория управления развитием отечественных СИТО_{св}

Требования к СИТО_{св} определяются сущностью связанной с ними ракетно-космической техники (РКТ) (в том числе средств выведения), целями и задачами предстоящих пусков. Эти требования могут быть полноценно сформулированы лишь после получения сведений, необходимых для разработки *программы телеметрических измерений* (ПТИ)⁴ и, соответственно, для адаптирования к новым задачам ИТО существующей СИТО_{св}. Поэтому обычно подготовка СИТО_{св} к новым задачам ИТО осуществляется в сжатые сроки, что создаёт предпосылки для ухудшения её качества.

Выходом из этой ситуации может быть использование прогнозов результатов развития РКТ и/или учёт влияния неопределённых факторов разной природы на результаты усовершенствования и применения СИТО_{св} и осуществление мер по противодействию им. Применение таких подходов нацелено на купирование угрозы неожиданного проявления подрывных технологий, создающих экстремальные (форс-мажорные) ситуации, чтобы осуществлять эффективную работу по развитию СИТО_{св} на упреждение [5].

В работах [2—7], касающихся развития отечественных СИТО_{св}, доминирует подход, связанный с учётом влияния неопределённых факторов $\Lambda_{иссл}$. В частности, показано [2], что неопределённые факторы $\Lambda_{от кол ТМП} (\Lambda_{от кол ТМП} \subset \Lambda_{иссл})$, проявляющиеся в большом разбросе количества ТМП в зависимости от *телеметрируемых объектов*, являются основной причиной неинвариантности существующего ТК к текущим задачам ИТО.

Вышеупомянутая неинвариантность проявляется в следующем: при увеличении количества ТМП пропорционально увеличивается количество комплексов БРТС⁵ и лавинообразно (из-за необходимости разнесённого приёма ТМИ) — ПТС ТК (прежде всего ПРС). Например, при подготовке космодрома Байконур к лётным испытаниям комплекса «Энергия-Буря» стоимость дооснащаемых средств ТК составила

³ГОСТ 19619-74. Оборудование радиотелеметрическое. Термины и определения. М.: Стандартинформ, 2005.

⁴См. ГОСТ 19619-74.

⁵Там же.

более 500 млн рублей в ценах 1970-х годов⁶. Только для приёмо-регистрации ТМИ понадобилось более 100, причём разнотипных, приёмно-регистрирующих станций (ПРС); при пуске РКН с РН «Союз» обычно задействуют 12—15 ПРС [2]. Чтобы уменьшить влияние неопределённых факторов, предложен комплекс мер, касающихся управления избыточностью данных телеизмерений, в том числе предложено [2] использовать известные методы и алгоритмы сжатия данных, прежде всего в месте зарождения ТМИ — на телеметрируемом объекте.

Следует заметить, что идея сжатия данных телеизмерений всегда оставалась и остается актуальной [2, 8, 12]. Однако задолго до сегодняшнего дня отмечена ситуация⁷, когда в смежных областях сжатие применяется давно и успешно, а в практической телеметрии — не применяется. При этом в технической литературе методы и алгоритмы сжатия данных телеизмерений относительно широко представлены⁸.

В случае со средствами выведения доминирует мнение специалистов (оно является определяющим), что из-за временной задержки на осуществление сжатия неизбежны потери ТМИ при возникновении полётной аварии на телеметрируемом объекте, когда ТМИ наиболее ценна. В то же время представленные [2] результаты исследований, показывающие большие возможности спасения ТМИ в аварийных ситуациях, пока остаются невостребованными.

Кратко описанное выше противодействие неопределённым факторам $\Lambda_{\text{от.кол.ТМП}}$ ($\Lambda_{\text{от.кол.ТМП}} \subset \Lambda_{\text{иссл}}$) относится лишь к отдельному аспекту развития СИТО_{св}, а рассмотренное сжатие данных телеизмерений является лишь одним из представленных [2] способов этого противодействия. Это описание сделано, чтобы наглядно показать сложность и неочевидность эффективных действий по развитию отечественных СИТО_{св}.

Заметим, что в случае лётных испытаний РКН типа «Энергия-Буран» сегодня — ситуация с количеством ПТС ТК (и ПРС) повторится. Правда, при дооснащении ТК сегодняшними ПТС (относительно малые масса и габариты, малая площадь технических зданий для размещения, малочисленный обслуживающий персонал и т. д.) может сложиться впечатление, что проблема неинвариантности «рассосалась» и управление избыточностью данных телеизмерений теперь не актуально.

Прежде всего нужно улучшить управление развитием СИТО_{св}, чтобы сосредоточиться на актуальных направлениях, которые необходимо правильно определить. Для этого целесообразно рассматривать

телеметрические средства как единое целое. Необходим системный подход. Однако зоны ответственности должностных лиц предприятий и организаций Роскосмоса определены так, что системный подход трудноосуществим. При этом изменение производственных отношений нельзя ставить во главу угла. Нужно обеспечить возможности выработки упреждающих (профилактических) мер по развитию СИТО_{св} в условиях влияния подрывных технологий, с которыми связаны значительные издержки вследствие вынужденного перехода на интенсивный путь развития, обычно усугубляемого жёсткими ограничениями материальных ресурсов и времени, а также необходимостью значительных изменений производственных отношений предприятий/организаций РКО, проявляющихся в соответствующих изменениях их организационно-штатной структуры [5]. Необходимы меры по эффективному использованию созидательных возможностей сотрудников предприятий/организаций РКО, а также вне РКО и, соответственно, необходим результативный механизм регламентирования управления развитием СИТО_{св}.

В истории решения задач ИТО отработки отечественных средств выведения всегда имели место высокий профессионализм, самоотверженный труд, разумная инициатива, стремление улучшать технические возможности средств ИТО^{9,10}. Однако, несмотря на очевидные достижения, перечисленные выше недостатки ИТО до сих пор не устранены, вышеупомянутый механизм регламентирования не создан. Хрестоматийным примером может быть НИР «Вершина-2» (1985—2000 годы)¹¹, цель выполнения которой заключалась в унификации структур ТМИ и телеметрических средств (прежде всего БРТС и ПРС), но так и не была достигнута. Возможно, из всего представленного в течение многолетней работы многочисленными участниками НИР «Вершина-2» не оказалось результатов, соответствующих цели НИР (по причинам, касающимся научно-технических аспектов), или не нашлось лица, принимающего решение, имеющего знания и полномочия, чтобы выбрать из представленных результатов нужные для достижения цели НИР (по причинам, касающимся организационно-технических аспектов). В итоге «за деревьями не увидели леса».

Суть механизма регламентирования управления развитием отечественных СИТО_{св}

В работе по усовершенствованию научно-методического обеспечения развития отечественных СИТО_{св} учтён опыт предшественников, показаны [2—4] широкие возможности использования результатов, полученных

⁶ Порошков В.В. Создание ПИК для РКК «Энергия-Буран» // Сб. материалов, документов, воспоминаний ветеранов измерительного комплекса космодрома «Байконур»: Измерительный комплекс космодрома Байконур. Байконур, 1999. С. 124—181.

⁷ Победоносцев В.А. 50 лет постановке проблемы сжатия данных (1948—1998) // Вестник МГТУ имени Н.Э. Баумана. Серия «Приборостроение». 1998. № 4. С. 114—122.

⁸ Ольховский Ю.Б., Новосёлов О.Н., Мановцев А.П. Сжатие данных при телеизмерениях / Под ред. В.В. Чернова. М.: Сов. радио, 1971. 304 с.

⁹ Сковорода-Лузин В.И. Телеметрия. Глаза и уши Главного конструктора. М.: ООО «Оверлей», 2009. 320 с.

¹⁰ Победоносцев В.А. Очерки истории развития отечественной ракетной радиотелеметрии (1946—2006 гг.) и место системы БРС-4 в этой истории. М.: Троянт, 2007. 160 с.

¹¹ Там же.

разными авторами. С учётом этого опыта, исключения масштабы работ и (как следствие) предпосылок к слабой управляемости ими, показано [5—7], что создание результативного механизма регламентирования управления развитием СИТО_{СВ} связано с разработкой официальной концепции развития СИТО_{СВ}, причём на основе предложенной [6] концепции, с построением соответствующей её требованиям системы стандартов телеметрии и созданием полноценной рабочей группы «СИТО_{СВ}».

Предлагаемая [3, 4] рабочая группа «СИТО_{СВ}» актуальна, чтобы регламентировать развитие СИТО_{СВ}, минимизируя издержки из-за необходимости согласования решаемых актуальных задач усовершенствования

СИТО_{СВ} в условиях существующих производственных отношений предприятий/организаций РКО. Она должна включать квалифицированных разносторонних специалистов-экспертов предприятий РКО (см. рис. 2) с делегированием функций председателя рабочей группы и секретариата одному из этих предприятий РКО. В дальнейшем нужно определить порядок формирования рабочей группы, регламент её работы, финансирование. Предполагается, что принятые рабочей группой решения утверждает руководитель департамента (подразделения) Госкорпорации «Роскосмос», в зоне ответственности которого находится информационно-телеметрическое обеспечение отработки средств выведения.



Рис. 2. Предприятия/организации, рабочая группа «СИТО_{СВ}»: отношения и зоны ответственности



Рис. 3. Роль и место стандартов телеметрии, относящейся к средствам выведения, в осуществлении концепции развития СИТО_{СВ}

Обоснованы и предложены [3, 4] следующие инструменты регламентирования развития СИТО_{СВ}:

- официальная концепция развития СИТО_{СВ} (с указанием направлений развития);
- система стандартов телеметрии, соответствующая этой концепции, обеспечивающая осуществление рациональных стратегий операций усовершенствования и применения по назначению СИТО_{СВ};
- административные положения по поддержанию и развитию концепции и стандартов телеметрии (устав рабочей группы «СИТО_{СВ}»).

Суть механизма регламентирования управления развитием отечественных СИТО_{СВ} пояснена [2] рисунком 3 (выше).

Необходимым условием результативного регламентирования управления развитием СИТО_{СВ} являются процедуры отбора рациональных стратегий операций по усовершенствованию и применению СИТО_{СВ}, обеспечивающих требуемые (заданные) общие (обобщённые) показатели эффективности.

Оценивание результативности стратегий операций усовершенствования и применения СИТО_{СВ}

Для оценивания результата операции Y , выполненной в соответствии со стратегией u , используют [10] три группы параметров, характеризующих полезный эффект q , материальные затраты C и оперативность T :

$$Y(u) = Y(q(u), C(u), T(u)) \quad (1)$$

Следовательно, исходя из (1), результат усовершенствования СИТО_{СВ} зависит от выбранной стратегии u_{yc} усовершенствования и заключается в полезном эффекте от усовершенствования (им является улучшение $\Delta Y_{прим}$ прим результата от применения усовершенствованной СИТО_{СВ}), в материальных затратах C_{yc} на усовершенствование и в оперативности T_{yc} процесса усовершенствования (при решении практических задач C_{yc} и T_{yc} могут являться затратами и сроками выполнения НИОКР в соответствии с Техническим заданием, или стратегией u_{yc}) [2]:

$$Y_{yc}(u_{yc}) = \langle \Delta Y_{прим}(u_{yc}), C_{yc}(u_{yc}), T_{yc}(u_{yc}) \rangle, u_{yc} \in U_{yc}, \quad (2)$$

Формульное выражение (2) преобразуется в

$$W_{эф_Y_yc} = \langle W_{эф_Y_прим}, W_{эф_C_yc}, W_{эф_T_yc} \rangle, \quad (3)$$

где $W_{эф_Y_yc}$ — общий показатель эффективности усовершенствования СИТО_{СВ}, $W_{эф_Y_прим}$, $W_{эф_C_yc}$, $W_{эф_T_yc}$ — частные показатели, соответствующие $\Delta Y_{прим}$, C_{yc} и T_{yc} , причём

$$W_{эф_Y_прим} = \langle \Delta W_{эф_W_ан_Σ}, \Delta W_{эф_C_прим}, \Delta W_{эф_T_прим} \rangle, \quad (4)$$

где $\Delta W_{эф_W_ан_Σ}$ — показатель улучшения качества данных для решения задач анализа, $\Delta W_{эф_C_прим}$, $\Delta W_{эф_T_прим}$ — показатели сокращения материальных затрат при решении задач ИТО и повышения оперативности решения задач ИТО (при осуществлении стратегий $U_{прим}$ применения СИТО_{СВ}) соответственно.

Подставив (4) в (3), получим

$$W_{эф_Y_yc} = \langle \Delta W_{эф_W_ан_Σ}, \Delta W_{эф_C_прим}, \Delta W_{эф_T_прим}, W_{эф_C_yc}, W_{эф_T_yc} \rangle \quad (5)$$

Показано [2], что необходимым условием (признаком) рациональных стратегий усовершенствования U_{yc} (применения $U_{прим}$) СИТО_{СВ} является *существенное* уменьшение потерь ТМИ (*существенное* увеличение дополнительной ТМИ). Для оценивания потерь ТМИ (получения дополнительной ТМИ) нужны соответствующие методики. Например, разработана модель источника помех в каналах разнесения, установлены критерии оценок, введены балльные оценки достоверности данных телеизмерений [2]. Оценивание может осуществляться также экспертным путём.

При построении стратегий усовершенствования U_{yc} (применения $U_{прим}$) СИТО_{СВ} важен выбор сигналов/данных и методов действий над ними: их свойства (характеристики) влияют на общие (обобщённые) показатели (5) СИТО_{СВ}.

При реализации стратегий U_{yc} ($U_{прим}$) изменяются сущности СИТО_{СВ} и, соответственно, изменяются производственные отношения предприятий/организаций РКО [2, 5]. Необходимы: согласование (гармонизация) целей развития этих предприятий/организаций и развития СИТО_{СВ} [2—4], организационные меры по управлению (менеджменту) процессом развития концепции и стандартов, а также по контролю за практическим выполнением представленных в них требований.

Актуальна работа, направленная на минимизацию издержек, порождаемых необходимостью устранения противоречий вследствие изменяющихся сущностей СИТО_{СВ} и изменяющихся производственных отношений предприятий/организаций РКО. В [3] показано, что наиболее результативные меры по устранению вышеупомянутых противоречий связаны с рабочей группой «СИТО_{СВ}».

Действия рабочей группы «СИТО_{СВ}» по отбору актуальных НИР/ОКР

Необходимым условием результативной работы рабочей группы «СИТО_{СВ}» по целевому назначению является осуществление механизма отбора актуальных НИР/ОКР, инициируемых предприятиями/организациями РКО и предприятиями/организациями вне РКО.

Прежде всего, в заявке на выполнение НИР/ОКР нужно указать сведения, обеспечивающие благоприятные возможности для принятия решения, касающегося ценности заявленного предложения.

Нужно указать, является ли НИР поисковой или прикладной.

В поисковых НИР представляют обоснованные направления развития СИТО_{СВ} с целью усовершенствования концепции [6] развития СИТО_{СВ} и соответствующей ей системы стандартов телеметрии, а в прикладных НИР/ОКР описывают стратегии усовершенствования СИТО_{СВ}, улучшающие *общие (обобщённые) показате-*

ли (5) [2, 3]. В прикладных НИР/ОКР могут рассматриваться не только СИТО_{св} в целом (в полном объёме), но и её фрагменты (подсистемы). При этом необходимы следующие сведения:

- в чём суть стратегии (стратегий) усовершенствования,
- какие *общие (обобщённые) показатели* (5) СИТО_{св} будут существенно улучшены.

Пример: Усовершенствование БРТС системы СИТО_{св}. Существенно сократятся материальные затраты на решение задач ИТО (уменьшится количество комплектов БРТС, размещаемых на РКН) применением новых методов сжатия данных телеизмерений в БРТС [8, 12, 13].

Таким образом, в заявке на НИР/ОКР нужно представить следующие сведения:

- поисковая НИР или прикладная НИР/ОКР;
- для поисковой НИР: суть новых направлений развития СИТО_{св}, краткое обоснование их актуальности и предложения по внесению соответствующих изменений в существующую концепцию [6] развития СИТО_{св};
- для прикладной НИР/ОКР: краткая характеристика предлагаемых стратегий усовершенствования СИТО_{св}, улучшающих её *общие (обобщённые) показатели* (5);
- предварительные оценки улучшения *общих (обобщённых) показателей* обобщённых показателей СИТО_{св} (для прикладных НИР/ОКР), а именно:
 - улучшение качества данных результатов обработки ТМИ, представленных для анализа функционирования объектов РКТ, характеризуемое прежде всего сокращением потерь информации или получением дополнительной информации,
 - уменьшение материальных затрат при применении усовершенствованной СИТО_{св},
 - повышение оперативности решения задач ИТО применением усовершенствованной СИТО_{св}.

При формулировании положений отечественных стандартов нужно рассматривать апробированные элементы СИТО_{св} (т. е. существующие элементы или те, по которым принято решение о внедрении), в частно-

сти, элементы, связанные с БРТС типа БРС-4¹² и «Орбита» [11]. Такой подход позволит добиться следующего:

- получить необходимый опыт разработки отечественных стандартов;
- прекратить внедрение датчиков-преобразующей аппаратуры, БРТС и ПТС ТК нестандартных разработок, значительно ухудшающее эффективность процесса развития СИТО_{св} (особенно в условиях подготовки к решению новых задач ИТО).

Заключение

Из анализа организационно-технических аспектов управления развитием отечественных СИТО_{св} следует следующее.

1. Необходимым условием результативного развития отечественных СИТО_{св} является научно-методическое обеспечение, отражающее научно-технические и организационно-технические аспекты управления развитием в условиях влияния подрывных технологий.
2. Организационно-технические аспекты связаны с целенаправленными действиями по построению, поддержанию и развитию официальной концепции развития СИТО_{св}, системы стандартов телеметрии и устава рабочей группы «СИТО_{св}», являющихся инструментами регламентирования развития отечественных СИТО_{св}.
3. Для построения, поддержания и развития вышеупомянутых инструментов регламентирования необходима рабочая группа «СИТО_{св}», объединяющая в своём составе взаимодополняющих и высококвалифицированных специалистов, обеспечивающая результативное использование созидательных возможностей предприятий/организаций через участие в управлении политической НИОКР, касающихся развития отечественных СИТО_{св}.

¹² Победоносцев В.А. Очерки истории развития отечественной ракетной радиотелеметрии (1946—2006 гг.) и место системы БРС-4 в этой истории. М.: Троянт, 2007. 160 с.

Литература

1. Бурый А.С., Лобан А.В., Ловцов Д.А. Модели сжатия массивов измерительной информации в автоматизированной системе управления // Автоматика и телемеханика. 1998. № 5. С. 3—26.
2. Воронцов В.Л. Система информационно-телеметрического обеспечения отработки средств выведения. Стратегии усовершенствования и применения. М.: Горячая линия — Телеком, 2021. 236 с. ISBN 978-5-0012-0895-6.
3. Воронцов В.Л., Давыдов И.А. Регламентирование процесса развития систем информационно-телеметрического обеспечения отработки средств выведения // Ракетно-космическое приборостроение и информационные системы. 2021. Т. 8. Вып. 2. С. 43—50.
4. Воронцов В.Л., Давыдов И.А., Медведев Е.В. Подходы к регламентированию процесса развития средств информационно-телеметрического обеспечения отработки объектов ракетно-космической техники // Ракетно-космическое приборостроение и информационные системы. 2022. Т. 9. Вып. 1. С. 42—54.

5. Воронцов В.Л. Управление развитием систем информационно-телеметрического обеспечения отработки средств выведения в условиях влияния подрывных технологий // Лесной вестник. 2023. Т. 27. № 6. С. 160—177.
6. Воронцов В.Л., Давыдов И.Д. Концепция развития систем информационно-телеметрического обеспечения отработки средств выведения // Радиоэлектронная отрасль: проблемы и их решения. 2023. № 3 (11). С. 24—32.
7. Воронцов В.Л., Давыдов И.А. Научно-технические и организационно-технические аспекты управления развитием отечественных систем информационно-телеметрического обеспечения отработки средств выведения // Информация и Космос. 2024. № 4. С. 170—181.
8. Ловцов Д.А. Теория защищенности информации в эргасистемах : монография. М. : РГУП, 2022. 276 с. ISBN 978-5-93916-896-0.
9. Надёжность и эффективность в технике : справочник : в 10 т. Т.1: Методология. Организация. Терминология. / Ред. совет: В.С. Авдеевский (предс.) и др. Под ред. А.И. Рембезы. М. : Машиностроение, 1986. 224 с.
10. Надёжность и эффективность в технике : справочник : в 10 т. Т.3: Эффективность технических систем / Ред. совет: В.С. Авдеевский (предс.) и др. Под общ. ред. В.Ф. Уткина, Ю.В. Крючкова. М. : Машиностроение, 1988. 328 с.
11. Теоретические и практические аспекты формирования и развития «Новой науки». Вып. 57. Уфа : ООО «АэтепBartrina-Rapesta J., et al. A lightweight contextual arithmetic coder for on-board remote sensing data compression. IEEE Transactions on Geoscience and Remote Sensing. 2017. № 55 (8). Pp. 4825–4835.
12. Coplin J., Yang A., Poppe A.R., Burtcher M. Increasing Telemetry Throughput Using Customized and Adaptive Data Compression. AIAA SPACE 2016. 2016. P. 5401.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

APPROACHES TO MANAGING THE DEVELOPMENT OF DOMESTIC INFORMATION AND TELEMETRY SUPPORT SYSTEMS

*Valerii Vorontsov, Ph.D. (Technology), Leading Research Engineer at the AO (JSC) "Rossiiskie kosmicheskie sistemy" (Russian Space Systems), Moscow, Russian Federation.
E-mail: a762642@yandex.ru*

Keywords: *information and telemetry support, software and hardware facilities, launch vehicle testing, telemetered object, telemetry information, spaceport telemetry complex.*

Abstract

Purpose of the paper: priority organizational and technical measures aimed at the development of domestic information and telemetry systems for launch vehicle testing.

Methods used in the study: system and expert analysis, conceptual modeling, formalized description.

Study findings: by systematizing and detailing the available knowledge, the task of significantly improving the management of the development of domestic information and telemetry support system for launch vehicle testing has been solved.

Practical value: the results obtained can be used in the development of measures to improve the management of the development of domestic information and telemetry support system for launch vehicle testing.

References

1. Buriy A.S., Loban A.V., Lovtsov D.A. Modeli szhatiia massivov izmeritel'noi informatsii v avtomatizirovannoi sisteme upravleniia. Avtomatika i telemekhanika. 1998. No. 5. Pp. 3–26.
2. Vorontsov V.L. Sistema informatsionno-telemetriceskogo obespecheniia otrabotki sredstv vyvedeniia. Strategii usovershenstvovaniia i primeneniia. M. : Goriachaia liniia – Telekom, 2021. 236 pp. ISBN 978-5-0012-0895-6.
3. Vorontsov V.L., Davydov I.A. Reglamentirovanie protsessa razvitiia sistem informatsionno-telemetriceskogo obespecheniia otrabotki sredstv vyvedeniia. Raketno-kosmicheskoe priborostroenie i informatsionnye sistemy. 2021. T. 8. Vyp. 2. Pp. 43–50.
4. Vorontsov V.L., Davydov I.A., Medvedev E.V. Podkhody k reglamentirovaniu protsessa razvitiia sredstv informatsionno-telemetriceskogo obespecheniia otrabotki ob"ektov raketno-kosmicheskoi tekhniki. Raketno-kosmicheskoe priborostroenie i informatsionnye sistemy. 2022. T. 9. Vyp. 1. Pp. 42–54.

5. Vorontsov V.L. Upravlenie razvitiem sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia v usloviakh vliianiia podryvnykh tekhnologii. Lesnoi vestnik. 2023. T. 27. No. 6. Pp. 160–177.
6. Vorontsov V.L., Davydov I.D. Kontsepsiia razvitiia sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia. Radioelektronnaia otasl': problemy i ikh resheniia. 2023. No. 3 (11). Pp. 24–32.
7. Vorontsov V.L., Davydov I.A. Nauchno-tekhnicheskie i organizatsionno-tekhnicheskie aspekty upravleniia razvitiem otechestvennykh sistem informatsionno-telemetricheskogo obespecheniia otrabotki sredstv vyvedeniia. Informat-siia i Kosmos. 2024. No. 4. Pp. 170–181.
8. Lovtsov D.A. Teoriia zashchishchennosti informatsii v ergasistemakh : monografiia. M. : RGUP, 2022. 276 pp. ISBN 978-5-93916-896-0.
9. Nadezhnost' i effektivnost' v tekhnike : spravochnik : v 10 t. T.1: Metodologiiia. Organizatsiia. Terminologiiia. Red. sovet: V.S. Avduevskii (preds.) i dr. Pod red. A.I. Rembezy. M. : Mashinostroenie, 1986. 224 pp.
10. Nadezhnost' i effektivnost' v tekhnike : spravochnik : v 10 t. T.3: Effektivnost' tekhnicheskikh sistem. Red. sovet: V.S. Avduevskii (preds.) i dr. Pod obshch. red. V.F. Utkina, Iu.V. Kriuchkova. M. : Mashinostroenie, 1988. 328 pp.
11. Teoreticheskie i prakticheskie aspekty formirovaniia i razvitiia "Novoi nauki". Vyp. 57. Ufa : OOO "Aeterna", 2021. 140 pp. ISBN 978-5-00177-264-4.
12. Bartrina-Rapesta J., et al. A lightweight contextual arithmetic coder for on-board remote sensing data compression. IEEE Transactions on Geoscience and Remote Sensing. 2017. No. 55 (8). Pp. 4825–4835.
13. Coplin J., Yang A., Poppe A.R., Burtscher M. Increasing Telemetry Throughput Using Customized and Adaptive Data Compression. AIAA SPACE 2016. 2016. P. 5401.

РАЗРАБОТКА И СИСТЕМНЫЙ АНАЛИЗ МЕТОДА ОЦЕНКИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЛОЖНОЙ СИСТЕМЫ

Лубенцов А.В.¹

Ключевые слова: сложная информационная система, декомпозиция, интервальные оценки, синтез, оценка эффективности, каскадный метод анализа иерархий.

Аннотация

Постановка проблемы. Архитектура современных сложных информационных систем (СИС) характеризуется высокой степенью сложности и многокомпонентности. Получение параметров эффективности функционирования СИС является актуальной и нетривиальной задачей. В современной инженерии недостаточно разработаны методики решения вопросов оценки эффективности СИС.

Цель работы. В настоящей работе исследуется проблема оценки эффективности работы сложных информационных систем с точки зрения обеспечения их безопасности. Эта задача интерпретируется как процесс формирования многомерных решений, основанный на анализе многопараметрических данных путем декомпозиции СИС и введения интервальных оценок.

Метод исследования. Предлагается синтез и применение нелинейной модели для оценки эффективности сложной информационной системы. В модели используется интервальная форма представления данных, позволяющая учесть неопределенности, ошибки в исходных данных, погрешности измерений и субъективность экспертных оценок.

Результаты. В рамках исследования был осуществлён системный анализ комплексных оценок информационной безопасности. Предложенная методология базируется на разделении функциональной структуры СИС на составные элементы с последующим упрощением до базовых модулей. Разработан инновационный подход, включающий формирование ключевых правил путем интеграции интервальных характеристик оценки кластеров и оценки суммарной эффективности.

Практическое значение. Полученные результаты и аналитические выводы служат основой для построения стратегий развития всей ИС (информационной системы) и её компонентов. Применен авторский каскадный метод анализа иерархий, обеспечивающий снижение влияния человеческого фактора в процессе ранжирования критериев. Это способствует значительному повышению объективности оценок эффективности как отдельных подсистем, так и всей системы безопасности информации.

Таким образом, внедрённые инновации существенно улучшают точность и надёжность процессов оценивания в сфере информационной безопасности.

DOI: 10.24412/1994-1404-2025-1-130-140

Введение

Современное ускоренное развитие многофункциональных сложных информационных систем (СИС) провоцирует рост угроз их безопасности из-за возрастающей сложности архитектур. Проблемы в любом элементе системы способны вызвать цепную реакцию нарушений, приводя к критическому снижению общей производительности. Поддержание надёжной работы систем сводится к непрерывному обеспечению стабильности каждого компонента обслуживания и программного обеспечения. Для этого требуется регулярное комплексное тестирование с по-

следующим глубоким анализом результатов, включающее оценку эффективности каждой части системы.

В рамках инженерии системных решений такие испытания неизменно выявляют как структурные (систематические), так и случайно возникающие ошибки. Ключевая цель — существенное сокращение этих неполадок через тщательную оценку эффективности каждого компонента системы. Важной задачей становится проведение точной, обоснованной экспертизы функционирования всей ИТ-системы и её отдельных частей для обеспечения их безупречности в эксплуатации.

¹ Лубенцов Александр Витальевич, кандидат географических наук, доцент, Воронежский институт ФСИИ России, г. Воронеж, Российская Федерация. ORCID: 0000-0003-0239-4843, SPIN-код: 6530-4715.
E-mail: lubensov@mail.ru

Эта актуальная проблема требует системного подхода к решению: необходима разработка методик оценки, повышение квалификации специалистов по тестированию и внедрение передовых технологий анализа данных.

Анализ существующих моделей

Анализ рассматриваемых моделей указывает на разнообразие подходов к оценке эффективности сложных систем, основанных на методиках моделирования, математического анализа и применения экспертных систем.

В работе [1] представлена математическая модель для оценки эффективности протоколов взаимодействия цифровых радиосетей стандартов APCO-25 и DRR. Результаты вычислительных экспериментов демонстрируют потенциал модели, однако остаются вопросы по установлению весов иерархии критериев в рамках такого подхода.

Исследование [2] посвящено разработке интегрированных правил определения эффективности структур поддержки безопасности информационных потоков в автоматизированных системах управления технологическими процессами (АСУ ТП). На фоне отсутствия официальных стандартов оценки систем обнаружения вторжений (СОВ) авторы предлагают для таких систем практическую реализацию на примере предприятия Иркутской области. В рамках исследования были разработаны рекомендации по модернизации существующих решений.

В исследовании [3] предложено сравнение информационных систем по уровню их эффективности через анализ и расчет энтропии, связанной с временными параметрами обработки данных. Построена иерархическая модель информационных потоков и проведен анализ радиолокационных структур. Авторы отмечают, что эффективность системы зависит от технической сложности, а также от временных затрат на обработку информации. На основе проведенного анализа сделан вывод, что сетевые структуры превосходят иерархические по обобщенному показателю информационной энтропии. Предлагается использовать энтропию как критерий оценки свойств информационных систем, хотя эффективность этого подхода чувствительна к характеристикам потока данных.

Работа [4] фокусируется на применении элементов имитационного моделирования для оценки эффективности систем защиты от кибератак. Для анализа используются практические примеры, включая СОВ. Здесь особое внимание уделено многофакторным задачам, возникающим при отражении кибератак, а также значимостью учета большого числа переменных, влияющих на результат.

Особое внимание уделяется термину «эффективность», который в зарубежной литературе часто трактуется как “performance”, подразумевающий и производительность, и результативность, что может вызывать

терминологическую путаницу. В ряде международных исследований применяются принципы анализа на основе «базовых правил» (BRB) [5].

Методы, основанные на использовании экспертных систем, получили широкое распространение в последние годы [6, 7]. Одним из подходов является использование случайных графов с экспоненциальным временным разделением для оценки сетевых параметров, применимых как для независимых, так и автокоррелированных сетей. Разработанная модель BRB позволяет учитывать неопределенность и неточности данных, а также используется для задач оценки надежности, диагностики неисправностей и производительности. Примером является созданная на базе BRB модель оценки безопасности сложных систем, обладающая интерпретируемостью результатов.

Практическое функционирование СИС осложняется высоким уровнем неопределенности среды и влиянием различных помех. Такие факторы делают невозможным полное оперирование исключительно данными о предыдущей работе системы, экспертными знаниями или изолированными моделями функционирования. Для обеспечения достоверной оценки требуется интеграция всех доступных видов информации. Точная числовая оценка не всегда способна учитывать тонкие динамические изменения в сложной среде функционирования. Это особенно актуально в условиях шумового воздействия на систему [8, 9, 10].

Оценка же эффективности СИС может представляться как классификационная задача, где оценка проводится на основе анализа характеристик и результатов тестирования системы в реальной операционной среде. Таким образом, процесс оценки трансформируется в задачу многокритериального выбора решений при интервальной неопределенности.

Структура и принципы работы СИС представляют собой сложную систему [11, 12]. Подходы, основанные на «базовых правилах», представляют перспективный инструмент для качественной обработки информации и повышения точности оценки эффективности таких систем.

Разработка модели оценочных индексов

В системе с гибридной структурой, где множество параметров и сложные взаимосвязи определяют поведение, специфические модели, основанные на базовых правилах, являются наиболее подходящими инструментами для её моделирования и анализа. Это обусловлено тем, что:

- 1) разнообразие элементов и их взаимодействие требуют детальной формализации процессов на микроуровне,
- 2) сложные коэффициенты корреляций и зависимости между компонентами нуждаются в точном описании через правила.

Модель позволяет агрегировать измеряемые показатели нижнего уровня, чтобы получить итоговую

оценку функционирования системы в целом. Этот процесс может показаться простым и линейным, но при этом зачастую упускается из виду состояние отдельных подсистем или оборудования внутри системы. Между тем для эффективной диагностики и оценки требуется учитывать их текущее рабочее состояние. При обнаружении несоответствий требованиям нормальной работы отдельных подсистем, принятие решений сводится к следующим шагам.

- Проведение диагностики для выявления конкретных причин нарушений.
- Рассмотрение вариантов устранения проблемы.
- Замена неисправных компонентов для обеспечения их соответствия техническим стандартам.
- Перенастройка параметров и конфигураций подсистем для оптимизации их работы.
- Проведение комплексного технического обслуживания с целью восстановления и поддержания работоспособности.

Эти меры направлены на восстановление целостности и эффективности функционирования всей системы, обеспечивая её стабильность и надежность.

Модель на основе базовых правил для оценки сложных систем с неопределёнными данными

В представленной работе рассмотрена методология оценки эффективности комплекса средств безопасности СИС путем применения подхода, основанного на базовых правилах в условиях неопределённых данных. Этот метод позволяет интегрировать разнородные данные и анализировать эффективность работы отдельных подсистем в рамках общей системы. Результаты такой оценки могут быть использованы для проведения системного анализа, что позволит лицам, принимающим решения, вырабатывать оптимальные стратегии эксплуатации и управления СИС. Предлагаемая структура метода включает три ключевых этапа (рис. 1).

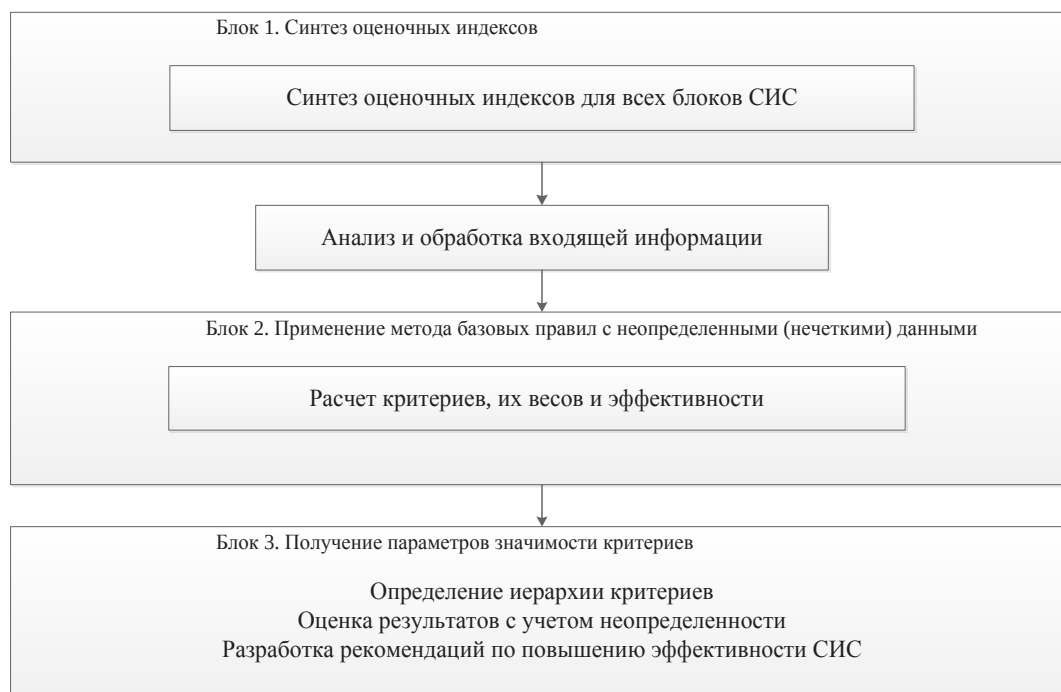


Рис. 1. Поэтапная модель оценки эффективности сложных систем

Синтез оценочных индексов представляет собой начальный этап разработанной модели. На втором этапе применяется метод формирования базовых правил с нечеткими элементами, которые учитывают неопределенность исходных данных. Завершающим этапом становится определение порядка важности критериев, позволяющих корректировать стратегии эксплуатации и управления.

Синтез системы индексов для модели оценки эффективности сложных систем

Создание индексов для анализа эффективности комплексных систем является ключевым инструмен-

том, который позволяет лучше понять и оценить работу различных элементов системы. Этот процесс основывается на необходимости разделения системы на несколько независимых подсистем, что продиктовано ее структурными особенностями и принципами функционирования. Когда подсистемы варьируются по сложности, их можно дополнительно разбить на более мелкие составляющие, что создает возможность получения объективных показателей для этих элементов. На основе данной многоуровневой структуры создается система индексной оценки. В процессе анализа применяется методика «снизу вверх», при которой результаты оценки нижних уровней становятся основой для разработки и обоснования индексов на более высоких

уровнях. В результате общий индекс для всей системы формируется поэтапно, объединяя данные со всех уровней. Структурная схема показателей оценки представлена на рис. 2.

Однако в реальных условиях системы зачастую имеют более сложную природную организацию, и их

невозможно просто разделить на независимые блоки. Между индексами различных уровней может существовать взаимное влияние, которое усложняет процесс оценки. Методика, описанная в данной работе, применима только к таким системам, которые можно условно кластеризовать (см. рис. 2).

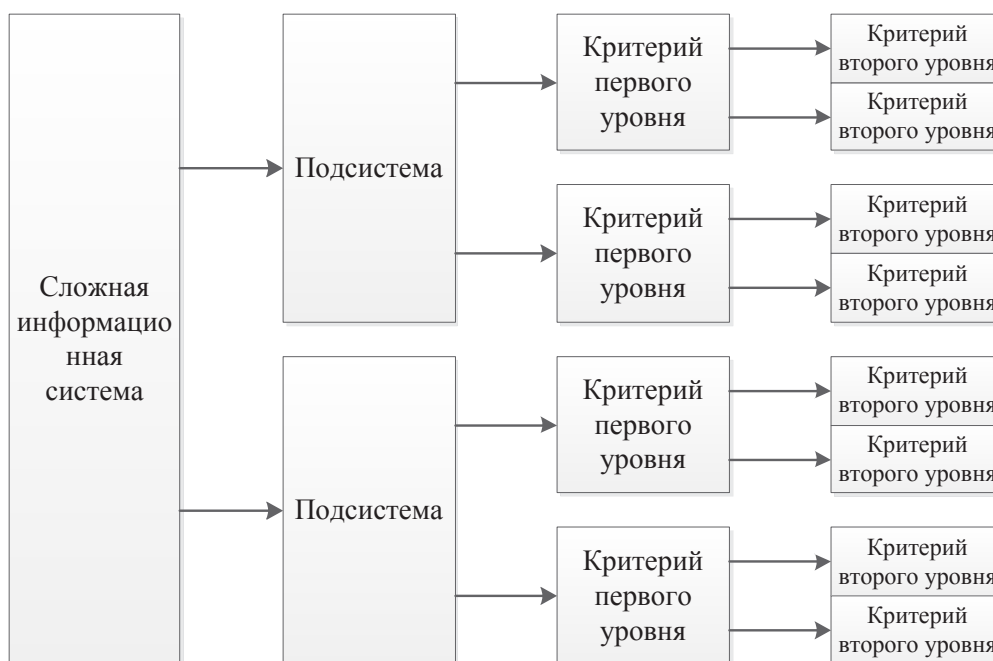


Рис. 2. Декомпозиция сложной системы для получения критериев эффективности на каждом уровне

Если же система не поддается разделению на несколько независимых частей, следует учитывать зависимость между блоками. В этом случае предлагаемый метод оценки необходимо дополнить моделью, учитывающей взаимовлияние между компонентами, что позволит учесть комплексную природу системы при формировании итоговых индексов.

В проведенных исследованиях, как отмечается в источнике [7], был предложен индекс, отражающий взаимосвязь элементов системы в рамках критериев. Этот показатель позволяет оценивать связи между различными составляющими системы, что играет центральную роль в понимании их взаимодействия. Для вычисления индекса взаимозависимости используются функции предельного и совместного правдоподобия, что даёт возможность учитывать вероятностный характер большинства критериев, основанных на этих функциях. Таким образом, индекс взаимозависимости может быть эффективно использован в рамках модели байесовской процедуры (БП), что особенно актуально в условиях неопределенности. На рис. 3 представлена трехуровневая структура системы, демонстрирующая процесс моделирования. На верхнем уровне располагается эффективность объекта оценки, которая является итоговым результатом анализа. Средний уровень посвящён расчету промежуточных индексов для раз-

личных подсистем, что позволяет детализировать оценку и выявить слабые места в каждой подсистеме. Нижний уровень, в свою очередь, представляет собой измеряемый оценочный индекс, который служит основой для дальнейших расчетов и выводов [13, 14, 15].

Измерение нижних индексов, доступное на данном уровне, влияет на осуществление обработки данных для расчета промежуточного индекса. В рамках данной модели вес обозначается как l_i , показатель эффективности параметров среди нижних индексов обозначен как p_i , а степень достоверности $b_{n,i}$ вычисляется посредством преобразования входных данных в n -ую оценку, где n может принимать значения от 1 до N . Например, степень достоверности $b_{n,1}(r_1)$ для промежуточного индекса r_1 вычисляется за счет объединения параметров k_1 и k_2 . Аналогично, параметры k_3 и k_4 комбинируются для получения оценки $b_{n,2}(r_2)$ для промежуточного индекса r_2 .

Важно отметить, что такая структура оценки позволяет не только выявить текущие показатели эффективности, но и проанализировать динамику изменений в системе. Например, при изменении условий функционирования одной из подсистем можно будет быстро оценить, как это повлияет на общую эффективность системы. Это особенно актуально для сложных систем, где взаимодействие между компонентами может быть

непредсказуемым. Кроме того, использование подхода, основанного на вероятностных моделях, позволяет учитывать неопределенности и вариации в данных, что делает результаты более надежными и применимыми в практических условиях. Например, в области управления проектами, где множество факторов могут влиять на итоговый результат, такой подход позволяет более точно предсказывать результаты и принимать обоснованные решения. Таким образом, синтез индексов для оцен-

ки эффективности сложных систем является многоуровневым и гибким инструментом, который может быть адаптирован под различные области применения. Это позволяет не только проводить глубокий анализ текущего состояния системы, но и разрабатывать стратегии для ее оптимизации и улучшения. В конечном итоге применение таких методов может значительно повысить эффективность работы сложных систем и обеспечить их устойчивое развитие в условиях меняющейся среды.



Рис. 3. Схема расчета индексов на каждом уровне трехслойной сложной системы

После получения значений $b_{n,1}(r_1)$ и $b_{n,2}(r_2)$ следует объединить эти промежуточные индексы для формирования окончательной оценки объекта W . Промежуточные индексы выражаются в форме степени достоверности, на основании которой необходимо установить соответствующие весовые коэффициенты и уровень надежности. Предполагаем, что максимальное значение суммарного веса составляет 1, а минимальное значение задаётся наибольшей величиной среди отдельных критериев. Итоговый вес рассчитывается следующим образом:

$$l_{k(E)} = (\max(l_i), 1) \quad (1)$$

Общая достоверность является функцией общего веса, которая рассчитывается как

$$p_{k(E)}(l_{k(E)}) = \frac{1 - r_{G(Q),k(E)}(1 + l_{k(E)})}{1 - r_{G(Q),k(E)}} \quad (2)$$

где E — количество критериев; $r_{G(Q),k(E)}$ — критерий остаточной достоверности, не попавший ни в один класс. Тогда общая достоверность определяется как

$$p_{k(E)}(l_{k(E)}) \in [p_{k(E)}(1), p_{k(E)}(\max(\omega_i))] \quad (3)$$

На основании уравнений (2) и (3) исходные массы вероятности, связанные с промежуточными индексами, объединяются для расчета итогового показателя верхнего уровня.

Поскольку достоверность и вес представлены нечетными значениями, стандартный метод построения

БП неприменим для расчета итоговой степени достоверности $b_{n,1}(W)$. В качестве метода получения результатов этой проблемы необходимо реализовать подход БП с вычислением неопределенных характеристик.

Использование базовых правил с комбинацией нескольких интервальных структур

Применение базовых принципов в сочетании с несколькими интервальными структурами часто оказывается полезным инструментом в инженерной практике. Дело в том, что точное определение ряда индексов на практике зачастую затруднено. В ходе тестирования неизбежно возникают разнообразные ошибки, которые влекут за собой статистическую погрешность полученных данных.

Необходимо также учесть, что непосредственное измерение некоторых показателей затруднено и требует привлечения экспертных оценок. При этом объективные факторы часто препятствуют лицам, принимающим решения, в предоставлении точных количественных оценок, что приводит к дополнительной субъективной неопределенности.

Представление данных в интервальном формате обладает неоспоримыми преимуществами перед точечным методом.

Во-первых, интервальный подход обеспечивает более достоверное и обоснованное отражение неопределенной информации, в отличие от точечных значе-

ний. Во-вторых, использование интервалов позволяет передать больший объем данных с большей точностью.

Следовательно, применение интервальных значений может существенно снизить вероятность ошибок. Поскольку интервал включает весь спектр возможных значений, такой подход особенно полезен для практических применений. В рамках метода базовых принципов (БП) интервальные параметры заменяют точечные значения при оценке производительности системы, что более точно отражает реальные инженерные условия.

Для оценки достоверности по методу БП предположим наличие двух независимых критериев, обозначенных как k_1 и k_2 , а также оценочных баллов H_1 и H_2 соответственно.

Основные значения промежуточных индексов или вероятностей могут быть получены в следующем виде:

$$r_{n,i} = l_n b_{n,i} \quad (4)$$

$$r_{H,i} = 1 - l_i \sum_{n=1}^N b_{n,i} \quad (5)$$

$$\bar{r}_{H,i} = 1 - l_i \quad (6)$$

$$r_{H,i}^* = l_i \left(1 - \sum_{n=1}^N b_{n,i} \right) \quad (7)$$

Здесь $\bar{r}_{H,i}$ представляет основные значения вероятностей, генерируемые относительной важностью критериев, $r_{H,i}^*$ — основные значения вероятности, вызванные неполнотой оценки; $r_{H,i}$ — результирующие значения вероятности после агрегирования и $r_{H,i} + r_{H,i}^* = r_{H,i}$. Взаимосвязь между ключевыми значениями вероятности и уровнем достоверности соответствует описанным выше уравнениям.

Интервальные значения базовых вероятностей равны:

$$r_{n,i} = r_i(H_n) \in [r_{n,i}^-, r_{n,i}^+] = [l_i^- b_{n,i}, l_i^+ b_{n,i}], \quad (8)$$

где $n = 1, 2, \dots, N$; $i = 1, 2, \dots, E$

$$r_{H,i} = 1 - l_i \sum_{n=1}^N b_{n,i}, \quad \text{где } i = 1, 2, \dots, E \quad (9)$$

$$\bar{r}_{H,i} = \bar{r}_i(H) = (1 - l_i) \in [1 - l_i^+, 1 - l_i^-], \quad (10)$$

где $i = 1, 2, \dots, E$

$$r_{n,i}^* = r_i^*(H_n) \in [r_{n,i}^{*-}, r_{n,i}^{*+}] = [l_i^- b_{n,i}, l_i^+ b_{n,i}], \quad (11)$$

где $i = 1, 2, \dots, E$

Постулируем, что сумма вероятностей (критериев) определяется:

$$\sum_{n=1}^N r_{n,i} + \bar{r}_{H,i} + r_{H,i}^* = 1$$

Оценочные баллы могут быть переведены в базовые вероятностные значения. После этого становится возможным использование интервальных значений вероятностей для объединения нескольких вероятностных данных посредством метода БП.

Рекурсивный процесс объединения вероятностей базовых интервалов

Объединение суммы компонентов критериев с применением метода БП происходит следующим образом:

$$r_{n,k(E)} = D_{k(E)} (r_{n,k(E-1)} r_{n,E} + r_{n,k(E-1)} r_{H,E} + r_{H,k(E-1)} r_{n,E}) \quad (12)$$

$$\bar{r}_{H,k(E)} = D_{k(E)} (\bar{r}_{H,k(E-1)} \bar{r}_{H,E}) \quad (13)$$

$$r_{H,k(E)}^* = D_{k(E)} (r_{H,k(E-1)}^* \bar{r}_{H,E} + r_{H,k(E-1)} r_{H,E}^* + r_{H,k(E-1)}^* r_{H,E}^*) \quad (14)$$

$$r_{H,k(E)} = \bar{r}_{H,k(E)} + r_{H,k(E)}^* \quad (15)$$

$$D_{k(E)} = \left(1 - \sum_{t=1}^2 \sum_{j \neq t}^2 r_{t,k(E-1)} r_{j,E} \right)^{-1} \quad (16)$$

Для достижения оптимального диапазона значений рекомендуется усовершенствовать методику комбинированной оценки критериев. В случае необходимости объединения нескольких параметров целесообразно использовать поэтапный подход. На первом этапе интегрируются первый и второй критерии, затем результат их объединения последовательно комбинируется с третьим критерием, и процесс продолжается аналогичным образом для всех остальных. Завершив этот процесс, можно приступить к комплексной оптимизации, которая позволит определить верхние и нижние границы интервала финального итогового значения.

Опираясь на проведенные вычисления, устанавливаются уровни надёжности для каждого из соответствующих классов.

Стоит отметить, что при раздельной оптимизации каждого компонента критериев и использовании оптимального интервала для последующего вычисления могут возникать некорректные результаты. В контексте задачи ограниченной оптимизации найденные решения, подходящие для каждой отдельной части, являются локально оптимальными, но не всегда обеспечивают глобальную оптимизацию. Поэтому для достижения глобального оптимума необходимо учитывать все ограничения и комбинированные процессы в рамках единой модели общей оптимизации объекта. Это позволяет гарантировать получение действительно глобального оптимального результата.

Использование каскадного метода анализа иерархий для ранжирования и отбора наиболее значимых критериев СИС

Применение каскадного метода анализа иерархий для отбора наиболее значимых критериев представляет собой важный этап в разработке эффективных решений. В сложных системах, таких как СИС, где каждая подсистема вносит свой вклад, критериев оценки может быть великое множество. Для достижения боль-

шей точности и достоверности среди них необходимо выделить наиболее релевантные. Эту задачу предполагается решать с использованием каскадного метода анализа иерархий (КМАИ).

Одним из ключевых недостатков метода анализа иерархий (МАИ) является значительный уровень субъективности, связанный с участием лиц, принимающих решения (ЛПР). Для минимизации этого воздействия предлагается модернизировать подход: разделить метод на две составляющие — субъективную и объективную. В первой части осуществляется выбор критериев, предлагаемых решений и их ранжирование, что в большей степени зависит от мнения ЛПР. Во второй части выполняются расчеты нормированных векторов приоритетов (НВП) и матриц, устраняя человеческий фактор.

Для повышения объективности процесса принятия решений предлагается использовать каскадный вариант МАИ.

Суть данного подхода заключается в формировании трех независимых групп участников: экспертов, руководителей объекта и конечных пользователей, которые будут непосредственно взаимодействовать с системой после ее внедрения. Участники каждой группы совместно определяют критерии оценки и возможные решения. Далее каждая группа ранжирует критерии и решения в соответствии со своими приоритетами, формируя индивидуальные матрицы предпочтений. На основе этих матриц для каждой группы рассчитываются три набора нормализованных весовых приоритетов (НВП): для критериев и предлагаемых решений.

На следующем этапе рассчитывается итоговый нормированный вектор приоритетов на основе данных каждой группы. Это достигается путем нормирования НВП критериев с учетом средних значений по всем группам. Такой подход позволяет учесть точку зрения каждой категории участников, выровнять влияние субъективной оценки и повысить общий уровень объективности процесса. Результатом применения данного подхода становится минимизация ошибок, связанных с субъективными предположениями при разработке критериев оценки и процесса принятия решений, что особенно важно в условиях сложных систем [9].

Литература

1. Пьянков О.В., Попов А.В. Математическая модель оценки эффективности протокола взаимодействия систем цифровой радиосвязи // Вестник ВИ МВД России. 2021. № 4.
2. Голдобина А.С., Исаева Ю.А., Никулин Д.М. Оценка эффективности систем обнаружения вторжения в информационной системе управления производством оборонно-промышленного комплекса // Интерэкспо Гео-Сибирь. 2020. № 1.
3. Пальгуйев Д.А. Сравнительная оценка эффективности информационных систем иерархической и сетевой структуры на основе энтропийного подхода // РТС. 2020. № 1 (37).
4. Жуков М.М., Баркалов Ю.М., Телков А.Ю. Методологический подход к имитационному моделированию при исследовании практической эффективности систем защиты от сетевых кибератак // Вестник ВИ МВД России. 2022. № 1.

Выводы

В ходе проведенного исследования был осуществлен системный анализ существующих подходов к оценке эффективности различных СИС.

Результаты анализа показали, что в инженерной практике непрерывный контроль эффективности таких систем является критически важным фактором для своевременного планирования их модернизации и разработки мер по минимизации рисков.

Для создания нового метода оценки эффективности сложных систем, на примере СИС было обосновано представление данной системы в виде многоуровневой и многокомпонентной структуры. Предложенная методология опирается на создание многоуровневой системы оценочных индексов, учитывающей не только структуру системы, но и фундаментальные принципы ее функционирования. На этой основе формируются базовые правила оценки.

Для минимизации влияния ошибок, информационных помех и неточностей экспертного анализа предлагается использовать пороговые значения интервалов для определения достоверности и весовых коэффициентов параметров, что совпадает с практическими результатами инженерных исследований.

Представленный в работе системный анализ таких параметров, как чувствительность, достоверность, весовые коэффициенты критериев в модели, разработанной на базе основных правил, позволил определить эффективность ключевых подсистем и компонентов, а также выявить факторы, оказывающие наибольшее влияние на итоговые результаты оценки. Результаты исследования могут послужить основой для формирования стратегий технического обслуживания и модернизации системы, что обеспечит её стабильную работу, повысит общий уровень эффективности и расширит функциональный потенциал. На основании проведенных расчетов также устанавливаются уровни точности, соответствующие заданным классам. Элементы предложенной методики неоднократно обсуждались на различных технических конференциях [16—31].

В перспективе планируется разработка модели оптимизации предлагаемого метода, включая анализ взаимозависимости критериев, что позволит обеспечить более точные и надежные результаты.

5. Zhou ZJ, Hu GY, Hu CH, et al. A survey of belief rule-base expertsystem. IEEE Trans Syst Ran Cybernet: Systers 2019.
6. Feng ZC, Zhou ZJ, Hu CH, et al. A safety assessment model based on belief rule base with new optimization method. Reliab Eng Syst Saf 2020.
7. Yang JB, Xu DL. Evidential reasoning rule for evidence combination. Artif Intell 2013;205:1—29.
8. Путятю М.М., Макарян А.С., Черкасов А.Н., Кучер В.А. Оценка функционирования SIEM-систем на основе комплекса критериев эффективности // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2024. Вып. 1 (336). С. 36—42. DOI: 10.53598/2410-3225-2024-1-336-36-42 .
9. Дидрих В.Е., Шелковников М.А., Юдаков Д.С., Митрофанова С.В. Оценка средней информационной эффективности декаметровых систем связи в режиме частотно-адаптивной радиоперелии // Воздушно-космические силы. Теория и практика. 2024. № 32.
10. Кочкаров А.А., Сомов Д.С., Крапчатова А. Повышение эффективности систем мониторинга сложных технических и информационно-управляющих систем. Метод структурно-интегрированных индикаторов // Вестник РГГУ. Серия «Экономика. Управление. Право». 2011. № 4 (66).
11. Lubentsov A.V., Bobrov V.N., Desyov D.B., Noev A.N. The advantage of the method of hierarchy analysis, the statistical methods of decision support. Journal of Physics: Conference Series. 17—19.12.2018, ВГУ. Международная научно-техническая конференция «Актуальные проблемы прикладной математики, информатики и механики». DOI: 10.1088/1742-6596/1203/1/012079 .
12. Лубенцов А.В. Использование каскадного метода анализа иерархий для оценки эффективности комплексной системы безопасности // Вестник Воронежского института ФСИИ России. 2022. № 4. С. 123—136.
13. Лубенцов А.В., Душкин А.В. Комплексные системы безопасности: системный анализ, архитектура, управление жизненным циклом. Воронеж : Научная книга, 2022. 254 с.
14. Лубенцов А.В. Системный анализ модели получения характеристик эффективности комплексной системы безопасности // Моделирование, оптимизация и информационные технологии, 2023;11 (1) сс. 1-8, УДК 007.51, 303.732, DOI: 10.26102/2310-6018/2023.40.1.030 .
15. Лубенцов А.В. Синтез метода оценки эффективности системы информационной безопасности // Известия высших учебных заведений. Электроника. 2024. Т. 29. № 1. С. 118—129. DOI: 10.24151/1561-5405-2024-29-1-118-129 . EDN: UJNZBJ.
16. Лубенцов А.В., Куфаева О.Ю., Кобзистый С.Ю. Системный анализ методов ранжирования систем безопасности с анализом их эффективности // Молодежь и системная модернизация страны : сборник научных статей 6-й Международной научной конференции студентов и молодых ученых, 20—21 мая 2021 г. Т. 2. С. 431—434. ISBN 978-5-9908449-7-3.
17. Лубенцов А.В., Кобзистый С.Ю. Системный анализ параметров сложной системы с применением каскадного метода анализа иерархий // ВИ ФСИИ РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2023. Т. 1. С. 187—191.
18. Лубенцов А.В., Кобзистый С.Ю. Моделирование оценки эффективности производительности контроллеров СКУД // ВИ ФСИИ РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы. 2023. Т. 1. С. 191—195.
19. Лубенцов А.В. Синтез интервальных оценок для построения модели оценки эффективности сложных систем // ВИ ФСИИ РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2023. Т. 1. С. 171—175.
20. Лубенцов А.В., Пузанкова А.И. Анализ основных моделей противодействия информационным атакам типа DoS и DDoS // В сб.: Радиолокация, навигация, связь. Сборник трудов XXX Международной научно-технической конференции. В 5 т. Воронеж, 2024. С. 112—120.
21. Лубенцов А.В., Власова А.И. Анализ методов защиты данных в интеллектуальных системах // IV научно-педагогические чтения молодых ученых им. проф. С.В. Познышева : сборник материалов Всероссийской научно-практической конференции курсантов и студентов. Воронеж : Воронежский институт ФСИИ России, 2024.
22. Лубенцов А.В., Лямчева А.В. Особенности защиты информации при организации видеоконференцсвязи в уголовно-исполнительной системе // IV научно-педагогические чтения молодых ученых им. проф. С.В. Познышева : сборник материалов Всероссийской научно-практической конференции курсантов и студентов. Воронеж : Воронежский институт ФСИИ России, 2024.
23. Лубенцов А.В., Миронова А.А. Безопасность систем баз данных в учреждениях пенитенциарной системы // IV научно-педагогические чтения молодых ученых им. проф. С.В. Познышева : сборник материалов Всероссийской научно-практической конференции курсантов и студентов. Воронеж : Воронежский институт ФСИИ России, 2024.
24. Лубенцов А.В., Папилова В.Г. Информационная безопасность в системах охранного видеонаблюдения на объектах ФСИИ // IV научно-педагогические чтения молодых ученых им. проф. С.В. Познышева : сборник материалов Всероссийской научно-практической конференции курсантов и студентов. Воронеж : Воронежский институт ФСИИ России, 2024.

25. Лубенцов А.В., Пузанкова А.И. Анализ системных различий и классификация по различным основаниям DoS и DDoS атак // IV научно-педагогические чтения молодых ученых им. проф. С.В. Познышева : сборник материалов Всероссийской научно-практической конференции курсантов и студентов. Воронеж : Воронежский институт ФСИН России, 2024.
26. Лубенцов А.В., Борщева Д.О. Вейвлет-анализ в системах видеонаблюдения: повышение точности обнаружения нарушений в УИС // ВИ ФСИН РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2024. Т. 1.
27. Лубенцов А.В., Власова А.И. Анализ обеспечения информационной безопасности в спутниковых сетях связи // ВИ ФСИН РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2024. Т. 1.
28. Лубенцов А.В., Гавриленко А.И. Методы повышения эффективности информационной безопасности // ВИ ФСИН РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2024. Т. 1.
29. Лубенцов А.В., Попова Д.А. Модель противодействия атакам вида MITM // ВИ ФСИН РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2024. Т. 1.
30. Лубенцов А.В., Новокшенов С.В. Анализ преимуществ IP-камер перед телевизионными в процессе защиты информации // ВИ ФСИН РФ. Труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2024. Т. 1.
31. Лубенцов А.В. Анализ применения моделей искусственного интеллекта в системе видеонаблюдения на объектах УИС // Всероссийская научно-практическая конференция «Информатизация и техническое обеспечение уголовно-исполнительной системы Российской Федерации: проблемы, решения и перспективы развития». НИИ ИТ ФСИН РФ, Тверь. Октябрь 2024.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

THE DEVELOPMENT AND SYSTEM ANALYSIS OF A METHOD FOR EVALUATING THE EFFICIENCY OF INFORMATION SECURITY OF A COMPLEX SYSTEM

Aleksandr Lubentsov, Ph.D. (Geography), Associate Professor at the Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russian Federation. ORCID: 0000-0003-0239-4843, SPIN code: 6530-4715.

E-mail: lubensov@mail.ru

Keywords: synthesis, decomposition, information security system, interval estimates, efficiency, efficiency assessment, cascade hierarchy analysis method.

Abstract

Problem statement: the architecture of modern complex information systems (SIS) is characterized by a high degree of complexity and multicomponence. Obtaining the parameters of the effectiveness of the system is an urgent and non-trivial task. In modern engineering, methods for solving the issues of evaluating the efficiency of the system have not been sufficiently developed.

Purpose of the work: this paper examines the problem of evaluating the effectiveness of complex information systems in terms of ensuring their security. This task is interpreted as a process of forming multidimensional solutions based on the analysis of multiparametric data by decomposing the system and introducing interval estimates.

Methods used in the study: the synthesis and application of a nonlinear model for evaluating the effectiveness of a complex information system is proposed. The model uses an interval form of data representation, which allows taking into account uncertainties, errors in the source data, measurement errors and the subjectivity of expert assessments.

Study findings: as part of the study, a systematic analysis of comprehensive information security assessments was carried out. The proposed methodology is based on the division of the functional structure of the system into its component elements, followed by simplification to basic modules. An innovative approach has been developed that includes the formation of key rules by integrating interval characteristics of cluster assessment and assessment of overall efficiency.

Practical significance. The obtained results and analytical conclusions serve as the basis for building development strategies for the entire IP (information system) and its components. The author's cascade hierarchy analysis method has been applied, which reduces the influence of the human factor in the criteria ranking process. This contributes to a significant increase in the objectivity of assessments of the efficiency of both individual subsystems and the entire information security system.

Thus, the implemented innovations significantly improve the accuracy and reliability of assessment processes in the field of information security.

References

1. P'iankov O.V., Popov A.V. Matematicheskaya model' otsenki effektivnosti protokola vzaimodeystviia sistem tsifrovoy radiosv'язi. Vestnik VI MVD Rossii. 2021. No. 4.
2. Goldobina A.S., Isaeva Iu.A., Nikulin D.M. Otsenka effektivnosti sistem obnaruzheniia vtorzheniia v informatsionnoi sisteme upravleniia proizvodstvom oboronno-promyshlennogo kompleksa. Interekspo Geo-Sibir'. 2020. No. 1.
3. Pal'guyev D.A. Sravnitel'naya otsenka effektivnosti informatsionnykh sistem ierarkhicheskoi i setevoi struktury na osnove entropiynogo podkhoda. RTS. 2020. No. 1 (37).
4. Zhukov M.M., Barkalov Iu.M., Telkov A.Iu. Metodologicheskii podkhod k imitatsionnomu modelirovaniyu pri issledovanii prakticheskoi effektivnosti sistem zashchity ot setevykh kiberatak. Vestnik VI MVD Rossii. 2022. No. 1.
5. Zhou ZJ, Hu GY, Hu CH, et al. A survey of belief rule-base expertsystem. IEEE Trans Syst Man Cybernet: Systems 2019.
6. Feng ZC, Zhou ZJ, Hu CH, et al. A safety assessment model based on belief rule base with new optimization method. Reliab Eng Syst Saf 2020.
7. Yang JB, Xu DL. Evidential reasoning rule for evidence combination. Artif Intell 2013;205:1–29.
8. Putiato M.M., Makarian A.S., Cherkasov A.N., Kucher V.A. Otsenka funktsionirovaniia SIEM-sistem na osnove kompleksa kriteriev effektivnosti. Vestnik Adygeiskogo gosudarstvennogo universiteta. Ser. Estestvenno-matematicheskie i tekhnicheskie nauki. 2024. Vyp. 1 (336). Pp. 36–42. DOI: 10.53598/2410-3225-2024-1-336-36-42.
9. Didrikh V.E., Shelkovnikov M.A., Iudakov D.S., Mitrofanova S.V. Otsenka srednei informatsionnoi effektivnosti dekametrovykh sistem sv'язi v rezhime chastotno-adaptivnoi radiolinii. Vozdushno-kosmicheskie sily. Teoriia i praktika. 2024. No. 32.
10. Kochkarov A.A., Somov D.S., Krapchatov A. Povyshenie effektivnosti sistem monitoringa slozhnykh tekhnicheskikh i informatsionno-upravliaiushchikh sistem. Metod strukturno-integrirovannykh indikatorov. Vestnik RGGU. Seriya "Ekonomika. Upravlenie. Pravo". 2011. No. 4 (66).
11. Lubentsov A.V., Bobrov V.N., Desytov D.B., Noev A.N. The advantage of the method of hierarchy analysis, the statistical methods of decision support. Journal of Physics: Conference Series. 17–19.12.2018, VGU. Mezhdunarodnaya nauchno-tekhnicheskaya konferentsiya "Aktual'nye problemy prikladnoi matematiki, informatiki i mekhaniki". DOI: 10.1088/1742-6596/1203/1/012079.
12. Lubentsov A.V. Ispol'zovanie kaskadnogo metoda analiza ierarkhii dlia otsenki effektivnosti kompleksnoi sistemy bezopasnosti. Vestnik Voronezhskogo instituta FSIN Rossii. 2022. No. 4. Pp. 123–136.
13. Lubentsov A.V., Dushkin A.V. Kompleksnye sistemy bezopasnosti: sistemnyi analiz, arkhitektura, upravlenie zhiznennym tsiklom. Voronezh : Nauchnaya kniga, 2022. 254 pp.
14. Lubentsov A.V. Sistemnyi analiz modeli polucheniia kharakteristik effektivnosti kompleksnoi sistemy bezopasnosti. Modelirovanie, optimizatsiya i informatsionnye tekhnologii, 2023;11 (1) ss. 1-8, UDK 007.51, 303.732, DOI: 10.26102/2310-6018/2023.40.1.030.
15. Lubentsov A.V. Sintez metoda otsenki effektivnosti sistemy informatsionnoi bezopasnosti. Izvestiya vysshih uchebnykh zavedenii. Elektronika. 2024. T. 29. No. 1. Pp. 118–129. DOI: 10.24151/1561-5405-2024-29-1-118-129. EDN: UJNZBJ.
16. Lubentsov A.V., Kufayeva O.Iu., Kobzisty S.Iu. Sistemnyi analiz metodov ranzhirovaniia sistem bezopasnosti s analizom ikh effektivnosti. Molodezh' i sistemnaya modernizatsiya strany : sbornik nauchnykh statei 6-i Mezhdunarodnoi nauchnoi konferentsii studentov i molodykh uchenykh, 20–21 maya 2021 g. T. 2. Pp. 431–434. ISBN 978-5-9908449-7-3.
17. Lubentsov A.V., Kobzisty S.Iu. Sistemnyi analiz parametrov slozhnoi sistemy s primeneniem kaskadnogo metoda analiza ierarkhii. VI FSIN RF. Trudy mezhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovovno-ispolnitel'noi sistemy". 2023. T. 1. Pp. 187–191.
18. Lubentsov A.V., Kobzisty S.Iu. Modelirovanie otsenki effektivnosti proizvoditel'nosti kontrollerov SKUD. VI FSIN RF. Trudy mezhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovovno-ispolnitel'noi sistemy. 2023. T. 1. Pp. 191–195.
19. Lubentsov A.V. Sintez interval'nykh otsenok dlia postroeniia modeli otsenki effektivnosti slozhnykh sistem. VI FSIN RF. Trudy mezhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovovno-ispolnitel'noi sistemy". 2023. T. 1. Pp. 171–175.

20. Lubentsov A.V., Puzankova A.I. Analiz osnovnykh modelei protivodeistviia informatsionnym atakam tipa DoS i DDoS. V sb.: Radiolokatsiia, navigatsiia, sviaz'. Sbornik trudov XXX Mezhhdunarodnoi nauchno-tekhnicheskoi konferentsii. V 5 t. Voronezh, 2024. Pp. 112–120.
21. Lubentsov A.V., Vlasova A.I. Analiz metodov zashchity dannykh v intellektual'nykh sistemakh. IV nauchno-pedagogicheskie chteniia molodykh uchenykh im. prof. S.V. Poznysheva : sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii kursantov i studentov. Voronezh : Voronezhskii institut FSIN Rossii, 2024.
22. Lubentsov A.V., Liamcheva A.V. Osobennosti zashchity informatsii pri organizatsii videokonferentssviasi v ugovno-ispolnitel'noi sisteme. IV nauchno-pedagogicheskie chteniia molodykh uchenykh im. prof. S.V. Poznysheva : sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii kursantov i studentov. Voronezh : Voronezhskii institut FSIN Rossii, 2024.
23. Lubentsov A.V., Mironova A.A. Bezopasnost' sistem baz dannykh v uchrezhdeniiakh penitentsiarnoi sistemy. IV nauchno-pedagogicheskie chteniia molodykh uchenykh im. prof. S.V. Poznysheva : sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii kursantov i studentov. Voronezh : Voronezhskii institut FSIN Rossii, 2024.
24. Lubentsov A.V., Papilova V.G. Informatsionnaia bezopasnost' v sistemakh okhrannogo videonabliudeniia na ob'ektakh FSIN. IV nauchno-pedagogicheskie chteniia molodykh uchenykh im. prof. S.V. Poznysheva : sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii kursantov i studentov. Voronezh : Voronezhskii institut FSIN Rossii, 2024.
25. Lubentsov A.V., Puzankova A.I. Analiz sistemnykh razlichii i klassifikatsiia po razlichnym osnovaniiam DoS i DDoS atak. IV nauchno-pedagogicheskie chteniia molodykh uchenykh im. prof. S.V. Poznysheva : sbornik materialov Vserossiiskoi nauchno-prakticheskoi konferentsii kursantov i studentov. Voronezh : Voronezhskii institut FSIN Rossii, 2024.
26. Lubentsov A.V., Borshcheva D.O. Veivlet-analiz v sistemakh videonabliudeniia: povyshenie tochnosti obnaruzheniia narushenii v UIS. VI FSIN RF. Trudy mezhhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovno-ispolnitel'noi sistemy". 2024. T. 1.
27. Lubentsov A.V., Vlasova A.I. Analiz obespecheniia informatsionnoi bezopasnosti v sputnikovykh setiakh sviasi. VI FSIN RF. Trudy mezhhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovno-ispolnitel'noi sistemy". 2024. T. 1.
28. Lubentsov A.V., Gavrilenko A.I. Metody povysheniia effektivnosti informatsionnoi bezopasnosti. VI FSIN RF. Trudy mezhhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovno-ispolnitel'noi sistemy". 2024. T. 1.
29. Lubentsov A.V., Popova D.A. Model' protivodeistviia atakam vida MITM. VI FSIN RF. Trudy mezhhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovno-ispolnitel'noi sistemy". 2024. T. 1.
30. Lubentsov A.V., Novokshchenov S.V. Analiz preimushchestv IP-kamer pered televizionnymi v protsesse zashchity informatsii. VI FSIN RF. Trudy mezhhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob'ektov ugovno-ispolnitel'noi sistemy". 2024. T. 1.
31. Lubentsov A.V. Analiz primeneniia modelei iskusstvennogo intellekta v sisteme videonabliudeniia na ob'ektakh UIS. Vserossiiskaia nauchno-prakticheskaiia konferentsiia "Informatizatsiia i tekhnicheskoe obespechenie ugovno-ispolnitel'noi sistemy Rossiiskoi Federatsii: problemy, resheniia i perspektivy razvitiia". NII IT FSIN RF, Tver'. Oktiabr' 2024.

ГЕНЕРАЦИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПОМОЩЬЮ БЛЕНДЕРА

Грозов В.А.¹, Будько М.Ю.², Гирик А.В.³

Ключевые слова: защита данных, ГОСТ Р 34.12-2015 «Кузнечик», криптографический алгоритм, индивидуальный ключ, min -энтропия, генератор случайных последовательностей, сеть Фейстеля.

Аннотация

Цель статьи: разработка метода генерации криптостойких псевдослучайных последовательностей (ПСП), применимых в задачах защиты данных на основе алгоритма блендера.

Методы исследования: методика генерации ПСП на основе криптостойких алгоритмов в соответствии с рекомендациями NIST SP 800-90. Методика тестирования: NIST. Сравнение и оценка качества ПСП с помощью min -энтропии, критерия Пирсона и линейной сложности.

Полученный результат: предложен метод генерации криптостойких ПСП, применимых при защите информации в киберфизических системах. Метод основан на использовании блендера в качестве средства генерации ПСП, а также механизма расширения ключей криптоалгоритма блочного шифрования ГОСТ Р 34.12-2015 «Кузнечик». Такой механизм позволяет получать индивидуальные ключи для генерации каждого блока, из которых формируется выходная последовательность, что обеспечивает повышение её криптостойкости. Алгоритм блендера позволяет генерировать блоки произвольной длины. Дополнительная случайность вводится за счет специальной структуры итерационных констант, содержащих секретную ключевую информацию. Оценка качества выходных последовательностей проведена на основе значений min -энтропии, критерия Пирсона и профиля линейной сложности. Исследование статистических свойств последовательностей и их степени случайности выполнялось с помощью пакетов NIST SP 800-22 и NIST 800-90B. Подтверждено высокое качество генерируемых последовательностей.

Научная и практическая значимость: разработка и оценка эффективности метода генерации ПСП с помощью блендера, основанного на применении ключей, индивидуальных для каждого блока выходной последовательности. Использование блендера позволяет получать блоки произвольной длины. Высокая скорость работы блендера и простота его алгоритма дают возможность применять предложенный метод генерации в приложениях информационной безопасности на различных платформах для киберфизических систем с ограниченными ресурсами. Кроме того, предложенная схема генерации позволяет легко распараллеливать вычислительные процессы в целях повышения скорости генерации.

DOI: 10.24412/1994-1404-2025-1-141-152

Введение

В области обеспечения информационной безопасности киберфизических систем (КФС), использование которых неуклонно растет в самых разных сферах деятельности, особое место занимают задачи, относящиеся к разнообразным системам, обладающим низкими ресурсами и в силу этого не обеспеченным достаточной защитой. Регулярный обмен ин-

формацией, необходимой для их функционирования, и всё более высокий уровень угроз требуют совершенствования методов и средств криптографической защиты передаваемых данных [1—3]. Это относится к оборудованию Интернета вещей [4], беспилотному транспорту [5], носимым медицинским устройствам [6] и т. п.

¹ Грозов Владимир Андреевич, преподаватель факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-7998-8175.

E-mail: vagrozov@itmo.ru

² Будько Михаил Юрьевич, кандидат технических наук, доцент факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-1444-277X.

E-mail: mbudko@itmo.ru

³ Гирик Алексей Валерьевич, кандидат технических наук, доцент факультета БИТ Университета ИТМО, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-4021-7605.

E-mail: avg@itmo.ru

Важной частью криптографических методов являются специальные ГПСП: генераторы псевдослучайных последовательностей (ПСП), создающие ПСП, близкие по свойствам к действительно случайным. Существует множество работ, описывающих как конструкцию ГПСП, так и способы улучшения качества получаемых ПСП и точности оценки их свойств. Продолжаются исследования, связанные с разнообразными подходами к генерации ПСП. При этом происходят как поиск новых алгоритмов, так и модификация существующих с целью повышения качества и криптостойкости создаваемых ПСП.

Широко используемые и простые генераторы ПСП, основанные на сдвиговых регистрах с линейной обратной связью (РСЛОС), обладают высокой производительностью. Однако такие генераторы из-за своей линейности неустойчивы к криптографическим атакам и не подходят для приложений криптографической защиты. Тем не менее предлагаются меры, направленные на повышение криптостойкости таких генераторов за счет различных вариантов внесения нелинейности в их алгоритмы. Например, в [7] разрабатывается метод получения ПСП на основе нечеткой логики. В [8] рассматриваются линеаризованные варианты генерации криптографических ПСП на основе клеточных автоматов. В работе предлагается алгоритм использования полученных ПСП в системах аутентификации и проверки целостности данных. Простота процедуры линеаризации дает возможность применения указанного способа генерации в системах, работающих в режиме реального времени. В [9] генерация ПСП выполняется на базе рекурсивного алгоритма вычисления кубических радикалов, что обеспечивает неограниченную длину последовательностей и отсутствие периодичности их элементов.

Повышение случайности некоторых выходных последовательностей КСГПСП может быть достигнуто за счет использования физических источников энтропии. В статье [10] представлен новый метод генерации псевдослучайных чисел, основанный на дискретных одинаково распределенных источниках колебаний. Однако такие разработки сложны в использовании для многих объектов криптографической защиты из-за их ограниченных ресурсов. Более применимыми представляются генераторы, построенные с помощью криптоалгоритмов, использующие в качестве начального ключа последовательности, близкие по своим свойствам к истинно случайным. В связи с этим наиболее активно используются схемы генерации ПСП, основанные на проверенных криптоалгоритмах, поскольку они дают гарантированное преимущество с точки зрения криптографической безопасности. Например, для получения случайных битов желаемого качества из случайных показаний датчиков БПЛА в [11] используется процесс перемешивания, основанный на потоковом шифре RC4. В работе [12] обсуждается метод генерации ПСП с использованием хэш-функции, основанный на алгоритмах блочного шифрования PRESENT-80 и PRESENT-128.

Необходимость обеспечения информационной безопасности КФС с низким уровнем ресурсов для генерации ПСП приводит к использованию облегченных криптографических алгоритмов [13—15]. Существуют различные решения, позволяющие сохранить баланс между снижением стоимости генерации ПСП и степенью их криптостойкости. Например, в [16] предлагается криптографическая генерация ПСП на основе облегченного блочного криптографического алгоритма Speck, модифицированного путем включения новой функции генерации ключей для повышения случайности выходных данных ПСП.

При всем разнообразии инструментов и подходов, одной из важнейших задач при разработке ГПСП, используемых для задач информационной безопасности, является обеспечение их криптостойкости. Многие распространенные способы ее решения, например, основанные на сложности используемых алгоритмов или увеличении количества циклов шифрования, вряд ли применимы для систем с ограниченными ресурсами. Таким образом, поиск новых быстрых и недорогих методов получения криптографически стойких ПСП является актуальной задачей.

В статье рассматривается метод генерации ПСП на основе блендера⁴, который удовлетворяет этим требованиям. Его структура позволяет получать последовательности, состоящие из блоков произвольной длины. Целью работы является повышение криптографической стойкости генерируемых последовательностей. Эта цель достигается за счет использования индивидуальных ключей и внесения дополнительной случайности в формирование каждого блока ПСП.

1. Материалы и методы

Подходы к генерации криптографически стойких ПСП

Эффективным способом генерации криптографически стойких ПСП является использование алгоритмов блочного шифрования в режимах обратной связи по выходу (OFB) и счетчика (CTR). В этих режимах блочные шифры работают по принципу поточного шифрования. Криптостойкость выходных последовательностей генераторов, реализованных таким образом, определяется стойкостью используемых алгоритмов. Обобщение результатов многочисленных исследований позволяет выделить следующие распространенные методы повышения криптостойкости, связанные с ключами, используемыми в алгоритмах генерации ПСП.

⁴Dodis Y., Elbaz A., Oliveira R., Raz R. Improved randomness extraction from two independent sources. In: K. Jansen, S. Khanna, J.D.P. Rolim, D. Ron (eds). Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. RANDOM APPROX. 2004. Lecture Notes in Computer Science. Vol. 3122. Springer, Berlin, Heidelberg. Pp. 334–344. DOI: 10.1007/978-3-540-27821-4_30.

- Частая смена ключевых последовательностей. Подобный подход реализован в технологиях распределения ключей («блуждающие ключи»).
- Внесение дополнительной случайности в ключевые последовательности. Это эффективно при наличии доступных и недорогих высококачественных источников случайных данных.
- Изменение размера ключа. Традиционный подход предполагает увеличение размера ключа.

Блендер как инструмент получения качественных ПСП

Важным вопросом при изучении способов генерации ПСП, близких по свойствам к истинно случайным последовательностям, является возможность их получения из слабых источников случайности. В работе авторов Santha и Vazirani⁵ доказано, что из нескольких потоков битов со слабой степенью случайности возможно получение потока битов большей случайности. Дальнейшие исследования в этом направлении привели к разработке серии экстракторов случайности для слабых источников. Одним из таких экстракторов является указанный выше блендер. Простой алгоритм блендера обеспечивает высокую скорость его работы и позволяет получать последовательности высокого качества при невысоких требованиях к входным потокам. Корректная работа блендера достигается при определенном уровне суммарной мин-энтропии входных последовательностей.

В работах [17, 18] рассматривалась возможность построения ГПСП с использованием блендера в качестве основного алгоритма на всех этапах работы генератора, а также оценивался уровень криптостойкости его выходных последовательностей.

Блендер преобразует две входные битовые последовательности $X = \{x_0, \dots, x_{l-1}\}$, $Y = \{y_0, \dots, y_{l-1}\}$ длины l в одну битовую последовательность $Z = \{z_0, \dots, z_{l-1}\}$ той же длины. Аналитически результат работы блендера можно записать, используя набор из l бинарных матриц полного ранга A_ℓ :

$$\text{BLE}_A : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,1\}^l : (x, y) \rightarrow \{0,1\}^l : (x, y) \rightarrow ((A_1 x) \cdot y, \dots, (A_l x) \cdot y) \quad (1)$$

Здесь $A_i x$ — матричное произведение A_ℓ на вектор x , символ « $\cdot$ » обозначает скалярное произведение ($i = 0, \dots, l-1$). Алгебраические операции над битовыми последовательностями рассматриваются в поле Галуа GF(2) и трактуются следующим образом: умножение эквивалентно логическому И, а сложение — логическому XOR.

Существуют различные варианты построения указанных матриц; например, предлагается способ, при

котором начальная матрица набора является единичной, а каждая последующая получается в результате выполнения циклического сдвига вправо столбцов предыдущей матрицы и операции XOR над первым столбцом результата сдвига и соответствующим базисным вектором, полученным в поле Галуа⁶. При этом доказывается, что блендер описанной конструкции обеспечивает экстракцию большего количества случайных битов, чем другие ранее разработанные экстракторы для двух слабых источников.

Важным преимуществом блендера является также возможность варьированием длин входных последовательностей получать на выходе любое требуемое количество битов.

Механизм расширения ключей шифра «Кузнечик»

Для последующего использования в схеме генерации ПСП выбран механизм расширения ключей алгоритма блочного шифрования «Кузнечик» (ГОСТ Р 34.12-2015). Этот криптоалгоритм сочетает высокую криптостойкость и производительность с простотой реализации. Расширение ключей производится на основе сети Фейстеля, на каждой итерации которой выполняются линейное и нелинейное преобразования (соответственно L и S). Сеть Фейстеля относится к распространенным и эффективным элементам криптографических алгоритмов. Обычно при шифровании выполняется несколько итераций сети Фейстеля с использованием одного набора входных данных, что приводит к перемешиванию и рассеиванию битов выходных ПСП, и, следовательно, повышает криптостойкость алгоритма шифрования. Сеть Фейстеля является удобным инструментом получения требуемого количества индивидуальных ключей. С учетом возможностей блендера для получения его входных последовательностей можно ограничиться одной итерацией. Еще одной привлекательной особенностью «Кузнечика» является наличие в нем итерационных констант C_i , которые, будучи преобразованы определенным образом, позволяют вносить дополнительную неопределенность во входные последовательности блендера. Благодаря включению в состав C_i значения счетчика генерация ПСП будет выполняться в режиме CTR. Таким образом, дополнение блендера модифицированным механизмом расширения ключей «Кузнечика» будет способствовать повышению криптостойкости результата генерации.

Методика оценивания качества ПСП

Исследование качества выходных последовательностей блендера проводилось с помощью оценки их линейной сложности, близости характера распределения к равномерному, статистических свойств и уровня

⁵ Santha M., Vazirani U.V. Generating quasi-random sequences from slightly-random sources. J. of Computer and System Sciences. 1986. Vol. 33 (1). Pp. 75–87. DOI: 10.1109/SFCS.1984.715945.

⁶ Johnston D. Random Number Generators—Principles and Practices. A Guide for Engineers and Programmers. DeG Press, 2018. 436 p.

min-энтропии. Min-энтропия определяется для независимой дискретной случайной величины X , принимающей значения $X = \{x_1, \dots, x_k\}$ с вероятностями p_i , как

$$H = \min_{1 \leq i \leq k} (-\log_2 p_i) = -\log_2 \left(\max_{1 \leq i \leq k} p_i \right) \quad (1)$$

и используется в качестве основной меры непредсказуемости случайной величины.

Числовые характеристики выходных ПСП были рассчитаны с использованием пакетов тестов NIST 800-22⁷ и NIST 800-90B⁸ (оценка статистических свойств и минимальной энтропии). Близость распределения выходных данных к равномерному определялась с помощью критерия Пирсона. Был построен также профиль линейной сложности, который является одной из мер криптографического качества ПСП [19].

2. Результаты

Аналитическое описание блендера

Блендер может быть описан различными способами, что позволяет выбирать наиболее удобные для решения поставленных задач. Исследование математических свойств блендера выполнялось с помощью теоретического подхода к его построению⁹. Для его аппаратной реализации наиболее эффективны логические схемы, а для целей программирования и исследования характеристик криптостойкости нелинейных преобразований блендера наиболее удобным является его представление в виде набора булевых функций¹⁰.

Рассмотрим подробнее алгоритм построения матриц блендера и получим их явные выражения. Далее будем использовать следующие обозначения: A_k — матрицы размерности $l \times l$, определяющие структуру блендера; B_k — базисные векторы-столбцы $l \times 1$; E , O — единичная и нулевая матрицы размерности $l \times l$; $k = 0, \dots, l-1$.

В качестве начальной матрицы A_0 выбирается некоторая сильно разреженная матрица полного ранга размерности $l \times l$. Базисные векторы B_k формируются как последовательности значений $1, 2^1, 2^2, 2^3, \dots, 2^{l-1}$, вычисленных в поле Галуа с помощью примитивного многочлена степени l . В силу существующего между полем Галуа $GF(2^l)$ и поля $\{0, 1\}^l$ изоморфизма эти векторы могут быть записаны в виде битовых последовательностей. Из их первых l элементов формируются базисные векторы B_k .

Процесс построения матриц, определяющих структуру блендера A_k , можно описать следующим образом.

1. Выбор начальных значений матриц и векторов. В качестве начальной матрицы A_1 размерностью $l \times l$ может быть выбрана единичная матрица $A_0 = E^{ij}$.

2. Формирование базисных векторов B_k как последовательности первых l значений $1, 2^1, 2^2, 2^3, \dots, 2^{l-1}$, элементов поля Галуа, вычисленных с помощью некоторого примитивного многочлена. Эти векторы могут быть записаны в виде битовых последовательностей. Например, для случая размерности блендера $l = 4$ десятичной последовательности $\{1, 2, 4, 8, 3, 6, 12, 11, 5, 10, 7, 14, 15, 13, 9\}$ соответствует двоичная последовательность $\{0001, 0010, 0100, 1000, 0011, 0110, 1100, 1011, 0101, 1010, 0111, 1110, 1111, 1101, 1001\}$. Из ее первых l членов и формируются базисные векторы B_k . В этом случае неприводимый многочлен имеет вид $x^4 + x + 1$.

3. Каждая следующая матрица A_k вычисляется путем циклического сдвига предыдущей матрицы вправо на один столбец (матрица A_{k-1}) и последующего выполнения операции XOR ($\oplus$) над 1-м столбцом сдвинутой матрицы и соответствующим базисным вектором B_k :

$$\begin{aligned} A_k^{(j)} &= A_{k-1}^{l-(l-j+1) \bmod l}, \\ A_k &= (A_k^{(1)} \oplus B_k, A_k^{(2)}, \dots, A_k^{(l)}), \\ j &= 1, \dots, l; \quad k = 1, \dots, l-1. \end{aligned} \quad (2)$$

Эквивалентное описание работы блендера с помощью булевых функций выглядит следующим образом:

$$\begin{aligned} f_0 &= x_{l-1}y_{l-1} \oplus x_{l-2}y_{l-2} \oplus \dots \oplus x_2y_1 \oplus x_0y_0, \\ f_1 &= x_{l-2}y_{l-1} \oplus \dots \oplus x_1y_2 \oplus x_0x_{l-1}y_1 \oplus x_{l-1}y_0, \\ &\quad \vdots \\ f_{l-1} &= x_0x_{l-1}y_{l-1} \oplus x_{l-1}x_{l-2}y_{l-2} \oplus \dots \oplus x_2x_1y_1 \oplus x_1y_0. \end{aligned} \quad (3)$$

Алгебраические операции над битовыми последовательностями рассматриваются в поле Галуа $GF(2)$ и трактуются следующим образом: умножение эквивалентно логическому И, а сложение — логическому XOR ($\oplus$). Знак логического И ($\wedge$) опускается.

На основе явного выражения для матриц блендера и его представления в виде набора булевых функций выполнена реализация алгоритма.

Генерация ПСП с помощью блендера

Генерация блоков выходных ПСП осуществляется с помощью блендера в сочетании с элементами механизма расширения ключей шифра ГОСТ Р 34.12-2015 «Кузнечик». Возможность получения ПСП, необходимых для корректной работы блендера даже при использовании минимального числа итераций сети Фейстеля, была подтверждена расчетами. Используемые в исходном алгоритме шифра ГОСТ Р 34.12-2015 итерационные константы определяются простым счетчиком, однако они допускают модификацию, направленную на повышение

⁷ Rukhin A., Soto J., Nechvatal J., et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. National Institute of Standards and Technology Special Publication 800-22, revision 1a, 2010.

⁸ Turan M., Barker E., Kelsey D., et al. Recommendation for the Entropy Sources Used for Random Bit Generation (Draft NIST Special Publication 800-90B). National Institute of Standards and Technology, 2018. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf>

⁹ Dodis Y., et al., 2004.

¹⁰ Johnston D., 2018.

криптостойкости. С помощью такого счетчика генерацию ПСП можно выполнять в режиме CTR.

Повышение криптостойкости в предлагаемом методе генерации базируется на применении блендера и использовании индивидуального ключа для получения очередного блока ПСП. Кроме того, для внесения в алгоритм генерации дополнительной неопределенности служат итерационные битовые константы C_i длины l , сформированные специальным образом.

Вначале рассмотрим задачу формирования входных последовательностей для блендера, которые в дальнейшем будут играть роль ключа и вектора инициализации. Их получение состоит в создании выходного потока битов длиной $m \times l$ (m — количество блоков) из короткого ключа длиной $2l$. Для решения этой задачи построен алгоритм на базе модернизированного механизма расширения ключей шифра ГОСТ Р 34.12-2015 «Кузнечик», использующего линейное (L) и нелинейное (S) преобразования.

Поскольку блендер предназначен для работы со слабыми источниками, допустимо некоторое снижение требований к его входным последовательностям, поэтому для сокращения времени работы алгоритма количество итераций при генерации блока выходного потока уменьшено с восьми (оригинальный алгоритм) до одной.

Предлагаемый метод генерации основан на применении блендера в сочетании с модифицированной сетью Фейстеля. Схема процесса генерации ПСП представлена на рис. 1, а. Модификация сети Фейстеля происходит следующим образом. На каждой ее итерации формируются новые значения ключа K и вектора инициализации IV , которые являются входными последовательностями блендера. При этом каждая итерация сети Фейстеля работает со своим набором входных данных. Таким образом, каждый блок последовательности генерируется с помощью индивидуальных ключа и вектора инициализации. Общее количество итераций сети Фейстеля равно m .

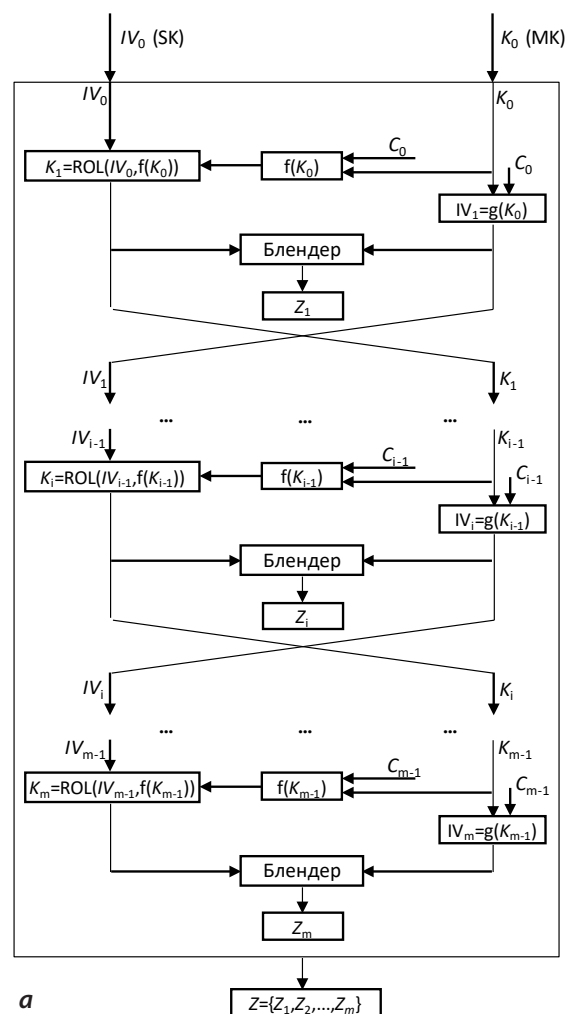
Перед началом генерации очередной ПСП задаются уникальные значения мастер-ключа $МК(K_0)$ и сеансового ключа $СК(IV_0)$. Их преобразование в соответствии со схемой g дает первые входные последовательности блендера — K_1 и IV_1 соответственно (рис. 1, б).

Отличительной особенностью предлагаемой схемы является совмещение в пределах одной итерации сети Фейстеля как генерации очередного блока ПСП, так и обновление входов блендера — ключа и вектора инициализации, с помощью которых будет формироваться следующий блок ПСП.

Перед подачей на блендер вектор инициализации и ключ модифицируются следующим образом. Во-первых, над значением ключа и итерационной константы C_i выполняется операция XOR, после чего к ее результату последовательно применяются преобразования S и L алгоритма «Кузнечик». Результатом этих преобразований является новое значение ключа (функция g). Во-вторых, вектор инициализации модифицируется с помощью побайтового циклического

сдвига влево. Для его программной реализации используется команда ассемблера ROL. Величина сдвига определяется тремя младшими битами, взятыми из каждого байта результата операции XOR над очередной ключевой последовательностью K_i и итерационной константой C_i (функция f , рис. 1, в). Использование циклического сдвига связано с тем, что он сохраняет баланс значений 0 и 1 во входных последовательностях, необходимый для корректной работы блендера.

Результат работы блендера образует очередной блок выходной ПСП генератора Z_i . Перед началом следующей итерации сети Фейстеля вектор инициализации и ключ меняются ролями и преобразовываются аналогичным образом.



а

б

в

Рис. 1. Процесс генерации ПСП:
а — общая схема, б — функция f , в — функция g

Процедура формирования итерационных констант C_i состоит в применении линейного преобразования L алгоритма «Кузнечик» к счетчику итераций C_i , изменяющемуся с каждой новой итерацией. Начальное заполнение счетчика итераций (C_0) выполняется следующим образом:

$$C_0 = (MK \wedge SK) \oplus MK. \quad (4)$$

Далее на каждой итерации значение счетчика C_0 сдвигается влево на число битов, необходимое для размещения номера итерации (i). Освободившиеся младшие биты заполняются значащими разрядами счетчика. Результатом является значение итерационного счетчика C_i . Этот метод формирования счетчика устраняет риск, связанный с наличием систематических входных данных. После применения линейного преобразования L к C_i получаются окончательные значения констант C_i , которые используются при формировании входных последовательностей блендера.

Таким образом, каждая итерация сети Фейстеля включает модификацию последовательностей K и IV ,

генерацию очередного блока ПСП с помощью блендера, а также смену ролей ключа и вектора инициализации.

Результаты численного исследования выходных последовательностей

Традиционным подходом при разработке криптостойких ГПСП является применение надежных криптоалгоритмов. Блендер изначально проектировался как экстрактор случайности, поэтому необходимо было провести исследование его возможностей обеспечивать необходимое качество выходных ПСП. Для этого выполнялось исследование качества выходных ПСП блендера по характеристикам, указанным во втором разделе. При этом использовались входные последовательности, разделенные на шесть уровней в соответствии со значениями min-энтропии (бит/байт) (табл. 1). Последовательности, сгенерированные для изучения возможностей блендера, имели длину 1 Мбит. Тестирование проводилось при уровне значимости $\alpha = 0,01$. Размерность блендера $l = 128$.

Таблица 1

Значения min-энтропии входных последовательностей

Min-энтропия (бит/байт)	Уровень энтропии входных последовательностей					
	1	2	3	4	5	6
Минимальная	0.7184	1.5392	2.2088	3.3464	4.5224	6.7192
Максимальная	0.7192	1.5416	2.2136	3.3592	4.5504	7.4304
Средняя	0.7192	1.54	2.212	3.3552	4.5344	7.1832

Результаты расчета криптографических характеристик стойкости выходных последовательностей блендера

в зависимости от среднего уровня min-энтропии входных последовательностей приведены в табл. 2 и на рис. 2.

Таблица 2

Характеристики выходных последовательностей блендера в качестве экстрактора

Min-энтропия (бит/байт)	Уровень энтропии входных последовательностей					
	1	2	3	4	5	6
Минимальная	0.7152	4.4448	5.8856	5.8856	6.4296	5.8856
Максимальная	0.7184	4.548	7.2976	7.2888	7.4488	7.2432
Средняя	0.7168	4.496	6.808	6.8032	6.8296	6.7912
Доля тестов NIST 800-22, пройденных на 99–100%	0	0.048	0.745	0.739	0.739	0.691
Критерий Пирсона χ^2	1.96·10 ⁶ –1.97·10 ⁶	1.32·10 ⁵ –1.33·10 ⁵	199–318	203–301	199–318	205–305

Представленные результаты показывают, что для блендера имеет место существенное влияние исходных данных на результаты работы. В случае блендера неудовлетворительные результаты соответствуют только двум низшим уровням входной min-энтропии. Таким образом, достаточная min-энтропия входных

данных должна превышать 2 бит/байт. При этом следует отметить, что уровень min-энтропии, обеспечивающий корректную работу блендера, заведомо превосходит такое значение. Таким образом, блендер обеспечивает необходимый уровень характеристик выходных последовательностей для достаточно широкого диапазона

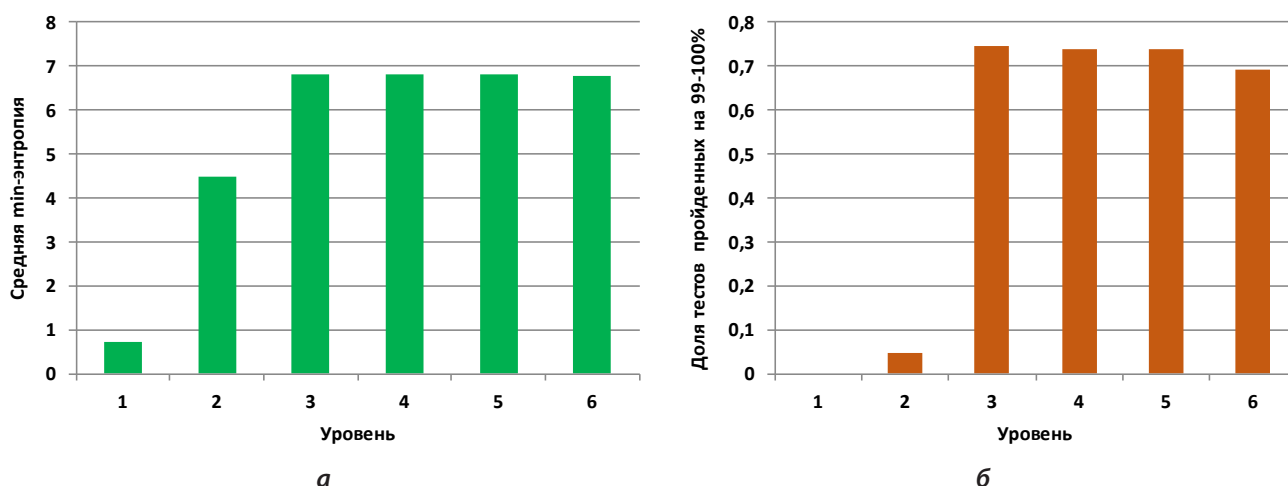


Рис. 2. Средняя min-энтропия (а) и доля пройденных тестов (б) для блендера

min-энтропии входных данных. В полном соответствии с указанным выше условием корректной работы блендера существует значительное влияние уровня min-энтропии входных последовательностей на качество выходных.

Относительно проверки статистических свойств выходных ПСП блендера следует заметить, что все тесты NIST 800-22 были успешно пройдены, начиная с третьего уровня min-энтропии входных данных. В четвертой строке табл. 2 приведены значения доли

тестов NIST 800-22, которые прошли все последовательности.

Представляет интерес сравнение полученных характеристик блендера с аналогичными характеристиками для генератора ПСП (на базе стандартного алгоритма ГОСТ 34-12.2015 «Кузнечик» в режиме OFB). Как видно из табл. 3 и рис. 3, результаты тестирования его выходных последовательностей также говорят об их хорошем качестве и мало зависят от уровня min-энтропии подаваемых на вход данных.

Таблица 3

Характеристики выходных ПСП генератора на основе алгоритма «Кузнечик» в режиме OFB

Min-энтропия (бит/байт)	Уровень энтропии входных последовательностей					
	1	2	3	4	5	6
Минимальная	5.9032	5.9032	5.9032	5.9032	5.9032	5.9032
Максимальная	7.3312	7.308	7.3584	7.408	7.312	7.3048
Средняя	6.7984	6.7832	6.7744	6.8152	6.8608	6.7832
Доля пройденных тестов NIST 800-22 (99-100%)	0.745	0.649	0.718	0.723	0.745	0.691
Критерий Пирсона χ^2	215–332	202–342	205–301	205–304	207–302	214–314

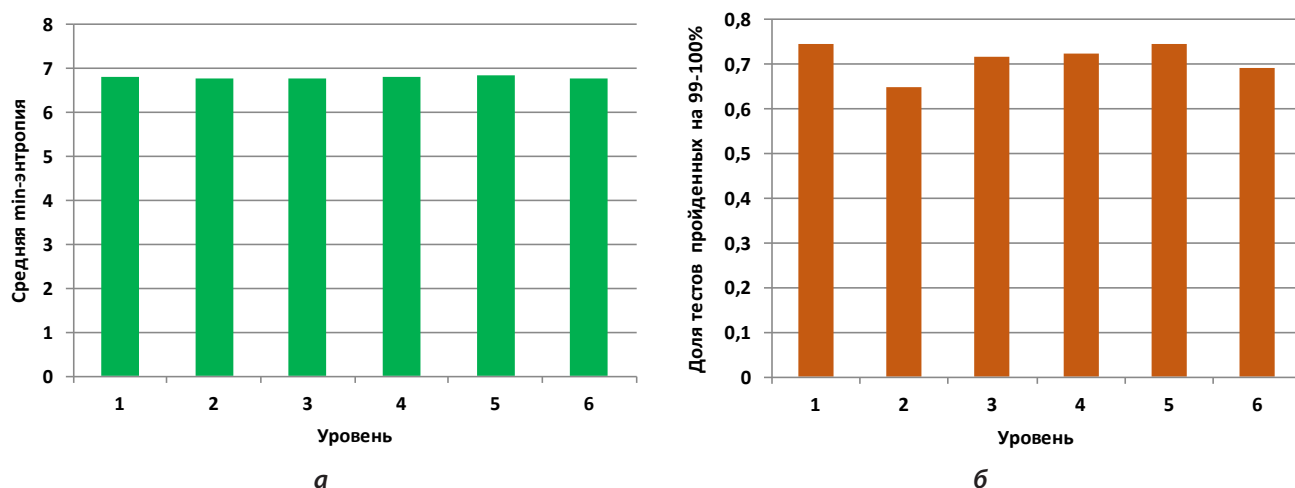


Рис. 3. Средняя min-энтропия (а) и доля пройденных тестов (б) для генератора ПСП на базе алгоритма ГОСТ Р 34.12-2015 «Кузнечик»

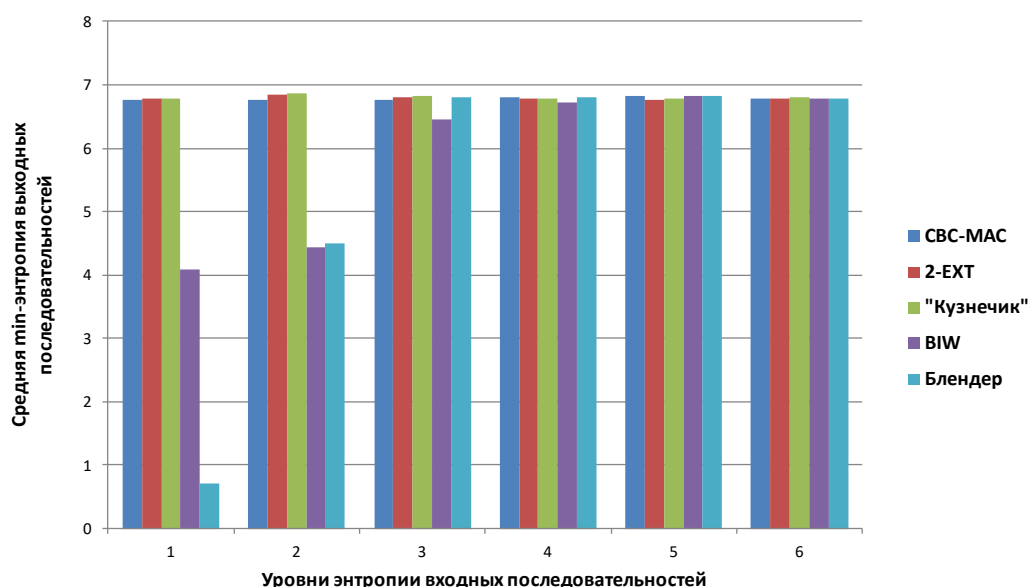


Рис. 4. Сравнение min-энтропии ПСП при разных вариантах генерации

Таблица 4

Характеристики выходных последовательностей генератора ПСП на основе блендера

Длина ключа, бит	Критерий Пирсона	Min-энтропия	NIST SP800-22	R ²
40	198—328	7.138	0.686	0.99993
48	203—308	7.134	0.649	0.999929
56	172—319	7.106	0.654	0.999927
64	208—303	7.125	0.665	0.999931
96	199—318	7.166	0.745	0.99993
128	203—319	7.138	0.729	0.999928
256	206—319	7.146	0.707	0.999929
512	202—327	7.122	0.718	0.999929
1024	199—307	7.136	0.718	0.99993

Таким образом, использование механизма шифра «Кузнечик» обеспечивает нужный уровень min-энтропии в ключах, играющих роль входных последовательностей генератора, созданного на базе блендера.

По рассмотренным характеристикам блендер также сравнивался с некоторыми известными экстракторами (CBC-MAC¹¹, 2-EXT, BIW¹²) и с генератором ПСП, основанном на надежном криптоалгоритме. Первые два средства извлечения используют криптографический

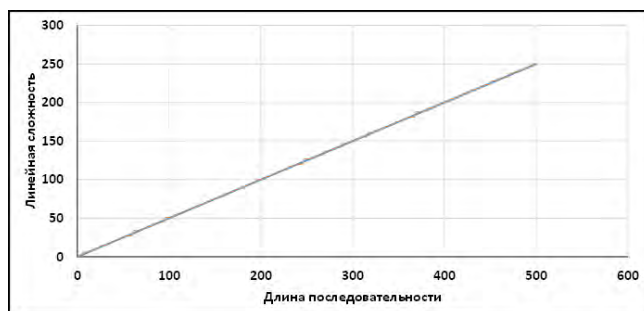
алгоритм AES. На рис. 4 представлена диаграмма, позволяющая сравнить среднюю min-энтропию всех рассмотренных экстракторов и генератора псевдослучайных последовательностей на основе алгоритма ГОСТ Р 34.12-2015 «Кузнечик».

Сравнение результатов и по остальным характеристикам показало, что блендер (при корректном его использовании) обеспечивает высокое качество выходных последовательностей. Это подтверждает перспективность использования блендера как ГПСР.

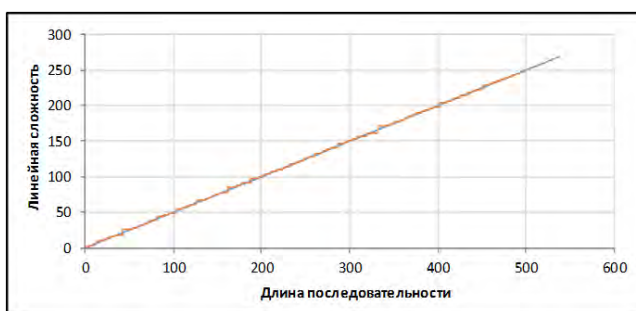
Для изучения качества выходных ПСП, полученных с использованием предложенного метода генерации, были выполнены расчеты их характеристик при различных длинах ключей. Результаты, представленные в табл. 4, соответствуют случаю, когда длины последовательностей, подаваемых в блендер, и длины выход-

¹¹ E. Barker and D. Kelsey, Recommendation for Random Bit Generator (RBG) Constructions (Draft NIST Special Publication 800-90C). National Institute of Standards and Technology, 2018. URL: https://csrc.nist.gov/csrc/media/publications/sp/800-90c/draft/documents/sp800_90c_second_draft.pdf

¹² Johnston D. Random Number Generators—Principles and Practices. A Guide for Engineers and Programmers. DeG Press, 2018. 436 p.



а



б

Рис. 5. Профили линейной сложности:
а — блендер, б — генератор Блум-Блума-Шуба (BBS)
(синий цвет — прямая $L_{seq}/2$)

ных блоков ПСП равны. Для оценки качества выходных данных было сгенерировано 1000 последовательностей по 4 Мбит каждая.

Наряду с показателями min-энтропии, степени прохождения статистических тестов и критерия Пирсона еще одной важной характеристикой криптографической стойкости генератора ПСП является линейная сложность его выходных последовательностей, вычисляемая на основе алгоритма Берлекампа-Мэсси¹³. На рис. 5 показаны диаграммы изменений линейной сложности. Для сравнения представлены аналогичные результаты для генератора Blum-Blum-Shub (BBS), который обладает доказанной высокой криптографической стойкостью¹⁴. Для всех рассмотренных ПСП линейные профили сложности хорошо аппроксимированы линией $L_{seq}/2$ (L_{seq} — длина последовательности), что указывает на высокую непредсказуемость рассматриваемых ПСП. Численно близость линейного профиля сложности к прямой $L_{seq}/2$ характеризуется значением R^2 (approximation confidence value). Его малое отклонение от единицы подтверждает высокую степень случайности исследуемых ПСП.

3. Обсуждение

В статье блендер рассматривается как инструмент, способный выполнять не только экстракцию случайности, но и собственно генерацию ПСП. Особенностью блендера является то, что он извлекает максимальную энтропию из относительно слабых источников. С помощью блендера можно также получить выходные ПСП, состоящие из блоков произвольной длины. Поскольку подтверждение криптографической стойкости выходных последовательностей блендера возможно только в результате комплексного исследования, была проведена оценка структуры самого блендера, характеристик ПСП и принципов их создания.

Исследование блендера как совокупности булевых функций, ранее выполненное авторами, показало, что они обладают свойствами, необходимыми для получения криптографически стойких ПСП. Результаты свидетельствуют также о близости характеристик булевых функций блендера ко многим важным характеристикам булевых функций известных криптоалгоритмов (например, AES) [18].

Помимо статистических свойств, исследуемых наиболее часто, рассматривалась min-энтропия как мера непредсказуемости последовательности. Степень близости результирующего распределения к равномерному оценивалась с использованием критерия Пирсона. Кроме того, близость исследуемой ПСП к истинно случайной была оценена с использованием такого значимого показателя, как линейная сложность.

В предложенном методе генерации используется комбинация алгоритма блендера и элементов криптоалгоритма «Кузнечик». Предлагаемый метод сочетает постоянную смену ключа при генерации блоков ПСП и внесение дополнительной случайности во входные данные блендера за счет специальной структуры итерационных констант. Их формирование выполняется с использованием секретного ключа. Таким образом, на каждой итерации (т. е. при формировании следующего блока ПСП) вводится добавочная случайность.

Необходимо особо отметить способность блендера использовать входные последовательности произвольной длины и получать блоки ПСП любой требуемой длины l за одну итерацию. Увеличение размера ключа традиционно рассматривается как положительный фактор с точки зрения криптостойкости. В то же время короткие ключи могут быть эффективны в определенных ситуациях. Например, блендер позволяет из сгенерированных блоков формировать гамму для последующего поточного шифрования. Размер блоков может варьироваться от одного символа до целого сообщения. В первом случае появление любого символа в зашифрованном тексте становится равновероятным, поскольку нарушаются все вероятностно-лингвистические связи алфавита. Во втором случае гамма, генери-

¹³ Menezes A., Oorschot P. van, Vanstone S. Handbook of Applied Cryptography. CRC-Press, 1996. 816 p.

¹⁴ Там же.

руемая блендером, превращается в псевдослучайный аналог одноразового блокнота¹⁵.

Кроме того, следует отметить следующие существенные преимущества блендера.

- Произвольный размер выходного блока ПСП.
- Независимость выходных битов от входных значений.
- Влияние входного бита на все выходные биты.

Выводы

Разработан метод генерации ПСП, основанный на использовании блендера и ключей, индивидуальных для каждого блока выходной последовательности. Генерация ключей осуществляется с использованием модифицированного механизма расширения ключа

шифра «Кузнечик», основанного на сети Фейстеля. Чтобы увеличить период последовательности и внести дополнительную случайность, были сформированы итерационные константы специальной структуры. Использование блендера позволяет получать последовательности, состоящие из блоков произвольной длины.

Исследования характеристик полученных ПСП подтвердили их высокое качество и возможность применения предложенного метода генерации в приложениях информационной безопасности для КФС.

Возможность варьирования размерности блендера позволяет реализовать предложенный метод генерации ПСП на различных платформах. Высокая скорость работы блендера и возможность использовать одну итерацию сети Фейстеля для получения блока ПСП обеспечивают высокую производительность генерации. Предлагаемый способ генерации не требует больших затрат памяти, что делает его применимым для устройств с ограниченными ресурсами.

¹⁵ Shannon C. Communication Theory of Secrecy Systems. Bell System Tech. J. 1949. Vol. 28 (4). Pp. 656–715.

Литература

1. Котенко И.В., Левшун Д.С., Чечулин А.А. и др. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров // Вопросы кибербезопасности. 2018. № 3 (27). С. 29—38. DOI: 10.21681/2311-3456-2018-3-29-38.
2. Cyber-Physical Systems: Cyber-Physical Systems: Modelling and Intelligent Control. Studies in Systems, Decision and Control. Vol. 338. A.G. Kravets, A.A. Bolshakov, and M.V. Shcherbakov, Eds. Springer, 2021. DOI: 10.1007/978-3-030-66077-2.
3. Arshad J., Azad M.A., Amad R., et al. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics. 2020. Vol. 9 (629). Pp. 1–24.
4. Perfect Secrecy in IoT: A Hybrid Combinatorial-Boolean Approach. Zolfaghari B., Bibak K., Eds. Springer, 2022. DOI: 10.1007/978-3-031-13191-2.
5. Syed F., Gupta S.K., et al. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. emerging telecommunications technologies. 2020. Vol. 32 (1). Pp. 1–34. DOI: 10.1002/ett.4133.
6. Yaqoob T., Abbas H., Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. A Review. IEEE Communications Surveys & Tutorials, 2019. Iss. 4. Pp. 3723–3768. DOI: 10.1109/comst.2019.2914094.
7. Anikin I.V., Alnajjar K. Secure Data Transmission in Cyber-Physical Systems Based on the New Approach for Stream Cipher's Gamma Generation. In: Cyber-Physical Systems, Springer, 2021. Pp. 333–346.
8. Кулешова Е.А. Методы применения клеточных автоматов в системах защиты информации // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2021. № 2. С. 81—93. DOI: 10.17308/sait.2021.2/3506.
9. Таныгин М.О., Крыжевнич Л.С., Зыков П.С. Разработка генератора псевдослучайных чисел на основе кубических радикалов // Изв. Юго-Зап. гос. университета. 2021. Т. 25 (4). С. 52—69. DOI: 10.21869/2223-1560-2021-25-4-52-69.
10. Sudeepa K.B., Aithal G. Generation of pseudo random number sequence from discrete oscillating samples of equally spread objects and application for stream cipher system. Concurrency and Computation Practice and Experience. 2019. Vol. 32 (3). Pp. 1–15. DOI: 10.1002/cpe.5181.
11. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones. Computer Science. IEEE Access. 2020. Vol. 8. Pp. 30343–30354. DOI: 10.1109/ACCESS.2020.2972958.
12. Susanti B.H., Jimmy J., Ardyani M.W. Evaluation with NIST Statistical Test on Pseudorandom Number Generators based on DMP-80 and DMP-128. In: Proc. of 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). 2022. Pp. 166–171. DOI: 10.1109/ISRITI56927.2022.10053041.
13. Ullah I., Meratnia N., Havinga P.J.M. Entropy as a service: a lightweight random number generator for decentralized IoT applications. In: Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (Austin, TX, USA, 2020). 2020. Pp. 1–6. DOI: 10.1109/PerComWorkshops48775.2020.9156205.
14. Ищукова Е.А., Толочаненко Е.А. Анализ алгоритмов шифрования малоресурсной криптографии в контексте интернета вещей // Современные наукоемкие технологии. 2019. № 3-2. С. 182—186.

15. Khan M.N., Rao A., Camtepe S. Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey. IEEE Internet of Things. 2021. Vol. 8 (6). Pp. 4132–4156. DOI: 10.1109/JIOT.2020.3026493.
16. Lusto R.A., Lusto F. Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things. IJ. Computer Network and Information Security. 2021. Vol. 13 (4). Pp. 14–25.
17. Grozov V., Guirik A., Budko M., Budko M. Construction of a Cryptographically Secure Pseudorandom Sequence Generator Based on the Blender Algorithm. In: Proc. of 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Virtual, Online, 2021. Pp. 156–161. DOI: 10.1109/ICUMT54235.2021.9631603.
18. Grozov V., Guirik A., Budko M., Budko M. Cryptographic Strength Study of the Pseudorandom Sequences Generator Based on the Blender Algorithm. In: Proc. of 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Valencia, Spain, 2022. Pp. 191–195. DOI: 10.1109/ICUMT57764.2022.9943350.
19. Гавришев А.А., Осипов Д.Л. Построение обобщенного критерия оценки качества криптостойких кодовых последовательностей, используемых в защищенных беспроводных системах связи // Научное приборостроение. 2023. Т. 33. № 4. С. 111—118.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

GENERATING CRYPTOGRAPHICALLY STRONG PSEUDORANDOM SEQUENCES USING A BLENDER

Vladimir Grozov, Lecturer at the Faculty of Secure Information Technologies of the ITMO University, St. Petersburg, Russian Federation. ORCID: 0000-0002-7998-8175.
E-mail: vagrozov@itmo.ru

Mikhail Bud'ko, Ph.D. (Technology), Associate Professor at the Faculty of Secure Information Technologies of the ITMO University, Saint Petersburg, Russian Federation. ORCID: 0000-0002-1444-277X.
E-mail: mbudko@itmo.ru

Alexei Girik, Ph.D. (Technology), Associate Professor at the Faculty of Secure Information Technologies of the ITMO University, Saint Petersburg, Russian Federation. ORCID: 0000-0002-4021-7605.
E-mail: avg@itmo.ru

Keywords: data protection, GOST R 34.12-2015 Kuznyechik, cryptographic algorithm, individual key, min-entropy, random sequence generator, Feistel network.

Abstract

Purpose of the paper: development of a method for generating cryptographically strong pseudorandom sequences (PRS) applicable in data protection tasks.

Methods used in the study: a technique for generating PRSs based on cryptographic algorithms in accordance with the recommendations of NIST SP 800-90. The NIST testing methodology. Comparison and evaluation of PRS quality using min-entropy, Pearson's criterion and linear complexity.

Study findings: a method for generating cryptographically strong PRSs applicable to the protection of information in cyber-physical systems is proposed. The method is based on using a blender as a means of generating PRSs, as well as a mechanism for expanding the keys of block cipher GOST R 34.12-2015 Kuznyechik. This mechanism allows to obtain individual keys for generating each block, from which the output sequence is formed, which ensures an increase in its cryptographic strength. The blender algorithm allows generating blocks of arbitrary length. Additional randomness is introduced due to the special structure of iterative constants containing secret key information. The quality of the output sequences was evaluated by means of the values of min-entropy, the Pearson criterion and the linear complexity profile. The statistical properties of sequences and their degree of randomness were assessed using the NIST SP 800-22 and NIST 800-90B test suits. The high quality of the generated sequences has been confirmed.

Research and practical significance: development and evaluation of the efficiency of a method for generating PRSs using a blender, based on the use of keys individual for each block of output sequence. Using a blender allows to generate blocks of arbitrary length. The high speed of the blender and the simplicity of its algorithm make it possible to apply the proposed generation method in information security applications on various platforms for cyber-physical systems with limited resources. In addition, the proposed generation scheme makes it easy to parallelize processes.

References

1. Kotenko I.V., Levshun D.S., Chechulin A.A. i dr. Kompleksnyi podkhod k obespecheniiu bezopasnosti kiberfizicheskikh sistem na osnove mikrokontrollerov. Voprosy kiberbezopasnosti. 2018. No. 3 (27). Pp. 29–38. DOI: 10.21681/2311-3456-2018-3-29-38.
2. Cyber-Physical Systems: Cyber-Physical Systems: Modelling and Intelligent Control. Studies in Systems, Decision and Control. Vol. 338. A.G. Kravets, A.A. Bolshakov, and M.V. Shcherbakov, Eds. Springer, 2021. DOI: 10.1007/978-3-030-66077-2.
3. Arshad J., Azad M.A., Amad R., et al. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. Electronics. 2020. Vol. 9 (629). Pp. 1–24.
4. Perfect Secrecy in IoT: A Hybrid Combinatorial-Boolean Approach. Zolfaghari B., Bibak K., Eds. Springer, 2022. DOI: 10.1007/978-3-031-13191-2.
5. Syed F., Gupta S.K., et al. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans. emerging telecommunications technologies. 2020. Vol. 32 (1). Pp. 1–34. DOI: 10.1002/ett.4133.
6. Yaqoob T., Abbas H., Atiquzzaman M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. A Review. IEEE Communications Surveys & Tutorials, 2019. Iss. 4. Pp. 3723–3768. DOI: 10.1109/comst.2019.2914094.
7. Anikin I.V., Alnajjar K. Secure Data Transmission in Cyber-Physical Systems Based on the New Approach for Stream Cipher's Gamma Generation. In: Cyber-Physical Systems, Springer, 2021. Pp. 333–346.
8. Kuleshova E.A. Metody primeneniia kletochnykh avtomatov v sistemakh zashchity informatsii. Vestnik Voronezhskogo gosudarstvennogo universiteta. Seriya: Sistemnyi analiz i informatsionnye tekhnologii. 2021. No. 2. Pp. 81–93. DOI: 10.17308/sait.2021.2/3506.
9. Tanygin M.O., Kryzhevich L.S., Zykov P.S. Razrabotka generatora psevdosluchainykh chisel na osnove kubicheskikh radikalov. Izv. Iugo-Zap. gos. universiteta. 2021. T. 25 (4). Pp. 52–69. DOI: 10.21869/2223-1560-2021-25-4-52-69.
10. Sudeepa K.B., Aithal G. Generation of pseudo random number sequence from discrete oscillating samples of equally spread objects and application for stream cipher system. Concurrency and Computation Practice and Experience. 2019. Vol. 32 (3). Pp. 1–15. DOI: 10.1002/cpe.5181.
11. Cho S.-M., Hong E., Seo S.-H. Random number generator using sensor for drones. Computer Science. IEEE Access. 2020. Vol. 8. Pp. 30343–30354. DOI: 10.1109/ACCESS.2020.2972958.
12. Susanti B.H., Jimmy J., Ardyani M.W. Evaluation with NIST Statistical Test on Pseudorandom Number Generators based on DMP-80 and DMP-128. In: Proc. of 5th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). 2022. Pp. 166–171. DOI: 10.1109/ISRITI56927.2022.10053041.
13. Ullah I., Meratnia N., Havinga P.J.M. Entropy as a service: a lightweight random number generator for decentralized IoT applications. In: Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (Austin, TX, USA, 2020). 2020. Pp. 1–6. DOI: 10.1109/PerComWorkshops48775.2020.9156205.
14. Ishchukova E.A., Tolomanenko E.A. Analiz algoritmov shifrovaniia maloresurnoi kriptografii v kontekste interneta veshchei. Sovremennye naukoemkie tekhnologii. 2019. No. 3-2. Pp. 182–186.
15. Khan M.N., Rao A., Camtepe S. Lightweight Cryptographic Protocols for IoT Constrained Devices: A Survey. IEEE Internet of Things. 2021. Vol. 8 (6). Pp. 4132–4156. DOI: 10.1109/JIOT.2020.3026493.
16. Lusto R.A., Lusto F. Modified Key Derivation Function for Enhanced Security of Speck in Resource-Constrained Internet of Things. IJ. Computer Network and Information Security. 2021. Vol. 13 (4). Pp. 14–25.
17. Grozov V., Guirik A., Budko M., Budko M. Construction of a Cryptographically Secure Pseudorandom Sequence Generator Based on the Blender Algorithm. In: Proc. of 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). Virtual, Online, 2021. Pp. 156–161. DOI: 10.1109/ICUMT54235.2021.9631603.
18. Grozov V., Guirik A., Budko M., Budko M. Cryptographic Strength Study of the Pseudorandom Sequences Generator Based on the Blender Algorithm. In: Proc. of 14th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), Valencia, Spain, 2022. Pp. 191–195. DOI: 10.1109/ICUMT57764.2022.9943350.
19. Gavrishev A.A., Osipov D.L. Postroenie obobshchennogo kriteriia otsenki kachestva kriptostoikikh kodovykh posledovatel'nostei, ispol'zuemykh v zashchishchennykh besprovodnykh sistemakh svyazi. Nauchnoe priborostroenie. 2023. T. 33. No. 4. Pp. 111–118.

ВИДЕОИГРЫ И ИГРОВЫЕ МЕХАНИКИ: ПРАВОВОЙ РЕЖИМ И ОХРАНА

Пагов А.Ж.¹

Ключевые слова: компьютерные игры, авторское право, патентное право, правила видеоигр, сравнительное правоведение.

Аннотация

Цель работы: анализ и разработка теоретико-правовых подходов к охране интеллектуальных прав на игровые механики в различных юрисдикциях. Исследование направлено на выявление закономерностей правоприменительной практики и определение правового режима игровых механик в контексте современных законодательных систем.

В работе использован комплексный метод исследования, включающий сравнительно-правовой анализ законодательства Российской Федерации, Республики Корея и США в сфере правовой охраны игровых механик. Проведен анализ научных концепций правового режима видеоигр, что позволило выделить ключевые аспекты регулирования. Кроме того, изучены патентные заявки и судебная практика, относящиеся к защите игровых механик, а также рассмотрены догматические и юрисдикционные перспективы их охраны.

Исследование показало, что, вопреки распространенному мнению о невозможности эффективного патентования игровых механик в Российской Федерации, выявлены примеры соответствующих объектов патентных прав, что свидетельствует о наличии правоприменительной практики в данном направлении. Анализ зарубежных юрисдикций продемонстрировал, что игровые механики могут быть защищены посредством авторского и патентного права, что опровергает тезис о невозможности их правовой охраны через сущность полезных моделей. На основе мониторинга патентных заявок и судебных решений выявлены характерные особенности правового регулирования игровых механик, включая их уникальные черты как объектов интеллектуальной собственности. Выявленные закономерности позволили сформулировать предложения по совершенствованию российской правовой системы в сфере защиты игровых механик, а также определить потенциальные направления дальнейших исследований в этой области.

DOI: 10.24412/1994-1404-2025-1-153-162

Введение и постановка задачи

Согласно аналитическим оценкам платформы Newzoo, к концу 2026 года объем мирового рынка игр составит 205,7 млрд долларов, а число игроков в мире достигнет 3,79 млрд². Если принять во внимание представленные подсчеты, то кажущаяся ранее для многих исследователей в онтологическом понимании тема видеоигр из «несерьёзной» и не требующей должного внимания трансформируется в предмет различных дискуссий как на уровне подачи материала на лекционных занятиях в университете, так и на уровне международных конференций³.

²Newzoo's Global Games Market Report 2023 // Newzoo. URL: <https://newzoo.com/resource/trend-reports/newzoo-global-games-market-report-2023-free-version> (дата обращения: 20.12.2024).

³Mastering the Game: Business and Legal Issues for Video Game Developers // World Intellectual Property Organization Baltic Sea Region Perspective. URL: https://www.wipo.int/meetings/ru/details.jsp?meeting_id=37864 (дата обращения: 20.12.2024).

Из разных идей и приложенных усилий разработчиков по сей день создаются уже не просто объекты для развлечений в виде компьютерного алгоритма, а главные активы многомиллионных корпораций в качестве результатов интеллектуальной деятельности, которые представляют из себя действительную (не вымышленную) коммерческую ценность. Разумеется, столь значимому объекту медиа необходима правовая охрана, однако удовлетворяет ли она всех заинтересованных лиц и решает ли возникающие теоретические и практические проблемы?

Данная статья также представляет мнение, противоположное тем авторам, которые подчеркивают, что «игровые механики не могут быть запатентованы на территории Российской Федерации» [1, с. 93], хотя были найдены соответствующие объекты патентных прав. Помимо этого, проведен анализ зарубежных юрисдикций, доказывающих обратное тезису «сущ-

¹ **Пагов Астемир Жирсланович**, студент 2 курса магистратуры Санкт-Петербургского государственного университета, юрист, г. Санкт-Петербург, Российская Федерация.

E-mail: apagov.legal@gmail.com

ность полезных моделей не позволяет применить их в сфере компьютерных игр» [1, с. 97].

Для ответа на вопрос автор:

1) провел анализ концепций правового режима видеоигр с дальнейшей постановкой ключевых аспектов, выделенных в двух юрисдикциях (Российская Федерация, Республика Корея);

2) рассмотрел с различных юрисдикционных и догматических перспектив правовую защиту игровых механик через призму трех юрисдикций (Российская Федерация, Соединенные Штаты Америки, Республика Корея);

3) осуществил мониторинг относимых и относительно оригинальных патентных заявок с некоторой правоприменительной практикой;

4) вывел ряд закономерностей и уникальных черт игровых механик как объектов определенной правовой сущности, а не только набора правил, реализуемых через действие алгоритмов.

Видеоигры и игровые механики

1. Общее о подходах к правовому режиму видеоигр

Видеоигры являются сложными авторскими произведениями, содержащими множество форм искусства, таких как музыкальное сопровождение, графические произведения, сюжетная составляющая и персонажи, которые предполагают вовлечение человека в виртуальный игровой мир при запуске видеоигры с помощью компьютерной программы на определенном оборудовании. Составляющие видеоигры могут быть защищены авторским правом, если они достигают определенного уровня оригинальности и креативности, однако это не единственный способ защиты, поскольку элементы внутри каждой конкретной игры различны, несмотря на общий элемент: компьютерный код, на основе которого разрабатывается видеоигра, в узком смысле [2, с. 7].

Эта глава будет посвящена сути видеоигр и игровых механик как правовых категорий, а в следующей главе автор углубится в проблематику защиты игровых механик (авторско-правовая и патентно-правовая дихотомия), используя конкретные акты правоприменения с примерами из трех юрисдикций. Выбор пал дополнительно на США и Южную Корею как по причине выбранного метода исследования — сравнительно-правовой, так и по причине высокого уровня развития игровой индустрии в представленных юрисдикциях (не говоря уже о потребительском влиянии целевой аудитории именно этих государств) [3, с. 289].

1.1. Российская Федерация

Отталкиваясь от необходимости жизненного взаимодействия с видеоиграми, в разных ситуациях возникают очевидно различные интерпретации понятия «видеоигра». Так, при анализе видеоигр через призму

спорта разумнее всего обратиться к части 1.1 раздела 1 «Правил вида спорта „компьютерный спорт“»:

«Видеоигра — инвентарь компьютерного спорта, состоящий из программного обеспечения, позволяющего осуществить организацию соревновательного процесса (геймплея) соревнующимся сторонам (спортсменам), формирующего соревновательное пространство (арену), создающее объекты управления, воспринимаемые органами чувств человека, где участник соревнований через устройства ввода/вывода воздействует на объекты управления. Видеоигра автоматически либо с помощью контролируемых настроек/запретов обеспечивает равные условия соревнующимся сторонам»⁴.

Рассматривая сущность игры через призму виртуального пространства, можно вывести более общее определение синонимичного термина:

«Компьютерная игра — виртуальное пространство, создаваемое компьютерными средствами и организованное в соответствии с правилами игры»⁵.

При этом какое бы мы ни дали определение видеоигре, конститутивные элементы должны идентифицировать его. Автору, без притязаний на абсолютную истину, таковыми кажутся следующие элементы.

Игры, в частности, видеоигры, используются для передачи идей и социальных сообщений⁶.

Видеоигры включают в себя визуальный и слуховой мир, в котором игрок-пользователь манипулирует виртуальным персонажем (или персонажами), а точнее, аватаром⁷.

Интерактивность — виртуальный мир существует на одном компьютере, но возможен доступ удаленно, то есть через Интернет-соединение.

Физичность — пользователи получают доступ к программе через интерфейс, который имитирует физическое окружение на экране используемого устройства.

Игры создают пространства с инструментарием, обеспечивающим возможность коммуникации и виртуального взаимодействия между большим количеством пользователей.

Предоставление пользователю способности реализовать суть игрового процесса — аутоотеличность⁸.

⁴ Правила вида спорта „компьютерный спорт“ (утв. приказом Минспорта России от 22.01.2020 № 22) // СПС «КонсультантПлюс» (дата обращения: 22.12.2024).

⁵ Интернет-право: учебник и практикум для бакалавриата и магистратуры / В.В. Архипов. М.: Юрайт, 2019. С. 234.

⁶ Brown v. Entertainment Merchants Assn., 564 U.S. 786, 131 S. Ct. 2729, 180 L. Ed. 2d 708 (2011) // Casetext: Legal Research. URL: <https://casetext.com/case/brown-v-entmt-merchants-assn/> (дата обращения: 23.12.2024).

⁷ Аватар (в контексте компьютерных игр и Интернета) — виртуальная репрезентация пользователя в компьютерной игре (например, персонаж) и (или) коммуникационном интернет-сервисе (например, фотография учетной записи). Термин «аватар» заимствован из индуизма. Исходный смысл термина — бог, нисшедший в материальный мир (Интернет-право. С. 231.).

⁸ Аутоотеличность (от греч. αὐτο- + τέλος, «цель в самом себе») — свойство деятельности, обуславливающее желание индивида участвовать в ней с целью получения опыта данной деятельности; самоценность; самодостаточность [4, с. 14].

С теоретической и практической точек зрения правовая природа видеоигр в рамках существующей парадигмы отечественного правового регулирования не считается однозначно определенной. Существует ряд подходов, анализ которых позволит вывести необходимые умозаключения для дальнейшей экстраполяции предмета статьи.

Первый подход предполагает отнесение видеоигры исключительно к программе ЭВМ, под которой понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения (ст. 1261 ГК РФ). Созданная на компьютере программа может порождать аудиовизуальные отображения в двух пониманиях:

1) воспроизводя добавленные в эту программу ранее отдельно созданные результаты интеллектуальной деятельности;

2) непосредственно в результате действия программного кода (когда в коде заложены команды, нацеленные на автоматическое создание отображения программными средствами и установленным функционалом) [5, с. 66].

Рассматривая указанный подход глубже, можно представить себе программу для ЭВМ, которая будет отвечать всем признакам компьютерной игры, однако при этом не иметь творческого характера в принципе, ибо презумпция творческого характера всех элементов компьютерной игры опровержима фактическими обстоятельствами.

Согласно второму подходу видеоигра может рассматриваться как мультимедийный продукт, считающийся разновидностью сложного объекта в соответствии со статьей 1240 ГК РФ. Представленный подход признает, что практически каждый элемент видеоигры имеет отдельного автора, внесшего творческие усилия, например, при разработке дизайна уровней, игрового дизайна, сценария. Представляется несправедливым, что их творческая деятельность относится к порождаемым ЭВМ аудиовизуальными изображениям и не наделяет авторов правами на созданное ими.

При квалификации видеоигры в качестве сложного объекта возникает возможность воспользоваться специальными положениями, содержащимися в ст. 1240 ГК РФ:

1) презумпцией приобретения заказчиком прав на результаты интеллектуальной деятельности, входящие в состав сложного объекта, на основании договора об отчуждении исключительного права;

2) презумпцией всемирного и ограниченного сроком действия исключительного права характера лицензии, предоставляемой на такие объекты (если права на них не были приобретены на основании договора об отчуждении прав);

3) недействительностью условий лицензионных договоров, ограничивающих условия последующего ис-

пользования результатов интеллектуальной деятельности, входящих в состав сложного объекта [6, с. 334].

Стоит учитывать, что не все игры имеют правовую природу в качестве сложного объекта, ибо элементы видеоигры, учитывая данный подход, должны быть результатами интеллектуальной деятельности или средствами индивидуализации и, соответственно, быть охраноспособными [7, с. 63—66]. При анализе предыдущего подхода выявлено, что если аудиовизуальные отображения, ранее созданные вне компьютерной программы, соединены в ней и впоследствии воспроизводятся, то имеет место правовая квалификация видеоигры в соответствии со ст. 1240 ГК РФ, в отличие от иного понимания порождения аудиовизуального отображения.

Кажется логичным и разумным вывод, что указанная проблема должна разрешаться в каждом конкретном случае с учетом обстоятельств, связанных с осуществлением процесса производства и технической реализацией определенной видеоигры.

1.2. Республика Корея

Законодательство Южной Кореи в сфере интеллектуальной собственности имеет тенденцию к осмыслению правового режима видеоигр и уделяет особое внимание контролю с защитой прав интеллектуальной собственности в видеоиграх.

Например, согласно пункту 1 статьи 13 Закона о развитии игровой индустрии № 14424 от 20 декабря 2016 года правительство должно разрабатывать политику защиты прав интеллектуальной собственности на игровые продукты, чтобы защищать и развивать творческую деятельность игр⁹.

В представленном законе есть и определение видеоигры («Игра») в статье 2:

«Игра относится к видеопродукту, созданному для развлечения с использованием технологии обработки информации или механических устройств, таких как компьютерные программы для использования в свободное время, обучения и упражнений».

С признанием роли видеоигр как культурного феномена усилился контроль за этой сферой, порой и чрезмерный. Как раз руководствуясь анализом последнего, в одном из своих решений Конституционный суд Республики Корея пришел к выводу, что ограничения и удаления видеопродуктов были неконституционными. В связи с этим регулирование, касающееся производства и распространения музыки, видеопродуктов и игровых продуктов, предполагалось кардинально изменить и смягчить¹⁰.

⁹ Закон о развитии игровой индустрии № 14424 от 20 декабря 2016 г. // CaseNote. URL: 법령/게임산업진흥에_관한_법률/제44조?c=2&d=20190228&h=&b=&a= (дата обращения: 28.12.2024).

¹⁰ Решение Конституционного суда № 401 от 28 февраля 2019 года по ходатайству о неконституционности статьи 44(2) Закона о развитии игровой индустрии // CaseNote. URL: casenote.kr/헌법재판소/2017헌바401 (дата обращения: 28.12.2024).

С одной стороны, видеоигры можно признать компьютерной программой по смыслу статей 2 и 8 Закона о защите компьютерных программ № 3920 от 31 декабря 1986 года, ибо

1) программой признается творческое произведение, выраженное в виде серии инструкций и команд, которые используются прямо или косвенно в устройстве, обладающем способностью обработки данных, таком как компьютер и т. п. с целью получения определенного результата;

2) авторское право на программу возникает с момента создания программы и не требует соблюдения каких-либо процедур или формальностей, а фактическое ядро любой видеоигры — это компьютерный код¹¹.

С другой стороны, видеоигры относят к кинематографическим произведениям в соответствии с системным толкованием статей 2 и 100 Закона об авторском праве № 18547 от 7 декабря 2021 (далее — «Закон об авторском праве»). Так, кинематографическим называют творческое произведение, содержащее непрерывные изображения (независимо от того, сопровождаются они звуком или нет), которые можно просмотреть или услышать путем воспроизведения изображений с помощью механического или электронного устройства. Права же на данный вид объектов авторского права считаются переданными видеопроизводителю (если нет специального соглашения между сторонами), однако права авторов художественных произведений или музыкальных произведений, использованных в производстве, не затрагиваются¹².

Согласно исследованию Всемирной организации интеллектуальной собственности (ВОИС), в результате судебная практика и доктрина Республики Кореи начали признавать видеоигры аудиовизуальными или кинематографическими произведениями в случаях, когда они удовлетворяют предпосылкам, установленным в Законе об авторском праве, поскольку предоставляется более эффективная и комплексная защита интеллектуальных прав большинства заинтересованных лиц, принявших участие в разработке видеоигры [2, с. 59—60].

Таким образом, правовой режим видеоигр в Республике Корея хоть и не закреплен напрямую законодательно, но также неустойчив под «гнетом» установления сложности элементов в видеоигре, так как гибридный режим «программа — кинематографическое произведение» подразумевается для защиты всех охраняемых элементов видеоигры. Однако подведенные итоги по правовому режиму видеоигр в РФ также применимы и к Южной Корее: проблема должна разрешаться в каждом конкретном случае с учетом обстоятельств, связанных с осуществлением процесса производства и технической реализацией определенной видеоигры.

2. «Алгоритмичность» игровых механик и их полезность

Название данного параграфа неслучайно является не только оммажем предмету статьи, ибо алгоритм, с одной стороны, есть совокупность инструкций, позволяющих решить проблему и достичь определенного заданного результата [8, с. 25], с другой стороны — основной компонент программы для ЭВМ по смыслу статьи 1261 ГК РФ, так как отражает точную и детерминированную последовательность действий компьютерного сигнала, записанного в виде человекочитаемого текста, кода, псевдокода, без которого не будет работать программа. Однако из установленного в п. 5 ст. 1259 ГК РФ следует, что алгоритм лишен правовой защиты, и охраняется лишь его реализация в виде последовательности операций и действий над этими операциями [8, с. 27].

В данной работе автором рассматриваются не просто игровые механики как некая последовательность действий, а реализация этих правил в компьютерной программе и на материальном носителе.

Сообщество разработчиков видеоигр обычно предпочитает термин «игровая механика» термину «правила игры», поскольку правила считаются печатными инструкциями, о которых игрок знает или должен знать для вхождения в игровую атмосферу, в то время как механика именно видеоигр скрыта от игрока, то есть реализована в программном коде, к которому у игрока нет прямого доступа через пользовательский интерфейс [9, с. 221].

Можно рассмотреть данное разграничение и с другой точки зрения. Игровые механики влияют на саму возможность пользователя видеоигры погрузиться в виртуальное игровое пространство (или просто запустить видеоигру, например, при плохой оптимизации игровых механик), в то время как правила игры предоставляют методику прохождения видеоигры для самого пользователя¹³.

Держа вышеуказанное в качестве важного уточнения, представляется разумным перейти к осмыслению игровых механик, а в дальнейшем термин «игровые механики» применять исключительно к видеоиграм.

Игровые механики помогают сбалансировать процесс прохождения игры таким образом, чтобы генерировать именно те впечатления, которые пользователи хотели получить от игры при достаточном вовлечении в **сюжет** (последовательность событий, которые разворачиваются в игре), **эстетику** (создание действительно запоминающегося впечатления игрока от процесса), **технологии** (сам носитель игры — физические объекты, которые делают ее возможной) [10, с. 53—54].

¹¹ Computer Programs Protection Act № 3920. December 31, 1986 // WIPO LEX. URL: <https://wipo.lex-res.wipo.int/edocs/lexdocs/laws/en/kr/kr003en.pdf> (дата обращения: 29.12.2024).

¹² Закон об авторском праве № 18547 от 7 декабря 2021 г. // Сайт Национального правового центра. URL: <https://www.law.go.kr/법령/저작권법> (дата обращения: 29.12.2024).

¹³ Это весьма условное разделение дефиниций, поскольку если правила игры абстрактны или вариативны, то видна разница между механиками и правилами. Однако в видеоиграх чаще всего нельзя выйти за пределы действующих правил в рамках ограниченного компьютерного кода, если не учитывать cheats, которые позволяют пройти игру «не по сценарию» разработчиков.

Далее Эрнест Адамс и Йорис Дорманс отмечают пять различных типов механик¹⁴:

- Физика — процесс перемещения, искажения, приращения, уничтожения игровых объектов;
- Внутренняя экономика — механика операций с игровыми элементами, которые собираются, потребляются и обмениваются пользователями друг с другом и с системой;
- Прогрессия — механика продвижения по уровням персонажа и виртуального игрового мира, которые блокируют или разблокируют доступ к определенным областям;
- Тактическое маневрирование — регулирование стратегических преимуществ;
- Социальное взаимодействие — коммуникация между игроками и создание мотивации к такой [9, с. 7].

Джесси Шелл, в свою очередь, выделяет семь типов игровых механик: пространство, время, действия, объекты, правила, навыки, случайность¹⁵.

Получается, что на одном уровне игровые механики — это очень объективные, четко сформулированные наборы законов виртуального игрового мира, однако на другом уровне они связаны с чем-то более «таинственным» [10, с. 166], так как разум пользователя разбивает все игры на ментальные модели, которые создают ощущение «клишированности». От последнего разработчики пытаются избавиться при помощи генерирования новых и компиляции старых игровых механик, выводя полезность конкретной механики в конкретном игровом событии.

Если же экстраполировать написанное, то можно представить и само определение игровых механик:

Игровые механики — это процедурные алгоритмы видеоигры, описывающие цель видеоигры и позволяющие сбалансировать другие конститутивные элементы игрового процесса, реализуемые в программном обеспечении.

Защита игровых механик: авторско-правовой и патентно-правовой подходы

1. Оригинальность и форма выражения сценария, изображений, танцев и подобных механик

Будучи на первый взгляд абстрактными идеями, игровые механики не считаются объективным выражением произведения. Кроме того, они являются «функциональ-

ными» для получения игроком удовольствия от игры. Таким образом, механика видеоигр часто приравнивается к правилам традиционных игр и как таковая не считается объектом авторского права, также не массово патентуется, по крайней мере, в Европе [11, с. 449].

Однако считать, что игровые механики не подлежат охране, равносильно фактической легализации клонов игр. Это хорошо известная дилемма особенно актуальна для игр-симуляторов, где аудиовизуальный результат может быть недостаточно творческим, чтобы пользоваться защитой авторского права, поскольку этот результат деятельности просто воспроизводит реальность¹⁶.

ГК РФ в статье 1259 устанавливает режим программ для ЭВМ как объекта авторских прав; при этом рассматривать всю видеоигру только как компьютерную программу, а игровые механики — исключительно как набор правил было бы неправильно.

Российская правоприменительная практика не пестрит изобилием судебных актов, рассматривающих отмеченную в статье проблематику, однако в немногочисленных найденных делах прослеживается общий вектор по вопросам охраноспособности игровых механик. Например, Тринадцатый арбитражный апелляционный суд сделал вывод о заимствовании нескольких элементов интерфейса и логики нескольких игр, однако заметил, что указанные элементы являются стандартными для многих других приложений и являются общеупотребительными¹⁷, с чем в дальнейшем согласился Суд по интеллектуальным правам и Верховный Суд РФ.

Каждый элемент видеоигры может быть охраноспособным, если были приложены творческие усилия или была пройдена процедура регистрации, например, товарного знака. Так, в США возникают авторские права на сюжет видеоигр как художественное произведение¹⁸, изображения¹⁹, татуировки²⁰, танцы²¹. Чаще всего в представленных категориях размышляют о применении доктрины “The Scenes of a Faire Doctrine” [12, с. 81], в соответ-

¹⁶ Stern Elecs., Inc. v. Kaufman, 669 F.2d 852, 856 (2d Cir. 1982) // CaseText. URL: <https://casetext.com/case/stern-electronics-inc-v-kaufman> (дата обращения: 06.01.2025).

¹⁷ Постановление Тринадцатого арбитражного апелляционного суда от 31 октября 2016 года № 13АП-25478/2016 по делу № А56-73596/2015 // СПС «КонсультантПлюс» (дата обращения: 06.01.2025). Постановление Девятого арбитражного апелляционного суда от 25 октября 2022 года № 09АП-67549/2022 по делу № А40-43579/2022 // СПС «КонсультантПлюс» (дата обращения: 06.01.2025).

¹⁸ Как защитить интеллектуальные права на видеоигру // Право.ру. URL: <https://pravo.ru/story/241226/> (дата обращения: 06.01.2025).

¹⁹ Nova Productions Ltd v Mazooma Games Ltd & Ors (CA). // 5RB. URL: <https://www.5rb.com/case/nova-productions-ltd-v-mazooma-games-ltd-ors-ca/> (дата обращения: 06.01.2025).

²⁰ Solid Oak Sketches, LLC v. 2K Games, Inc., 449 F. Supp. 3d 333 (S.D.N.Y. 2020) // CaseText. URL: <https://casetext.com/case/solid-oak-sketches-llc-v-2k-games-inc-2017> (дата обращения: 07.01.2025).

²¹ California District Court Holds Dance Moves in Fortnite Did Not Infringe Copyright // Lexology. URL: <https://www.lexology.com/library/detail.aspx?g=c55e1387-520a-48db-9b2d-52e09d6da63c> (дата обращения: 07.01.2025).

¹⁴ Отдельно стоит отметить, что скрупулезный анализ данных механик не является необходимым для представленной статьи, поскольку целью параграфа является показать мнения, существующие среди разработчиков видеоигр. Также намеренно не были представлены все вариации игровых механик, например, дискретные и непрерывные.

¹⁵ В данной типологии видна вышеописанная неопределенность в терминологии между «игровыми механиками» и «игровыми правилами». Шелл указывает, что правила делают возможными все механики, которые и добавляют решающий элемент, делающий игру игрой — цель [10, с. 184].

ствии с которой некоторые выражения идеи не могут быть охраноспособны как таковые, поскольку представляют собой набор стандартных элементов результатов интеллектуальной деятельности одного вида или жанра²². Американскими судами также отмечается, что отсутствие «минимального художественного выражения», необходимого для признания авторско-правовой охраны дизайна и конфигурации дисплея видеоигры, является причиной непредоставления правовой охраны видеоигре, а не финансовые доходы или общественная популярность, ибо «во главе угла» стоит оригинальность и креативность²³.

Переходя к анализу практике Республики Корея, важно указать: ранее суды придерживались позиции, что поскольку

1) под произведением понимается «творческое выражение идеи и мысли, полученное посредством умственных усилий человека в области культуры, такой как литература, наука или искусство»;

2) произведение относится к конкретному внешне-му выражению идей²⁴,

то игра со своими игровыми механиками не что иное, как своего рода «идея», поскольку с самого начала была принята позиция, согласно которой правила и методы игры трудно защитить от авторских прав.

Однако в 2019 году Верховный суд Республики Корея привлек внимание, вынеся решение, которое отличается от его предыдущих позиций²⁵. Верховный суд, рассматривая спор о схожести двух мобильных игр от Авокадо Энтертейнмент Инкорпорейтед и King.com Лимитед, не только определил игровые продукты как произведения сложного характера, сочетающие в себе литературные, музыкальные художественные произведения, произведения компьютерных программ и т. д., но и определил необходимость установления того, является ли игровой продукт творческим, через призму креативности каждого из компонентов, которые являются подмножеством самого игрового продукта²⁶.

Так, при рассмотрении креативности игрового продукта необходимо рассматривать креативность каждого компонента: персонажи, предметы виртуальной игровой реальности, интерфейс и остальные игровые механики, а вопрос, как выбирать, компоновать и комбинировать их, учитывается при составлении основного производственного замысла и сценария, технически реализуемого при выборе и расположении основных элементов. То есть судом напрямую исследовалась уникальность и креативность игровых механик не только для определения охраноспособности видеоигры в целом, но и сама возможность игровых механик при определенных условиях быть объектом авторского права.

Автором не было найдено в представленной судебной практике ни РФ, ни США, ни Республики Корея упоминания доктрины «слияния», которая проявляется лишь косвенно. Данная доктрина в авторском праве гласит, что если идея и ее выражение настолько связаны друг с другом, что они представляют собой единое целое, т. е. существует только один мыслимый способ или ограниченное число способов выразить и воплотить идею в произведении, то объективное выражение в реальном мире этой идеи не подлежит правовой защите в рамках авторского права [13, с. 781]. Хотя во всех трех юрисдикциях доктрина активно применяется²⁷.

В итоге: видеоигры состоят из множества охраноспособных и неохраноспособных элементов в зависимости от сложности разработки игры, а также формальных требований оригинальности и формы выражения, которые, в свою очередь, «расщепляются» на отдельные требования. Однако, как это видно из анализа правоприменительной практики трех юрисдикций, хоть указанные выводы применяются по отношению к видеоигре в целом и к каждой части отдельно, авторско-правовая защита игровых механик, по мнению автора, сомнительна в связи с особенностями игровых механик и повышенным требованиям авторского права к форме интеллектуального продукта, а не его содержания, по общему правилу.

2. Новизна, наличие изобретательского уровня, промышленная применимость диалогового окна и pay-to-win

Как отмечается в отечественной литературе, российское законодательство не препятствует патентованию алгоритма, который реализуется программой для ЭВМ и изложен в виде признаков способа как объекта

²² Walker v. Time Life Films, Inc. 784 F.2d 44 (2d Cir. 1986) // CaseMine. URL: <https://www.casemine.com/judgement/us/5914c27fadd7b049347c00d8> (дата обращения: 07.01.2025); Blizzard Entertainment, Inc v. Lilith Games Co. 2015 WL 8178826 (N.D. Cal. 2015) // Justia US Law. URL: <https://law.justia.com/cases/federal/districtcourts/california/candce/3:2015cv04084/290949/35/> (дата обращения: 07.01.2025).

²³ Atari Games Corp. v. Oman, U.S. District Court for the District of Columbia – 693 F. Supp. 1204 (D.D.C. 1988) May 25, 1988 // Justia US Law. URL: <https://law.justia.com/cases/federal/district-courts/FSupp/693/1204/2357614> (дата обращения: 07.01.2025).

²⁴ Решение Верховного Суда от 8 июня 1993 г. // CaseNote. URL: <https://casenote.kr/대법원/93다3073> (дата обращения: 08.01.2025); Решение Верховного суда от 25 ноября 1997 г. // CaseNote. URL: <https://casenote.kr/대법원/97도2227> (дата обращения: 08.01.2025).

²⁵ Несмотря на отсутствие прецедентного права в правовой системе Южной Кореи, как и в РФ, толкования закона в актах вышестоящих судов даже по конкретным делам считаются квазиобязательными к применению. Например, Решение Верховного суда от 16 мая 2013 г. [Gong 2013 2, 1077] // CaseNote. URL: <https://casenote.kr/대법원/2012다202819> (дата обращения: 08.01.2025).

²⁶ Решение Верховного суда от 27 июня 2019 г. [Gong 2019 2, 1447] // CaseNote. URL: <https://casenote.kr/대법원/2017다212095> (дата обращения: 08.01.2025).

²⁷ «Метод выражения, принятый Samsung в этом случае, является стандартом в соответствующей отрасли, поэтому кажется, что не существует другого более действенного метода». — Решение Верховного суда от 27 января 2005 г. [Jip 53, 407; Gong 2005.3.1.(221), 359]. // CaseNote. URL: <https://casenote.kr/대법원/2002도965> (дата обращения: 14.02.2025). См. также постановление Девятого апелляционного суда от 24 июня 2019 г. № 09АП-28070/2019 по делу № А40-60319/2018 // СПС «Консультант Плюс» (дата обращения: 14.02.2025); Educational. Testing Services v. Katzman, 793 F.2d 533, 539 (3d Cir. 1986) // CaseText. URL: <https://casetext.com/case/educational-testing-services-v-katzman-2> (дата обращения: 14.02.2025).

изобретения, если изложенный способ не представляет собой описание лишь последовательности выполнения конкретных математических операций²⁸.

В Российской Федерации патентование программы для ЭВМ в качестве изобретения не представляется возможным в силу императивности пунктов 4 и 5 статьи 1350 ГК РФ, поскольку правила и методики игр предполагают разработанную идею без формы, а многие компьютерные программы разрабатываются путем внесения поступательных изменений или улучшений в уже существующие программы, поэтому изобретательский уровень отсутствует по причине очевидности для специалистов [14, с. 42].

Представляется обоснованным осуществлять правовую защиту игровой механики в рамках полезной модели как техническому решению, относящемуся к устройству, так как полезной модели предоставляется правовая охрана, если она является новой и промышленно применимой, согласно статье 1351 ГК РФ.

Однако для соблюдения законодательных предписаний игровой механике недостаточно быть программным кодом: она должна осуществлять какую-то новую и полезную функцию в комплексе с основным материальным объектом.

При осуществлении мониторинга далее удалось найти патент на изобретения такого уровня в рамках мониторинга. Уже прекративший действие патент № 2 676 667 представляет механику движения, в которой принимаются входные данные от одного или нескольких ездовых при помощи схемы интерфейса транспортного средства, а отдельный игровой контроллер выполнен с возможностью принимать информацию от схемы интерфейса транспортного средства²⁹.

В Соединенных Штатах Америки существует четыре основных требования к патентоспособности согласно статье 52(1) Закона США «О патентах» № 117-168 от 1951 г.:

- должно существовать изобретение, относящееся к любой области техники;
- изобретение должно быть пригодным для промышленного применения;
- изобретение должно быть новым;
- изобретение должно иметь изобретательский уровень³⁰.

При мониторинге патентных заявок было выявлено наибольшее количество именно в США, что неудивительно, ибо они отказались от подхода, согласно которому патентоспособное изобретение

должно обязательно существовать в материальной форме [15, с. 7—8].

Патент США № 8360866 на игру Luchene описывает изобретение, которое подталкивает пользователей к совершению внутриигровых покупок, когда они сталкиваются со сложным сценарием³¹. При этом видеоигра может предоставить предложение игроку в тот момент, когда игрок столкнулся со значительной трудностью или неоднократно столкнулся с трудностями.

Далее, типичный пример механики pay-to-win — это патент США № 10099140. Сообщения от помощи в прохождении настроены для игрока на основе его или ее поведенческих данных, таких как уровень интереса или удовлетворенности игрой. Маркеры для таких сообщений могут включать «выигрыш или проигрыш заранее определенного количества игр подряд». Данные сообщения могут включать рекламные акции, связанные с микротранзакциями или загружаемым контентом³².

Патент США № 9795886 описывает систему, которая позволяет начинающим пользователям приобретать внутриигровую поддержку дешевле, чем опытным пользователям, то есть цены на улучшение в онлайн-игре на основе силы и/или мощности пользователя в игре³³.

Механика pay-to-win, как было показано на примерах, связана с целевым маркетингом. Из интересных данных можно выделить мнение некоторых ученых о том, что целевой маркетинг приносит пользу как рекламодателям, так и целевым потребителям. Так, целевой маркетинг сокращает потери, поскольку позволяет избежать навязывания рекламы лицам, которые вряд ли будут восприимчивы к рекламе [16, с. 85].

Полезность, новизну и неочевидность Патентное ведомство США нашло и в патенте № 9017169, который предоставлял возможность игрокам коммуницировать с помощью интерфейса: выведение на экран диалогового окна, память для хранения данных, связанных с игрой, один или несколько процессоров, соединенных с интерфейсом и памятью, генерирование первых графических данных, представляющие виртуальную игровую среду, принадлежащей второму игроку³⁴.

В Республике Корея также регистрируют патенты на игровые механики в случаях, предусмотренных в Законе о патентах № 19007 от 18 октября 2022 г. (далее — «Закон о патентах»), а именно пункта 1 статьи 2

²⁸ Джермакян В.Ю. Комментарий к главе 72 «Патентное право» Гражданского кодекса РФ (постатейный). 3-е изд., перераб. и доп. // СПС «Консультант Плюс» (дата обращения: 21.02.2025).

²⁹ Патент № 2676 667 // ФИПС. URL: <https://www.fips.ru/iiss/document.xhtml?facesredirect=true&id=e7908b0721f612d63776541bb7063f41> (дата обращения: 21.02.2025).

³⁰ Patents Law, 35 U.S.C. §§ 1 et seq. 1951 // Congress. Gov. URL: <https://www.congress.gov/117/plaws/publ169/PLAW-117publ169.pdf> (дата обращения: 21.02.2025).

³¹ U.S. Patent № 8360866 (filed Jan. 29, 2013) // USPTO. URL: <https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/8360866> (дата обращения: 21.02.2025).

³² U.S. Patent №. 10099140 (filed Oct. 16, 2018) //USPTO. URL: <https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/10099140> (дата обращения: 22.02.2025).

³³ U.S. Patent № 9795886 (filed Oct. 24, 2017) // USPTO. URL: <https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/9795886> (дата обращения: 22.02.2025).

³⁴ U.S. Patent №. 9017169 (filed Apr. 28, 2015) // Google Patents. URL: <https://patentimages.storage.googleapis.com/a1/ba/03/3f80bd263ff2c4/US9017169.pdf> (дата обращения: 22.02.2025).

и статьи 29³⁵: «Изобретения должны относиться к **сложным творениям (принцип изощренности)**, с технической **идеей** и использованием **законов природы**»³⁶.

В решении Патентного суда № 2921 от 4 июля 2016 года была отменена защита патента, так как его можно было легко воссоздать на основе уже опубликованного игрового сервера для конкурентного онлайн-обучения и его метода. Суд указал, что «технически не сложно выделить функцию сервера аутентификации, которая была внутренним компонентом в предыдущем изобретении, и перенести её на отдельный сервер. Кроме того, концепция сервера аутентификации уже широко применяется в интернет-технологиях. Даже человек без технического образования может легко понять и воспроизвести этот компонент изобретения».

Таким образом, существует множество патентов на различные игровые механики, удовлетворяющие требованиям национальных законодательств, если эти игровые механики хоть и являются синергией идеи и программного кода, но являются не просто функцией, а составляют неотъемлемую и центральную часть технического решения конкретной задачи комплекса материальной и нематериальной сущности.

Заключение

В представленной статье был осуществлен сравнительно-правовой анализ правового регулирования видеоигр в целом, а также представлены концепции дихотомии правовой защиты игровых механик, которые имеют свои достоинства и недостатки в зависимости от конкретных параметров. Приведенные результаты анализа оказались возможны благодаря скрупулезному мониторингу патентных заявок и некоторой правоприменительной практики.

Автор предлагает не претендующий на абсолютную истину вклад в юридический научный дискурс, состоящий из:

1) выведенного авторского определения игровых механик для целей права, а также ряда закономерностей

и уникальных черт игровых механик, реализуемых через действие алгоритмов;

2) перенесения зарубежного опыта интерпретации игровых механик через расширение объема защиты авторских прав за счет включения рассуждений о том, как выбираются, составляются, комбинируются игровые механики в видеоигре (в интерпретации сложного объекта) для целей установления как самостоятельной творческой ценности механик, так и общего представления о видеоигре в качестве системы неотъемлемых подмножеств;

3) более детальное описание правового ландшафта с демонстрацией общих паттернов судебной и патентной практики трех юрисдикций, одна из которых не затрагивалась так подробно в научном сообществе.

Сделаны следующие выводы:

1) несмотря на ряд отечественных и зарубежных исследований, пока еще рано заявлять о едином представлении правового режима видеоигр даже в рамках условных групп (что видно на примере РФ и Республики Кореи);

2) для авторско-правовой охраны игровых механик, помимо установления оригинальности и формы, необходимо определение неких стандартов (возможно, для проверяющих и судебных органов³⁷), которые точно будут определять зависимость стабильной «работоспособности» игрового процесса от используемых игровых механик как в совокупности, так и по отдельности. Указанное не противоречит юридическим доктринам, например, слияния, а, наоборот, наполняет их глубиной правового анализа творческого вклада;

3) для патентно-правовой охраны игровых механик в каждой из проанализированных юрисдикций существуют свои особенности удовлетворения патентной заявки, однако общей закономерностью является выражение игровых механик в необходимой законом форме, и не просто выполнение в алгоритме конкретной функции, а наличие факта неотъемлемости технического решения конкретной задачи комплекса материальной и нематериальной сущности объекта патентных прав.

Данный подход кажется оптимальным при теоретической правовой защите игровых механик, нежели иной, поскольку

а) патентное право предлагает временное ограничение, что позволит третьим лицам по истечению срока действия патента воспользоваться технологией для дальнейшего развития отрасли;

б) принцип внесения имеет материально-правовое и конститутивное значение, выступая в качестве необходимого условия для возникновения или перехода прав на объекты патентных прав, а также осуществляет уведомительную функцию для третьих лиц.

³⁵ Закон о патентах №19007 от 18 октября 2022. // CaseNote. URL: <https://www.law.go.kr/법령/특허법> (дата обращения: 23.02.2025).

³⁶ «Естественный закон природы» относится к причине или явлению мира природы как к постоянному и неизменному неизбежному закону, происходящему в мире природы. Например, «вода течет с высокого места на низкое» или «гравитация действует на все предметы» — это законы природы. Однако игровые методы не являются законами природы и не могут быть предметом изобретения.

«Техническая идея» относится к идее, которая рационально создана для достижения определенной цели. Технологическая идея — это мысль, идеал или идея, которая существует в сознании человека и относится к ряду идей, задуманных для решения проблемы или достижения цели на основе технологии. Технические идеи должны быть конкретными.

«Изоощренность изобретения» относится к высокому уровню технологии, которую не может легко изобрести человек с обычными знаниями в соответствующей технической области. Напротив, фундаментальное различие между полезной моделью и изобретением заключается в том, что первое не требует высокой степени изобретательности в соответствии с Законом о патентах.

³⁷ Судя по новейшей судебной практике, правоприменительные органы стали больше углубляться в структуру и суть видеоигр, как это было в своём роде предсказано Ластовкой. См. Lastowka G. Copyright Law and Video Games: A Brief History of an Interactive Medium // SSRN. URL: https://www.wipo.int/meetings/ru/details.jsp?meeting_id=37864 (дата обращения: 02.03.2025).

Литература

1. Киселева Л.Ю. Видеоигры как объекты права интеллектуальной собственности // Образование и право. 2022. № 3. С. 93—99.
2. Abrams M.S. The Legal Status of Video Games: Comparative Analysis in National Approaches. WIPO Working Paper. 2013. 96 p.
3. Матвеев А.Г., Синельникова В.Н. Объекты интеллектуальной собственности, получающие охрану в XXI веке // Вестник Пермского университета. Юридические науки. 2019. № 2. С. 281—309.
4. Казакова Н.Ю. Гейм-дизайн (художественно-проектный подход к созданию цифровой игровой среды) : автореф. дис. ... докт. искусств. наук. М., 2017. 40 с.
5. Архипов В.В. Интеллектуальная собственность в индустрии компьютерных игр: проблемы теории и практики // Закон. 2015. № 11. С. 61—69.
6. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. М. : Статут, 2016. 640 с.
7. Чурилов А.Ю. Правовое регулирование интеллектуальной собственности в игровой индустрии // Интеллектуальная собственность. Авторское право и смежные права. 2017. № 10. С. 59—68.
8. Талапина Э.В. Алгоритмы и искусственный интеллект сквозь призму прав человека // Журнал российского права. 2020. № 10. С. 25—39.
9. Adams E., Dormans J. Game mechanics: Advanced Game design. Berkeley: New Riders Games. 2012. 353 p.
10. Schell J. The Art of Game Design: A Book of Lenses. Boca Raton: Taylor & Francis. 3rd edition. 2019. 610 p.
11. Boyden B. Games and Other Uncopyrightable Systems. George Mason Law Review. No. 439. 2011. P. 449.
12. Kurtz A. Copyright: The Scenes of a Faire Doctrine. Florida Law Review. Vol. 41. 1989. Pp. 79–114.
13. Murray M.D. Copyright, Originality, and the End of the Scenes a Faire and Merger Doctrines for Visual Works. Law Faculty Scholarly Articles. Vol. 58 (3). 2006. Pp. 779–860.
14. Чурилов А.Ю. Патентная охрана в индустрии видеоигр через призму патентования программ для ЭВМ // ИС. Промышленная собственность. 2020. № 12. С. 42—50.
15. Guntersdorfer M. Software Patent Law: United States and Europe Compared. Duke Law & Technology Review. 2003. Vol. 2. Iss. 1. Pp. 1–11.
16. Sigmon K.A. Pay to play: video game monetization patents and the doctrine of moral utility. Georgetown Law Technology Review. 2021. No. 5 (1). Pp. 72–98.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

VIDEO GAMES AND GAME MECHANICS: LEGAL REGIME AND PROTECTION

Astemir Pagov, 2nd year master's student at Saint Petersburg State University, lawyer, Saint Petersburg, Russian Federation. E-mail: apagov.legal@gmail.com

Keywords: computer games, copyright, patent law, video games rules, comparative law.

Abstract

Purpose of the paper: analysing and developing legal science approaches to protecting intellectual rights to game mechanics in different jurisdictions. The study is aimed at identifying patterns in law enforcement practice and determining the legal regime for game mechanics in the context of modern legal systems.

A manifold method of study was used in the paper which included a comparative legal analysis of laws of the Russian Federation, the Republic of Korea, and the USA in the field of game mechanics protection. An analysis of scholarly concepts of the legal regime of video games was carried out which allowed to single out the key aspects of regulation. In addition, patent claims and court practice related to game mechanics protection were studied, and dogmatic and jurisdictional prospects for their protection were considered.

The study showed that, contrary to a widespread belief that efficient patenting of game mechanics is impossible in Russia, examples of such objects of patent rights were found which means that there exists a law enforcement practice in this field. An analysis of foreign jurisdictions showed that game mechanics can be protected by copyright and patent law which refutes the argument that their legal protection using the essence of useful models is impossible. Based on monitoring patent claims

and court decisions, specific features of legal regulation of game mechanics were identified including their unique traits as intellectual property objects. The identified patterns allowed to word proposals for improving the Russian legal system in the field of game mechanics protection and to determine potential areas of further research in this field.

References

1. Kiseleva L.Iu. Videoigry kak ob"ekty prava intellektual'noi sobstvennosti. *Obrazovanie i pravo*. 2022. No. 3. Pp. 93–99.
2. Abrams M.S. The Legal Status of Video Games: Comparative Analysis in National Approaches. WIPO Working Paper. 2013. 96 p.
3. Matveev A.G., Sinel'nikova V.N. Ob"ekty intellektual'noi sobstvennosti, poluchaiushchie okhranu v XXI veke. *Vestnik Permskogo universiteta. Iuridicheskie nauki*. 2019. No. 2. Pp. 281–309.
4. Kazakova N.Iu. Geim-dizain (khudozhestvenno-proektnyi podkhod k sozdaniyu tsifrovoi igrovoi sredy) : avtoref. dis. ... dokt. iskusstv. nauk. M., 2017. 40 pp.
5. Arkhipov V.V. Intellektual'naia sobstvennost' v industrii komp'yuternykh igr: problemy teorii i praktiki. *Zakon*. 2015. No. 11. Pp. 61–69.
6. Savel'ev A.I. Elektronnaia kommertsii v Rossii i za rubezhom: pravovoe regulirovanie. M. : Statut, 2016. 640 pp.
7. Churilov A.Iu. Pravovoe regulirovanie intellektual'noi sobstvennosti v igrovoi industrii. *Intellektual'naia sobstvennost'. Avtorskoe pravo i smezhnye prava*. 2017. No. 10. Pp. 59–68.
8. Talapina E.V. Algoritmy i iskusstvennyi intellekt skvoz' prizmu prav cheloveka. *Zhurnal rossiiskogo prava*. 2020. No. 10. Pp. 25–39.
9. Adams E., Dormans J. *Game mechanics: Advanced Game design*. Berkeley: New Riders Games. 2012. 353 p.
10. Schell J. *The Art of Game Design: A Book of Lenses*. Boca Raton: Taylor & Francis. 3rd edition. 2019. 610 p.
11. Boyden B. Games and Other Uncopyrightable Systems. *George Mason Law Review*. No. 439. 2011. P. 449.
12. Kurtz A. Copyright: The Scenes of a Faire Doctrine. *Florida Law Review*. Vol. 41. 1989. Pp. 79–114.
13. Murray M.D. Copyright, Originality, and the End of the Scenes a Faire and Merger Doctrines for Visual Works. *Law Faculty Scholarly Articles*. Vol. 58 (3). 2006. Pp. 779–860.
14. Churilov A.Iu. Patentnaia okhrana v industrii videoigr cherez prizmu patentovaniia programm dlia EVM. *IS. Promyshlennaia sobstvennost'*. 2020. No. 12. Pp. 42–50.
15. Guntersdorfer M. Software Patent Law: United States and Europe Compared. *Duke Law & Technology Review*. 2003. Vol. 2. Iss. 1. Pp. 1–11.
16. Sigmon K.A. Pay to play: video game monetization patents and the doctrine of moral utility. *Georgetown Law Technology Review*. 2021. No. 5 (1). Pp. 72–98.