

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
Алексей Сергеевич Бурый

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 24.06.2025 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

Поздравления к 50-летию образования ФБУ НЦПИ при Минюсте России Толстой П.О.	4
Поздравления к 50-летию образования ФБУ НЦПИ при Минюсте России Таран С.Д.	5
НЕКОТОРЫЕ СТРАНИЦЫ ИСТОРИИ НАУЧНОГО ЦЕНТРА ПРАВОВОЙ ИНФОРМАЦИИ Морозов А.В.	6
Государственно-правовые науки	
СЛАБЫЕ МЕСТА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ПРОБЛЕМЫ ЕГО ИСПОЛЬЗОВАНИЯ В ПРОГРАММЕ «ПРАВОВАЯ ПОМОЩЬ» МИНИСТЕРСТВА ЮСТИЦИИ РОССИИ Батулин Ю.М.	10
ПУТИ ДИВЕРСИФИКАЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ФИНАНСОВЫХ ОТНОШЕНИЙ Васянина Е.Л., Запольский С.В.	16
ПОЛИТИКА ИМПОРТОЗАМЕЩЕНИЯ ДЕСЯТЬ ЛЕТ СПУСТЯ: ОПЫТ, ПРОБЛЕМЫ И ПОЛОЖИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ Кобзарь-Фролова М.Н.	23
ИНФОРМАЦИОННОЕ ПРАВО И ЦИФРОВАЯ РЕАЛЬНОСТЬ: РАЗВИТИЕ, ПРИОРИТЕТЫ И ПРОБЛЕМЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ Полякова Т.А., Троян Н.А.	31
О ПРЕДЕЛАХ ПРИМЕНЕНИЯ И ОСНОВАНИЯХ АДМИНИСТРАТИВНОГО ПРИНУЖДЕНИЯ Запольский С.В.	42
АКТУАЛЬНОСТЬ ВОПРОСА КОДИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА, РЕГУЛИРУЮЩЕГО ОТНОШЕНИЯ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ Савченко Е.А.	47
АКТУАЛЬНЫЕ ВОПРОСЫ СИСТЕМАТИЗАЦИИ ПРАВОВЫХ АКТОВ, ОБЕСПЕЧЕНИЯ ЕДИНСТВА ПРАВОВОГО ПРОСТРАНСТВА, ПРАВОВОЙ ПОМОЩИ И ПРАВОВОГО ПРОСВЕЩЕНИЯ Троян Н.А.	57
ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ МИНЮСТА РОССИИ Токолов А.В.	66
НОВЫЙ ВЕКТОР В РЕГУЛИРОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ: ПРОБЛЕМЫ И НЕОБХОДИМЫЕ ШАГИ ДЛЯ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ РУНЕТА Шварц Л.В.	72
Информационные и автоматизированные системы и сети	
КВАНТОВОПОДОБНЫЕ ФЕНОМЕНЫ РАСПРОСТРАНЕНИЯ КОЛЛЕКТИВНЫХ ЭМОЦИЙ В СОЦИАЛЬНЫХ СЕТЯХ: МОДЕЛЬ, НАБОР ДАННЫХ И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ Гнидко К.О., Лисов Д.Н.	79
МЕТОД ОЧИСТКИ ОБУЧАЮЩЕЙ ВЫБОРКИ ДЛЯ ЗАДАЧ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ЧЕРЕЗ ОБНАРУЖЕНИЕ АНОМАЛИЙ Арустамян А.Б., Цирлов В.Л., Шишкин И.И.	95
МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ Лубенцов А.В.	103
ПОНЯТИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ: ТЕХНИЧЕСКИЕ И НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ Метельков А.Н.	112
ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРАВА НА ДОСТУП К ИНФОРМАЦИИ В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА Геращенко А.И., Беда А.А.	119
БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ, НОРМАТИВНО-ПРАВОВАЯ ОСНОВА Муравьев А.Г., Шифрин Б.М.	132
ПРОГНОЗНАЯ МОДЕЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ Авраменко В.С., Саенко И.Б., Котенко И.В.	140

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
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
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
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
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
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
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
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 TERENT'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
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. 2

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
Aleksei Burii

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 24th of June, 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

<i>Congratulations on the 50th anniversary of the National Center for Polytechnic Studies under the Ministry of Justice of the Russian Federation Petr O. Tolstoy</i>	<i>4</i>
<i>Congratulations on the 50th anniversary of the National Center for Polytechnic Studies under the Ministry of Justice of the Russian Federation Sergey D. Taran</i>	<i>5</i>
SOME PAGES OF THE HISTORY OF THE SCIENTIFIC CENTER OF LEGAL INFORMATION <i>Andrey V. Morozov</i>	<i>6</i>
Constitutional law	
THE WEAK POINTS OF ARTIFICIAL INTELLIGENCE AND PROBLEMS OF USING IT IN THE LEGAL AID PROGRAMME OF RUSSIA'S MINISTRY OF JUSTICE <i>Iurii Baturin</i>	<i>10</i>
WAYS FOR DIVERSIFYING LEGAL REGULATION OF FINANCIAL RELATIONS <i>Elena Vasianina, Sergei Zapol'skii</i>	<i>16</i>
THE IMPORT SUBSTITUTION POLICY AFTER 10 YEARS: EXPERIENCE, PROBLEMS, AND POSITIVE RESULTS <i>Margarita Kobzar'-Frolova</i>	<i>23</i>
INFORMATION TECHNOLOGY LAW AND DIGITAL REALITY: DEVELOPMENT, PRIORITIES, AND PROBLEMS IN THE CONTEXT OF DIGITAL TRANSFORMATION <i>Tat'iana Poliakova, Natal'ia Troian</i>	<i>31</i>
ON THE LIMITS OF AND GROUNDS FOR APPLYING ADMINISTRATIVE COERCION <i>Sergei Zapol'skii</i>	<i>42</i>
THE TOPICALITY OF THE QUESTION OF CODIFYING LAWS REGULATING RELATIONS IN VIRTUAL SPACE <i>Elena Savchenko</i>	<i>47</i>
TOPICAL QUESTIONS OF SYSTEMATISING LEGAL REGULATIONS, SECURING A SINGLE LEGAL SPACE, LEGAL AID, AND RAISING LEGAL AWARENESS <i>Natal'ia Troian</i>	<i>57</i>
USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE WORK OF THE MINISTRY OF JUSTICE OF THE RUSSIAN FEDERATION <i>Aleksandr Tokolov</i>	<i>66</i>
A NEW VECTOR IN REGULATING INFORMATION RESOURCES: PROBLEMS AND STEPS NEEDED FOR ENSURING THE SECURITY OF RUNET <i>Larisa Schwartz</i>	<i>72</i>
Information and automated systems and networks	
QUANTUM-LIKE PHENOMENA IN THE PROPAGATION OF COLLECTIVE EMOTIONS IN SOCIAL NETWORKS: MODEL, DATASET, AND EXPERIMENTAL RESEARCH RESULTS <i>Konstantin Gnidko, Dmitrii Lisov</i>	<i>79</i>
A METHOD OF CLEARING THE TRAINING DATASET FOR MACHINE LEARNING MODEL TASKS BY ANOMALY DETECTION <i>Aleksandr Arustamian, Valentin Tsirlov, Ivan Shishkin</i>	<i>95</i>
A MODEL FOR EVALUATING THE EFFICIENCY OF OPERATION OF COMPUTING SYSTEMS IN AN EMERGENCY <i>Aleksandr Lubentsov</i>	<i>103</i>
THE CONCEPT OF INFORMATION SYSTEM: TECHNICAL AND LEGAL ASPECTS <i>Aleksandr Metel'kov</i>	<i>112</i>
PROBLEMS OF EXERCISING THE RIGHT TO ACCESS TO INFORMATION IN THE CONTEXT OF DEVELOPMENT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES <i>Alena Gerashchenko, Aleksandr Beda</i>	<i>119</i>
CRITICAL INFORMATION INFRASTRUCTURE SECURITY: PHYSICAL PROTECTION SYSTEMS, LEGAL FOUNDATION <i>Aleksandr Murav'ev, Boris Shifrin</i>	<i>132</i>
A PROGNOSTIC MODEL OF INFORMATION PROTECTION IN INFORMATION COMMUNICATION SYSTEMS BASED ON A RECURRENT NEURAL NETWORK <i>Vladimir Avramenko, Igor' Saenko, Igor' Kotenko</i>	<i>140</i>

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



П.О. Толстой,
Заместитель
Председателя
Государственной
Думы ФС РФ

Уважаемый Сергей Дмитриевич! **Уважаемые друзья и коллеги!**

Рад приветствовать вас на научно-практическом круглом столе «Право и цифровая реальность», приуроченном к 50-летию создания федерального бюджетного учреждения «Научный центр правовой информации при Министерстве юстиции Российской Федерации».

История развития правовой информатизации России непосредственным образом связана с Научным центром правовой информации, который стал первой в стране организацией, решавшей на современном научно-техническом уровне задачи поиска, учета и хранения правовой информации, систематизации законодательства. В настоящее время Научный центр имеет большой опыт в научно-исследовательской и экспертной работе, успешно реализует единую научно-техническую политику в области информатизации Минюста России.

Цифровая реальность стремительно меняет мир и правовое поле. Очевидна необходимость правовой регламентации общественных отношений, формирующихся в связи с применением новых технологий, искусственного интеллекта. Цифровые и информационные технологии позволяют усовершенствовать многие процессы в сфере управления обществом и государством, повысить эффективность юридических процедур. Вместе с тем цифровая реальность генерирует новые риски и угрозы. Цифровая эпоха ставит перед государством задачу создать эффективное правовое поле для контроля рисков в данной сфере и обеспечения безопасности общества.

Вопросы, вынесенные на обсуждение в рамках мероприятия, имеют приоритетное значение как для России, так и для большинства стран. Международное участие открывает возможность для конструктивного обмена мнениями с представителями науки и практики разных стран.

Уверен, что качественный диалог позволит сформулировать практические предложения и рекомендации, в том числе по совершенствованию российского законодательства в информационной сфере, а резолюция по итогам круглого стола станет для парламентариев материалом для дальнейшей законотворческой деятельности.

Желаю всем участникам мероприятия интересных дискуссий, новых идей и плодотворной работы, а Научному центру правовой информации при Министерстве юстиции Российской Федерации дальнейшего развития и процветания.

Успехов всем!



С.Д. Таран,
Директор
ФБУ НЦПИ
при Минюсте
России

Дорогие коллеги!

В эти дни Научный центр правовой информации празднует своё 50-летие. 50 лет деятельности — это серьёзная цифра для любой организации, прошедшей вместе с страной сложный путь исторических перемен, но эта цифра совершенно уникальна для учреждения, работающего в сфере распространения правовых знаний с помощью современных технологий — в момент создания НЦПИ этой сферы деятельности просто не существовало. НЦПИ был первой в стране организацией, решающей на современном научно-техническом уровне проблемы автоматизированной обработки правовой информации — здесь создана первая правовая информационная система АИПС-«Законодательство».

Всё время своего существования НЦПИ занимается информационной поддержкой деятельности Минюста, внедрением передовых технологий в его деятельность, содействуя обеспечению прав организаций и граждан на доступ к информационным ресурсам. Значительна роль НЦПИ в области правового просвещения — здесь издаются известные в стране научные журналы, книги по распространению правовых знаний среди различных категорий граждан. В НЦПИ готовятся патриотические и правовоспитательные издания, поддерживающие государственное направление на повышение роли культурных традиционных ценностей, — книги по истории юстиции, о выдающихся личностях, известных своим стремлением к справедливости, всё увеличивающие свою ценность книги о Великой Отечественной войне.

Поздравляю наш Научный центр правовой информации — всех причастных к его деятельности на протяжении славных 50 лет. Уверен в его не менее славном будущем. НЦПИ был первым и долгое время уникальным учреждением в своей области, и, несомненно, его ценность для государства будет расти с каждым новым десятилетием!

НЕКОТОРЫЕ СТРАНИЦЫ ИСТОРИИ НАУЧНОГО ЦЕНТРА ПРАВОВОЙ ИНФОРМАЦИИ

Морозов А.В.¹

Ключевые слова: Министерство юстиции, Генеральная прокуратура, судейское сообщество.

Аннотация

50 лет исполнилось уникальному учреждению нашей страны — Научному центру правовой информации (далее — НЦПИ). Мудрое государственное решение 1975 года положило начало новой сферы деятельности — правовой информатике. Это, во-первых, активное внедрение средств информационно-вычислительной техники в юридическую деятельность, во-вторых, развитие правовых норм в информационной сфере, что привело к возникновению новой отрасли юриспруденции — информационного права.

Однако, начало 1996 года было омрачено пунктом 10 Указа Президента Российской Федерации от 29 января 1996 г. № 117 «Вопросы Администрации Президента Российской Федерации», в котором предписывалось внести предложения по ликвидации НЦПИ при Минюсте России, что в принципе ставило под угрозу существования всю систему правовой информации Минюста России.

Прошло уже почти 30 лет с начала описываемых событий, которые, я думаю, для истории правовой информатизации России представляют определенную значимость. Многие их участники сильно состарились или даже ушли из жизни. Я попытался описать лишь факты, подтверждаемые пожелтевшими документами, файлы которых хранятся у меня еще на 3,5 дюймовых дискетках. Когда я получил Указ № 117, то первая мысль была лечь на черный кожаный диванчик, стоявший в моем кабинете и объявить голодовку. Но придя в себя, я попытался предпринять некоторые усилия, чтобы сохранить уникальное учреждение в ведении Минюста России. Согласитесь, что не исполнить указ Президента Российской Федерации не у всякого получится.

DOI:10.24412/1994-1404-2025-2-6-9

50 лет исполнилось уникальному учреждению нашей страны — Научному центру правовой информации (далее — НЦПИ). Мудрое государственное решение 1975 года положило начало новой сферы деятельности — правовой информатике. Это, во-первых, активное внедрение средств информационно-вычислительной техники в юридическую деятельность², во-вторых, развитие правовых норм в информационной сфере, что привело к возникновению новой отрасли юриспруденции — информационного права³.

Последнее десятилетие XX века явилось периодом бурного развития баз данных правовой информации, в создании которых существенно преуспели извест-

ные коммерческие структуры, а также в построения государственной системы правовой информации⁴, где значительных результатов добились государственные органы и учреждения, одно из которых НЦПИ⁵.

Однако, начало 1996 года было омрачено пунктом 10 Указа Президента Российской Федерации от 29 января 1996 г. № 117 «Вопросы Администрации Президента Российской Федерации»⁶, в котором предписывалось внести предложения по ликвидации НЦПИ при Минюсте России, что в принципе ставило под угрозу существования всю систему правовой информации Минюста России.

⁴ Морозов А.В. Система правовой информации Минюста России. (Монография). М.: «Издательство Триумф», 1999 — 464 с.; ил. ISBN 5-89392-026-0

⁵ Морозов А.В. Уникальное учреждение. Труды НЦПИ. Страницы истории Научного центра правовой информации. К 35-летию НЦПИ. Выпуск 6 / под ред. Н.С. Козленко. — М.: ФГУ НЦПИ при Минюсте России, 2010. — 56 с.

⁶ Указ Президента Российской Федерации от 29 января 1996 г. № 117 «Вопросы Администрации Президента Российской Федерации» (Собрание законодательства Российской Федерации, 1996, № 6, ст. 532).

² Морозов А.В. Основные задачи программы информатизации судов и органов юстиции на 1996-1997 годы. (Статья). Правовая информатика: Сборник № 1. — М.: Министерство юстиции Российской Федерации, НЦПИ, 1996.

³ Морозов А.В. Информационное право как самостоятельная научная специальность Юридическое образование и наука. № 1 — 2013. — М.: ИГ «ЮРИСТ», 2013, 40 с.

¹ **Морозов Андрей Витальевич**, доктор юридических наук, кандидат технических наук, профессор, академик РАЕН, профессор кафедры компьютерного права и информационной безопасности Высшей школы государственного аудита МГУ имени М.В. Ломоносова, действительный государственный советник юстиции 2 класса.

E-mail: av_morozov@list.ru

В указе говорилось: «В месячный срок представить предложения об образовании Федерального информационного центра как организации, находящейся в ведении Администрации Президента Российской Федерации, рассмотрев возможность реорганизации в этих целях научно-технического центра правовой информации «Система», Научного центра правовой информации Министерства юстиции Российской Федерации, издательства «Юридическая литература Администрации Президента Российской Федерации».

В интервью начальника отдела Государственного правового управления Президента Российской Федерации Б.В. Гузанова «Российской газете» было заявлено, что в структуре Администрации Президента Российской Федерации будет создан Федеральный центр правовой информации, в который скоро «вольется» НЦПИ при Минюсте России. Только огромными усилиями при активной поддержке высших должностных лиц государства, в том числе руководителей судейского сообщества и правоохранительных органов удалось сохранить уникальное учреждение правовой информации в системе Министерства юстиции Российской Федерации.

Надо пояснить, что в середине девяностых годов XX века основным направлением деятельности Министерства юстиции было обеспечение деятельности судов Российской Федерации. По значимости это примерно такая же функция, как сегодня в системе Минюста обеспечение деятельности ФСИН и ФССП России. Поэтому главным аргументом при спасении НЦПИ был аргумент об обеспечении судов Российской Федерации программными комплексами и базами данных правовой информации.

Министр юстиции Российской Федерации В.А. Ковалев в письме «О позиции Минюста России по реорганизации НЦПИ» к Руководителю Администрации Президента Российской Федерации Н.Д. Егорову писал, что «Успешному выполнению поставленных задач в значительной степени способствует информационно-правовое обеспечение деятельности профессиональных юристов. Эту задачу выполняет НЦПИ при Минюсте России.

Однако, *постоянно* (курсив автора) появляются предложения ликвидации НЦПИ в форме реорганизации Отторжение (ликвидация) НЦПИ означает дезорганизацию судебной системы, поскольку Центр является единственным в стране государственным учреждением, обеспечивающим тысячи судов Российской Федерации правовой информацией и базами данных.

Позицию Минюста России по этому вопросу одобряют и поддерживают также Генеральная прокуратура Российской Федерации, Конституционный и Высший Арбитражный Суды Российской Федерации, Совет Судей и Высшая квалификационная коллегия судей Российской Федерации, другие правоохранительные органы, взаимодействующие с судебной системой по реализации программы борьбы с преступностью.

Отторжение НЦПИ также существенно снизит эффективность работы центрального аппарата Минюста

России, финансируемого в условиях резко ограниченного объема, поскольку он на 80 процентов укомплектован компьютерной техникой Центра и полностью за счет хозрасчетных средств НЦПИ осуществляется техническое обслуживание и ремонт оргтехники.»

Обращаю внимание на слово «*постоянно*» в письме Министра юстиции. В меру возможностей попытаюсь объяснить смысл происходящих событий. При создании научно-технического центра правовой информации «Система» ему было выделено ценою в миллиард здание в центре Москвы, судьба которого до сих пор неоднозначна. Видимо тогда в головах некоторых высокопоставленных руководителей созрел план убить сразу двух зайцев. Освободить ценное государственное имущество для других нужд, расположив НТЦ «Система» в здании НЦПИ, и приобрести без особых трудозатрат уникальные технологии обработки правовой информации.

Генеральный прокурор Российской Федерации Ю.И. Скуратов в письме к Руководителю Администрации Президента Российской Федерации Н.Д. Егорову писал: «В органах прокуратуры используется база данных правовой информации «ЭТАЛОН» НЦПИ (авторские права). Она внедрена в Генеральной прокуратуре и в прокуратурах субъектов Российской Федерации.

Информационная база данных «ЭТАЛОН» по своей полноте и актуальности полностью удовлетворяет нашим потребностям в правовой информации.

Кроме того, НЦПИ является по существу информационным центром Минюста России, с которым Генеральная прокуратура и другие правоохранительные ведомства имеют общий территориально распределенный банк статистической информации и судебной практики.

В связи с изложенным, считаю, что в настоящее время решение вопроса о реорганизации НЦПИ преждевременно ...».

В письме Конституционного Суда Российской Федерации было указано, что «НЦПИ является по существу единственным государственным учреждением, обеспечивающим в течение 20 лет правовой информацией и базами данных с использованием вычислительных и телекоммуникационных средств различные ведомства. Поэтому прекращение его деятельности при не налаженной работе Федерального информационного центра может отрицательно сказаться на правовом обеспечении различных ведомств, включая высшие органы судебной власти».

Председатель Высшего Арбитражного Суда В.Ф. Яковлев в письме в Администрацию Президента Российской Федерации указывал: «Без создания необходимых условий для обеспечения такой функции (*компьютеризация судов*) изъятие из ведения Минюста России НЦПИ может привести к негативным последствиям.

Председатель Высшей Квалификационной коллегии судей А.В. Жеребцов в своем обращении к Президенту Российской Федерации указал, что «Реорганизация приведет к потере уникальных технологий сбора и об-

работки правовой информации, судебной статистики, автоматизации делопроизводства судов, безусловно отрицательно скажется на претворении в жизнь судебной реформы.

Информационная база данных «ЭТАЛОН» НЦПИ по своей полноте и актуальности полностью удовлетворяет нашим потребностям в правовой информации.

Совещание Председателей квалификационных коллегий судей России убедительно просит Вас, уважаемый Борис Николаевич, не предпринимать мер по реорганизации НЦПИ, обеспечивающего информационную самостоятельность судебной системы, как независимой ветви государственной власти».

Совет судей Российской Федерации принял Постановление «О позиции Совета судей Российской Федерации по реорганизации НЦПИ», в котором было указано «Совет судей Российской Федерации имеет серьезные основания полагать, что намечаемая реорганизация и присоединение НЦПИ к Федеральному информационному центру может нарушить проявившей себя с положительной стороны порядок обеспечения судов правовой информацией и тем самым повлиять на оперативность и эффективность осуществления правосудия, что в условиях исключительно напряженной работы судебной системы является крайне нежелательным.

Просить Президента Российской Федерации на существующем этапе информационного обеспечения судов Российской Федерации не предпринимать мер по реорганизации НЦПИ, обеспечивающего информационную самостоятельность судебной системы».

Помощник Президента Российской Федерации М.А. Краснов высказал свое мнение Руководителю Администрации Президента Российской Федерации Н.Д. Егорову: «Полностью согласен с позицией Министра юстиции. Новые задачи Минюст не в состоянии выполнять без мощной информационной базы».

Руководитель Администрации Президента Российской Федерации Н.Д. Егоров, учитывая позицию судебного сообщества, а также Генеральной прокуратуры и Минюста подвел итог: «С предложением В.А. Ковалева полностью согласен». Все описываемые события происходили в течение нескольких месяцев после выхода Указа № 117.

Однако, процесс вероятного уничтожения НЦПИ длился целый год. На 24 января 1997 года у Руководителя Администрации Президента Российской Федерации было назначено совещание по вопросу создания Федерального центра правовой информации, на которое в том числе был приглашен Министр юстиции. В качестве материалов к совещанию были приложены проект указа Президента Российской Федерации «Вопросы Федерального центра правовой информации» и почему-то проект положения «О Федеральном информационном центре «Система»», где в пункте 2 указывалось, что «Центр является правопреемником Научного центра правовой информации при Министерстве юстиции Российской Федерации и научно-технического центра правовой информации «Система».

Но произошло чудо — указ президента не был исполнен. Как-то встретив руководителя Государственного правового управления Президента Российской Федерации Р.Г. Орехова (аспирант С.М. Шахрая еще со времен лаборатории правовой информатизации МГУ, сменил его на посту руководителя ГПУ после известных событий начала октября 1993 года), я спросил его о дальнейшей судьбе НЦПИ. «Вы же всех подняли, чтобы оставить НЦПИ в Минюсте» — резко ответил он.

После чудесного спасения НЦПИ расцвел. Можно вспомнить важное событие в деятельности Министерства юстиции в сфере правовой информатизации России. Это проведенный в НЦПИ в июне 1997 года в рамках программы мероприятий ООН в области предупреждения и борьбы с преступностью, уголовного правосудия и информатизации правовой сферы международный семинар, в котором среди двухсот участников были эксперты США и Канады, стран Совета Европы и бывших республик СССР, ведущие фирмы и специалисты в сфере правовой информатизации. Участники семинара отметили достижения в правовой информатизации Минюста России и результаты, достойные признания на международном уровне.

Прошло уже почти 30 лет с начала описываемых событий, которые, я думаю, для истории правовой информатизации России представляют определенную значимость. Многие их участники сильно состарились или даже ушли из жизни. Я попытался описать лишь факты, подтверждаемые пожелтевшими документами, файлы которых хранятся у меня еще на 3,5 дюймовых дискетках. Когда я получил Указ № 117, то первая мысль была лечь на черный кожаный диванчик, стоявший в моем кабинете и объявить голодовку. Но придя в себя, я попытался предпринять некоторые усилия, чтобы сохранить уникальное учреждение в ведении Минюста России. Согласитесь, что не исполнить указ Президента Российской Федерации не у всякого получится. Иногда по разным причинам. видя проблемы и трудности, с которыми НЦПИ как «золушка» сталкивается на протяжении последних 30 лет, я думаю, что может быть я зря это сделал. Ведь живет же и великолепно развивается в составе администрации президента аналогичный белорусский центр. И государственная система правовой информации Республики Беларусь лучшая в мире!

А диванчик, кстати, и сейчас стоит на четвертом этаже НЦПИ в главном корпусе в одном из кабинетов. В этом же кабинете висят и часы с надписью «25 лет НЦПИ». Такие же точно часы тикают и у меня дома. Удивительно, что часы, купленные как китайский ширпотреб для подарка гостям в честь празднования 25-летнего юбилея НЦПИ, проработали уже более четверти века.

Пять лет назад в статье⁷, посвященной 45-летию НЦПИ я написал: «Я как директор был участником и организатором 20 и 25-летних юбилеев этой замечатель-

⁷ Морозов А.В. История правовой информатизации Минюста России. Правовая информатика. № 2 — М. ФГУ НЦПИ при Минюсте России, 2020, С. 92 — 99.

ной организации. В моем кабинете висят и точно ходят часы с логотипом НЦПИ (это карта Советского Союза — информация не имеет границ) и надписью 25 лет. Мне бы очень хотелось отметить с коллегами 50-летний юбилей, а моим детям его столетие».

Первая часть желания исполнилась, осталось дожидаться столетнего юбилея.

Желаю Научному центру правовой информации при Министерстве юстиции Российской Федерации производственного долголетия, а его коллективу стабильности и спокойствия в работе, руководству долгой несменяемости и дальнейших успехов в реализации задач правовой информатизации России.

Литература

1. Морозов А.В. Основные задачи программы информатизации судов и органов юстиции на 1996-1997 годы. Правовая информатика: Сборник № 1.- М.: Министерство юстиции Российской Федерации, НЦПИ, 1996.
2. Морозов А.В. Информационное право, как самостоятельная научная специальность // Юридическое образование и наука. № 1 — 2013. — 40 с.
3. Морозов А.В. Уникальное учреждение. Труды НЦПИ. Страницы истории Научного центра правовой информации. К 35-летию НЦПИ. Выпуск 6 / под ред. Н.С. Козленко. — М.: ФГУ НЦПИ при Минюсте России, 2010. — 56 с.
4. Морозов А.В. Система правовой информации Минюста России. (Монография). М.: «Издательство Триумф», 1999 — 464 с.; ил. ISBN 5-89392-026-0.
5. Морозов А.В. История правовой информатизации Минюста России // Правовая информатика. № 2 –2020. С. 92 — 99.

SAVING THE SCIENTIFIC CENTER OF LEGAL INFORMATION

Morozov A. V.⁸

Keywords: *Ministry of Justice, Prosecutor General's Office, judicial community.*

Abstract

The unique institution of our country, the Scientific Center for Legal Information (hereinafter referred to as NCLI), has turned 50 years old. A wise government decision in 1975 marked the beginning of a new field of activity — legal informatics. This is, firstly, the active introduction of information technology into legal activities, and secondly, the development of legal norms in the information sphere, which led to the emergence of a new branch of jurisprudence — information law.

However, the beginning of 1996 was overshadowed by paragraph 10 of the Decree of the President of the Russian Federation of January 29, 1996 No. 117 "Questions of the Administration of the President of the Russian Federation", which ordered the submission of proposals for the liquidation of the NCPI under the Ministry of Justice of Russia, which in principle threatened the existence of the entire system of legal information of the Ministry of Justice of Russia.

Almost 30 years have passed since the events described began, which, I think, are of certain significance for the history of legal informatization of Russia. Many of their participants have aged greatly or even passed away. I have tried to describe only the facts confirmed by yellow documents, the files of which are still stored on 3.5-inch floppy disks. When I received Decree No. 117, my first thought was to lie down on the black leather sofa in my office and declare a hunger strike. But having come to my senses, I tried to make some efforts to preserve the unique institution under the jurisdiction of the Ministry of Justice of Russia. You can agree that not everyone will be able to disobey the decree of the President of the Russian Federation.

References

6. Morozov A.V. Osnovnie zadachi programmi informatizacii sudov i organov usticii na 1996-1997 godi. Pravovayi informatica: Sbornic № 1.- М.: Minust Rossii, NCPI, 1996.
7. Morozov A.V. Informacionnoe pravo kak samostoyitelnaya nauchnaya specialnost // Uridicheskoe obrazovanie i nauka. № 1 — 2013. 40 p.
8. Morozov A.V. Unikalnoe uchregdenie. Trudi NCPI. Stranici istorii NCPI. K 35-letiu NCPI. Vipusk 6 / pod red. N.S. Kozlenko. — М. FGU NCPI pri Minusta Rossii, 2010. — 56 с.
9. Morozov A.V. Sistema pravovoi informacii Minusta Rossii. (Monografiyi). М.: «Izdatelstvo Triumf», 1999 — 464 p.; il. ISBN 5-89392-026-0.
10. Morozov A.V. Istoriy pravovoi informatizacii Minusta Rossii // Pravovay informatica. No. 2 –2020, pp. 92 — 99.

⁸ Andrey V. Morozov, Doctor of Law, Ph.D. (of tech.), Professor, Academician of the Russian Academy of Natural Sciences, Professor of the Department of Computer Law and Information Security of the Higher School of State Audit of Lomonosov Moscow State University, Active State Counselor of Justice of the 2nd class. Email: av_morozov@list.ru

СЛАБЫЕ МЕСТА ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ПРОБЛЕМЫ ЕГО ИСПОЛЬЗОВАНИЯ В ПРОГРАММЕ «ПРАВОВАЯ ПОМОЩЬ» МИНИСТЕРСТВА ЮСТИЦИИ РОССИИ

Батурин Ю.М.¹

Ключевые слова: искусственный интеллект, большая языковая модель, правовая помощь, Министерство юстиции.

Аннотация

Цель работы: выявить слабые места искусственного интеллекта, применяемого в информационной системе «Правовая помощь», которой предстоит стать основной общероссийской цифровой платформой для оказания бесплатной юридической помощи и порталом правового просвещения граждан.

Методы исследования: экспериментальное тестирование различных версий больших языковых моделей на юридическом контенте.

Результаты исследования: показаны слабые места больших языковых моделей в работе с юридическим контентом, предназначенных для системы «Правовая помощь» Министерства юстиции Российской Федерации.

Научная новизна: проведена классификация изъянов и даны рекомендации по их устранению.

DOI: 10.24412/1994-1404-2025-2-10-15

Государственная программа Российской Федерации «Юстиция», утвержденная постановлением Правительства Российской Федерации от 15.04.2014 № 312 (в ред. от 14.11.2024 № 1549), предусматривает «создание широкого спектра цифровых правовых сервисов и ресурсов, развитие и цифровизация государственных услуг и функций, ориентация на развитие и широкое применение информационных технологий и внедрение искусственного интеллекта»². Комитет Совета Федерации Федерального Собрания Российской Федерации по конституционному законодательству и государственному строительству совместно с Советом по развитию цифровой экономики при Совете Федерации провели круглый стол «Информатизация профессиональной юридической деятельности: LegalTech и искусственный интеллект». Выступая на нем, первый заместитель председателя Комитета Совета Федерации по конституционному законодательству и государственному строительству И.В. Рукавишников заявил: «Важной сферой цифровизации с использованием технологий искусственного интеллекта является оказа-

ние юридической помощи гражданам с применением электронных сервисов. Речь идет о создаваемой Минюстом России информационной системе «Правовая помощь», которая станет основной общероссийской цифровой платформой для оказания бесплатной юридической помощи и порталом правового просвещения граждан, обеспечивая их актуальной юридической информацией в разных жизненных ситуациях»³. Эксплуатация информационной системы «Правовая помощь» начата Минюстом РФ в экспериментальном режиме 20 декабря 2022 г.⁴ на основании распоряжения Правительства Российской Федерации от 26 ноября 2021 г. № 3340-р при участии МВД России и Минцифры России, а также органов исполнительной власти ряда субъектов Российской Федерации⁵. Для удобства граждан все жизненные ситуации сгруппированы

³ И. Рукавишников: Технология искусственного интеллекта будет задействована для оказания юридической помощи гражданам. URL: <http://council.gov.ru/events/news/140599/> (дата обращения: 03.06.2025).

⁴ Информационная система «Правовая помощь». URL: <https://minjust.gov.ru/ru/events/49231/> (дата обращения: 03.06.2025).

⁵ Распоряжение Правительства РФ от 26 ноября 2021 г. № 3340-р «О повышении эффективности и качества предоставления гражданам бесплатной юридической помощи с применением электронных сервисов, а также доступности для граждан правовой информации» // СПС «Гарант» (дата обращения: 03.06.2025).

² Постановление Правительства Российской Федерации от 15.04.2014 г. № 312 «Об утверждении государственной программы Российской Федерации «Юстиция» (в ред. от 14.11.2022 № 1548) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 03.06.2025).

¹ **Батурин Юрий Михайлович**, доктор юридических наук, заведующий кафедрой компьютерного права и информационной безопасности Высшей школы государственного аудита (факультет) Московского государственного университета имени М.В. Ломоносова, г. Москва, Российская Федерация.

E-mail: yubat@mail.ru

по категориям и подкатегориям так, чтобы гражданин получил необходимую рекомендацию для разрешения своей жизненной ситуации. Особенностью платформы является то, что информация подается в простом и доступном для понимания изложении. Пилотный проект длился до 30 сентября 2023 г. На состоявшемся в конце октября 2023 г. совещании с членами Правительства РФ Президент России поручил Минюсту России совместно с Минцифры России обеспечить создание федеральной государственной информационной системы «Правовая помощь», предусмотрев ее взаимодействие с Единым порталом государственных и муниципальных услуг (функций) и подключение к ней участников государственной системы бесплатной юридической помощи во всех субъектах РФ к 1 октября 2025 г.⁶ 7 апреля 2025 г. Министерство юстиции РФ опубликовало доклад о реализации государственной политики в области обеспечения граждан бесплатной юридической помощью в 2024 году. В нем, в частности, отмечается, что количество посетителей важной части системы, информационного портала ВПРАВЕ.РФ, за 2024 год увеличилось более чем в пять раз. Количество жизненных ситуаций, размещенных на портале, было увеличено до 255. Они затрагивают наиболее важные для граждан вопросы, касающиеся, например, пенсионного обеспечения, оформления наследства, регистрации брака, утраты близкого человека, использования средств материнского капитала, жилищно-коммунального хозяйства, защиты прав потребителей, а также получения различных выплат, в том числе связанных с участием в специальной военной операции⁷. Планируется в 2025 г. довести количество жизненных ситуаций до тысячи⁸.

Искусственный интеллект (ИИ) уже давно используется в социальных сетях для рекомендации соответствующих постов, статей, видео и рекламы. Но юриспруденция — значительно более сложная и ответственная область. Говоря об информационной системе «Правовая помощь», вице-президент Федеральной палаты адвокатов О.В. Баулин сдержанно заметил: «Думаю, говорить об осторожном или неосторожном оптимизме либо пессимизме пока рано. Во всяком случае, создание и сопровождение правового сервиса вовсе не является ни легкой, ни примитивной задачей»⁹. И он прав: имеющийся мировой опыт использования больших

языковых моделей (БЯМ, англ. Large Language Models, LLM), в том числе и в юридической практике, показывает наличие слабых мест БЯМ, некоторые из которых удается купировать, а другие, напротив, при смене поколений БЯМ усугубляют свои изъяны. Рассмотрим некоторые из них.

Функция юридического консультирования граждан с помощью системы ИИ, несомненно, чрезвычайно востребована. Граждане сталкиваются с юридическими проблемами в самых разных областях: трудовая занятость, финансы, социальное обеспечение и льготы, проблемы потребителей. Но не каждый может позволить себе оплатить качественную юридическую консультацию. Многие обращаются к Интернету в поисках юридической помощи. Система «Правовая помощь» Минюста РФ и его региональных органов, использующие генеративный ИИ, окажутся значительно удобнее Интернета. Как показывает практика различных юридических компаний, БЯМ могут быстро объяснить сложную юридическую информацию на простом разговорном языке, что и требуется обычным гражданам, не специалистам. Но насколько они точны? Оказывается, ответы систем ИИ не всегда надежны. Типичные ошибки таковы.

Системы ИИ, основанные на БЯМ, первоначально обученные на зарубежном законодательстве, чаще всего американском, дают ответ, подверженный сильному влиянию права соответствующей страны, даже при дообучении БЯМ на отечественном законодательстве. При ответах, как правило, не указывается юридический источник, а также не учитываются различия нормативных правовых актов субъектов РФ. Последнюю особенность обязательно необходимо учитывать при построении централизованной системы юридического консультирования Российской Федерации.

Для нейросетей не существует различия между прошлым, настоящим и будущим. БЯМ обучаются на больших объемах данных, которые могут не включать в себя самые последние правовые события, и ответ может основываться на устаревшей норме.

Некоторые ответы оказываются слишком общими: предоставляется лишняя необходимых деталей информация по теме, а не конкретное решение сформулированной юридической проблемы. Интересно, что чат-боты значительно более предметно предлагали неюридические решения проблем, которые хотя и оказываются полезными в качестве первого шага, явно недостаточны для выбора индивидуального правового пути, ведущего к успеху.

Многие БЯМ дают неверные или вводящие в заблуждение советы при консультировании по вопросам семейного и трудового права. Ответы на жилищные и потребительские вопросы оказываются точнее, но пробелы в ответах сохраняются. Иногда они упускают действительно важные аспекты закона или объясняют его неправильно. Ответы БЯМ обычно хорошо написаны, что делает их более убедительными. Но пользователям, не обладающим юридическими знаниями,

⁶ Перечень поручений по итогам совещания с членами Правительства (утв. Президентом РФ 5 декабря 2024 г.) № Пр-2567 // СПС «Гарант» (дата обращения: 03.06.2025).

⁷ Опубликован доклад о реализации государственной политики в области обеспечения граждан бесплатной юридической помощью в 2024 году. URL: <https://minjust.gov.ru/ru/events/50632/> (дата обращения: 03.06.2025).

⁸ Минюст России внедрит искусственный интеллект в правовую помощь. URL: <https://www.ferra.ru/news/v-rossii/minyust-rossii-vnedrit-iskusstvennyi-intellekt-v-pravovuyu-pomoshh-31-10-2024.htm> (дата обращения: 03.06.2025).

⁹ Государственная информационная система «Правовая помощь» начала работу. URL: <https://www.advgazeta.ru/novosti/gosudarstvennaya-informatsionnaya-sistema-pravovaya-pomoshch-nachala-rabotu/> (дата обращения: 03.06.2025).

сложно определить, является ли полученный ответ правильным и как его применить к их личным обстоятельствам.

БЯМ склонны отвечать с уверенностью, даже если ответ фактически неверен, потому что их научили верить в эту информацию. БЯМ новых поколений чаще дают ошибочные ответы на простые вопросы, в то время как их модели предшествующих поколений старались избегать ответов на сложные для них задания. Например, GPT-4 может показаться более точным в ответах, однако на самом деле он просто значительно увереннее предоставляет правдоподобные, но неверные ответы. Казалось бы, зачем выдавать неправильный ответ вместо того, чтобы просто ответить «Боюсь, я не могу этого сделать»? Такое поведение стимулировано разработчиками, создающими модели, которые «никогда не уклоняются от ответа».

Методы, позволяющие сделать БЯМ более мощными и адаптивными, основаны на постоянном масштабировании (то есть увеличении объема данных и вычислительных ресурсов) и на индивидуальной настройке. Начиная с ранних БЯМ, модели масштабировались (обучались с большим числом параметров, на больших наборах данных и с более длительным временем обучения), а также корректировались обратной связью от оператора или специалиста в данной профильной области с использованием таких методов, как настройка инструкций, обучение с подкреплением или методы постфильтрации. Так, улучшалась устойчивость к различным естественным формулировкам одного и того же вопроса, однако масштабированные БЯМ в некоторых отношениях становятся и менее надежными. Например, масштабированные модели чаще дают на первый взгляд разумный, но неправильный ответ, включая ошибки в сложных вопросах, которые часто упускают из виду даже юристы, специализирующиеся по другому профилю.

Технологии развиваются, и когда-нибудь наступит время, когда БЯМ будут предоставлять вполне удовлетворительные юридические консультации. Но пока их разработчики должны ясно представлять риски, связанные с их использованием для решения юридических проблем граждан, обращающихся к ИИ за консультацией¹⁰.

Полученные результаты подчеркивают необходимость фундаментальных изменений в проектировании и разработке БЯМ, особенно в сфере права, где ошибки имеют первостепенное значение. Когда БЯМ не знают ответа, они галлюцинируют, как это произошло у одного адвоката из Нью-Йорка (США), готовившего с помощью БЯМ речь защитника в суде. ИИ придумал судебные прецеденты, которые судья, конечно, легко рас-

познал как «галлюцинации»¹¹. Такое происходит, когда БЯМ поручено генерировать текст по теме, с которой они нечасто сталкивались, или когда они ошибочно смешивают информацию из разных источников. По-видимому, эта проблема неразрешима в рамках нейросетей. Попытка убирать галлюцинации после ответа БЯМ и по каждому случаю — явно не выход. То же самое можно сказать и о БЯМ, усиливающих стереотипы или дающих западно-ориентированные ответы. Кстати, повисает в воздухе и вопрос об ответственности за некорректные или ошибочные ответы, поскольку сложно установить, как БЯМ вообще пришла к такому выводу, а компании, производящие БЯМ, отказываются брать на себя ответственность за ошибки. Склонность БЯМ к воспроизводству предвзятости, галлюцинациям и прямой дезинформации вряд ли может быть устранена постепенными улучшениями моделей. Несомненно, БЯМ — большое инженерное достижение. Их результаты при реферировании текстов и в переводе впечатляют. Они значительно повышают производительность труда (в нашем случае) высокопрофессиональных юристов, осведомленных о «галлюцинациях» и замечающих их ошибки. Тем не менее у них есть большой потенциал для введения в заблуждение, потому что их выводы всегда основаны на вероятностях, а не на понимании.

Конечно, БЯМ обладают большим потенциалом использования в праве, но, как показано, существуют неизбежно сопутствующие риски, не говоря уже о нерегулируемом их использовании в системе юстиции. Реальность такова: если ИИ будет продолжать развиваться, нам понадобятся такие системы ИИ, которые адаптируются к новым задачам всего на нескольких примерах, проверяют свое восприятие задания, могут выполнять разные задачи и надежно оперировать сложными рассуждениями. БЯМ, при всех их впечатляющих достижениях, не таковы: они работают, используя технику, называемую глубоким обучением, в процессе которого они поглощают огромные объемы текстовых данных, используют статистику и корреляции, которые и определяют, каким должно быть следующее слово или фраза в любом заданном ответе. Каждая БЯМ вместе со всеми изученными ею текстами и закономерностями хранится в мощных компьютерах в крупных центрах обработки данных, известных как нейронные сети. БЯМ могут рассуждать, используя процесс, называемый цепочкой высказываний. Они генерируют сложные (многошаговые последовательные) ответы, имитируя логику людей, основываясь на закономерностях, наблюдаемых в обучающих данных. Коротко говоря, разработчики БЯМ успешно заменили проблему семантики (сочетания слов для создания смысла) статистикой, соединяя слова на основе частоты их пре-

¹⁰ Ryan F., Hardie E. We asked ChatGPT for legal advice – here are five reasons why you shouldn't. URL: <https://theconversation.com/we-asked-chatgpt-for-legal-advice-here-are-five-reasons-why-you-shouldnt-229147> (дата обращения: 03.06.2025).

¹¹ Patterson J. Fighting fake 'facts' with two little words: A new technique to ground a large language model's answers in reality. URL: <https://techxplore.com/news/2023-08-fake-facts-words-technique-ground.html> (дата обращения: 03.06.2025).

дыдущего использования. Это называется «компетентность без понимания»¹².

Постоянно масштабируемым БЯМ требуется так много обучающих данных, что теперь их обучение приходится проводить на синтетических данных, то есть данных, созданных БЯМ предшествующих поколений, а они могут копировать и усиливать ошибки из собственных исходных данных, так что новые модели наследуют слабости старых. В результате стремительно растет стоимость программирования ИИ для повышения точности после их обучения — процедура, известная как «post-hoc выравнивание модели». Программистам же становится всё труднее обнаруживать причины ошибок, потому что количество шагов в процессе рассуждений модели становится всё больше. Фактически, происходит масштабирование «компетентности без понимания». Юриспруденция — это образ мышления, включающий знание и понимание норм, сбор доказательств, анализ составов, сопоставление условий, выявление причинно-следственных связей и т. п., а для БЯМ критерием является статистический факт, что по большей части определенные слова в некотором наборе следуют друг за другом. Но БЯМ не могут узнать о причинах и следствиях только из данных, на которых они проходили обучение; они могут находить только корреляции. Современные БЯМ не могут отличать причины от следствий, за исключением специализированных игровых приложений. Использование БЯМ неявно основывается на утверждении, что статистические трюки эквивалентны обоснованным знаниям. Но нельзя путать согласованность с пониманием. Человеческие ценности, такие как правда и справедливость, принципиально важные для права, не встроены в БЯМ на фундаментальном уровне — программисты пока не знают, как это сделать¹³.

Популярный обходной путь называется «человек в контуре»: это означает, что на «выходе» всегда находится специалист, использующий БЯМ, т. е. окончательные решения доверяют только человеку. Но и он может быть введен в заблуждение «галлюцинациями» БЯМ.

Если мы вспомним предыдущий этап развития ИИ (1980-е годы), то увидим принципиально иной подход: в компьютеры закладывались формальные правила

(тоже вид обучения), которые они затем могли применять к новой информации. Такой вид ИИ получил название символического (в смысле оперирования символами). Глубокое обучение обозначило наступление следующего этапа в 2010-х годах.

Возникает вопрос: а нельзя ли использовать достоинства символического ИИ для компенсации недостатков БЯМ? Возникающая область нейросимволического ИИ (англ. neuro-symbolic AI) может решить рассмотренные выше проблемы, а также сократить огромные объемы данных, необходимых для обучения БЯМ. Он более энергоэффективен, поскольку не придется хранить огромные массивы данных. Это также более справедливо, что особенно важно для юридических информационных систем, поскольку ИИ можно заставить следовать уже существующим правилам, принятым в законодательстве, таким как недопустимость дискриминации человека по полу, возрасту, расе и т. д.

Так что же такое нейросимволический ИИ и как он работает?

Нейросимволический ИИ сочетает прогнозирующее обучение (англ. predictive learning) нейронных сетей — метод машинного обучения, при котором модель получает новые данные для распознавания среды, своих возможностей и ограничений — с обучением ИИ ряду формальных логических правил (например, «если а, то b»), математических правил («если $a = b$ и $b = c$, то $a = c$ ») и согласованным значениям слов, символов, диаграмм. Некоторые из них вводятся непосредственно в ИИ, в то время как другие он будет выводить сам на основе обучающих данных («извлечение знаний»). Такой ИИ не будет галлюцинировать и будет обучаться быстрее, структурируя знания. Нейросимволический ИИ синтезирует обучение и формальные рассуждения, используя процесс, известный как «нейросимволический цикл»: частично обученный ИИ извлекает правила из обучающих данных, а затем внедряет сводные знания обратно в сеть для дальнейшего обучения на новых данных¹⁴.

По программе правовая помощь предоставляется бесплатно, однако нельзя исключать, что ИИ, вероятно, породит множество судебных разбирательств, связанных с неверными советами, последовав которым, граждане понесут определенный ущерб. Поэтому надо торопиться с системным нормативным правовым регулированием использования ИИ.

¹² Saunders N. Evolution is making us treat AI like a human, and we need to kick the habit. URL: <https://theconversation.com/evolution-is-making-us-treat-ai-like-a-human-and-we-need-to-kick-the-habit-205010> (дата обращения: 03.06.2025).

¹³ Scharth M. AI might be seemingly everywhere, but there are still plenty of things it can't do — for now. URL: <https://theconversation.com/ai-might-be-seemingly-everywhere-but-there-are-still-plenty-of-things-it-cant-do-for-now-197050> (дата обращения: 03.06.2025).

¹⁴ Garcez A. Neurosymbolic AI is the answer to large language models' inability to stop hallucinating // The Conversation, May 30, 2025. URL: <https://theconversation.com/neurosymbolic-ai-is-the-answer-to-large-language-models-inability-to-stop-hallucinating-257752> (дата обращения: 03.06.2025).

Литература

1. Постановление Правительства Российской Федерации от 15.04.2014 г. № 312 «Об утверждении государственной программы Российской Федерации «Юстиция» (в ред. от 14.11.2022 № 1548). URL: <http://www.pravo.gov.ru> (дата обращения: 03.06.2025).

2. Распоряжение Правительства РФ от 26 ноября 2021 г. № 3340-р «О повышении эффективности и качества предоставления гражданам бесплатной юридической помощи с применением электронных сервисов, а также доступности для граждан правовой информации» // СПС «Гарант» (дата обращения: 03.06.2025).
3. Перечень поручений по итогам совещания с членами Правительства (утв. Президентом РФ 5 декабря 2024 г.) № Пр-2567 // СПС «Гарант» (дата обращения: 03.06.2025).
4. Государственная информационная система «Правовая помощь» начала работу. URL: <https://www.advgazeta.ru/novosti/gosudarstvennaya-informatsionnaya-sistema-pravovaya-pomoshch-nachala-rabotu/> (дата обращения: 03.06.2025).
5. Информационная система «Правовая помощь». URL: <https://minjust.gov.ru/ru/events/49231/> (дата обращения: 03.06.2025).
6. И. Рукавишников: Технология искусственного интеллекта будет задействована для оказания юридической помощи гражданам. URL: <http://council.gov.ru/events/news/140599/> (дата обращения: 03.06.2025).
7. Минюст России внедрит искусственный интеллект в правовую помощь. URL: <https://www.ferra.ru/news/v-rossii/minyust-rossii-vnedrit-iskusstvennyi-intellekt-v-pravovuyu-pomoshch-31-10-2024.htm> (дата обращения: 03.06.2025).
8. Опубликован доклад о реализации государственной политики в области обеспечения граждан бесплатной юридической помощью в 2024 году. URL: <https://minjust.gov.ru/ru/events/50632/> (дата обращения: 03.06.2025).
9. Garcez A. Neurosymbolic AI is the answer to large language models' inability to stop hallucinating. The Conversation, May 30, 2025. URL: <https://theconversation.com/neurosymbolic-ai-is-the-answer-to-large-language-models-inability-to-stop-hallucinating-257752> (data obrashcheniia: 03.06.2025).
10. Patterson J. Fighting fake 'facts' with two little words: A new technique to ground a large language model's answers in reality. URL: <https://techxplore.com/news/2023-08-fake-facts-words-technique-ground.html> (data obrashcheniia: 03.06.2025).
11. Ryan F., Hardie E. We asked ChatGPT for legal advice – here are five reasons why you shouldn't. URL: <https://theconversation.com/we-asked-chatgpt-for-legal-advice-here-are-five-reasons-why-you-shouldnt-229147> (data obrashcheniia: 03.06.2025).
12. Saunders N. Evolution is making us treat AI like a human, and we need to kick the habit. URL: <https://theconversation.com/evolution-is-making-us-treat-ai-like-a-human-and-we-need-to-kick-the-habit-205010> (data obrashcheniia: 03.06.2025).
13. Scharth M. AI might be seemingly everywhere, but there are still plenty of things it can't do – for now. URL: <https://theconversation.com/ai-might-be-seemingly-everywhere-but-there-are-still-plenty-of-things-it-cant-do-for-now-197050> (data obrashcheniia: 03.06.2025).

SECTION:
CONSTITUTIONAL LAW

THE WEAK POINTS OF ARTIFICIAL INTELLIGENCE AND PROBLEMS OF USING IT IN THE LEGAL AID PROGRAMME OF RUSSIA'S MINISTRY OF JUSTICE

Iurii Baturin, Dr. Sc. (Law), Head of the Department of Computer Law and Information Security of the Higher School of Government Audit (faculty) of the Lomonosov Moscow State University, Moscow, Russian Federation.

E-mail: yubat@mail.ru

Keywords: artificial intelligence, large language model, legal aid, Ministry of Justice.

Abstract

Purpose of the study: identifying the weak points of artificial intelligence used in the Legal Aid Information System which is expected to become the main digital platform in Russia for rendering free legal aid as well as the portal for raising legal awareness of citizens.

Methods used in the study: experimentally testing different versions of large language models using legal content.

Study findings: weak points of large language models destined for the Legal Aid System of the Ministry of Justice of Russia as regards legal content are highlighted.

Research novelty: a classification of shortcomings is carried out and recommendations for eliminating them are given.

References

1. Postanovlenie Pravitel'stva Rossiiskoi Federatsii ot 15.04.2014 g. No. 312 "Ob utverzhdenii gosudarstvennoi programmy Rossiiskoi Federatsii "Iustitsiia" (v red. ot 14.11.2022 No. 1548). URL: <http://www.pravo.gov.ru> (data obrashcheniia: 03.06.2025).
2. Rasporiazhenie Pravitel'stva RF ot 26 noiabria 2021 g. No. 3340-r "O povyshenii effektivnosti i kachestva predostavleniia grazhdanam besplatnoi iuridicheskoi pomoshchi s primeneniem elektronnykh servisov, a takzhe dostupnosti dlia grazhdan pravovoi informatsii". SPS "Garant" (data obrashcheniia: 03.06.2025).
3. Perechen' poruchenii po itogam soveshchaniia s chlenami Pravitel'stva (utv. Prezidentom RF 5 dekabria 2024 g.) No. Pr-2567. SPS "Garant" (data obrashcheniia: 03.06.2025).
4. Gosudarstvennaia informatsionnaia sistema "Pravovaia pomoshch'" nachala rabotu. URL: <https://www.advgazeta.ru/novosti/gosudarstvennaya-informatsionnaya-sistema-pravovaya-pomoshch-nachala-rabotu/> (data obrashcheniia: 03.06.2025).
5. Informatsionnaia sistema "Pravovaia pomoshch'". URL: <https://minjust.gov.ru/ru/events/49231/> (data obrashcheniia: 03.06.2025).
6. I. Rukavishnikova: Tekhnologiiia iskusstvennogo intellekta budet zadeistvovana dlia okazaniia iuridicheskoi pomoshchi grazhdanam. URL: <http://council.gov.ru/events/news/140599/> (data obrashcheniia: 03.06.2025).
7. Miniust Rossii vnedrit iskusstvennyi intellekt v pravovuiu pomoshch'. URL: <https://www.ferra.ru/news/v-rossii/minyust-rossii-vnedrit-iskusstvennyi-intellekt-v-pravovuyu-pomosh-31-10-2024.htm> (data obrashcheniia: 03.06.2025).
8. Opublikovan doklad o realizatsii gosudarstvennoi politiki v oblasti obespecheniia grazhdan besplatnoi iuridicheskoi pomoshch'iu v 2024 godu. URL: <https://minjust.gov.ru/ru/events/50632/> (data obrashcheniia: 03.06.2025).
9. Garcez A. Neurosymbolic AI is the answer to large language models' inability to stop hallucinating. The Conversation, May 30, 2025. URL: <https://theconversation.com/neurosymbolic-ai-is-the-answer-to-large-language-models-inability-to-stop-hallucinating-257752> (data obrashcheniia: 03.06.2025).
10. Patterson J. Fighting fake 'facts' with two little words: A new technique to ground a large language model's answers in reality. URL: <https://techxplore.com/news/2023-08-fake-facts-words-technique-ground.html> (data obrashcheniia: 03.06.2025).
11. Ryan F., Hardie E. We asked ChatGPT for legal advice – here are five reasons why you shouldn't. URL: <https://theconversation.com/we-asked-chatgpt-for-legal-advice-here-are-five-reasons-why-you-shouldnt-229147> (data obrashcheniia: 03.06.2025).
12. Saunders N. Evolution is making us treat AI like a human, and we need to kick the habit. URL: <https://theconversation.com/evolution-is-making-us-treat-ai-like-a-human-and-we-need-to-kick-the-habit-205010> (data obrashcheniia: 03.06.2025).
13. Scharth M. AI might be seemingly everywhere, but there are still plenty of things it can't do – for now. URL: <https://theconversation.com/ai-might-be-seemingly-everywhere-but-there-are-still-plenty-of-things-it-cant-do-for-now-197050> (data obrashcheniia: 03.06.2025).

ПУТИ ДИВЕРСИФИКАЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ФИНАНСОВЫХ ОТНОШЕНИЙ

Васянина Е.Л.¹, Запольский С.В.²

Ключевые слова: альтернативные правовые конструкции, параллельное право, финансовые обязательства, ответственность, налоговый контроль, налоги, расходы, правовой эксперимент.

Аннотация

Цель статьи: исследование направлений диверсификации правового регулирования финансовых отношений в рамках развития концепции современного финансового права.

Применение общелогических методов исследования, в том числе анализа и синтеза, формально-юридического метода, позволили авторам прийти к выводам о том, что под альтернативными правовыми конструкциями следует понимать действие в рамках единого правового поля специального правового инструментария, использование которого продиктовано нестандартными или не предусмотренными заранее ситуациями в ходе правового регулирования финансовых отношений. Диверсификация правового регулирования не должна вызывать варианты в действиях правоприменителя, т. е. приводить к выбору между законным и полузаконным регулированием финансовых отношений. Альтернативный подход следует рассматривать как правовосстановительный и субсидиарный к основному правовому режиму.

Сформулированные по результатам проведенного анализа выводы и направления развития финансового законодательства не претендуют на точность и безупречность. Однако факты и аналитические материалы могут быть полезны для проведения дальнейших научных исследований в фокусе финансово-правовой науки.

DOI: 10.24412/1994-1404-2025-2-16-22

Введение

Новые правовые институты, паллиативные правовые конструкции, позиции судов, а также квазиправовое регулирование социально-экономических отношений являются предметом многих современных научных исследований [7].

Изучению правовых институтов, аккумулирующих методы государственного администрирования экономики и горизонтального управления, являющихся субсидиарными к основному правовому режиму в условиях социально-экономических кризисов, посвящена, в частности, диссертация И.И. Шувалова «Правовое регулирование предпринимательской деятельности в период социально-экономического кризиса (теория и практика)» [18]. Особое внимание уделено исследованию отдельных финансово-правовых режимов [3], включая правовой эксперимент [14].

Далеко не случайно в современных экономических реалиях ученые-правоведы проявляют интерес к вопросам формирования новых правовых конструкций и паллиативных правовых институтов. Эти отклоняющиеся от официального права образования позволяют увидеть недостатки существующей модели правового регулирования социально-экономических отношений, определить ключевые направления развития права, отвечающие современным экономическим вызовам.

Появление ранее не применявшихся правовых конструкций регулирования финансовых отношений вызвано, с одной стороны, формированием многополярной системы внешнеэкономических отношений и необходимостью противодействия геополитическим рискам, а с другой стороны — потребностью диверсификации механизма финансово-правового регулирования.

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: elnavasianina@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 Российской Федерации, г. Москва, Российская Федерация.

E-mail: zpmoscow@mail.ru

Причины появления новых правовых институтов

Причины возникновения ранее неизвестных правовых инструментов регулирования финансовых отношений кроются прежде всего в дуалистическом характере права, проявляющемся «...в сосуществовании двух правовых систем, основанных на одновременном действии двух основных источников права — правовом обычае и законодательном акте» [13], а нередко в стремлении законодателя и правоприменителей создать условия функционирования финансовой системы, отвечающие потребностям экономического развития государства. Иными словами, их появление вызвано неспособностью механизма финансово-правового регулирования универсально отражать объективные потребности субъектов финансовых правоотношений.

На современном этапе причиной появления альтернативных направлений правового регулирования финансовых отношений явились новые условия функционирования системы мирового хозяйства, которые привели к обходу норм международного права, принципов рыночной экономики и неприкосновенности частной собственности. В сложившейся обстановке «...государства уже не могут, опираясь на известный правовой инструментарий, прогнозировать развитие социальных и экономических преобразований» [15].

Изменение баланса сил в международных отношениях, направленное на переход к новой многополярной системе мироустройства, неизбежно вызывает появление нового вектора развития международного права, и, как следствие, — создание обновленной модели механизма финансово-правового регулирования, функционирование которой осложняется «...двойной бухгалтерией международной политики, двумя внешнеполитическими и внешнеэкономическими программами и стратегиями действий» [11].

Это приводит к формированию в российском правовом поле двух параллельных направлений правового регулирования внешнеэкономических отношений, когда наряду с общими правилами и устоявшимися правовыми институтами применяются специальные правовые нормы, распространяющие свое действие на недружественные государства и их резидентов. В результате возникают специальные правила исполнения иностранными покупателями обязательств перед российскими поставщиками природного газа, временный порядок исполнения государством обязательств перед некоторыми иностранными кредиторами в рублях и т. д. В рассматриваемых случаях речь идет о параллельных правовых институтах регулирования финансовых отношений, появление которых вызвано необходимостью противодействия геополитическим рискам и враждебным действиям стран коллективного Запада.

Существенное преобразование и диверсификация правового обеспечения экономических отношений является не только вынужденной мерой на пути создания нового правового порядка. Их возникновение вызвано

также несовершенством механизма финансово-правового регулирования, который, как оказалось, «...не готов выдержать обвал негативных процессов переходного периода» [1], обеспечить резистентность финансовой системы к экономическим кризисам и сохранить должный уровень гарантий защиты прав субъектов финансовых правоотношений. Появление субсидиарного правового регулирования финансовой сферы напрямую связано с цифровизацией и глобализацией экономических отношений, включая деятельность цифровых платформ, которые фактически диктуют правила функционирования рынка цифровых услуг, навязывают невыгодные условия осуществления финансовых операций, в том числе введение условий о паритете цен³, введение запрета на использование сторонних платежных систем, установление не охватываемых финансовым законодательством платежей (эквайринговых комиссий, взимаемых банками, комиссий, взимаемых технологическими компаниями от продажи приложений, которые устанавливаются через технологические компании, и др.).

В современных условиях наблюдается активизация процесса создания многочисленных правовых режимов, направленных на конкретных субъектов финансовых правоотношений и (или) соответствующие условия развития финансового рынка. В частности, стремительное развитие получают экспериментальные правовые режимы, представляющие собой модели регулирования, реагирующие на быстро меняющиеся условия функционирования финансовой системы.

В настоящий момент действует Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», однако еще задолго до его принятия такие «регуляторные песочницы» вводились ЦБ РФ в целях развития финансовых технологий. С внедрением цифровых инструментов фискального администрирования связаны правовые эксперименты по прослеживаемости товаров⁴, по введению специального правового режима «налога на профессиональный доход»⁵, автоматизированной упрощенной системы налогообложения и др. Фактически в рассматриваемых случаях наряду с общим порядком фискального администрирования применяются специальные правила реализации контролирующим органом надзорной функции в условиях применения информационных систем и цифровых сервисов.

³ Определение ВС РФ от 21 июня 2022 № 305-ЭС22-10220, дело № А40-19473/2021.

⁴ Постановление правительства Российской Федерации от 25.07.2019 г. № 807 «О проведении эксперимента по прослеживаемости товаров, выпущенных на территории Российской Федерации в соответствии с таможенной процедурой выпуска для внутреннего потребления».

⁵ Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима „Налог на профессиональный доход“ в городе федерального значения Москве, в Московской и Калужской областях, а также в Республике Татарстан (Татарстан)».

Развитие процессов диверсификации права зачастую связывают с развитием правоприменительной практики [12], нередко вступающей в противоречие с действующими императивными нормами. Применение в целях регулирования финансовых отношений судебных актов, а также писем министерств и ведомств, содержащих не закрепленные финансовым законодательством приемы регулирования, — явление довольно частое, позволяющее говорить о развитии правоприменительного права.

Расхождение хозяйственной практики с действующими финансово-правовыми нормами обусловлено прежде всего отсутствием четко закрепленных в законе условий осуществления финансовых обязательств. В частности, об этом свидетельствует обширная судебная практика по вопросам исполнения государственных контрактов и соглашений о предоставлении субсидий, иных инвестиционных соглашений, в которых конкретизируются условия осуществления финансовых расходных обязательств, что нередко не вписывается в параметры правового акта о бюджете и систему государственных программ и национальных проектов. Учитывая изложенное, порядок исполнения государственных (муниципальных) контрактов, а также концессионных и иных долгосрочных инвестиционных соглашений нуждается в механизме приведения в соответствие с принципами осуществления бюджетного процесса посредством конкретизации в финансовом законе условий осуществления финансовых расходных обязательств. Цели и объемы расходов по таким обязательствам не могут превышать объем средств, предусмотренных на реализацию соответствующих мероприятий правовым актом о бюджете и системой государственных программ и национальных проектов.

В сфере фискального регулирования отдельные правила осуществления налоговых обязательств в свое время были закреплены в постановлении Пленума ВАС от 12 октября 2006 г. № 53 «Об оценке налогоплательщиками обоснованности налоговой выгоды». И только в августе 2017 года эти правила появились в ст. 54.1 Налогового кодекса России (НК РФ). Вместе с тем не имеют закрепления в НК РФ такие применяемые на практике инструменты определения параметров налогового обязательства, как «налоговая реконструкция», «налоговая оговорка». Эти выработанные в рамках судебной практики правовые инструменты позволяют определять элементы юридического состава налога в случае недобросовестного поведения налогоплательщика, его контрагента, когда обоснованность полученной налоговой выгоды ставится налоговыми органами под сомнение. Активное распространение в практике налогообложения получили такие регулируемые гражданским правом конструкции, как «возмещение убытков», «заверения об обстоятельствах». Фактически складывается параллельное регулирование налоговых отношений, субсидиарное к НК РФ.

Тенденции развития правового регулирования отдельных групп финансовых отношений

Появление новелл в правовом регулировании финансовых отношений во многом вызвано возрастающей конвергенцией частного и публичного права, устранением жесткого водораздела между ними. В актах финансового законодательства всегда закреплялись положения, направленные на возможность использования частноправовых конструкций, которые могут быть эффективными инструментами регулирования финансовых отношений [2]. Наблюдаемый в современных условиях процесс усиления взаимопроникновения частного и публичного права, проявляющийся в расширении рецепции универсальных юридических конструкций в финансовом законодательстве, как представляется, вызван цифровизацией государственного управления.

Внедрение информационных систем, упрощающих механизм взаимодействия субъектов финансовых правоотношений, приводит к сокращению круга закрепленных финансовым законодательством административных процедур, в результате чего возникает потребность в применении альтернативных инструментов воздействия на финансовые отношения, в качестве которых выступают межотраслевые универсальные юридические конструкции. В рамках судебной и правоприменительной практики выработаны подходы, легализующие регулирование финансовых отношений посредством многих частноправовых конструкций, приущих гражданскому праву.

Складывающийся подход в регулировании финансовых отношений, нацеленный на преодолении разрыва между отраслями права, не только не противоречит природе финансов, но соответствует предоставительско-обязывающему характеру права и положительно сказывается на развитии финансового законодательства [9]. Вместе с тем, поскольку активно внедряемые в механизм финансово-правового регулирования универсальные юридические конструкции начинают конкурировать с установленными финансовым законодательством административными ограничениями, возникает альтернативное правовое регулирование финансовых отношений, что может привести к негативным последствиям, в том числе к неосновательному обогащению субъектов финансовых правоотношений. Например, возникающие споры об оценке обоснованности налоговой выгоды, о восстановлении нарушенного экономического положения налогоплательщика в условиях альтернативного правового регулирования могут разрешаться не только в рамках закрепленных НК РФ процедур, но и на основе договора, заключенного между налогоплательщиком и его контрагентом. В результате налогоплательщик может одновременно с применением предусмотренной НК РФ процедурой возврата налога восстановить свое нарушенное экономическое положение посредством использования таких конструкций, как заверение об обстоятельствах

или возмещение убытков в сумме налоговой выгоды, признанной налоговым органом необоснованной, предъявляя соответствующие требования к своему недобросовестному контрагенту⁶.

Представляется, что появление альтернативных (параллельных) правовых институтов в сфере финансово-правового регулирования связано со стойким мнением законодателя о том, что финансовое право не имеет собственного эффективного правового инструментария, а финансы регулируются административным, гражданским и уголовным правом. В частности, вместо того, чтобы применять предусмотренные законом меры финансового принуждения в случае неуплаты или уклонения от уплаты налогов, правоприменитель прибегает к уголовному преследованию, а также к применению мер административной ответственности.

Сложившийся в законодательстве подход негативно сказался на регулировании отношений, складывающихся в сфере привлечения к ответственности за нарушение финансового законодательства [6]. Одновременно применяются положения НК РФ, КоАП РФ, УК РФ и даже ГК РФ, что, в свою очередь, приводит к усложнению механизма привлечения к ответственности за финансовые правонарушения и требует проведения работы по упорядочению системы мер юридической ответственности.

В качестве эффективного правового инструмента мог бы выступать «...метод возложения имущественной ответственности в виде специального (штрафного) финансового обязательства» [10], позволяющий сместить инициативу по уплате экономических санкций в бюджет с государства на бизнес, применение которого будет нацелено на преодоление разрыва между отраслями права в сфере применения механизма привлечения к юридической ответственности. Предлагаемый подход не является новым, он как идея вытекает из принятого в советский период постановления Совмина СССР от 30 июля 1988 года № 929 «Об упорядочении системы экономических (имущественных) санкций, применяемых к предприятиям, объединениям и организациям», направленного на упорядочение системы мер имущественной ответственности посредством расширения сферы применения таких универсальных мер ответственности, как взыскание неустойки и возмещения убытков, а также правового инструментария финансового права (пени, уплата налога в двойном размере и др.).

С позиции применения обязательственного метода воздействия на отношения, складывающиеся в области применения мер принуждения, целесообразно рассмотреть вопрос о расширении сферы использования закрепленных финансовым законодательством мер финансово-правового принуждения, вытекающих из условий осуществления финансовых обязательств, к числу которых относятся: уплата налога в двойном

размере, отказ в предоставлении налоговых вычетов (возмещения налога), возмещение убытков. Некоторые из обозначенных мер финансово-правового принуждения на сегодняшний день точно закреплены в актах финансового законодательства применительно к конкретным видам финансовых обязательств. Так, согласно ст. 396 НК РФ уплата земельного налога производится в двукратном или четырехкратном размере вследствие отсутствия на земельном участке, предоставленном для жилищного строительства, построенного объекта недвижимости.

Расширение области применения таких специфических мер финансово-правового принуждения позволило бы в перспективе избежать параллельного регулирования отношений в сфере применения мер ответственности за нарушение финансового законодательства. Предложенный подход не противоречит обязательственному характеру финансовых правоотношений, не потребует кардинальных преобразований, а вполне соответствует наметившейся в законодательстве тенденции развития института имущественной ответственности в финансовом праве. Например, в ст. 35 НК РФ закреплены положения о возмещении налогоплательщикам убытков, причиненных неправомерными действиями налоговых органов. Согласно ст. 270.2 БК РФ контролирующий орган вправе предъявить требование о возмещении ущерба к подконтрольному субъекту, нарушившему бюджетное законодательство, а положения УПК РФ о возмещении ущерба, причиненного бюджетной системе, фактически блокируют применение мер уголовной ответственности, предусмотренных ст. 198—199.2 УК РФ.

Развитие альтернативного правового регулирования выражается и в том, что в обход финансового законодательства развивается сформированный в рамках правоприменительной практики налоговых органов параллельный правовой институт регулирования контрольно-надзорной деятельности. Его появление связано с применением контролирующими субъектами административных процедур, а также форм контроля, не предусмотренных финансовым законодательством и являющихся альтернативой предусмотренным НК РФ налоговым проверкам. Например, на основании письма от 10.07.2018 № ЕД-4-15/13247@ «О профилактике нарушений налогового законодательства» появился порядок аннулирования налоговых деклараций, определены не предусмотренные НК РФ правила проведения допроса руководителя юридического лица, индивидуального предпринимателя, осуществления таких мероприятий налогового контроля, как осмотр помещений по адресу местонахождения юридического лица, истребование документов у банков и т. д., установлены сроки проведения этих мероприятий⁷.

⁶ Определение Верховного суда Российской Федерации от 09 сентября 2021 г. № 302-ЭС21-5294 по делу № А33-3832/2019.

⁷ На основании письма Минюста Российской Федерации от 12.10.2018 № 01-134776/18 это письмо ФНС России было отозвано с исполнения.

На сегодняшний день единственным источником регулирования мероприятий предпроверочного анализа является определение Конституционного Суда РФ от 7 апреля 2022 г. № 822-О [17], согласно которому право налоговых органов на истребование документов не может быть использовано вместо контрольных полномочий, подлежащих применению в рамках проведения налоговой проверки.

Очевидно, что причины происходящего во многом объясняются противоречивым характером налогово-правовых норм в части определения полномочий налоговых органов, а также пренебрежением ключевыми принципами организации государственного управления, в результате чего инструменты реализации контрольно-надзорной деятельности превращаются в механизм давления на подконтрольных субъектов. Прежде всего речь идет о противоречивости положений НК РФ о праве ФНС России на осуществление нормотворческих полномочий в фискальной сфере. Устанавливая в п. 2 ст. 4 НК РФ запрет контрольно-надзорному органу на принятие нормативных правовых актов, в других статьях кодекса законодатель это право субъекту делегирует, что приводит к негативным последствиям, выражающимся в отступлении механизма правового регулирования контрольно-надзорной деятельности от функционального подхода к управлению развитием экономики, в рамках которого «...правильное определение функций каждого органа является определяющим моментом при установлении правомочий и ответственности в управлении» [4].

Именно отклонение от функционального подхода привело к смешению государственных функций между федеральными органами исполнительной власти, наделению контрольно-надзорных органов нормотворческими полномочиями, что в конечном счете выразилось в применении налоговыми органами не предусмотренных законом административных процедур и форм осуществления налогового контроля [5]. Это явилось причиной возникновения параллельного правового регулирования контрольно-надзорной деятельности, осуществление которой легализовано Федеральным законом от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» и Федеральным законом от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации», конкретизация положений которого фактически привела к формированию существенного правового массива регулирования контрольно-надзорной деятельности, а «регуляторная гильотина» из одноразового приема регулирования контрольно-организационных отношений превратилась в перманентный правовой режим.

Помимо развития параллельного правового института регулирования контрольно-надзорной деятельности, на сегодняшний день стремительно разрастается массив нормативных правовых актов, закрепля-

ющих порядок установления, введения и взимания квазианалогов и сборов, не охватываемых сферой регулирования НК РФ. Количество не регулируемых НК РФ фискальных взиманий, по некоторым данным, достигло уровня 70, что свидетельствует о формировании параллельной налоговой системы в государстве в обход налогового законодательства Российской Федерации.

Причиной сложившейся ситуации также являются противоречащие друг другу законоположения, регулирующие порядок установления фискальных взиманий. Например, одновременно с положениями о запрете на установление вне рамок НК РФ платежей, отвечающих признакам налогов и сборов, в п. 3 ст. 1 НК РФ закреплена норма, допускающая установление сборов и страховых взносов отдельными отраслевыми законами. Согласно указанному пункту ст. 1 действии НК РФ распространяется на отношения по установлению, введению и взиманию сборов, страховых взносов в тех случаях, когда это прямо предусмотрено НК РФ.

Помимо изложенного, происходит правовая девиация обязательных платежей и штрафных санкций в сфере осуществления расчетов с участием банков, порядок установления и взимания которых не подчиняется общим принципам установления фискальных платежей и принудительных изъятий, сформированных в рамках финансового права. Речь идет об эквайринговых комиссиях, комиссионных вознаграждениях по договорам банковского вклада, платежах за денежные переводы, которые фактически являются скрытыми фискальными взиманиями, а также о штрафных санкциях, порядок применения которых в отношении банков в отдельных случаях устанавливается решениями Агентства по страхованию вкладов.

Заключение

Проведенный анализ позволяет сформулировать следующие промежуточные выводы.

1. Параллельное (альтернативное) правовое регулирование финансовых отношений есть не что иное, как проявление стойкого мнения законодателя, состоящее в том, что финансовое право не имеет собственного инструментария, а финансы регулируются административным, гражданским и уголовным правом. Вместе с тем финансовое право — самодостаточная отрасль права и может решить все вопросы без заимствования инструментов из других отраслей права. Избежать параллельного регулирования отношений в сфере применения мер юридической ответственности за нарушение финансового законодательства следует посредством применения метода возложения имущественной ответственности в виде соответствующего финансового обязательства. Этого можно достичь посредством расширения сферы применения

закрепленных финансовым законодательством мер финансово-правового принуждения, вытекающих из условий осуществления финансовых обязательств, к числу которых относятся: уплата налога в двойном размере, отказ в предоставлении налоговых вычетов (возмещения налога), возмещение убытков и т. д.

2. Во избежание появления параллельных правовых институтов в фискальной сфере следует сосредоточиться на вопросах упорядочения правового регулирования отношений в сфере установления, введения, взимания фискальных платежей. Это важное направление развития механизма финансово-правового регулирования может быть реализовано посредством выделения в системе финансового права такого крупного правового массива, как фискальное право, направленное на создание единого правового поля фискальной деятельности государства.

3. Не исключая возможности применения в некоторых ситуациях альтернативного правового регулирования, полагаем, что применение этого подхода не должно вызывать варианты действий правоприменителя, т. е. выбора между законным и полузаконным регулированием финансовых отношений. Альтернативный подход следует рассматривать как правосстановительный и субсидиарный к основному правовому режиму.

Речь следует вести в аспекте признания за субъектами финансовых отношений субъективного финансового права как самостоятельной юридической ценности, подлежащей защите в форме закона, акта управления, судебного решения или же констатации положения о распространении на эту сферу общего (универсального) правового режима регулирования имущественных отношений, допускающего широкую альтернативность в применении юридических конструкций.

Литература

1. Абрамова А.А. Эффективность механизма правового регулирования : автореф. дис. ... канд. юрид. наук: 12.00.01; Краснояр. гос. ун-т. Красноярск, 2006. 23 с.
2. Алексеев С.С. Собрание сочинений в 10 т. Т. 7: Философия права и теория права. М. : Статут, 2010. С. 350.
3. Андриевский К.В. Финансово-правовые режимы : дис. ... докт. юрид. наук. М., 2022.
4. Бачило И.Л. Функции органов управления (правовые проблемы оформления и реализации). М., 1976. С. 5.
5. Васянина Е.Л. Актуальные проблемы правового регулирования финансовых отношений // Пролог: журнал о праве. 2022. № 3 (35). С. 44—51.
6. Галкин Д.В. Роль института административно-правовой ответственности в обеспечении финансовой безопасности государства // Финансовое право. 2009. № 5.
7. Гетьман-Павлова И.В. Международное частное право. 4-е изд., перераб. и доп. М. : Юрайт, 2020. 416 с.
8. Занина А. Приватизация без срока давности // Коммерсантъ. 2022. 30 мая.
9. Запольский С.В., Васянина Е.Л. Обязательство — ключевая категории теории финансового права // Государство и право. 2022. № 8. С. 111—120.
10. Запольский С.В. Самофинансирование предприятий: (Правовые вопросы). М. : Юрид. лит., 1988. С. 133.
11. Зорькин В.Д. Право России: Альтернативы и риски в условиях глобального кризиса // Российская газета. 2022. 29 июня.
12. Кандыбко А.И. Параллельное право // Северокавказский юридический вестник. 2012. № 2.
13. Леснова Н.И. Правовой дуализм в России XVIII — начала XX века : автореф. дис. ... канд. юрид. наук: 12.00.01; Нижегород. гос. ун-т им. Н.И. Лобачевского. Нижний Новгород, 2007. 21 с.
14. Поветкина Н.А. Правовой эксперимент как новая тенденция развития бюджетного права // Финансовое право. 2020. № 9. С. 21—25.
15. Савенков А.Н. Глобальный кризис современности как предмет философии права // Государство и право. 2022. № 2. С. 103—117.
16. Сморгачева Л.Н. Экспериментальный правовой режим как средство административного регулирования экономической сферы // Право и практика. 2021. № 3. С. 10—15.
17. Тарибо Е.В. Конституционные рамки препроверочного анализа // Налоговед. 2022. № 8. С. 17—21.
18. Шувалов И.И. Правовое регулирование предпринимательской деятельности в период социально-экономического кризиса (теория и практика) : дис. ... докт. юрид. наук. М., 2022.

WAYS FOR DIVERSIFYING LEGAL REGULATION OF FINANCIAL RELATIONS

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

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 Federation, Moscow, Russian Federation.

E-mail: zpmoscow@mail.ru

Keywords: alternative legal constructs, parallel law, financial obligations, liability, tax control, taxes, expenses, legal experiment.

Abstract

Purpose of the paper: studying ways for diversifying legal regulation of financial relations within the framework of development of the concept of modern financial law.

Using general logical research methods, including analysis, synthesis, and the formal legal method, allowed the authors to come to the conclusion that alternative legal constructs should be understood as special legal tools within a single legal space whose use is caused by non-standard or unforeseen situations arisen in legal regulation of financial relations. A diversification of legal regulation should not entail variety in the actions of the law enforcer, that is, cause a choice between the legal and semi-legal regulation of financial relations. The alternative approach must be considered as restorative justice and a subsidiary one in respect of the main legal regime.

The presented conclusions and ways of development of financial laws based on the results of the performed analysis make no claims as to accuracy and perfection. However, the facts and analytical materials can be useful for further research in the field of financial law.

References

1. Abramova A.A. Effektivnost' mekhanizma pravovogo regulirovaniia : avtoref. dis. ... kand. iurid. nauk: 12.00.01; Krasnoiar. gos. un-t. Krasnoiar'sk, 2006. 23 pp.
2. Alekseev S.S. Sbranie sochinenii v 10 t. T. 7: Filosofii prava i teorii prava. M. : Statut, 2010. P. 350.
3. Andrievskii K.V. Finansovo-pravovye rezhimy : dis. ... dokt. iurid. nauk. M., 2022.
4. Bachilo I.L. Funktsii organov upravleniia (pravovye problemy oformleniia i realizatsii). M., 1976. P. 5.
5. Vasianina E.L. Aktual'nye problemy pravovogo regulirovaniia finansovykh otnoshenii. Prolog: zhurnal o prave. 2022. No. 3 (35). Pp. 44–51.
6. Galkin D.V. Rol' instituta administrativno-pravovoi otvetstvennosti v obespechenii finansovoi bezopasnosti gosudarstva. Finansovoe pravo. 2009. No. 5.
7. Get'man-Pavlova I.V. Mezhdunarodnoe chastnoe pravo. 4-e izd., pererab. i dop. M. : Iurait, 2020. 416 pp.
8. Zanina A. Privatizatsiia bez sroka давности. Kommersant". 2022. 30 maia.
9. Zapol'skii S.V., Vasianina E.L. Obiazatel'stvo – klichevaia kategorii teorii finansovogo prava. Gosudarstvo i pravo. 2022. No. 8. Pp. 111–120.
10. Zapol'skii S.V. Samofinansirovanie predpriatii: (Pravovye voprosy). M. : Iurid. lit., 1988. P. 133.
11. Zor'kin V.D. Pravo Rossii: Al'ternativy i riski v usloviakh global'nogo krizisa. Rossiiskaia gazeta. 2022. 29 iunia.
12. Kandybko A.I. Parallelnoe pravo. Severokavkazskii iuridicheskii vestnik. 2012. No. 2.
13. Lesnova N.I. Pravovoi dualizm v Rossii XVIII – nachala XX veka : avtoref. dis. ... kand. iurid. nauk: 12.00.01; Nizhegor. gos. un-t im. N.I. Lobachevskogo. Nizhnii Novgorod, 2007. 21 pp.
14. Povetkina N.A. Pravovoi eksperiment kak novaia tendentsiia razvitiia biudzhethnogo prava. Finansovoe pravo. 2020. No. 9. Pp. 21–25.
15. Savenkov A.N. Global'nyi krizis sovremennosti kak predmet filosofii prava. Gosudarstvo i pravo. 2022. No. 2. Pp. 103–117.
16. Smorchkova L.N. Eksperimental'nyi pravovoi rezhim kak sredstvo administrativnogo regulirovaniia ekonomicheskoi sfery. Pravo i praktika. 2021. No. 3. Pp. 10–15.
17. Taribo E.V. Konstitutsionnye ramki preproverochnogo analiza. Nalogoved. 2022. No. 8. Pp. 17–21.
18. Shuvalov I.I. Pravovoe regulirovanie predprinimatel'skoi deiatel'nosti v period sotsial'no-ekonomicheskogo krizisa (teorii i praktika) : dis. ... dokt. iurid. nauk. M., 2022.

ПОЛИТИКА ИМПОРТОЗАМЕЩЕНИЯ ДЕСЯТЬ ЛЕТ СПУСТЯ: ОПЫТ, ПРОБЛЕМЫ И ПОЛОЖИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

Кобзарь-Фролова М.Н.¹

Ключевые слова: управление, политика, экономика, санкции, конкурентоспособность, предпринимательство, стимулирование, финансирование.

Аннотация

Цель работы: подведение некоторых итогов политики российского государства, взявшего в 2014 году курс на импортозамещение.

Методы исследования: аналитический, логический, историко-правовой и др.

Актуальность темы — в ее злободневности, а также в том, что автор провел анализ мер, принятых в результате введения грубой санкционной политики странами коллективного Запада. Приведен перечень нормативных правовых актов, в которых закреплены меры, направленные на стимулирование и поддержку российского производителя.

Результаты исследования: обобщение административно-правовых и финансово-экономических мер, принятых для проведения политики импортозамещения. Новым является и то, что импортозамещение рассмотрено не как экономическая категория или режим, а как управленческая категория, как часть социально-экономической политики.

Научная новизна: обобщение положительных и отрицательных сторон политики импортозамещения на основе десятилетнего опыта ее проведения. И это тоже выделяет эту работу среди аналогичных трудов.

DOI: 10.24412/1994-1404-2025-2-23-30

Введение

В научных работах российских ученых импортозамещение исследуется преимущественно как концепция, как режим, как система административно-правовых и экономических мер [2, с. 46—58; 3; 4, с. 197—205; 15, с. 108].

Представляется, что каждый из перечисленных подходов является весьма узким, усеченным. Осмелюсь предположить, что в современный период наиболее правильно рассматривать и исследовать вопросы импортозамещения с точки зрения государственной политики и тех мер и приемов, которые способствуют ее проведению. Вне сомнения, вопросы импортозамещения, например, отдельных комплектующих могут решаться на уровне отдельно взятых предприятий изготовителей. В условиях свободных рыночных отношений каждый вправе делать выбор в пользу экономии, качества и проч.

В статье будут рассмотрены вопросы импортозамещения в глобальном аспекте. Речь пойдет о выборе страной курса на импортозамещение в ключевых

отраслях и направлениях экономики, промышленности, сельском хозяйстве, — курса, который был избран на высшем государственном уровне.

Опыт развития крупных экономически развитых государств показывает, что наибольший рост экономика показывает в том случае, когда ей удалось встроиться в мировую глобальную систему производства и потребления. В августе 2012 года Российская Федерация стала полноправным членом ВТО, имея к этому времени прочные торговые связи со многими странами и крупнейшими производителями. К 2013 году правительством России было заключено около сотни соглашений об избежании двойного налогообложения по поводу взаимного обмена товарами, работами, услугами.

Однако в 2014 году США, Европейский союз, Австралия и Канада ввели пакет экономических санкций против Российской Федерации. Это было реакцией на акт присоединения Крыма к России в середине марта 2014 года. С началом специальной военной операции на Украине (февраль 2022 г.) Россия встретила

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

с новыми мощными вызовами от США, Европейского союза и ряда других стран, которые ввели еще более обширные ограничения в отношении российской экономики, финансовой системы страны и крупнейших производителей комплектующих, товаров и услуг. К началу 2025 года в отношении России, ее юридических лиц и даже отдельных граждан принято 14 пакетов санкций. Один из последних введен Европейским Союзом 24 июня 2024 года [5].

По данным ФТС России, из-за введения санкций и ограничений внешнеторговый оборот Российской Федерации сократился на 7% по сравнению с 2013 годом, при этом экспорт сократился на 5,75%, а импорт на 9,2%². Казалось бы, величины в относительных показателях незначительные. Но это лишь отражение отдельных принятых в срочном порядке мер по переориентации в поставках и поставщиках.

С 2014 года действует продовольственное эмбарго — запрет на ввоз в Россию отдельных товаров и продукции сельскохозяйственного назначения, сырья и продовольствия, страной происхождения которых является государство, принявшее решение о введении экономических санкций. Все это вместе взятое привело к дефициту ряда товаров на оптовом и розничном рынках, и, как следствие, повышению инфляции. В первую очередь последствия кризиса испытали на себе предприятия энергетической промышленности, оборонные, сельскохозяйственные и другие предприятия, которые встретились с проблемой невыполнения поставщиками договорных обязательств. В связи с возникшими перебоями в поставках товаров, нехваткой комплектующих деталей и сырья было принято решение о взятии курса на импортозамещение.

Политика (курс) импортозамещения

Согласно Конституции Российской Федерации, государственную политику в стране определяет Президент Российской Федерации. И именно Президент определяет «основные направления внутренней и внешней политики государства»³, принимает меры по охране суверенитета Российской Федерации, ее независимости и государственной целостности, обеспечивает согласованное функционирование и взаимодействие органов государственной власти⁴.

В условиях сложившейся ситуации, в августе 2014 года, выступая на пленарном заседании в Санкт-Петербурге на ежегодно проводимом Петербургском международном экономическом форуме, президент России В.В. Путин говорил о том, что страна встретила с достоинством международные вызовы и «Россия к осени 2014 года выработает свою стратегию в обла-

сти импортозамещения». Не нарушая норм международной торговли и не вводя каких-либо ограничений и барьеров, за счет модернизации промышленности, строительства новых предприятий, локализации конкурентного производства в России, страна сможет поднять собственный рынок, сказал президент. В планах — развитие российского производства программного обеспечения, радиоэлектронного оборудования, текстильной промышленности, рост рынка продовольствия. Перед Правительством Российской Федерации он поставил задачу: в короткие сроки проанализировать возможности конкурентного импортозамещения промышленности и сельском хозяйстве и определить перечень товаров, необходимых для государственных и муниципальных нужд, которые могут быть замещены и будут закупаться исключительно у российских производителей или государств — членов Таможенного союза. Путин добавил: специалисты Общероссийского народного фронта подсчитали, что замещение импортных компонентов и материалов отечественными образцами может давать России в ближайшие 8 лет экономический рост на 5—7% ежегодно [13].

Вместе с тем хотелось бы развеять миф о том, что проблема импортозамещения впервые возникла в России именно в 2014 году. Для России эта проблема не нова. Так, молодая советская Россия после революции, оказавшись в изоляции, остро нуждалась в станках, оборудовании, продовольствии. Для посевных работ нужны были тракторы, а Россия не производила ни тракторов, ни иных машин. Машиностроение полностью зависело от поставок комплектующих из-за рубежа. Для решения проблемы продовольствия В.И. Ленин остро поставил вопрос о начале производства в России собственных тракторов и комплектующих к ним. 2 декабря 1920 года он подписывает декрет Совета народных комиссаров «О едином тракторном хозяйстве». Было принято решение о строительстве на Урале в Челябинске тракторного завода [9, с. 127—128, 138—139, 164].

Политика импортозамещения стала модным трендом в 1950-х годах прошлого века. Разработкой стратегии импортозамещения, независимой импортозамещающей индустриализации, занимался аргентинский экономист Рауль Пребиш [10, с. 26—27; 18, с. 251—273; 19]. События Второй мировой войны разделили большинство развивающихся стран на два лагеря. Одни поддерживали идеи Пребиша об импортозамещении, другие, как Советский Союз и страны социалистического лагеря, пошли по пути кооперации и экономической взаимопомощи. В 1949 году был создан Совет экономической взаимопомощи, приоритетными направлениями которого были: экономическое и научно-техническое сотрудничество стран-членов, включая развитие взаимной торговли, поставку (обмен) сырья, продовольствия, оборудования, машины и прочее. СЭВ прекратил свое существование с развалом Советского союза (1991 г.). Но нужно сказать, что за годы существования СЭВ странами-участниками была создана система международной кооперации и разделения труда. Эта

² Показатели внешней торговли России в 2014 году. URL: <https://russian-trade.com/> (дата обращения: 28.04.2025).

³ П. 3 ст. 80 Конституции Российской Федерации // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 04.07.2020.

⁴ Там же, п. 2 ст. 80.

система обладала способностью восполнять потребности в основных товарах, комплектующих, технологиях и машинах.

Шоковая экономика 90-х годов в России, финансовый кризис и девальвация рубля привели к разрушению выстроенных годами торговых связей с зарубежными поставщиками. Часто меняющееся законодательство не оставляло шансов войти на российский рынок новым товаропроизводителям. Тогда вопрос об импортозамещении встал как необходимое условие и инструмент выживания. Казалось, что это позволит загрузить свободные мощности предприятий, создать рабочие места и выплачивать рабочим реальную зарплату, а не платить людям выпускаемой продукцией. И какое-то время это давало положительные результаты. Но по мере укрепления национальной валюты отечественная продукция стала существенно расти в цене и потеряла свою конкурентоспособность по отношению к импортной, к тому же производимая продукция зачастую существенно уступала по качеству, потребительским свойствам и не могла конкурировать с зарубежными аналогами [7, с. 109—116; 8]. В этой связи в начале 2000-х вопрос импортозамещения постепенно сошел на нет.

События 2014 года лишь подняли новую волну. В сложившейся ситуации была нужна инициатива со стороны государства и поддержка российских производителей и иных предпринимателей. К тому же к 2014 году Россия уже была признана страной с высокоразвитой экономикой и занимала по уровню ВВП и паритету покупательской способности (ППС) 7 место в мире⁵. По мнению президента страны, она обладала способностью к импортозамещению. В этой связи российское правительство ответило странам коллективного Запада контрсанкциями и выработало комплекс правовых и экономических мер, направленных на поддержку политики импортозамещения.

Юридические меры обеспечения политики импортозамещения

Нужно сразу заметить, что никаких специальных законов принимать не потребовалось. Это обусловлено тем, что экономическая и социальная политика Российской Федерации уже более 30 лет направлена на развитие предпринимательства, поддержку российских производителей, одобрение их инициативы, самостоятельность и проч. Вместе с тем Правительство Российской Федерации как орган публичной власти, призванный, согласно Конституции РФ, обеспечить проведение государственной политики, приняло ряд подзаконных нормативных правовых актов, направленных на обеспечение реализации курса на импортозамещение. 30 сентября 2014 года распоряжением Правительства Российской Федерации № 1936-р утверждена дорожная карта «План содействия импортозамещению в про-

мышленности». Дорожная карта — документ внутреннего, служебного пользования; официально опубликован он не был и на данный момент исчерпал свою юридическую силу. Но его принятие имело огромное значение, поскольку на основе этого плана была разработана и принята система ведомственных нормативных правовых актов, продолжающих действовать. Например, Минпромторгом России были разработаны отраслевые планы мероприятий по импортозамещению в гражданских отраслях промышленности Российской Федерации.

По инициативе Президента РФ создается специализированный Фонд развития промышленности — институт развития, назначение которого — предоставление на льготных условиях займов промышленным компаниям в целях развития импортозамещающих производств (комплексов) и переход действующих предприятий на новейшие технологии⁶.

Пройдя некоторый путь проб и ошибок, стало очевидным, что механизм импортозамещения нужно пересматривать, а программу нужно было разрабатывать не в целом по вопросам импортозамещения (так она останется на уровне деклараций), а по конкретным стратегически значимым технологиям и комплектующим, которые предстояло определить. В этой связи Минпромторг разработал перечень приоритетных и критически важных видов продукции, услуг и программного обеспечения в целях импортозамещения и обеспечения национальной безопасности. Перечень формировался на основе спроса предприятий-производителей, столкнувшихся с проблемами отсутствия и перебоев в поставках комплектующих и деталей. Это позволило оценить потенциал импортозамещения на отраслевом (макро-) уровне. Все последующие управленческие решения принимались по отраслям с учетом замещения импортируемых видов продукции.

Созданный механизм реализации планов импортозамещения работает по настоящее время и включает следующие элементы:

- приоритеты промышленной политики;
- перечень субъектов и направления поддержки,
- программа стимулирования потенциальных инвесторов;
- мониторинг исполнения отраслевых планов в гражданских отраслях промышленности⁷ и проч.

К настоящему времени планами Минпромторга задействовано 22 отрасли, преимущественно машиностроение, станкостроение, металлургия, авиация,

⁶ Документ опубликован не был. Официальный сайт Фонда развития промышленности — институт развития. URL: <https://frprf.ru/>

⁷ Приказ от 15 июня 2015 г. № 1544 «Об организации в Минпромторге России работы по мониторингу исполнения отраслевых планов мероприятий по импортозамещению в гражданских отраслях промышленности Российской Федерации в целях реализации «Плана содействия импортозамещению в промышленности», утвержденного распоряжением Правительства Российской Федерации от 30 сентября 2014 г. № 1936-р».

⁵ ВВП стран по ППС. URL: <https://total-rating.ru/1360-vvp-stran-po-pps-2014.html>

радиоэлектроника, судостроение, лесная, химическая, фармацевтическая промышленность и проч.

По инициативе Правительства РФ в 2015 году была создана общественная комиссия, которая провела ряд общественных слушаний, по итогам которых был осуществлен отбор наиболее прогрессивных и экономически эффективных проектов по вопросам импортозамещения⁸. Комиссия действует и в наши дни. Ее работа организована по двум ключевым направлениям (подкомиссии) — по вопросам оборонно-промышленного комплекса и гражданских отраслей экономики⁹. Цель комиссии — координация деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Федерации, органов местного самоуправления и организаций по вопросам реализации государственной политики в сфере импортозамещения.

В 2016 году Правительство разрабатывает Стратегию развития промышленности строительных материалов¹⁰. В этом же году принимается решение об установлении приоритета закупки товаров российского происхождения по отношению к товарам, происходящим из иностранного государства, а также работам, услугам, выполняемым и оказываемым иностранными лицами¹¹. В 2020 г. правительство РФ устанавливает запрет на закупки импортных товаров для государственных нужд¹², а также минимальную обязательную долю закупок товаров отечественного производства¹³. Для этих нужд нормативными актами Минпромторга России были регламентированы особенности ввоза на территорию РФ отдельных видов и категорий то-

варов, например, средства связи радиоэлектронные (в 2021 году — 50 %, с 2022 года и далее — 90%).

Все это потребовало прорыва в науке и технологиях. Правительство РФ в срочном порядке определяет базовые инструменты поддержки НИОКР, разрабатывает правила субсидирования из федерального бюджета затрат на проведение НИОКР в рамках реализации инновационных проектов¹⁴. Высокий темп освоения новых знаний и создание наукоемкой продукции на собственной технологической основе становятся ключевым фактором, определяющим конкурентоспособность национальной экономики и показатель обеспечения экономической безопасности государства [14, с. 15—18].

Следующим шагом президент РФ указом от 30.03.2022 года № 166¹⁵ устанавливает запрет органам государственной власти (заказчикам) использовать иностранные программные продукты на значимых объектах критической информационной инфраструктуры.

Важную роль в определении политики импортозамещения президент РФ отводит IT-технологиям. В 2022 г. президент РФ подписывает Указ № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в РФ»¹⁶. Стратегия импортозамещения в отраслях IT предполагает:

- дополнительные бюджетные ассигнования на осуществление грантовой поддержки перспективных отечественных разработок и решений в области IT;

- финансовую поддержку работников IT-сферы на улучшение жилищных условий и повышения уровня их заработной платы;

- предоставление льготных кредитов (под 3% годовых);

- освобождение от плановых проверок;

- финансовые инструменты льготной ипотеки и проч.

Требования и критерии к проектам технологического суверенитета нормативно закреплены в постановлении Правительства № 603¹⁷.

⁸ Документ опубликован не был. Постановление Правительства РФ от 04.08.2015 № 785 «О Правительственной комиссии по импортозамещению» (вместе с «Положением о Правительственной комиссии по импортозамещению») // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 28.05.2024.

⁹ Положение о подкомиссии по вопросам гражданских отраслей экономики Правительственной комиссии по импортозамещению (утв. Правительством РФ 29.08.2015). Документ опубликован не был. Текст размещен на сайте <http://m.government.ru>

¹⁰ Распоряжение Правительства РФ от 10.05.2016 № 868-р «О Стратегии развития промышленности строительных материалов на период до 2020 года и дальнейшую перспективу до 2030 года» // Собрание законодательства РФ. 2016. № 20. Ст. 2863.

¹¹ Постановление Правительства РФ от 16.09.2016 № 925 (ред. от 16.05.2022) «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» // Собрание законодательства РФ. 2016. № 39. Ст. 5649.

¹² Постановление Правительства РФ от 30.04.2020 № 616 «Об установлении запрета на допуск промышленных товаров, происходящих из иностранных государств, для целей осуществления закупок для государственных и муниципальных нужд, а также промышленных товаров, происходящих из иностранных государств, работ (услуг), выполняемых (оказываемых) иностранными лицами, для целей осуществления закупок для нужд обороны страны и безопасности государства» // Собрание законодательства РФ. 2020. № 19. Ст. 2993.

¹³ Постановление Правительства РФ от 03.12.2020 № 2014 «О минимальной обязательной доле закупок российских товаров и ее достижении заказчиком» // Собрание законодательства РФ. 2020. № 50 (ч. IV). Ст. 8220.

¹⁴ Постановление Правительства РФ от 12.12.2019 № 1649 «Об утверждении Правил предоставления субсидий из федерального бюджета российским организациям на финансовое обеспечение затрат на проведение научно-исследовательских и опытно-конструкторских работ по современным технологиям в рамках реализации такими организациями инновационных проектов и о признании утратившими силу некоторых актов Правительства Российской Федерации» // Собрание законодательства РФ. 2019. № 51 (ч. II). Ст. 7619.

¹⁵ Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2022. № 14. Ст. 2242.

¹⁶ Указ Президента РФ от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» // Собрание законодательства РФ. 2022. № 10. Ст. 1468.

¹⁷ Постановление Правительства РФ от 15.04.2023 № 603 (ред. от 06.11.2024) «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

В 2023 году президент РФ дал правительству РФ новый перечень поручений¹⁸. Ответом на данный перечень стала Концепция технологического развития на период до 2030 года¹⁹. В ней впервые с 2014 года органом публичной власти дано определение понятию импортозамещение, которое рассматривается как *процесс создания новых или развития существующих современных конкурентоспособных производств и технологий в Российской Федерации, предназначенных для замещения импортируемых товаров, услуг и технологий*.

Концепция закрепляет две формы импортозамещения:

- 1) локализация собственных производств, технологий и
- 2) переориентация трансграничных производственных цепочек на устойчивых (надежных) поставщиков.

Реализация Концепции предполагает достижение к 2030 году трех ключевых целей:

- 1) полный контроль над воспроизводством критических и сквозных технологий (в области микроэлектроники, станкостроения, биоинженерии и проч.);
- 2) переход к инновационно ориентированному экономическому росту экономики и социальной сферы;
- 3) технологическое обеспечение устойчивого функционирования и развития производственных систем.

Изучение и анализ задач, закрепленных в Концепции, позволяет говорить о том, что особая роль в её реализации и достижении целевых ориентиров отводится субъектам Российской Федерации и международному сотрудничеству. На территориях субъектов предполагается:

- создание инновационных научно-технологических центров и иных форм преференциальных режимов;
- формирование научно-производственных образовательных кластеров;
- учреждение промышленных парков, опытных полигонов, центров трансфера технологий и инженеринговых услуг и прочее.

В рамках международного сотрудничества планируется:

- укрепить многосторонние связи, направить их на создание и освоение новых технологий;
- ввести трансграничные механизмы поддержки деятельности технологических инноваций;

организовать совместные образовательные программы;

обеспечить условия для выращивания технологических компаний — мировых лидеров.

Для решения этих задач планируется наиболее полное привлечение потенциала Евразийского экономического союза, Шанхайской организации сотрудничества (ШОС), стран БРИКС, Регионального сотрудничества в области связи, задействовать потенциал Союзного государства и проч. [6, с. 15—24; 11, с. 36—44; 12, с. 111—115].

Подводя итоги

Немногим более 10 лет назад Президент Российской Федерации В.В. Путин обратился к нации по вопросу импортозамещения. За это время в России реализовано более тысячи самых разных проектов в этом направлении. Наиболее успешными и состоявшимися на данный момент признаны: «МойОфис» (пакет офисных программ как альтернатива MicrosoftOffice); RuStore (российская программа приложений); «Аврора» (мобильная операционная система, способная заменить Android и IOS); «Яндекс Диск» как замена GoogleDrive и много других.

Вне сомнения, десять лет — это тот период, когда уже четко вырисовались положительные и отрицательные стороны политики импортозамещения.

К **положительным** представляется возможным отнести:

- качественный рост занятости населения (существенное снижение уровня безработицы);
- на отечественный рынок поступил широкий ассортимент российских товаров;
- первое и второе вместе взятое поддерживает уровень жизни граждан на достаточно высоком уровне (уровень бедности населения снижается);
- повысился уровень доверия населения к финансовой системе и предпринимаемым мерам;
- возросла предпринимательская активность населения, налоговые органы отмечают рост зарегистрированных предприятий;
- повсеместная информатизация и компьютеризация общества привела к появлению новых, ранее не известных социальных сфер деятельности, расширяется их направленность, внедряются отечественные операционные системы с характеристиками, аналогичными зарубежным;
- поддержка предпринимательства способствовала появлению новых российских конкурентоспособных брендов, готовых выступать наравне с зарубежными, развиваются собственные технологии;
- замена (переориентация) зарубежных поставщиков позволила получить новые виды продукции, комплектующих, материалов, повысился импульс экономики в целом, активизируются процессы индустриализации страны;

к организациям, уполномоченным представлять заключения о соответствии проектов требованиям к проектам технологического суверенитета и проектам структурной адаптации экономики Российской Федерации» // Собрание законодательства РФ. 2023. № 17. Ст. 3141.

¹⁸ Перечень поручений по итогам пленарного заседания съезда и встречи с членами бюро РСПП (утв. Президентом РФ 29.04.2023) № Пр-872. URL: <http://www.kremlin.ru>

¹⁹ Распоряжение Правительства РФ от 20.05.2023 № 1315-р «Об утверждении Концепции технологического развития на период до 2030 года» (вместе с «Концепцией технологического развития на период до 2030 года») // Собрание законодательства РФ. 2023. № 22. Ст. 3964.

- созданы предпосылки для обеспечения производственной безопасности страны, сократилась зависимость от международного рынка (и труда, и товаров, и комплектующих и проч.);
- обширная производственная база позволяет отстаивать интересы государства в мировом масштабе на принципиально новом уровне.

Подводя итог положительной стороне политики импортозамещения, хотелось бы добавить, что всё это вместе взятое, вне сомнения, способствовало социальной солидарности гражданского общества. У россиян крепнет чувство гордости за свою страну. По данным ВЦИОМ, чувство гордости за страну и проводимую политику охватывает 64% россиян (в 2024 году), что на 2% больше, чем в 2023. Абсолютное большинство наших сограждан гордятся Россией, её историей и культурой (92%) [16].

Вместе с тем выявились и **отрицательные последствия** политики импортозамещения:

- у отечественного производителя существенно возросли затраты на капитальные вложения, соответственно выросли траты на производство, это отразилось на росте уровня цен для конечного потребителя;
- пока еще слаба конкуренция, это не способствует ориентации на качество продукции, которое не только не соответствует импортным аналогам, но и ожиданиям потребителя;
- по сравнению с досанкционным периодом произошло сужение ассортимента товаров на торговых площадках и на полках магазинов.
- существенно возрос уровень субсидирования, выросли затраты бюджетов в инвестирование

на импортозамещение и наоборот, бюджеты недополучают часть доходов от введения льгот и часть налогового бремени объективно ложится на граждан;

- в недостаточной степени работает механизм стимулирования и поддержки сферы IT, специалисты отмечают провалы в работе данного механизма (продолжается отток кадров из-за относительно низких зарплат, слабой финансовой заинтересованности и проч.) и проч.

Среди прочих отрицательных качеств эксперты также отмечают расширение сферы влияния государства, органов местного самоуправления на бизнес в целом и предпринимательскую деятельность в частности, отмечается также усиление налогового контроля за деятельностью предпринимателей [1; 17, с. 557—71].

И, пожалуй, **главный вывод**: ориентация страны на полный переход к импортозамещению обеспечит изоляцию страны, существенное отставание в уровне технологического, экономического и социального развития. И этого допустить нельзя. Нужно укреплять международные, в том числе торговые связи и внимательно рассматривать предложения об аналогах товаров, комплектующих, деталях и проч.

Вместе с тем можно согласиться с мнением о том, что «импортозамещение — это процесс качественных экономических изменений на государственном уровне» [15, с. 108], который направлен на собственное инновационное развитие, достижение новых эффективных результатов и форм работы, тесно связан с повышением качества и обеспечением конкурентоспособности российских товаров и производителей.

Литература

1. Васянина Е.Л., Запольский С.В. Правовое регулирование финансового рынка России : монография / Под общ. ред. М.Н. Кобзарь-Фроловой. М. : ИГП РАН, 2023. 243 с.
2. Веселова Э.Ш. Импортозамещение: не допустить кампанейщины // ЭКО. 2015. № 3. С. 46—58.
3. Виноградова Е.В., Запольский С.В., Щукина Т.В. и др. Правовые инструменты обеспечения финансовой стабильности Российской Федерации : монография. Воронеж : ИПЦ «Новая книга», 2023. 354 с.
4. Евтушенков В. Импортозамещение без самоизоляции // Россия в глобальной политике. Т. 13. № 1. С. 197—205.
5. Как ЕС вводил санкции против России в связи с Украиной. URL: <https://tass.ru/info/18080751>, 24.06.2024.
6. Капустин А.Я. Международные модели регулирования конкуренции: к постановке проблемы // Журнал российского права. 2017. № 1. С. 15—24.
7. Кобзарь-Фролова М.Н. К вопросу о правовом регулировании инвестиционной деятельности в Российской Федерации // Государство и право. 2023. № 6. С. 109—116.
8. Кобзарь-Фролова М.Н. Теоретико-правовые и прикладные основы налоговой деликтологии : дис. ... д-ра юрид. наук. Люберцы : РТА, 2011.
9. Ленинский сборник XXXV. Проект «Исторические материалы». С. 127, 128, 138—139, 164.
10. Нуреев Р.М. Экономика развития: Модели становления рыночной экономики. М. : Норма, 2008. С. 26—37.
11. Редкоус В.М. К вопросу о формировании правовой основы импортозамещения в государствах — участниках СНГ // Юридическая гносеология. 2024. № 5. С. 36—44.
12. Редкоус В.М. Административно-правовые средства обеспечения импортозамещения государствах — участниках СНГ // Закон и право. 2024. № 12. С. 111—115.
13. Путин В.В. Выступление на пленарном заседании ПМЭФ. URL: <https://ria.ru/20140523/1009042783.html> (дата обращения: 28.04.2025).
14. Сморгочова Л.Н. К вопросу о методологии административно-правового регулирования в сфере экономики // Административное право и процесс. 2024. № 6. С. 15—18.

15. Титова О.В., Восканян Н.А. Импортозамещение: понятие, сущность, особенности // Инновационная экономика: перспективы развития и совершенствования. 2021. № 7 (57). С. 108.
16. У россиян крепнет чувство гордости за свою страну. Данные ВЦИОМ. URL: <https://dzen.ru/a/Zbrmm2uKWSIOT7Jc>
17. Щукина Т.В., Кобзарь-Фролова М.Н. Правовое регулирование процессов цифровизации в экономической деятельности государства и управленческой практике судебных органов, органов государственной власти // Вопросы экономики и права. 2021. № 9 (159). С. 57—71.
18. Prebisch R. Commercial Policy in the Underdeveloped Countries // American Economic Review. 1959. Vol. 49. Pp. 251–273.
19. Williamson J. The Washington Consensus Revisited / Economic and Social Development in the XXI Century / Ed. by L. Emmerij. Washington, DC: Inter-American Development Bank; Baltimore, MD: Distributed by the Johns Hopkins University Press, 1997. Pp. 48–80.

SECTION:
CONSTITUTIONAL LAW

THE IMPORT SUBSTITUTION POLICY AFTER 10 YEARS: EXPERIENCE, PROBLEMS, AND POSITIVE RESULTS

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

Keywords: *management, policy, economy, sanctions, competitiveness, business, stimulation, financing.*

Abstract

Purpose of the study: summing-up some results of the policy of Russia's government which took in 2014 a course towards import substitution.

Methods used in the study: the analytical, logical, historical-cum-legal methods, etc.

The importance of the study lies in its topicality, as well as in the author's analysis of measures taken as a result of introduction of a rough sanction policy by the countries of the collective West. A list of legal regulations is given where the measures are laid down aimed at stimulating and supporting Russian producers.

Study findings: summarising the administrative legal and financial economic measures taken for carrying on the import substitution policy. What is also new is that import substitution is considered not as an economic category or a regime but as a management category, as a part of socio-economic policy.

Research novelty: summarising the positive and negative aspects of the import substitution policy based on a 10 years' experience of its implementation, which, too, makes this study stand out among similar works.

References

1. Vasianina E.L., Zapol'skii S.V. Pravovoe regulirovanie finansovogo rynka Rossii : monografiia. Pod obshch. red. M.N. Kobzar'-Frolovoi. M. : IGP RAN, 2023. 243 pp.
2. Veselova E.Sh. Importozameshchenie: ne dopustit' kampaneishchiny. EKO. 2015. No. 3. Pp. 46–58.
3. Vinogradova E.V., Zapol'skii S.V., Shchukina T.V. i dr. Pravovye instrumenty obespecheniia finansovoi stabil'nosti Rossiiskoi Federatsii : monografiia. Voronezh : IPTs "Novaia kniga", 2023. 354 pp.
4. Evtushenkov V. Importozameshchenie bez samoizoliatsii. Rossiia v global'noi politike. T. 13. No. 1. Pp. 197–205.
5. Kak ES vvodil sanktsii protiv Rossii v sviazi s Ukrainoi. URL: <https://tass.ru/info/18080751>, 24.06.2024.
6. Kapustin A.Ia. Mezhdunarodnye modeli regulirovaniia konkurentsii: k postanovke problemy. Zhurnal rossiiskogo prava. 2017. No. 1. Pp. 15–24.
7. Kobzar'-Frolova M.N. K voprosu o pravovom regulirovanii investitsionnoi deiatel'nosti v Rossiiskoi Federatsii. Gosudarstvo i pravo. 2023. No. 6. Pp. 109–116.
8. Kobzar'-Frolova M.N. Teoretiko-pravovye i prikladnye osnovy nalogovoi deliktologii : dis. ... d-ra iurid. nauk. Liubertsy : RTA, 2011.
9. Leninskii sbornik XXXV. Proekt "Istoricheskie materialy". Pp. 127, 128, 138–139, 164.
10. Nureev R.M. Ekonomika razvitiia: Modeli stanovleniia rynochnoi ekonomiki. M. : Norma, 2008. Pp. 26–37.

11. Redkous V.M. K voprosu o formirovanii pravovoi osnovy importozameshcheniia v gosudarstvakh – uchastnikakh SNG. Iuridicheskaia gnoseologiya. 2024. No. 5. Pp. 36–44.
12. Redkous V.M. Administrativno-pravovye sredstva obespecheniia importozameshcheniia gosudarstvakh – uchastnikakh SNG. Zakon i pravo. 2024. No. 12. Pp. 111–115.
13. Putin V.V. Vystuplenie na plenarnom zasedanii PMEF. URL: <https://ria.ru/20140523/1009042783.html> (data obrashcheniia: 28.04.2025).
14. Smorchkova L.N. K voprosu o metodologii administrativno-pravovogo regulirovaniia v sfere ekonomiki. Administrativnoe pravo i protsess. 2024. No. 6. Pp. 15–18.
15. Titova O.V., Voskanian N.A. Importozameshchenie: poniatie, sushchnost', osobennosti. Innovatsionnaia ekonomika: perspektivy razvitiia i sovershenstvovaniia. 2021. No. 7 (57). Pp. 108.
16. U rossiian krepnet chuvstvo gordosti za svoiu stranu. Dannye VTsIOM. URL: <https://dzen.ru/a/Zbrmm2uKWSIOT7Jc>
17. Shchukina T.V., Kobzar'-Frolova M.N. Pravovoe regulirovanie protsessov tsifrovizatsii v ekonomicheskoi deiatel'nosti gosudarstva i upravlencheskoi praktike sudebnykh organov, organov gosudarstvennoi vlasti. Voprosy ekonomiki i prava. 2021. No. 9 (159). Pp. 57–71.
18. Prebisch R. Commercial Policy in the Underdeveloped Countries. American Economic Review. 1959. Vol. 49. Pp. 251–273.
19. Williamson J. The Washington Consensus Revisited. Economic and Social Development in the XXI Century. Ed. by L. Emmerij. Washington, DC: Inter-American Development Bank; Baltimore, MD: Distributed by the Johns Hopkins University Press, 1997. Pp. 48–80.

ИНФОРМАЦИОННОЕ ПРАВО И ЦИФРОВАЯ РЕАЛЬНОСТЬ: РАЗВИТИЕ, ПРИОРИТЕТЫ И ПРОБЛЕМЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ¹

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, технологическая политика.

Аннотация

Цель работы: исследовать проблемы и приоритеты развития информационного права в условиях цифровой трансформации и возрастающего значения достижения национального суверенитета России, реализации стратегических задач научно-технологического развития Российской Федерации.

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

Результаты исследования: информационное право рассматривается авторами как базовая отрасль для развития правового регулирования новых информационных отношений и цифровых пространств. Оно направлено на противодействие новым вызовам и угрозам, которые возникают перед государством, обществом и гражданином.

Научная новизна: в условиях цифровой трансформации на современном этапе необходим новый междисциплинарный подход к систематизации информационного законодательства (включая цифровое) в целях его упорядочивания для достижения информационного суверенитета. При этом особое значение приобретает проведение фундаментальных научных исследований и применение комплексного подхода к развитию цифровых платформ, государственных сервисов и услуг. Выявлено значение систематизации и кодификации информационного законодательства, разработки кодексов, необходимых для упорядочения информационного законодательства, что, в свою очередь, будет способствовать достижению информационного суверенитета Российской Федерации, развитию экономики данных и цифровой трансформации государства.

DOI: 10.24412/1994-1404-2025-2-31-41

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

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

В связи с реализацией новых национальных проектов, направленных на развитие экономики данных и цифровой трансформации управления, по мнению авторов, заслуживает особого внимания вопрос о месте информационного права, с учетом его генезиса и перспектив развития в системе публично-го права, как современного движителя развития этого нового научного направления с междисциплинарных позиций и публично-правовой (государственно-правовой) науки. На современном этапе важно развитие теории информационного права в целях формирования экономики данных для достижения стратегических задач, связанных с обеспечением национальных приоритетов в области научно-технологического развития и информационной безопасности, включая вопросы кибербезопасности.

В этой связи цифровая трансформация приобретает свои реальные контуры и представляет собой новую парадигму, которая не только трансформирует цифровые процессы, но и ставит задачу адаптации перед к изменяющимся условиям. Цифровая экономика определяет статус информационного права не просто как нового направления науки, но и как динамично развивающейся отрасли права, которая продолжает эволюционировать в государстве и правовой системе, включая в себя формирование экономики данных и решение стратегических вопросов национального суверенитета в информационной сфере, а также аспекты информационной безопасности и кибербезопасности в условиях цифровой среды [1, с. 160]. На современном этапе в условиях цифровой трансформации возникает необходимость осмысления проблем и перспектив развития публично-правовой науки, объединяющей совокупность практически самостоятельных научных направлений государственно-правовой науки и отраслей права. Особое значение приобретает развитие правовой доктрины. Сокращение (оптимизация) правовых научных специальностей в результате проведенной недавно в России реформы привела к интеграции различных научных направлений, составлявших традиционные отрасли права, такие как конституционное, административное, финансовое, налоговое, бюджетное, экологическое (включая земельное, аграрное и градостроительное), трудовое и информационное право [2, с. 103]. Необходимо признать, что на современном этапе одним из ключевых факторов, определяющих модернизацию правовых доктрин в условиях постоянно меняющегося мира, являются научные исследования общих основ правового обеспечения процессов цифровизации всех сфер жизнедеятельности человека и информационной безопасности. Эти исследования формируют горизонты этой отрасли под влиянием активного развития цифровых технологий в условиях геополитического кризиса. В этой связи информационное право приобретает значение универсального регулятора социальной действительности в условиях

формирования цифровой реальности. Как справедливо отмечает член-корреспондент⁴ РАН А.Н. Савенков, «в условиях... усиливающейся динамики развития информационного общества, «электронного государства», цифровой экономики, роста вызовов и угроз информационной безопасности особую роль играет формирование и реализация государственной политики, направленной на учет современных информационных тенденций развития всех сфер жизни общества и государства, выработку научно обоснованных, выверенных, взвешенных подходов регулирования новых информационных отношений» [3, с. 64].

В связи со 100-летием Института государства и права РАН, отмечаемом в 2025 г., роль и значение информационного права как составляющей публично-правовой (государственно-правовой) науки возрастает и требует осмысленного, обоснованного, но динамичного развития, также как усиление роли правового просвещения, правовой культуры и культуры информационной безопасности, а в целом — подготовки молодых ученых для информационного и уже цифрового будущего [4, с. 55].

Развитие информационного права в эпоху цифровизации: историческое наследие кибернетики, информатики и вызовы XXI века

Полагаем важным в рамках настоящего исследования обратить внимание на то, что в истории развития отечественного права правовая кибернетика и правовая информатика сыграли весьма важную роль. Эти науки активно применялись для изучения информационной сущности права и правовой системы в целом, а также архитектуры права. Справедливым является утверждение В.А. Копылова относительно того, что право и правовая система по своей природе являются информационными системами, которые основываются на создании, передаче и распространении нормативных правовых актов⁵. Кибернетика как научная дисциплина сформировалась в середине XX века, когда в 1948 г. Н. Винер опубликовал знаменитую книгу «Кибернетика»⁶, в которой подчеркнул информационную сущность управления, наличие движения информации в контуре регулирования. Следует отметить, что открытие, сделанное этим известным ученым в дальнейшем, оказало значительное влияние на множество областей, включая робототехнику, искусственный интеллект (ИИ), социологию и даже биологию. Но, к сожалению, в тот период в СССР кибернетика наряду

⁴ Пока готовилась статья, 30 мая 2025 г. А.Н. Савенков был избран действительным членом (академиком) РАН. Редакция нашего журнала поздравляет Александра Николаевича!

⁵ Копылов В.А. Информационное право: вопросы теории и практики. М. : Юристъ, 2003. С. 23.

⁶ Бродель Ф. История и общественные науки. Историческая длительность // Философия и методология истории / Общ. ред. И.С. Кона. М., 1977. С. 115—142.

с генетикой не была признана, а была объявлена лженаукой. Только в середине 1950-х гг. кибернетика как наука была признана и востребована. При Академии наук был создан Научный совет по комплексной проблеме «Кибернетика», который возглавил А.И. Берг, а вскоре в 1959 г. была создана секция «Кибернетика и право» под руководством Д.А. Керимова⁷. В Институте государства и права АН СССР (ИГП РАН) не было создано самостоятельного структурного подразделения по этим вопросам. Но эти вопросы были в фокусе внимания В.Н. Кудрявцева⁸, О.А. Гаврилова⁹, В.А. Леванского¹⁰ и целого ряда других исследователей [4, с. 26]. С тех пор кибернетика значительно расширила свои горизонты, пройдя несколько этапов развития. В 1960-х и 1970-х годах она объединилась в работы по системному анализу и моделированию, что способствовало созданию первых автоматизированных систем и технологий управления. В 1980-х и 1990-х гг., с развитием вычислительной техники и ростом интереса к информатике, кибернетика активно применяется в различных отраслях, таких как экономика, медицина и экология. Кибернетика как наука об общих законах управления продолжает развиваться, вписываясь в актуальные технологические тренды. На современном этапе кибернетика широко используется в различных областях, связанных с ИИ и машинным обучением, прежде всего в тех сферах, где алгоритмы управления и обработки информации становятся ключевыми для разработки интеллектуальных систем, развития робототехники, автоматизации производства и самоуправляемых транспортных средств, которые, несомненно, связаны с реализацией кибернетических принципов. Поэтому сегодня в условиях цифровой трансформации государственного управления возрастает значение кибернетики как науки управления. В этой связи необходимо отметить, что сегодня кибернетика признана ключевым компонентом не только в инженерных и научных исследованиях, но и в социальных науках, включая новые подходы к решению сложных мировых проблем и поиску устойчивого развития в условиях быстро меняющегося технологического ландшафта.

Информатика как наука начала формироваться в середине XX века, в связи с внедрением технических средств для обработки информации. Она изучает закономерности получения, отбора, хранения, передачи, преобразования и применения информации в производственной, научной, общественно-политической

и культурной деятельности людей¹¹. С одной стороны, наука изучает правовые аспекты информатики, а с другой — применяется для исследования правовой системы. По этому поводу Ф.Е. Темников отмечал: «Информатика — натуральная наука об информации вообще, состоящая из трех основных частей — теории информационных элементов, теории информационных процессов и теории информационных систем»¹². В развитие правовой информатики большой вклад внесли российские ученые: И.Л. Бачило, Ю.М. Батулин, А.Б. Венгеров, В.Б. Исаков, Д.А. Керимов, В.Н. Кудрявцев, П.У. Кузнецов, А.В. Морозов, Т.А. Полякова, Л.В. Филатова, С.С. Москвин, М.М. Рассолов, С.Г. Чубукова, Г.И. Элькин и другие. Несмотря на свою недолгую историю в качестве официальной научной дисциплины, информатика внесла фундаментальный вклад в науку и общество¹³. По сути, информатика наряду с электроникой является одной из основополагающих наук современной эпохи человеческой истории, которую принято называть информационной эпохой. В этой связи информатика занимает ведущую роль в информационной революции. Необходимо отметить, что кибернетика и информатика являются неотъемлемой частью информационного права и нашли широкое отражение в различных отраслях науки, создав базу, которая способствовала правовому регулированию в сфере информационных технологий [5, с. 25].

Как вполне справедливо отмечала И.Л. Бачило, «нелинейность развития информационных процессов в России выявляет проблемы, возникающие в ходе процессов информатизации»¹⁴. Очевидно, что постановка задач, связанных с познанием и развитием теории информационного права, а также его методологических основ, имеет фундаментальный характер. Это касается и вопросов о возрастающей роли информационного права в условиях технологического развития. Это самая молодая отрасль российского права, с достаточно четким определённым предметом и являющаяся комплексной по методам правового регулирования отношений, которые содержатся практически во всех правовых отраслях. В связи с этим вопрос о возрастающем значении информационно-правовой науки, её места в развитии юридической науки представляется исключительно значимым, и это касается не только публично-правовой науки, но и множества междисциплинарных институтов. Следует признать, этому послужили научные исследования в различных областях права. Вот уже более четверти века не только сохраняется, но и динамично развивается преемственность научной деятельности, связанной с развитием этого фундаментального научного направления, кото-

⁷ Андреев Н.Д., Керимов Д.А. О возможностях кибернетики при решении правовых проблем // Вопросы философии. 1960. № 7. С. 106—110; Керимов Д.А. Кибернетика и право // Советское государство и право. 1962. № 11. С. 98—104.

⁸ Кудрявцев В.И. О программировании процесса применения норм права // Вопросы кибернетики и право. С. 84—99.

⁹ Гаврилов О.А. Курс правовой информатики. Учебник для вузов. М.: НОРМА : ИНФРА-М, 2002. 432 с.

¹⁰ Леванский В.А. Моделирование в социально-правовых исследованиях. М.: Наука, 1986. 157 с.

¹¹ Советский энциклопедический словарь. М.: 1979. С.504.

¹² Михайлов А.И., Черный А.И., Гиляровский Р.С. Основы информатики. М.: 1968.

¹³ Копылов В.А. Информационное право: вопросы теории и практики. М.: Юрист, 2003. С. 29.

¹⁴ Бачило И.Л. Информационное право М.: Высшее образование : Юрайт-Издат, 2009. 454 с.

рое, на наш взгляд, по праву можно считать формированием научной школы информационного права в ИГП РАН [4, с. 45]. При этом в настоящее время, в период цифровой трансформации, в условиях принятия в России нового перечня научных специальностей, в котором информационное право включено в публично-правовую специальность, возрастает значение современных междисциплинарных, межатраслевых подходов к решению теоретико-методологических проблем, возникающих в информационном праве под влиянием цифровых технологий, искусственного интеллекта и машинного обучения, квантовых технологий, облачных вычислений, больших данных, виртуальной и дополненной реальности и др. [6, 7]. Полагаем важным в данном исследовании обратить внимание на вопросы, касающиеся роли информационного права в развитии правовой системы и правового регулирования отношений в области информационно-коммуникационных технологий, включая компоненты инфраструктуры и общественные процессы, технологии, информационные ресурсы и сетевые коммуникации, а также все отношения, связанные с использованием цифровых технологий и инноваций в законодательстве¹⁵. Начало XXI в. для России, учитывая динамику развития ИКТ-технологий, по сути, можно считать новым этапом формирования информационного общества, в теории и практике на основе анализа и междисциплинарных подходов, выявления проблем и приоритетов.

Как отмечает И.Л. Бачило в «Концепции Информационного кодекса Российской Федерации», разработанного более 10 лет назад в ИГП РАН, в России сформировалась отрасль информационного права и основы теории развития информационного общества. Именно в период с 2000 по 2013 гг. в нашей стране были заложены основы правового регулирования информационных отношений и кодификации информационного законодательства¹⁶. В ходе исследований сектора информационного права под ее руководством был выявлен ряд закономерностей и обоснованы выводы, положенные в основу доктрины информационного права. Это позволило разработать подходы к классификации проблем информатизации как процесса создания и усвоения продукции информационных технологий, формирования и использования информационных ресурсов, освоения и использования средств коммуникаций и т. д. Особое значение и сегодня имеют фундаментальные исследования генезиса развития информационного права, направленные на проблемы систематизации и кодификации информационного законодательства, требующие своего продолжения. Определенная новая важная веха развития связана с разработанной сектором в 2014 г. концепцией указанного кодекса, ставшей прорывом и получившей достаточно высокую оценку

в юридическом сообществе, в значительной степени не утратившей своего значения и сегодня, и является хорошим заделом для сохранения и, безусловно, дальнейшего развития научной школы информационного права в ИГП РАН. Как справедливо указывал М.А. Кудрявцев в своей статье в сборнике научных трудов первых бачиловских чтений «Новые горизонты информационного права»¹⁷, в которой выражал необходимость развивать предложенный им ранее и приобретший широкую известность тезис о роли информационного права в современной правовой системе как своеобразного «дирижера оркестра» правовой системы как таковой, т. е. одного из важнейших ее организующих начал, и обосновывал свою позицию тем, что «информационное право, помимо своих специальных отраслевых задач, имеет и универсальные правовые задачи»¹⁸. В настоящее время определяются современные тенденции значительного расширения ландшафта выделения в информационном праве, связанные с формированием межатраслевых институтов в условиях цифровой трансформации и развитием публично-правовой сферы, с учетом перспективных направлений и задач развития Российской Федерации [8]. Сегодня информационное право как научное направление активно развивается в условиях многочисленных дискуссий о его роли и месте в системе российского права, под влиянием научно-технологического развития в сложных условиях изменения мироустройства, оказывающих значительное влияние на информационную сферу и появление новых вызовов и угроз информационной безопасности. Безусловно, на развитие научных исследований в рассматриваемой сфере существенное влияние оказывает модернизация перечней научных специальностей, активное формирование системы субъектов информационного права влияющих на новые темы научных исследований [9, с. 97].

Исторический путь правовой информатизации в России. Значение НЦПИ в формировании правовой информатизации

В условиях цифровой трансформации управления и экономики данных новыми национальными проектами определены приоритетные задачи, однако их реализация в значительной степени зависит от развития национальной системы правовой информации; это подтверждает потребность общества в колоссальном расширении информационной сферы, требующая обеспечения национального суверенитета. Заслуживают отдельного внимания исследования генезиса развития правовой информатизации и роль Министерства юстиции России.

¹⁵ Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М. : ИГП РАН : Канон+ : РООИ «Реабилитация», 2014. С. 14.

¹⁶ Там же. С. 9.

¹⁷ Кудрявцев М.А. Новые горизонты информационного права. Информационное пространство: обеспечение информационной безопасности и право : сб. науч. трудов / Под. ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалева. М. : ИГП РАН, 2018. С. 94 — 112.

¹⁸ Там же. С. 100.

Информационная сфера колоссально расширяется, вопрос правовой информатизации в нашей стране и роль Минюста России становится важной. Именно правовая информатизация, как отмечает А.В. Морозов, направлена на повышение уровня правового информирования общества, обеспечивая органы государственной власти, должностных лиц и граждан актуальной и достоверной информацией о действующих законодательных и других правовых актах в условиях автоматизации информационных процессов. Это является одной из ключевых задач Минюста России как федерального органа исполнительной власти¹⁹. Вопрос о правовой информатизации встал в нашей стране еще в 70-х годах в связи с развитием автоматизированных систем управления (АСУ) различных уровней. Министерство юстиции СССР одним из первых начало применять новейшие технологии в области правового информирования. В 1973 г. во Всероссийском научно-исследовательском институте советского законодательства (ВНИИСЗ), который входил в структуру Минюста России, был создан сначала сектор информационно-поисковых языков, а затем отдел правовой информации, ставший впоследствии основой Научного центра правовой информации (НЦПИ), созданного 25 июня 1975 года²⁰. Одной из ключевых задач было определено создание общесоюзной системы правовой информации, состоящей из взаимосвязанных автоматизированных информационно-поисковых систем (АИПС). Сегодня мы отмечаем 50-летие НЦПИ, подчёркивая его роль как передовой системы, обладающей программным, техническим, лингвистическим и методическим обеспечением хорошего уровня. НЦПИ был, по сути, единственным учреждением, обеспечивающим высшие органы власти правовой информацией²¹. С 1991 г. в России активно развивалась правовая информатизация. В этой связи нельзя не отметить значение Концепции правовой информатизации России²², определившей задачи создания информационно-правовой системы, направленной на информатизацию правовой сферы и правовое регулирование общественных отношений в области информатизации. Кроме того, в 1999 г. Указом Президента Российской Федерации от 02.08.1999 № 954 было утверждено Положение о Министерстве юстиции Российской Федерации²³, в соответствии с которым на Минюст России возложен ряд полномочий по предоставлению правовой информации Президенту Российской Федерации и Правительству Российской Федерации, участие в разработке программ правовой информатизации, ведение государственного учета

нормативных правовых актов субъектов Российской Федерации.

Важной вехой в развитии правовой информатизации Минюста России является утверждение Концепции информатизации Министерства юстиции Российской Федерации, утвержденной Приказом Минюста России от 21.01.2000 № 10²⁴, определяющий основные направления и цели информатизации системы юстиции. Таким образом, была создана правовая основа для дальнейших инициатив и проектов, направленных на развитие и совершенствование правовой системы и доступности правовой информации. На основе этого приказа был разработан и внедрен ряд организационно-технических мероприятий, способствующих развитию электронных услуг и информационных технологий в системе юстиции, что, в свою очередь, позволило повысить уровень прозрачности и доступности правовой информации. При этом основной целью совершенствования системы информатизации является эффективное выполнение задач, стоящих перед Минюстом России, с использованием современных информационных технологий. В целях реализации государственной политики в сфере информатизации было утверждено постановление Правительства РФ от 29 ноября 2000 г. № 904 о ведении федерального регистра нормативных правовых актов субъектов Российской Федерации²⁵, направленное на упорядочение процедуры регистрации и учёта нормативных правовых актов, принимаемых органами государственной власти субъектов Российской Федерации, обеспечивающее централизованный учёт и доступ к правовой информации о нормативных актах, прозрачность правоприменительной практики и защиту прав и интересов граждан. Согласно этому положению данный регистр включает в себя все правовые акты субъектов Российской Федерации, в том числе и экспертные заключения о проведении правовой экспертизы. Это позволило создать основы для обеспечения систематизированного учета и оценки нормативных правовых актов субъектов Российской Федерации Минюстом России в целях повышения эффективности полномочий Минюста России по формированию единого информационно-правового пространства. Кроме того, информационно-технологическое обеспечение осуществлялось НЦПИ и центрами правовой информатизации Министерства юстиции Российской Федерации в различных субъектах Федерации. Для эффективного функционирования правовой системы в соответствии с Приказом Минюста России от 18 сентября 2000 г. № 273 был утвержден план мероприятий по реализации Указа Президента Российской Федерации

¹⁹ Морозов А.В. История правовой информатизации Минюста России на рубеже веков // Правовая информатика. 2013. № 1. С. 4.

²⁰ Там же. С. 4.

²¹ Там же. С. 6.

²² Указ Президента Российской Федерации от 28.06.1993 № 966 «О Концепции правовой информатизации России» (с изменениями и дополнениями) // Российские вести. 1993. № 132.

²³ Там же.

²⁴ Приказ Минюста России от 21.01.2000 № 10 «Об утверждении Концепции информатизации Министерства юстиции Российской Федерации». Документ опубликован не был.

²⁵ Постановление Правительства России от 29 ноября 2000 года № 904 (ред. от 26.03.2018) «Об утверждении Положения о порядке ведении федерального регистра нормативных правовых актов субъектов Российской Федерации» // Собрание законодательства РФ. 2000. № 49. Ст. 4826.

от 10 августа 2000 г. № 1486²⁶, который предусматривает, в целях обеспечения верховенства Конституции РФ и федеральных законов, реализацию конституционного права граждан на получение достоверной информации о нормативных правовых актах субъектов Российской Федерации, создание федерального банка нормативных правовых актов субъектов Российской Федерации — федерального регистра нормативных правовых актов субъектов Российской Федерации.

Безусловно, приоритетным было и развитие системы мониторинга правоприменения, включая его информационно-правовое обеспечение в целях достижения полноты и достоверности данных о состоянии законодательства, а также развитие Единого регистра нормативных правовых актов в системе мониторинга. Главной составляющей проведения государственной политики по формированию системы мониторинга правоприменения во исполнение Указа Президента Российской Федерации от 20.05.2011 № 657 «О мониторинге правоприменения в Российской Федерации»²⁷ является создание координирующего центра мониторинговой деятельности, а также определение субъектов государственного мониторинга на федеральном и региональном уровнях.

Важно отметить, что научные исследования в области информационно-правовых проблем развития правовой информации и информационных правовых систем проводились рядом ученых, среди которых следует отметить А.Б. Венгерова, В.А. Копылов, И.Л. Бачило, В.Б. Исакова, П.У. Кузнецова, А.В. Морозова, Т.А. Полякову, Л.В. Филатову и многих других. Эти исследования играют важную роль в совершенствовании правовых информационных систем в Российской Федерации. В условиях цифровой трансформации важна согласованность правотворческой деятельности в режиме реального времени. Безусловно, решение поставленных задач имеет как теоретическое, так и практическое значение не только для нормотворческой деятельности, но и для правоприменительной практики, учитывая, что под воздействием цифровых технологий система нормативных актов подвержена быстрым изменениям [14]. Минюстом России создан федеральный банк нормативных правовых актов субъектов Российской Федерации и ведется соответствующий регистр, включающий сегодня более 2,3 млн правовых актов. Важно, что к федеральному регистру обеспечен свободный доступ в электронном виде по каналам сети Интернет (сайт <http://pravo-minjust.ru>). Минюст России также проводит системный мониторинг доступа к муниципальному регистру, где сегодня насчитывается более

13,5 млн нормативных правовых актов муниципальных образований. Кроме того, всего в информационном банке данных содержится более 16,7 млн правовых актов. Необходимо учитывать исторически сложившийся опыт работы Министерства юстиции Российской Федерации как уполномоченного федерального органа исполнительной власти, осуществляющего на протяжении более 200 лет деятельность в области систематизации законодательства, аккумулирования значительных массивов правовой информации и выполнения ряда полномочий по правовому просвещению, правовому мониторингу и учету нормативных правовых актов федеральных органов исполнительной власти, электронных информационно-правовых ресурсов, относящихся к компетенции Минюста России.

Сегодня Министерство юстиции Российской Федерации в условиях цифровой трансформации активно применяет цифровые технологии для эффективной деятельности и улучшения качества предоставления госуслуг, а эта сфера очень динамично развивается. Одним из ключевых приоритетов является внедрение электронных систем и цифровых платформ, позволяющих гражданам и юридическим лицам получать доступ к разнообразным услугам в режиме онлайн. Возрастает значение интеграции цифровой трансформации, больших данных в условиях развития экономики данных на основе межведомственного взаимодействия. Ярким примером этого является регистр населения; соответствующий федеральный закон вступил в силу в 2025 г.

Очевидно, что цифровизация открывает новые горизонты для работы с правовой информацией и доступа к нормативным правовым актам, судебным решениям и другим документам, что необходимо для повышения правовой грамотности населения [18, 19]. Следует отметить, что в целях оптимизации и координации деятельности Минюста России в области правового просвещения утвержден ряд правовых актов, в которых определены принципы и содержание государственной политики в сфере развития правовой грамотности и правосознания граждан²⁸. Таким образом, цифровая трансформация Минюста России открывает множество инновационных возможностей, направленных на улучшение качества государственных услуг, повышение прозрачности и эффективности работы, а также на защиту прав граждан нового поколения.

Цифровая трансформация: право в эпоху цифровой реальности

Полагаем, что, несмотря на многочисленные дискуссии о приоритете сегодня задач по систематизации (кодификации) цифрового законодательства над информационным, его позиции только укрепляются. Его уже

²⁶ Указ Президента РФ от 10.08.2000 № 1486 (ред. от 26.12.2016) «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» // Собрание законодательства РФ. 2000. № 33. Ст. 3356.

²⁷ Указ Президента Российской Федерации 20.05.2011 № 657 «О мониторинге правоприменения в Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 20.02.2025.

²⁸ Основы государственной политики Российской Федерации в сфере развития правовой грамотности и правосознания граждан (утв. Президентом РФ 28.04.2011, № Пр-1168) // Российская газета. 14.07.2011. № 151.

рассматривают и как самостоятельную отрасль права, и не только как новое научное направление, но и отрасль инновационного характера, базовую в определенной степени и активно развивающуюся 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 кибербезопасности в цифровой среде [1, с. 162]. Развитие информационных и цифровых отношений обусловлено появлением новых субъектов и объектов в области информационного права, внедрением передовых технологий, созданием новых информационных пространств, а также необходимостью защиты интересов государства, общества и граждан от новых вызовов и угроз, возникающих в глобальном информационном пространстве [15]. Эти вопросы заслуживают не только пристального внимания со стороны государства, но и активного обсуждения в научном сообществе для развития теории информационного права. В связи с этим в современных условиях созрел вопрос о совершенствовании российской доктрины информационного права, информационного законодательства, а также международных правовых актов, направленных на регулирование цифровой среды. При этом в условиях активного развития технологической политики России в качестве приоритетных направлений выделены сквозные технологии, являющиеся ключевым фактором роста экономики и повышения уровня жизни населения. В последние годы внимание исследователей и практиков сосредоточено на сквозных технологиях как перспективных, ориентированных на межотраслевое использование и обеспечение создания инновационных продуктов и услуг. Эти технологии могут существенно повлиять на развитие экономики данных, кардинально меняя существующие рынки²⁹. По сути, сквозные технологии определяют перспективный облик экономики и отдельных отраслей на ближайшее будущее и перспективы [10, с. 131]. В этой связи появилась необходимость приведения законодательства в соответствие с потребностями цифровизации, «сквозных» информационных технологий и надёжного контроля за поддержанием глобальной информационной безопасности — одна из ключевых задач всех отраслей права [16, с. 139].

В рамках данного исследования нельзя обойти вниманием вопрос о том, что одной из ключевых задач и функций государства является обеспечение и защита национального суверенитета в информационном пространстве, поскольку сегодня очевидна необходимость

сосредоточиться на проблемах технологического суверенитета, связанных в первую очередь с обеспечением реализации политики импортозамещения. Ведутся также активные дискуссии относительно обеспечения цифрового суверенитета, сетевого, научно-технологического и т. д., хотя, по сути, все эти выделяемые виды суверенитета являются государственным (национальным) суверенитетом и связаны с правовым обеспечением информационной безопасности [11, с. 46]. Принцип суверенитета является по-прежнему одним из ключевых (базовых) принципов, закреплённых в Уставе ООН³⁰ в Декларации принципов построения информационного общества (2003)³¹ и др. Изучение политико-правовой ситуации, связанной с ростом угроз информационной безопасности и вызовами для права как на национальном, так и на международном уровнях, свидетельствует об острой необходимости разработки новых концептуальных подходов к вопросам защиты государственного суверенитета в информационном пространстве. Необходим обоснованный правовой ответ на данный вопрос в целях развития как национального, так и международного информационного права, обеспечения защиты государственного суверенитета в информационном пространстве. Неслучайно ст. 67 Конституции РФ дополнена частью 2.1: «Российская Федерация обеспечивает защиту своего суверенитета и территориальной целостности»³². Это свидетельствует о значении вопроса установления на конституционном уровне гарантий информационной безопасности и защиты суверенитета. Понятие обеспечения государственного суверенитета охватывает более широкий спектр вопросов, чем защита суверенитета. Такой подход требует комплексных междисциплинарных исследований и обоснований в условиях усиливающегося влияния процессов глобализации и мировых кризисов на суверенитет государств. Необходимо также четко определить, что такое суверенитет в информационной сфере и киберпространстве, а также какова взаимосвязь (соотношение) между информационным, цифровым и другими видами суверенитета, что требует фундаментальных исследований. В условиях современных геополитических трансформаций и глобальной технологической революции, а также в контексте экстерриториальности значительно возрастает значение цифрового суверенитета для обеспечения национальной

²⁹ Распоряжение Правительства РФ от 20 мая 2023 г. №1315-р «Об утверждении Концепции технологического развития на период до 2030 г.» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 20.02.2025; 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>, 10.04.2025.

³⁰ Устав Организации Объединённых Наций (с изм. на 16 сентября 2005 г.). Статут Международного Суда // Сборник действующих договоров, соглашений и конвенций, заключённых СССР с иностранными государствами. Вып. XII. М.: Госполитиздат, 1956.

³¹ Женевская декларация принципов «Построение информационного общества — глобальная задача в новом тысячелетии». Принята 12 декабря 2003 г. // Официальный сайт Организации Объединённых Наций. URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsiv.pdf (дата обращения: 27.09.2022).

³² О совершенствовании регулирования отдельных вопросов организации и функционирования публичной власти: Закон РФ о поправке к Конституции РФ от 14 марта 2020 г. № 1-ФКЗ // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 19.12.2025).

безопасности. В условиях цифровой трансформации важно не только определить проблемы, но и выработать приоритеты, рассмотреть перспективы правового регулирования и определить ключевые направления научных исследований в сфере информации. Представляется актуальной задача изучения соотношения между информационным правом и цифровым правом. Сегодня требуется объединение усилий в области обеспечения безопасности и формирования доверия, а также защиты информационного и правового пространства, поскольку любая правовая система является, по сути, информационной системой. В условиях цифровой трансформации вопросы информационной безопасности приобретают ключевое значение. Необходимо разработка концептуальных подходов, учитывающих изменения в информационном и киберпространстве. Это связано с реализацией стратегических целей по обеспечению национальной безопасности, включая вопросы информационной безопасности, отражающие состояние защищённости национальных интересов России. Это, в свою очередь, способствует защите конституционных ценностей и обеспечению суверенитета Российской Федерации в информационном пространстве [1, с. 170]. В условиях цифровой трансформации системы информационного права меняются как теоретические, так и классические подходы, проявляются различия в правовом регулировании и сорегулировании, возрастает значение этики, например, в робототехнике и технологиях искусственного интеллекта и т. д. Следует признать, что в качестве приоритетных направлений развития информационного права сегодня необходимо рассматривать разработку методологии (обоснование с позиции информационного права появления новых информационных, технологических и иных методов); обоснование институционализации правовых норм в области персональных данных, идентификации, аутентификации, конфиденциальности, информационной инфраструктуры, юридической ответственности, «цифровой зрелости» и др.; нового понятийного и терминологического аппарата, формирования системы обеспечения информационной безопасности, правового и иного регулирования в области ИИ и робототехники, модификация и актуализация классификаторов и рубрикаторов для систематизации законодательства на современном уровне, обеспечение доступности правовой информации, новых подходов к систематизации и кодификации информационного законодательства и др. [12, с. 21].

Цифровой или Информационный кодекс Российской Федерации? Трансформация информационного права в условиях цифровой реальности

Систематизация информационного законодательства является приоритетной задачей в реализации национальной программы «Экономика данных и цифровая трансформация государства», направленной

на достижение национальной цели развития цифровой трансформации государственного и муниципального управления, экономики и социальной сферы³³. В условиях цифровой трансформации и перехода к цифровой эпохе разработанная в 2014 г. концепция Информационного кодекса, безусловно, нуждается в современных подходах, основанных на новых концептуальных решениях в режиме реального времени. Как справедливо отмечает В.Д. Зорькин, «информационное законодательство в России нуждается в систематизации, это избавит от повторов и приведет его понятийный аппарат в стройное, непротиворечивое состояние и признает целесообразность принятия Информационного кодекса Российской Федерации»³⁴. Как уже отмечалось, сегодня всё чаще возникают многочисленные споры о необходимости Цифрового кодекса. Эти дискуссии отражают интерес специалистов и юристов к совершенствованию и развитию теоретической базы информационного права для формирования государственной политики и развития системы правового регулирования в этой области. Об этом свидетельствует и то, что на протяжении многих лет предпринимались различные попытки разработки концептуальных подходов к решению этой сложной задачи. В развитии информационного права предметом его регулирования являются общественные отношения в информационной сфере, возникающие при использовании цифровых технологий. Разработка и принятие Информационного кодекса необходимы для системного развития регулирования уже имеющихся цифровых отношений на уровне федерального законодательства, в целях упорядочения общественных отношений в сфере информационно-коммуникационных технологий, унификации правовых норм и устранения правовых пробелов и коллизий [13, 14]. Кодификация законодательства как высшая форма систематизации законодательства в теории государства и права — процесс сложный и долговременный, в рамках которого происходит не только обсуждение, моделирование проекта кодифицированного акта, но и прогнозирование последствий его принятия [17]. С нашей точки зрения, сегодня нецелесообразно рассматривать вопрос о формировании Цифрового кодекса, а тем более отдельной отрасли права. Следует признать, что в рамках информационного законодательства продолжается активное развитие процессов, которые постепенно переходят в цифровую область. Поэтому правовое регулирование в сфере цифровых технологий в настоящее время можно считать лишь активно развивающейся частью информационного права, поэтому оно не сможет полностью заменить Информационный кодекс. В условиях цифровизации информационная сфера яв-

³³ Национальный проект «Экономика данных и цифровая трансформация государства». URL: <http://government.ru/rugovclassifier/923/about/> (дата обращения: 31.05.2025).

³⁴ Зорькин поддержал идею создания информационного кодекса. URL: <https://ria.ru/20180529/1521642848.html?ysclid=mbdkkfwwlm407527562> (дата обращения: 31.05.2025).

ляется новым измерением, парадигмой для развития информационного общества, требующей новых фундаментальных научных исследований на основе применение комплексного подхода к цифровым платформам, сервисам и услугам.

Необходимо признать, что место информационного права в системе публичного права становится все более значительным: оно приобретает новые очертания в условиях цифровой реальности, несмотря на активные дискуссии якобы о сдаче его позиций перед цифровым правом; несомненно, необходимо правильно оценивать сохранение его позиций в российской правовой системе, учитывая как сложные проблемы его становления и развития, так и объективную консервативность в достижении цели

решения стратегических задач государственной информационно-правовой политики для достижения общественной стабильности и реагирования; оно неизбежно реагирует на трансформацию регулируемых общественных отношений, на новые вызовы, риски и угрозы, определяющие современную повестку и векторы развития.

В заключение необходимо отметить, что информационное право развивается во многом как публично-правовая отрасль, ориентированная на правовое обеспечение и функционирование информационной среды, в том числе и цифровой среды, а также направлено на защиту национального суверенитета и информационной безопасности Российской Федерации в информационной сфере.

Литература

1. Полякова Т.А., Минбалеев А.В., Наумов В.Б. Современные приоритеты развития информационного права: правовое обеспечение государственного суверенитета и информационной безопасности в информационном пространстве России // Государство и право. 2025. № 1. С. 160—173.
2. Полякова Т.А. Модернизация информационно-правовой науки в России в условиях цифровой трансформации // Право.by. 2023. № 6 (86). С. 101—106.
3. Савенков А.Н. Философия права и становление российского государства-цивилизации : монография. М. : Наука, 2024. 739 с.
4. Правовое обеспечение суверенитета и кодификации информационного законодательства : монография / Отв. ред.: Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : Институт государства и права РАН, 2024. 237 с.
5. Батурин Ю.М. Метаморфозы информационного права // Трансформация информационного права : монография / Отв. ред.: Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : Институт государства и права РАН, 2023. 256 с.
6. Карцхия А.А., Макаренко Г.И. Правовые горизонты технологий искусственного интеллекта: национальный и международный аспект // Вопросы кибербезопасности. 2024. № 1 (59). С. 2—14.
7. Карцхия А.А., Макаренко Г.И., Макаренко Д.Г. Правовые перспективы технологий искусственного интеллекта // В сб.: Безопасные информационные технологии. Сборник трудов XII Международной научно-технической конференции. М., 2023. С. 154—161.
8. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права // Государство и право. 2021. № 12. С. 97—108.
9. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Основные тенденции и проблемы развития науки информационного права // Государство и право. 2022. № 9. С. 94—104.
10. Троян Н.А. Роль правовой информации в Российской Федерации в условиях цифровой трансформации // Мониторинг правоприменения. 2024. № 2 (51). С. 131—139.
11. Полякова Т.А., Троян Н.А. Обеспечение суверенитета в информационном пространстве — стратегическая задача национальной политики // Правовая политика и правовая жизнь. 2024. № 1. С. 41—53.
12. Модели правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе : монография / Под общ. ред. д.ю.н., проф. Т.А. Поляковой. Саратов : Амирит, 2020. 254 с.
13. Троян Н.А. К вопросам систематизации российского законодательства: тенденции на современном этапе в условиях цифровизации // Право и управление. Научно-правовой журнал. 2025. № 2. С. 60—67.
14. 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.
15. Савенков А.Н. Философия права в России как идейно-теоретическая основа национальной правовой идеологии: история, современность и перспективы // Государство и право. 2023. № 8. С. 7—23.
16. Жуков В.И., Раттур М.В. Некоторые вопросы трансформации права в эпоху цифровизации: действующие нормы, отклонения и вектор развития // Государство и право. 2022. № 10. С. 129—140.
17. Полякова Т.А., Троян Н.А. Современные подходы к систематизации информационного законодательства России в условиях цифровизации: проблемы и перспективы развития // Мониторинг правоприменения. 2022. № 4 (45). С. 5—58.

18. Троян Н.А. Современный подход и перспективы развития правовой грамотности и правосознания граждан // Мониторинг правоприменения. 2017. № 3 (24). С. 77—85.
19. Рыбакова О.С. Право граждан на бесплатную юридическую помощь в системе конституционных ценностей Российской Федерации // Вестник МГПУ. Серия: Юридические науки. 2020. № 3 (39). С. 56—67.

SECTION:
CONSTITUTIONAL LAW

INFORMATION TECHNOLOGY LAW AND DIGITAL REALITY: DEVELOPMENT, PRIORITIES, AND PROBLEMS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Tat'iana Poliakova, Dr.Sc. (Law), Professor, 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, Honoured Lawyer of the Russian Federation, 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, knowledge intensive technologies, digital platforms, technological policy.*

Abstract

Purpose of the paper: studying problems and priorities of development of the information technology law in the context of digital transformation and increasing importance of achieving Russia's national sovereignty and implementing strategic tasks of research and technological development of the Russian Federation.

Methods used in the study: general scientific methods of analysis and synthesis as well as the system method allowing to analyse the genesis, state and problems of development of Russia's information technology laws in fields where digital technologies are used.

Study findings: information technology law is viewed by the authors as the basic branch of law for developing legal regulation of new information relations and digital spaces. It is aimed at countering new emerging challenges and threats to the state, society, and citizens.

Research novelty: in the context of digital transformation at the modern stage, a new interdisciplinary approach to systematising the information technology laws (including digital ones) is needed, with a view to its streamlining for achieving information sovereignty. What is of special importance is carrying out fundamental research and using a manifold approach to developing digital platforms, government as well as other services. The significance of systematisation and codification of information technology laws, development of codices necessary for their streamlining is identified, which, in turn, would contribute to achieving the information sovereignty of the Russian Federation, development of data economy and digital transformation of the government.

References

1. 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. 2025. No. 1. Pp. 160–173.
2. Poliakova T.A. Modernizatsiia informatsionno-pravovoi nauki v Rossii v usloviakh tsifrovoy transformatsii. Pravo.by. 2023. No. 6 (86). Pp. 101–106.
3. Savenkov A.N. Filosofiya prava i stanovlenie rossiiskogo gosudarstva-tsivilizatsii : monografiya. M. : Nauka, 2024. 739 pp.

4. Pravovoe obespechenie suvereniteta i kodifikatsii informatsionnogo zakonodatel'stva : monografiia. Otv. red.: T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava RAN, 2024. 237 pp.
5. Baturin Iu.M. Metamorfozy informatsionnogo prava. Transformatsiia informatsionnogo prava : monografiia. Otv. red.: T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : Institut gosudarstva i prava RAN, 2023. 256 pp.
6. 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.
7. Kartskhiia A.A., Makarenko G.I., Makarenko D.G. Pravovye perspektivy tekhnologii iskusstvennogo intellekta. V sb.: Bezopasnye informatsionnye tekhnologii. Sbornik trudov XII Mezhdunarodnoi nauchno-tekhnikeskoi konferentsii. M., 2023. Pp. 154–161.
8. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Razvitie nauki informatsionnogo prava i pravovogo obespecheniia informatsionnoi bezopasnosti: formirovanie nauchnoi shkoly informatsionnogo prava. Gosudarstvo i pravo. 2021. No. 12. Pp. 97–108.
9. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Osnovnye tendentsii i problemy razvitiia nauki informatsionnogo prava. Gosudarstvo i pravo. 2022. No. 9. Pp. 94–104.
10. Troian N.A. Rol' pravovoi informatsii v Rossiiskoi Federatsii v usloviakh tsifrovoy transformatsii. Monitoring pravoprimeneniia. 2024. No. 2 (51). Pp. 131–139.
11. Poliakova T.A., Troian N.A. Obespechenie suvereniteta v informatsionnom prostranstve – strategicheskaiia zadacha natsional'noi politiki. Pravovaia politika i pravovaia zhizn'. 2024. No. 1. Pp. 41–53.
12. Modeli pravovogo regulirovaniia obespecheniia informatsionnoi bezopasnosti v usloviakh bol'shikh vyzovov v global'nom informatsionnom obshchestve : monografiia. Pod obshch. red. d.iu.n., prof. T.A. Poliakovoi. Saratov : Amirit, 2020. 254 pp.
13. Troian N.A. K voprosam sistematizatsii rossiiskogo zakonodatel'stva: tendentsii na sovremennom etape v usloviakh tsifrovizatsii. Pravo i upravlenie. Nauchno-pravovoi zhurnal. 2025. No. 2. Pp. 60–67.
14. Poliakova T.A., Minbaleev A.V., Naumov V.B. K voprosu o kodifikatsii informatsionnogo zakonodatel'stva v usloviakh tsifrovoy transformatsii. Gosudarstvo i pravo. 2024. No. 1. Pp. 81–91.
15. Savenkov A.N. Filosofii prava v Rossii kak ideino-teoreticheskaiia osnova natsional'noi pravovoi ideologii: istoriia, sovremennost' i perspektivy. Gosudarstvo i pravo. 2023. No. 8. Pp. 7–23.
16. Zhukov V.I., Rattur M.V. Nekotorye voprosy transformatsii prava v epokhu tsifrovizatsii: deistvuiushchie normy, otkloneniia i vektor razvitiia. Gosudarstvo i pravo. 2022. No. 10. Pp. 129–140.
17. Poliakova T.A., Troian N.A. Sovremennye podkhody k sistematizatsii informatsionnogo zakonodatel'stva Rossii v usloviakh tsifrovizatsii: problemy i perspektivy razvitiia. Monitoring pravoprimeneniia. 2022. No. 4 (45). Pp. 5–58.
18. Troian N.A. Sovremennyi podkhod i perspektivy razvitiia pravovoi gramotnosti i pravosoznaniia grazhdan. Monitoring pravoprimeneniia. 2017. No. 3 (24). Pp. 77–85.
19. Rybakova O.S. Pravo grazhdan na besplatnuiu iuridicheskuiu pomoshch' v sisteme konstitutsionnykh tsennostei Rossiiskoi Federatsii. Vestnik MGPU. Serii: iuridicheskie nauki. 2020. No. 3 (39). Pp. 56–67.

О ПРЕДЕЛАХ ПРИМЕНЕНИЯ И ОСНОВАНИЯХ АДМИНИСТРАТИВНОГО ПРИНУЖДЕНИЯ

Запольский С.В.¹

Ключевые слова: право, правовое регулирование, правовое принуждение, превенция, пресечение, юридическая ответственность, публичные интересы, безопасность.

Аннотация

Цель работы: определение соотношения административного принуждения с правоохранительной деятельностью и пресечением правонарушений.

Методы исследования: сравнительное правоведение, метод социальных наблюдений, метод догматического толкования.

Результаты исследования: аргументировано предположение о более широком применении принуждения в целом и административно-правового принуждения, нежели только в рамках правового регулирования. По мысли автора, принуждение осуществляется и независимо от предполагаемого правонарушения, в целях обеспечения и защиты различных публичных интересов.

DOI: 10.24412/1994-1404-2025-2-42-46

Введение

Вопросы правового принуждения с учетом сложной социально-экономической обстановки в стране и международной напряженности приобретают особо важное значение.

Актуальность статьи предопределяется расширением сфер административно-правового принуждения на области управления экономикой в целом и ее отдельными частями, такими как налогообложение, таможенное дело, кредитно-банковские отношения и др. Кроме того, административно-правовое принуждение в силу необходимости применяется в борьбе с пандемиями, эпидемиями и эпизоотиями, в частности, в недавней профилактике КОВИД-19.

Принуждение — способ реализации права

Проблема правового принуждения, давно известная и, казалось бы, хорошо изученная, получила особую актуальность в последние годы ввиду новых вызовов как международного, так и внутреннего характера для безопасности нашей страны. Это — пандемия КОВИД-19, Специальная военная операция, террористические действия со стороны коллективного Запада, а также природные и техногенные катастрофы. В этих

условиях принудительное осуществление превентивных и пресекающих мер выходит на одно из важнейших направлений исполнительно-распорядительной деятельности, равно как и обеспечение безопасности общества.

В юридической литературе правовому принуждению в целом и административному принуждению в частности уделяется значительное внимание, но сущность принуждения пока не вызвала устойчивой, разделяемой большинством ученых определенности. К мерам принуждения нередко относят любые, в том числе технические меры. Ряд экспертов причисляют к мерам принуждения весь комплекс средств правового воздействия, за исключением убеждения и стимулирования; как правило, к принуждению относят и юридическую ответственность². Представляется, что и терминологически и сущностно правовое принуждение, особенно в его административном осуществлении, требует дополнительного анализа.

Общепринято мнение, что реализация права осуществляется в трех основных формах, а именно — соблюдения, использования и исполнения, отличаю-

² Общее административное право. Воронеж : изд-во Воронежского университета, 2007. С. 473—491.

¹ 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

щихся друг от друга степенью зависимости происходящего от правового воздействия³. При этом соблюдение и использование касаются поведения субъекта в его отношениях с равными ему или не равными, но не наделенными властными полномочиями, применение же права характеризует носителя властных полномочий публичного характера.

Во всех трех случаях реализация права предполагает возникновение правоотношений соответствующего вида и ту или иную степень взаимодействия и взаимопроникновения статуса, прав и юридических интересов участников этих отношений. Существенное значение имеет принадлежность предметов правоотношений к сферам экономики, межличностных связей или публичному управлению. Государственный, политический строй наделяет того или иного правосубъекта соответствующим комплексом прав и обязанностей в целях взаимодействия между собой и достижения эффекта правового урегулирования интересов субъектов-участников. Именно снятию конфликта, если таковой имеется, достижению гармонии интересов субъектов, получению социально-экономического эффекта служит реализация права в трех его способах правового регулирования.

Разделяя эту концепцию, зададимся вопросом о распространяемости правового регулирования на все без исключения сферы правового воздействия, особенно на те, которые в силу своих «генетических» особенностей предполагают ограничение прав человека, либо организации, сокращения средств защиты этих прав, а равно возможность использования права в особом (разрешительном) порядке.

В случае ограничения прав хотя бы одного субъекта отношения с другим субъектом, на наш взгляд, оставаясь правовыми, перестают отвечать признакам правового регулирования. Так, отношения больного эпидемиологической болезнью с администрацией лечебного учреждения не могут быть юридически равными и включают в себя административное принуждение в виде ограничения свободы не в связи с правонарушением, но по другим основаниям.

Речь может идти о существовании иного комплекса правового воздействия, нежели правовое регулирование, а именно правового принуждения. Парадоксально, но правовое регулирование не может охватить всю сферу правового воздействия хотя бы в силу того, что традиционное правовое регулирование служит инструментом гармонизации прав и интересов сторон правоотношений при сохранении правосубъектности и субъективного права, даже в случае его неудовлетворения полностью или частично. Правовое регулирование преследует цель реализации прав двух и более участников правоотношения, тогда как правовое принуждение рассчитано на реализацию права одного субъекта или группы субъектов, все из которых представляют одну управляющую сторону. Правовое при-

нуждение, более того, включает в себя ограничение прав и свобод соответствующих субъектов (другой стороны) в целях реализации прав и обязанностей соответствующих субъектов⁴.

Дабы не быть голословным, обратимся к ч. 3 ст. 55 Конституции РФ, которая допускает в поименованных случаях ограничивать права граждан. Напрашивается вопрос: какова цель этого ограничения? В каких-то случаях этого достаточно, чтобы обеспечить интересы, но более вероятно другое развитие событий — ограничение прав и свобод создает возможность осуществления неких малопопулярных, но необходимых действий и мероприятий. Так, в частности, развиваются события в случаях эпидемий, пандемий, природных катаклизмов и техногенных катастроф, а равно военных действий и других экстраординарных событий.

Скорее, события развиваются наоборот — сначала осуществляются эвакуационные и иные спасательные мероприятия, и только затем актами компетентных на то органов легализуются действия, ограничивающие права и свободы граждан и организаций. Иного, впрочем, не дано в упомянутых и многих других ситуациях, характерных недостатком времени и нарастающим публичных угроз и опасностей...

Роль принуждения в управлении

Для правового принуждения главным признаком служит временное или одномоментное, но исчерпывающее по глубине решений превалирование публичного интереса над частными интересами правосубъектов, ограниченное, пожалуй, только уголовным законом и нормами Конституции. Таким образом, здесь речь идет не о толковании хорошо известных общеправовых ценностей, но о признании существования в российском праве крупного правоприменительного комплекса, не являющегося правовым регулированием, но выполняющим не менее важные функции и выполняющим последние в экстраординарных случаях.

Небольшой экскурс в историю. В середине 1970 года в южных районах страны распространилась эпидемия холеры, потребовавшая энергичных и категоричных действий и решений медицинского характера, не имевших на то время никаких законодательных обоснований. Речь тогда шла об ограничении передвижения граждан, их интернировании, блокировании на продолжительное время пассажирских поездов в пустынных местностях и т. д. Наряду с признательностью медикам, предотвратившим эпидемию, а возможно, и пандемию, это породило общественный и научный резонанс, результировавший впоследствии в нормативные акты ведомственного характера. Но проблема не была решена еще долгие годы, вплоть до принятия Конституции РФ и появления в ней ст. 55.

В современных условиях, когда вероятность катастрофических природных явлений дополняется враж-

³ Алексеев С.С. Собр. соч., т. 8. 2009. С. 222.

⁴ Попов Л.Л. Административное право : учебник. 2004. С. 291.

дебным поведением коллективного Запада, ограничение прав и свобод граждан и организаций и правовое принуждение их, а также органов отраслевого управления, хозяйственных систем, муниципалитетов к согласованным действиям в публичных интересах из морально-нравственной категории превращается в обязанность конституционного характера. Скорее всего, мы говорим о правоприменительном комплексе, охватывающем разновеликие по характеру общественной значимости, отраслевой принадлежности, степени императивности, процедуре осуществления административно-правовые мероприятия. Их изучение крайне целесообразно для выработки принципов, правовых конструкций, оснований введения и осуществления государственного (публичного) принуждения с тем, чтобы снять с этого института флер экстраординарности, гармонизировать его с иными сферами правоприменения в форме регулирования и, самое главное, — предотвратить нарушения прав человека.

В литературе прослеживается тенденция понимать правовое принуждение как институт, всецело связанный с борьбой с правонарушениями; вне правоохранительных отношений применение принуждения не имеет основы⁵. Безусловно, правонарушение является необходимым фактором принуждения как средство превенции, пресечения делящегося, кара за совершенное и средство правосознания. Так, П.И. Кононов определяет правовое принуждение как деятельность властных органов и/или судов, направляемую на выявление правонарушений, пресечение этих действий, привлечение правонарушителей к ответственности⁶. Однако ограничивается ли правовое принуждение только сферой правоприменения? Обращение к ст. 55 Конституции РФ, на наш взгляд, позволяет признать принуждение следствием ограничения прав граждан и организаций вполне уместным и допустимым тогда, когда соответствующие публичные цели и интересы находятся в опасности и могут пострадать вследствие природных, техногенных и политических событий или даже опасности их возникновения. Если в случае правонарушения принуждение преследует умаление прав правонарушителя, то в других случаях возможно ограничение прав и применение правового принуждения и к правомерно действующим гражданам и организациям. Напрашивается предположение, что правовое принуждение — более широкий институт, нежели последствия правонарушения.

Ключевой позицией в определении природы правового принуждения должно быть решение вопроса о соотношении ограничения прав и свобод (ч. 3 ст. 55 Конституции РФ) с правовым принуждением. Ограничивая права и свободы, правоприменитель должен преследовать правомерную, более того, конституци-

онно значимую цель, очевидно, более высокой значимости, чем та, которая вытекает из права, подвергаемого ограничению. Правоприменитель, беря на себя эту функцию и эту ответственность, принимает обязанность достичь этой цели организационными, информационными и техническими средствами, недоступными иным субъектам.

О пределах правового принуждения

Достаточно ясно, что правовое принуждение, являясь «сквозной» категорией для всего права, концентрируется в его публичных отраслях — правовых комплексах, имеющих предметом публичные правоотношения. Для применения принуждения в частном праве характерно вторжение публичного регулирования в нехарактерную для него сферу, но с той же целью — защиты этим путем соответствующих прав и интересов. Таково, например, принуждение для заключения хозяйственного договора, применение мер ювенальной юстиции, обеспечение безопасности труда и ряд других мер. Не будет преувеличением считать, что всё принуждение относится целиком к административному праву как к таковому и к его интервенционным проявлениям в других регулятивных комплексах, таких как финансовое, банковское, иммиграционное, процессуальное, земельное право и, в строго ограниченном числе случаев, в гражданско-правовом регулировании⁷. Как юридический институт административно-правовое принуждение дополняет, а можно предположить — и восполняет пробелы правового регулирования в разных сферах социально-экономической жизни. Более того, принуждение «обогащает» правовое воздействие на поведение физических и юридических лиц, создавая альтернативу между цивилизованным и принудительными путями достижения целей общества и индивидуума в их гармонии.

Марксова мысль о том, что насилие есть повивальная бабка истории, вполне уместна для понимания сущности административного принуждения. Насилие в той или иной степени, характерное для возникновения любой политической формации, не исчезает вообще, но трансформируется, приобретая легальную форму системы мер административного принуждения. Одновременно возникает юридический предел (лимит) решения тех или иных социальных вопросов силовыми методами в рамках существующей правовой системы, для ужесточения которого потребуются законодательные меры.

Как представляется, институт административного принуждения, понимаемый как ограничитель применения силы, служит действенным средством демократизации государственного управления и нуждается в развитии и совершенствовании. Но для этого следовало бы решить две серьезные проблемы. Одна

⁵ Каплунов А.И. О классификации мер государственного принуждения // Государство и право. 2006. № 3. С. 11.

⁶ Кононов П.И. Этюды по административному праву и процессу. Киров, 2021. С. 108.

⁷ Общее административное право. Издание Воронежского университета. 2007. С. 473—491.

из них — формально очерченный круг мер административного принуждения, в который разные ученые включают несовпадающие и разнонаправленные меры правового характера. Так, авторы «Общего административного права» [1] считают, что административное принуждение делится на предупредительные меры и меры пресечения, относя к первой группе проверки соблюдения правил, проверка документов, досмотр вещей, карантин, а ко второй — административный надзор, принудительное лечение, применение огнестрельного оружия, административное задержание, изъятие опасного имущества у незаконного владельца. К административному принуждению относят также административно-восстановительные меры и охрану общественного порядка и общественной безопасности. Иное, более близкое к позиции автора этих строк мнение высказывал Л.Л. Попов⁸. Нередко считают, что принуждение служит только средством осуществления процессуального воздействия при судопроизводстве и исполнительном производстве. Очевидно, здесь требуется содействие законодателя, который сможет

определить исчерпывающий круг мер административно-правового принуждения.

Второй проблемой представляется правовой статус лица (физического или юридического), подвергнутого административному принуждению. На этот аспект впервые обратила внимание М.Б. Разгильдиева, поставив вопрос о правомерности понимания лица, претерпевающего административное принуждение, объектом правоотношения⁹. Если претерпевание есть третий эффект после ограничения субъективного права и административного принуждения, то есть все основания считать это состояние особым видом правового воздействия, рассчитанным на субъект права, несмотря на оправданное, нормирование и ограничение его прав и свобод.

В заключение следует отметить, что в силу новизны вопроса для полноценного понимания правового принуждения как параллельного правовому регулированию пути реализации права нужна серьезная дискуссия с участием представителей разных школ права и отраслей юридической науки. Автор лишь пытается привлечь внимание ученых-юристов на эту проблематику.

⁸ Попов Л.Л. Административное право : учебник. 2004. С. 134.

⁹ Разгильдиева М.Б. Финансово-правовое принуждение. Тамбов, 2011. С. 65.

Литература

1. Общее административное право. Воронеж : изд-во Воронежского университета, 2007. С. 473—491.
2. Алексеев С.С. Собр. соч., т. 8. 2009. С. 222.
3. Попов Л.Л. Административное право : учебник. 2004. С. 291.
4. Каплунов А.И. О классификации мер государственного принуждения // Государство и право. 2006. № 3. С. 11.
5. Кононов П.И. Этюды по административному праву и процессу. Киров, 2021. С. 108.
6. Спиридонов П.Е. Понятие, сущность и виды мер административно-процессуального принуждения // Вестник ВГУ. 2022. № 10. С. 150.
7. Разгильдиева М.Б. Финансово-правовое принуждение. Тамбов, 2011. С. 65.

SECTION:
CONSTITUTIONAL LAW

ON THE LIMITS OF AND GROUNDS FOR APPLYING ADMINISTRATIVE COERCION

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 Federation, Moscow, Russian Federation.

E-mail: adminlaw@igpran.ru

Keywords: law, legal regulation, legal coercion, prevention, suppression, legal responsibility, public interests, security.

Abstract

Purpose of the study: determining the relation between administrative coercion, law enforcement activities and suppression of law violations.

Methods used in the study: comparative law, social observation method, dogmatic interpretation method.

Study findings: the assumption on using coercion in general, and administrative coercion in particular, more broadly than just within the framework of legal regulation is argued. In the author's opinion, coercion is also carried out independently from the supposed violation of law, with a view to secure and protect various public interests.

References

1. Obshchee administrativnoe pravo. Voronezh : izd-vo Voronezhskogo universiteta, 2007. Pp. 473–491.
2. Alekseev S.S. Sobr. soch., t. 8. 2009. P. 222.
3. Popov L.L. Administrativnoe pravo : uchebnik. 2004. P. 291.
4. Kaplunov A.I. O klassifikatsii mer gosudarstvennogo prinuzhdeniia. Gosudarstvo i pravo. 2006. No. 3. P. 11.
5. Kononov P.I. Etiudy po administrativnomu pravu i protsessu. Kirov, 2021. P. 108.
6. Spiridonov P.E. Poniatie, sushchnost' i vidy mer administrativno-protssesual'nogo prinuzhdeniia. Vestnik VGU. 2022. No. 10. P. 150.
7. Razgil'dieva M.B. Finansovo-pravovoe prinuzhdenie. Tambov, 2011. P. 65.

АКТУАЛЬНОСТЬ ВОПРОСА КОДИФИКАЦИИ ЗАКОНОДАТЕЛЬСТВА, РЕГУЛИРУЮЩЕГО ОТНОШЕНИЯ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

Савченко Е.А.¹

Ключевые слова: информационное пространство, систематизация законодательства, нормативные правовые акты, цифровая трансформация, Интернет, инфраструктура, новые информационные технологии, национальные проекты.

Аннотация

Цель работы: определить понятие виртуального пространства, рассмотреть вопросы о возможности кодификации законодательства, регулирующего отношения в виртуальном пространстве.

Методы исследования: классические общенаучные и традиционные методы юридической науки.

Результаты исследования: принятие в 2025 году новых федеральных проектов цифровой трансформации актуализирует проблематику вопроса о кодификации законодательства, регулирующего отношения в виртуальном пространстве. Результатом исследования стали выводы о том, что целесообразна разработка именно Информационного (цифрового) кодекса в качестве комплексного кодифицированного акта, в котором отдельной главой будут регулироваться отношения в виртуальном пространстве. В числе задач кодификации законодательства, регулирующего отношения в виртуальном пространстве, — ликвидация повторов и пробелов, которых достаточно накопилось в законодательстве, регулирующем отношения в виртуальном пространстве.

DOI: 10.24412/1994-1404-2025-2-47-56

Систематизация законодательства «обусловлена постоянным изменением общественных отношений и необходимостью упорядочения нормативных правовых актов, устранения пробелов и противоречий»². Многочисленные нормативные правовые акты в сфере информации требуют систематизации этого массива актов. Развитие новых информационных технологий определяет практически всё: от качества жизни людей и условий развития экономической деятельности до национальной безопасности и эффективности оказания государственных услуг³.

В конце прошлого года на заседании Совета по стратегическому развитию и национальным проектам были подведены итоги выполнения ключевых общенациональных программ⁴ и утвержден Паспорт национального проекта «Экономика данных и цифровая транс-

формация государства»⁵, который должен быть реализован в период с 2025 по 2030 гг.

Паспорт национального проекта разработан во исполнение Указа Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» и включает в себя девять федеральных проектов:

- «Инфраструктура доступа к информационно-телекоммуникационной сети Интернет»,
- «Цифровые платформы в отраслях социальной сферы»,
- «Искусственный интеллект»,
- «Цифровое государственное управление»,
- «Отечественные решения»,
- «Прикладные исследования и перспективные разработки»,
- «Инфраструктура кибербезопасности»,
- «Кадры для цифровой трансформации» и «Государственная статистика».

² Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1 (110). С. 3—29.

³ 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.

⁴ URL: <http://www.kremlin.ru/events/president/transcripts/75762> (дата обращения: 05.02.2025).

⁵ Утвержден Протоколом заочного голосования членов президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 20 декабря 2024 г. № 12пр.

¹ Савченко Елена Алексеевна, кандидат юридических наук, научный сотрудник отдела социального законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Российская Федерация. ORCID: 0000-0001-8346-8829.

E-mail: elen_savchenko@bk.ru

В обновлённых федеральных проектах цифровой трансформации делается акцент на повышении прозрачности и эффективности государственного управления. Управленческие решения на всех уровнях должны приниматься на основе данных, что позволяет сделать уже накопленная информация. Вице-премьер — Руководитель аппарата Правительства Дмитрий Григоренко подчеркнул, что «доступ к качественным услугам не должен зависеть от географического положения граждан»⁶. В этих целях необходимо обеспечение высокоскоростного Интернета, развитие инфраструктуры мобильной и фиксированной связи в малонаселённых и труднодоступных населённых пунктах, развитие инфраструктуры обмена данными.

Кроме того, до конца 2025 года должны быть сформированы региональные программы цифровой трансформации, которые будут включать следующие региональные проекты:

- «Цифровые платформы в отраслях социальной сферы»,
- «Цифровое государственное управление»,
- «Отечественные решения».

В этих целях внесены изменения в государственную программу Российской Федерации «Информационное общество»⁷, вступившие в силу в январе 2025 года, касающиеся софинансирования расходных обязательств субъектов Российской Федерации, которые возникают при реализации региональных проектов, обеспечивающих достижение результатов федерального проекта «Цифровые платформы в отраслях социальной сферы».

В государственной программе акцентируется внимание на том, что «формирование информационного пространства должно иметь своей целью удовлетворение потребности граждан и общества в получении качественных и достоверных сведений, а также укрепление нравственных и патриотических принципов в общественном сознании»⁸.

Принятие новых федеральных проектов цифровой трансформации актуализирует проблематику вопроса о кодификации законодательства, регулирующего отношения в виртуальном пространстве.

Исследуя рассматриваемую тему, прежде всего нужно отметить, что нет устоявшегося понятия «виртуальное пространство». По мнению профессора Ю.А. Тихомирова, «виртуальное пространство представляет собой обозримую и воображаемую часть географического поля, доступную правовому освоению и регулированию»⁹.

⁶ URL: <http://government.ru/news/53746/> (дата обращения: 05.02.2025).

⁷ Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // *Собрание законодательства РФ* 05.05.2014, № 18 (ч. II), ст. 2159.

⁸ Там же.

⁹ *Право и виртуальное пространство : монография / О.О. Журавлева, П.П. Кабытов, О.В. Моцная и др.; отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2024. С. 14.*

По мнению автора, термин «виртуальное пространство», используемый в науке, идентичен также используемым терминам «киберпространство», «интернет-пространство», «кибернетическое пространство»¹⁰.

Источниками права, регулирующего отношения в виртуальном пространстве, являются:

- конституционные (например, ст. 71 Конституции РФ) и иные нормы национального законодательства (Гражданский кодекс РФ, Налоговый кодекс РФ, Трудовой кодекс РФ, Уголовный кодекс РФ, Кодекс РФ об административных правонарушениях, а также другие кодексы и иные федеральные законы, которые содержат положения, обеспечивающие регулирование и охрану отношений в виртуальном пространстве¹¹);
- международные регуляторы — конвенции, декларации, модельные акты, стандарты, регламенты;
- нормы саморегулирования бизнес-структур, научных организаций, отраслевых профессиональных ассоциаций и т. п.;
- технологические императивы — признанные, согласованные или «де-факто»¹².

Среди федеральных подзаконных источников, регулирующих отношения в виртуальном пространстве, отметим прежде всего указы Президента Российской Федерации, например, «О развитии искусственного интеллекта в Российской Федерации»¹³, и постановления Правительства Российской Федерации, например, о Единой цифровой платформе Российской Федерации «ГосТех»¹⁴. Значительный объем подзаконных актов регулирует вопросы защиты информации. Например, акты Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ) регулирующие отношения, связанные с использованием криптографии¹⁵.

¹⁰ Ефимова Л.Г. Источники правового регулирования общественных отношений в киберпространстве // *Lex russica*. 2020. № 3. С. 114—120.

Рассолов И.М. *Право и Интернет. Теоретические проблемы*. 2-е изд., доп. М. : Норма, 2009.

Грибанов Д.В. *Правовое регулирование кибернетического пространства как совокупности информационных отношений*: дис. ... канд. юрид. наук. Екатеринбург, 2003.

¹¹ Общие законы об информации, информационных технологиях и о защите информации; об электронной подписи; о связи; о персональных данных; о средствах массовой информации и др.); законы о цифровых финансовых активах, цифровой валюте; о совершении финансовых сделок с использованием финансовой платформы; об экспериментальных правовых режимах в сфере цифровых инноваций и др.; другие законы, содержащие отдельные положения, регулирующие отношения в виртуальном пространстве. Например, о государственной социальной помощи, о лицензировании отдельных видов деятельности и др.

¹² Там же.

¹³ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // *Собрание законодательства РФ*, 14.10.2019, № 41, ст. 5700.

¹⁴ Вайпан В.А. *Источники цифрового права* // *Вестник арбитражной практики*. 2024. № 1 (110). С. 3—29.

¹⁵ Например, приказ ФСТЭК России от 21.12.2017 № 235, приказ ФСБ России от 19.06.2019 № 282, приказ ФСБ России от 19.06.2019 № 281, устанавливающий порядок, технические условия установок

Как отмечает Ю.А. Тихомиров, «опыт показывает, что виртуальное пространство допускает использование государственного и международного регулирования, саморегулирования»¹⁶. Рассматривая международные регуляторы отношений в виртуальном пространстве, следует отметить модельные законы Межпарламентской ассамблеи СНГ¹⁷.

Однако «виртуальное пространство предполагает формирование комплексного нормативного массива, включающего не только правовые нормы»¹⁸, но и этические нормы¹⁹ и технические регуляторы²⁰, что «позволяет вести речь о формировании такой отрасли права, как виртуальное»²¹.

Например, ключевым событием I международного форума «Этика искусственного интеллекта (ИИ): начало доверия» стало подписание Кодекса этики искусственного интеллекта, который дал старт добровольному саморегулированию и внедрению инструмента «мягкой силы» в достижение согласия между ИИ и человеком.

В рамках технического направления научного знания развивается компьютерно-техническая трактовка виртуальной реальности (погружение и навигация субъекта в искусственно созданной при помощи компьютеров трехмерной среде, а также манипулирование ее объектами)²². Позволим предложить своё понимание данного термина.

Виртуальное пространство — это пространство обмена данными (данные — это поддающееся многократной интерпретации представление информации в формализованном виде, пригодном для передачи, связи или обработки)²³ между вычислительными устройствами — компьютерами, серверами²⁴, маршрутизатора-

ми²⁵ и другим оборудованием или программным обеспечением²⁶. В этой связи целесообразно обратиться к международному стандарту ИСО/МЭК 27033-1:2009²⁷, который определяет понятие «виртуальная вычислительная сеть» (VLAN и VPN)²⁸.

Виртуальная вычислительная сеть построена на использовании ресурсов другой физической сети:

- вычислительной (например, компьютерной сети),
- телефонной сети, и/или
- среды передачи данных²⁹.
- Исходя из этого следует согласиться с М.А. Рожковой, что в этом контексте можно говорить о «цифровой среде, которая включает в себя:
- информационные и коммуникационные технологии, в том числе Интернет,
- мобильные и связанные с ними технологии и устройства, а также
- цифровые сети, банки данных, контент и услуги»³⁰.

Однако, как правильно утверждает С.А. Сеницын, «цифровое пространство не может быть позиционировано как параллельный мир или реальность, а только как новые возможности и средства человеческих коммуникаций. По этой причине не представляется возможным согласиться с делением правового пространства на виртуальное и реальное, с вынесением цифрового субстрата за пределы регулируемых правом общественных отношений»³¹.

Поэтому на сегодняшний день основным вектором развития правового регулирования виртуального пространства является «дополнение действующих нормативных правовых актов, упорядочивающих отношения

и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак.

¹⁶ Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. Т. 27. № 3. С. 5—16.

¹⁷ Например, Модельный информационный кодекс для государств — участников СНГ, модельные законы о цифровом пространстве, о цифровой трансформации сферы услуг государств — участников СНГ (постановление № 55-10); о цифровых финансовых активах (постановление № 55-11); о цифровых правах (постановление № 55-12); о цифровом здравоохранении (постановление № 55-22) и др.

¹⁸ Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. Т. 27. № 3. С. 5—16.

¹⁹ Кодекс этики в сфере искусственного интеллекта.

²⁰ Например, ГОСТ Р ИСО/МЭК 24668-2022.

²¹ Право и виртуальное пространство : монография / О.О. Журавлева, П.П. Кабытов, О.В. Мощная и др.; отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2024. С. 15.

²² Орлов С.В. Виртуальная реальность как искусственно созданная форма материи: структура и основные закономерности развития // Философия и гуманитарные науки в информационном обществе. 2016. № 1 (11). С. 16.

²³ ISO/IEC 2382-1:1993 Информационные технологии. Словарь. Часть 1. Основные термины (2382-1:93 "Information technology – Vocabulary – Part 1: Fundamental terms"; NEQ).

²⁴ Программное обеспечение или специальное компьютерное оборудование.

²⁵ Специализированное устройство, которое пересылает данные на основе правил и таблиц маршрутизации.

²⁶ 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.

²⁷ Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1. Обзор и концепции» (ISO/IEC 27033-1:2009 "Information technology – Security techniques – Network security – Part 1: Overview and concepts").

²⁸ Виртуальная локальная вычислительная сеть (virtual local area network): независимая сеть, созданная с логической точки зрения внутри физической сети. «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» (утв. и введен в действие Приказом Росстандарта от 01.12.2011 № 683-ст).

²⁹ ГОСТ Р МЭК 61131-9-2017. Национальный стандарт Российской Федерации. Контроллеры программируемые. Часть 9. Одноточечный интерфейс цифровой связи для небольших датчиков и исполнительных устройств (утв. и введен в действие Приказом Росстандарта от 14.09.2017 № 1124-ст).

³⁰ Рожкова М.А. Виртуальная реальность и Метавселенная: предмет правового исследования // Закон.ру. 2021. 12 января. URL: https://zakon.ru/blog/2022/1/12/virtualnaya_realnost_i_metavselennaya_predmet_pravovogo_isследования_virtual_reality_and_metaverse (дата обращения: 05.02.2025).

³¹ Сеницын С.А. Личные неимущественные права и безопасность человека в виртуальном пространстве // Журнал зарубежного законодательства и сравнительного правоведения. 2023. № 1. С. 13—24.

в виртуальном пространстве»³². Но если рассматривать вопрос шире, а именно о кодификации значительного по объему законодательства, регулирующего информационные отношения, то, по мнению автора, такая необходимость возникла. Как известно, кодификация — это не только объединение и систематизация, но и переработка законодательства, имеющая целью обеспечение полноты регулирования соответствующих правоотношений. Задачей кодификации является также и ликвидация повторов и пробелов, которых достаточно накопилось в законодательстве, регулирующем информационные отношения.

Например, в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 года (далее Стратегия)³³ «искусственный интеллект» определяется через понятие «комплекс технологических решений», однако определение данного понятия в законодательстве отсутствует.

В соответствии со Стратегией в состав комплекса технологических решений включены: информационно-коммуникационная инфраструктура, программное обеспечение³⁴, процессы и сервисы по обработке данных и поиску решений. Понятие «информационно-коммуникационная инфраструктура» в законодательстве также отсутствует. В Стратегии всего лишь отмечается, что «дополнительными благоприятными факторами развития технологий искусственного интеллекта в России являются современная базовая информационно-коммуникационная инфраструктура», под которой в Стратегии понимается:

- 1) высокий уровень доступа к сети «Интернет»,
- 2) развитие сети радиотелефонной связи третьего и четвертого поколений
- 3) и доступность мобильной передачи данных.

Вызывает удивление, что, несмотря на широкое использование понятия «Интернет», единого легального определения этого понятия в российском законодательстве до сих пор нет.

В американском законодательстве дефиниция «Интернет» означает совокупность множества компьютерных и телекоммуникационных средств, в которых используется протокол управления передачей данных, т. е. интернет-протокол или любые предшествующие или последующие протоколы, для передачи информации всех видов по проводам или радио³⁵.

Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации было предложено определить структуру ООН, ответственную за разработку и внедрение правовых норм и стандартов в области управления Интернетом; компетенциями, необходимыми для исполнения такой роли, обладает Международный союз электросвязи (МСЭ). В нынешней схеме управления Интернетом государства играют декоративную роль, поэтому Россия последовательно выступает за введение управления Интернетом в сферу международного права³⁶.

Необходимо отметить, что в законах о связи³⁷, о средствах массовой информации³⁸ и ряде других акцентируется, что Интернет — это информационно-телекоммуникационная сеть. В соответствии с п. 4 ст. 2 Закона об информации³⁹ под информационно-телекоммуникационной сетью понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

В ст. 2 Модельного закона об основах регулирования Интернета⁴⁰ Интернет определяется как глобальная информационно-телекоммуникационная сеть, связывающая информационные системы и сети электросвязи различных стран посредством глобального адресного пространства, основанная на использовании комплексов интернет-протоколов (Internet Protocol, IP) и протокола передачи данных (Transmission Control Protocol, TCP) и предоставляющая возможность реализации различных форм коммуникации, в том числе размещения информации для неограниченного круга лиц.

Учёные, исследуя право на доступ в Интернет, считают, что только при наличии такого права есть гарантия реализации права на информацию, например, делая вывод о том, что «мы накануне международного признания нового фундаментального права — права на доступ в Интернет»⁴¹. Ряд учёных, анализируя содержание права на доступ в Интернет, в качестве его составляющих включают:

- качественный сервис и доступ к технологическим возможностям,
- свободу выбора и использования устройств и программного обеспечения, с которых осуществляется доступ,
- сетевую и технологическую нейтральность,

³² Анисимова А.С. Механизм правового регулирования интернет-отношений: проблемы теории и практики : дис. ... канд. юрид. наук. Саратов : Саратовская государственная юридическая академия, 2019. С. 15.

³³ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года).

³⁴ В соответствии с ГОСТ Р 51904-2002, программное обеспечение (ПО) — это совокупность компьютерных программ и программных документов, необходимых для эксплуатации этих программ.

³⁵ URL: <https://www.law.cornell.edu/uscode/text/15> (дата обращения: 12.02.2025).

³⁶ URL: <http://digital.gov.ru/ru/> (дата обращения: 12.02.2025).

³⁷ Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895.

³⁸ Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации» // Ведомости СНД и ВС РФ, 13.02.1992, № 7, ст. 300.

³⁹ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

⁴⁰ Принят в г. Санкт-Петербурге 16 мая 2011 г. постановлением 36–9 на 36-м пленарном заседании Межпарламентской Ассамблеи.

⁴¹ Талапина Э.В. Право на информацию в свете теории субъективного публичного права // Сравнительное конституционное обозрение. 2016. № 6 (115). С. 70—83.

- запрет дискриминации сетевого трафика и качества услуг,
- обеспечение максимального охвата для доступа с мобильных устройств в общественных местах⁴².

Нельзя не отметить и исследования конституционалиста Лоуренса Лессига, который подробно анализирует место Интернета в современной жизни⁴³.

Согласно ГОСТ Р 55387-2012⁴⁴ под услугой «доступ в Интернет» понимается совокупность действий оператора связи по подключению оконечного оборудования или локальной сети пользователя к сети оператора и обеспечению возможности доступа пользователю к ресурсам и услугам Интернет (веб-службам, передаче файлов по протоколу FTP и др.). Подробное нормативное регулирование доступа к сети Интернет содержится в Правилах телематических услуг связи⁴⁵ и в Правилах услуг по передаче данных⁴⁶. Доказывание отсутствия технической возможности для предоставления доступа к сети передачи данных лежит на операторе связи (абз. 4 п. 22, п. 23, 24 Правил телематических услуг связи). Под технической возможностью предоставления доступа к сети передачи данных понимается:

- одновременное наличие незадействованной монтированной емкости узла связи, в зоне действия которого запрашивается подключение пользовательского (оконечного) оборудования к сети передачи данных,
- и незадействованных линий связи, позволяющих сформировать абонентскую линию связи между узлом связи и пользовательским (оконечным) оборудованием.

К сожалению, легального определения телематических услуг связи нет. Анализируя законодательство в сфере связи, можно сказать, что это комплекс услуг, предоставляемых пользователям информационно-телекоммуникационной сети (за исключением услуг телеграфной и телефонной связи). Примером телематических услуг являются голосовая и электронная почта, факс, видео посредством Skype, видео- и аудиоконференции, учебные программы, видеоуроки и обучение в онлайн-режиме. Например, в определении Верховного Суда РФ от 12.12.2013 № АПЛ13-538 указано, что телематические услуги связи — это любые услуги связи, предусматривающие использование кибернетическо-

го пространства. Одним из видов оказания этих услуг является, в частности, предоставление доступа к сети Интернет.

В решениях Магаданского УФАС России от 21.12.2016 по делу № 04-30/143-2016, Приморского УФАС России от 29.05.2018 № 476/04-2018, в частности, отмечается: телематические услуги связи — это комплекс услуг, которые оператор предоставляет клиентам в части электронных коммуникаций, с присвоением каждому из них кода идентификации (адреса).

По мнению автора, телематические услуги связи — это:

- услуги связи, оказываемые оператором на основании соответствующей лицензии в соответствии с договором, заключенным с абонентом,
- с присвоением абонентам кода идентификации и обеспечивающие
- доступ к информационным системам информационно-телекоммуникационных сетей, в том числе к сети Интернет,
- прием и передачу телематических электронных сообщений, передачу сигналов оповещения и экстренной информации об опасностях, связанных с чрезвычайными ситуациями.
- Что касается услуг связи по передаче данных, то нужно отметить, что такие услуги подразделяются:
- на услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации,
- и услуги связи по передаче данных для целей передачи голосовой информации.

Легального определения услуги связи по передаче данных тоже нет; анализируя законодательство о связи, можно сказать, что передача данных — это перенос данных в виде сигналов от точки к нескольким точкам средствами электросвязи по каналу передачи данных, для последующей обработки средствами вычислительной техники. Примерами подобных каналов могут служить ВОЛС или беспроводные каналы передачи данных.

В соответствии с утратившим силу внутренним документом «Сети и службы передачи данных», утвержденным приказом Министерства РФ по связи и информатизации от 12.11.2001 № 225⁴⁷, под сетью передачи данных понималась совокупность узлов и каналов электросвязи, специально созданная для организации связей между определенными точками с целью обеспечения передачи данных между ними.

В постановлении Правительства РФ от 24.11.2014 № 1240⁴⁸ дается определение сети передачи данных органов власти, которые определяются как элемент

⁴² См. например: Хуснутдинов А.И. Право на доступ в Интернет в системе конституционных прав и свобод : дис. ... канд. юрид. наук; Щербович А.А. Реализация конституционных прав и свобод в Интернете. М. : ТЕИС, 2015. С. 147.

⁴³ См.: Lessig L. Code 2.0. URL: <http://codev2.cc/download+remix/Lessig-Codev2.pdf> (дата обращения: 01.02.25).

⁴⁴ Национальный стандарт Российской Федерации. Качество услуги «Доступ в Интернет». Показатели качества (утв. и введен в действие Приказом Росстандарта от 27.12.2012 № 2091-ст).

⁴⁵ Правила оказания телематических услуг связи, утв. постановлением Правительства РФ от 31.12.2021 № 2607 // Собрание законодательства РФ, 17.01.2022, № 3, ст. 579.

⁴⁶ Правила оказания услуг связи по передаче данных, утв. Постановлением Правительства РФ от 31.12.2021 № 2606 // Собрание законодательства РФ, 17.01.2022, № 3, ст. 578.

⁴⁷ Приказ Минсвязи России от 12.11.2001 № 225 // СПС «КонсультантПлюс». Документ не опубликован и утратил силу.

⁴⁸ Постановление Правительства РФ от 24.11.2014 № 1240 «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» // Собрание законодательства РФ. 01.12.2014. № 48. Ст. 6876.

инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, в целях осуществления государственных функций⁴⁹.

Возвращаясь к понятию информационно-коммуникационной инфраструктуры, необходимо отметить, что такое определение даётся только в проекте Концепции развития информационно-коммуникационной инфраструктуры и технологий в Российской Федерации, которая так и не была принята (далее — Концепция)⁵⁰. В соответствии с глоссарием Концепции, под информационно-коммуникационной инфраструктурой понимается совокупность информационных и коммуникационных инфраструктур. Под коммуникационной инфраструктурой понимается сетевая инфраструктура, обеспечивающая передачу информации между территориально распределёнными источниками и получателями, состоящая из

- линий связи, использующих различные среды распространения электромагнитных сигналов,
- и оборудования, обеспечивающего прием, передачу этих сигналов и их обработку в процессе этой передачи.

Под информационной инфраструктурой в глоссарии понимается взаимосвязанная совокупность информационных систем и подсистем.

Напомним, что, по мнению А.С. Пиголкина, «кодификация — это форма совершенствования законодательства по существу, и ее результатом является новый сводный законодательный акт стабильного содержания (кодекс, положение и т. п.), заменяющий собой ранее действовавшие нормативные акты по данному вопросу»⁵¹.

С.Н. Братусь акцентировал внимание на том, что кодификация является не единственной, но высшей формой систематизации, «поскольку кодекс — единый нормативный акт, построенный по определенной системе и регулирующий либо всю совокупность однородных общественных отношений, т. е. определенный их вид, либо, по крайней мере, основную, важнейшую часть таких отношений»⁵².

По мнению А.В. Мицкевича, именно «путем кодификации одновременно достигаются как цели обновления законодательства, так и цели его упорядочения»⁵³.

⁴⁹ Савченко Е.А. Правовое регулирование разрешительной деятельности в сфере связи : специальность 12.00.14 «Административное право; административный процесс» : дис. ... канд. юрид. наук / Савченко Елена Алексеевна, 2021. 168 с.

⁵⁰ URL: <http://digital.gov.ru/ru/documents/3464/> (дата обращения: 05.02.2025).

⁵¹ Систематизация законодательства в Российской Федерации / Под ред. А.С. Пиголкина. СПб. : Юридический центр Пресс, 2003. С. 47.

⁵² Братусь С.Н. Вступительная статья // Развитие кодификации советского законодательства. М., 1968. С. 3, 5.

⁵³ Мицкевич А.В. Некоторые общие проблемы систематизации хозяйственного законодательства // Научная конференция «Вопросы систематизации хозяйственного законодательства в СССР»: тез. докл. и сообщений, 26—27 мая 1969 г. / ВНИИСЗ. М., 1969. С. 3.

Идеи и проблемы кодификации законодательства в сфере правового регулирования использования, хранения и распространения информации давно обсуждаются в юридической науке⁵⁴. Прежде всего, необходимо уточнить понятийный аппарат.

Например, Е.А. Суханов отмечает, что термин «информация» является слишком общим и под ним можно понимать все, что угодно, в том числе завещание, договоры и расписки⁵⁵.

Кроме того, необходимо переработать законодательство, регулирующее всю совокупность однородных общественных отношений по поводу информации, поскольку на сегодняшний день «в составе информационного законодательства принято около 400 законов, регулирующих отношения по поводу информации»⁵⁶, в том числе и предоставляемой с помощью новых (цифровых) технологий.

По мнению И.Л. Бачило, под информационным кодексом нужно понимать «базовый закон отрасли информационного права, нормы и институты которого создают фундамент для полноценного развития информационного законодательства с учетом динамики процессов информационного общества и взаимодействия с другими структурами правовой системы России»⁵⁷. В особенную часть информационного кодекса можно включить уже сложившиеся институты⁵⁸. В общую часть должны быть включены определения, общие положения о регулировании новых отношений, которые обусловлены возникновением и внедрением цифровых технологий, и о безопасности информации.

Вопрос принципиально новых отношений, которые обусловлены возникновением и внедрением цифровых технологий, подробно исследован Т.Я. Хабриевой и Н.Н. Черногором. Ученые отмечают необходимость урегулирования отношений, связанных с появлением виртуальных (цифровых) личностей, прав человека в виртуальном (цифровом) пространстве, нетипичных объектов правоотношений, «прежде всего информации, цифровых технологий (например, финансовых и регулирующих) и создаваемых посредством их при-

⁵⁴ В качестве примера острой дискуссии о правовой природе цифрового права, возможности кодификации информационного (цифрового) законодательства и концепции Цифрового кодекса можно привести совместную научно-практическую конференцию (секцию) и экспертную сессию рабочей группы «Нормативное регулирование» АНО «Цифровая экономика» по теме «Правовое обеспечение цифрового суверенитета России: проблемы и перспективы (о цифровом праве и Цифровом кодексе)», которая состоялась 23 ноября 2023 г. на юридическом факультете МГУ имени М.В. Ломоносова в рамках XIII Московской юридической недели (см.: URL: https://www.youtube.com/watch?v=IKC1MMKuTRE&ab_channel=) (дата обращения: 05.02.2025).

⁵⁵ Абдиева Д.А. Систематизация законодательства в условиях перехода к новому технологическому укладу : дис. ... канд. юрид. наук.

⁵⁶ Бачило И.Л. Информационное право : учебник для вузов. 5-е изд., перераб. и доп. М. : Юрайт, 2023. 419 с.

⁵⁷ Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М. : ИГП РАН : Канон+ : РООИ «Реабилитация», 2014. С. 159.

⁵⁸ Подробно: там же. С. 160.

менения новых цифровых сущностей (например, криптовалют) и объектов материального мира»⁵⁹.

Таким образом, можно говорить о расширении состава как объектов информационного права, так и субъектов информационных правоотношений, что требует от юридической науки объединить выводы из естественных и гуманитарных наук. В.С. Степин подчёркивал, что «сегодня познавательное и технологическое освоение сложных саморазвивающихся систем начинает определять стратегию переднего края науки и технологического развития»⁶⁰. Нужно согласиться, что «нормы, регулирующие информационные отношения, включены во все отрасли системы права, они представляют собой комплексный нормативный правовой массив»⁶¹. По мнению С.С. Алексеева, информационное право относится именно к комплексным отраслям права, поскольку юридические особенности комплексной отрасли выражены не в специфических методах и механизмах регулирования, а в некоторых особых принципах и общих положениях⁶².

Как автор уже отмечал выше, к общим законам в исследуемом вопросе относятся законы: об информации, информационных технологиях и о защите информации; об электронной подписи; о связи; о персональных данных; о средствах массовой информации, которые содержат базовые нормы информационного законодательства, которые и могут войти в общую часть информационного кодекса.

Специальные же законы устанавливают те или иные особенности, например, закон о цифровых финансовых активах «устанавливает особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператора обмена цифровых финансовых активов»⁶³.

Таким образом, в основе отраслевых норм должны быть нормы общих законов (или общей части информационного кодекса), которые содержат базовые нормы информационного законодательства.

С.С. Алексеев акцентировал внимание на том, что, несмотря на то, что «нормы комплексной отрасли или института можно и нужно «распределять» по основным отраслям, «замкнуть» их только в рамках основных отраслей нельзя»⁶⁴. Нужно согласиться, что «природа и содержание общих (базовых) норм информационного законодательства обусловлены уникальностью

объектов соответствующих правоотношений»⁶⁵, что подчеркивает необходимость кодификации информационного (цифрового) законодательства.

Не удивительно, что в Стратегии развития отрасли связи Российской Федерации на период до 2035 года⁶⁶ говорится о необходимости систематизации отраслевого законодательства в целях установления:

- единых принципов регулирования отношений в сфере связи и информационно-коммуникационных технологий,
- создания единообразного понятийного аппарата,
- унификации правовых институтов,
- устранения пробелов и коллизий, особенно касающихся обеспечения информационной безопасности в сетях связи для Интернета вещей,
- актуализации нормативно-правовой базы услуг спутниковой связи.

По мнению автора, целесообразна разработка именно Информационного (цифрового) кодекса в качестве комплексного кодифицированного акта⁶⁷. Примером комплексной кодификации являются транспортные кодексы Российской Федерации⁶⁸.

Нужно согласиться с В.А. Вайпаном, что «все основные понятия и общие положения в сфере информационных и цифровых правоотношений, правовые принципы регулирования использования цифровых технологий и т. п. могут быть собраны в едином кодифицированном федеральном законе — Информационном (цифровом) кодексе»⁶⁹. В этих целях необходимо «рассмотреть возможность признания информационных, в т. ч. цифровых, отношений, в качестве однородного предмета регулирования для нового самостоятельного кодифицированного акта»⁷⁰.

Исходя из вышесказанного, сделаем следующие выводы:

1) рассматривая вопрос о кодификации законодательства, регулирующего отношения в виртуальном пространстве, под виртуальным пространством автор предлагает понимать пространство обмена данными между вычислительными устройствами — компьютерами, серверами, маршрутизаторами и другим оборудованием или программным обеспечением;

⁵⁹ Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 94—96.

⁶⁰ Степин В.С. Синергетика и системный анализ // Синергетическая парадигма. Когнитивно-коммуникативные стратегии современного научного познания. М., 2004. С. 61.

⁶¹ Кузнецов П.У. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 6. С. 154—161.

⁶² Антонова Е.Е. Правовое регулирование формирования и использования реестровой информации : дис. ... канд. юрид. наук.

⁶³ Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1 (110). С. 3—29.

⁶⁴ Алексеев С.С. Общая теория права. Т. 1. С. 256.

⁶⁵ Кузнецов П.У. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 6 (123). С. 154—161.

⁶⁶ Распоряжение Правительства РФ от 24.11.2023 № 3339-р «Об утверждении Стратегии развития отрасли связи Российской Федерации на период до 2035 года» // Собрание законодательства РФ, 11.12.2023, № 50, ст. 9094.

⁶⁷ Рожкова М.А. Является ли цифровое право отраслью права и ожидать ли появления Цифрового кодекса? // Хозяйство и право. 2020. № 4. С. 11.

⁶⁸ Например, Воздушный кодекс Российской Федерации от 19.03.1997 № 60-ФЗ // Собрание законодательства РФ, 24.03.1997, № 12, ст. 1383.

⁶⁹ Вайпан В.А. Понятие и правовая природа цифрового права // Право и бизнес. 2024. № 2. С. 10—17.

⁷⁰ Там же.

2) целесообразна разработка именно Информационного (цифрового) кодекса в качестве комплексного кодифицированного акта, в котором отдельной главой будут регулироваться отношения в виртуальном пространстве;

3) одной из основных задач кодификации законодательства, регулирующего отношения в виртуальном пространстве, будет являться ликвидация повторов

и пробелов, которых достаточно накопилось в законодательстве, регулирующем отношения в виртуальном пространстве; в частности, необходимо решить проблему «терминологического вакуума», например, дать легальное определение понятий таких понятий, как «информационно-коммуникационная инфраструктура», «Интернет», «телематические услуги связи» и «услуги связи по передаче данных в российском законодательстве».

Литература

1. Алексеев С.С. Общая теория права: в 2 т. Т. I. М., 1981. 359 с.
2. 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.
3. Право и виртуальное пространство : монография / Отв. ред. Ю.А. Тихомиров. М. : Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2024. 176 с.
4. Ефимова Л.Г. Источники правового регулирования общественных отношений в киберпространстве // Lex russica. 2020. № 3. С. 114—120.
5. Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. ... канд. юрид. наук. Екатеринбург, 2003.
6. Вайпан В.А. Источники цифрового права // Вестник арбитражной практики. 2024. № 1 (110). С. 3—29.
7. Тихомиров Ю.А. Креативные регуляторы в правовом и виртуальном пространстве // Журнал российского права. 2023. Т. 27. № 3. С. 5—16.
8. Орлов С.В. Виртуальная реальность как искусственно созданная форма материи: структура и основные закономерности развития // Философия и гуманитарные науки в информационном обществе. 2016. № 1 (11). С. 16—31.
9. Рожкова М.А. Виртуальная реальность и Метавселенная: предмет правового исследования // Закон.ру. 2021. 12 января. URL: https://zakon.ru/blog/2022/1/12/virtualnaya_realnost_i_metavselennaya_predmet_pravovogo_issledovaniya_virtual_reality_and_metaverse (дата обращения: 05.02.2025).
10. Сеницын С.А. Личные неимущественные права и безопасность человека в виртуальном пространстве // Журнал зарубежного законодательства и сравнительного правоведения. 2023. № 1. С. 13—24.
11. Анисимова А.С. Механизм правового регулирования интернет-отношений: проблемы теории и практики : дис. ... канд. юрид. наук. Саратов : Саратовская государственная юридическая академия, 2019.
12. Талапина Э.В. Право на информацию в свете теории субъективного публичного права // Сравнительное конституционное обозрение. 2016. № 6 (115). С. 70—83.
13. Хуснутдинов А.И. Право на доступ в Интернет в системе конституционных прав и свобод : дис. ... канд. юрид. наук. М., МГУ, 2024.
14. Щербович А.А. Реализация конституционных прав и свобод в Интернете. М. : ТЕИС, 2015. 147 с.
15. Савченко Е.А. Правовое регулирование разрешительной деятельности в сфере связи : дис. ... канд. юрид. наук. Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М., 2021. 168 с.
16. Систематизация законодательства в Российской Федерации / Под ред. А.С. Пиголкина. СПб. : Юридический центр Пресс, 2003. 380 с.
17. Братусь С.Н. Вступительная статья // Развитие кодификации советского законодательства. М., 1968. 247 с.
18. Мицкевич А.В. Некоторые общие проблемы систематизации хозяйственного законодательства // Научная конференция «Вопросы систематизации хозяйственного законодательства в СССР» : тез. докл. и сообщений. 26—27 мая 1969 г. ВНИИСЗ. М., 1969. 33 с.
19. Абдиева Д.А. Систематизация законодательства в условиях перехода к новому технологическому укладу : дис. ... канд. юрид. наук.
20. Бачило И.Л. Информационное право : учебник для вузов. 5-е изд., перераб. и доп. М. : Юрайт, 2023. 419 с.
21. Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М. : ИГП РАН : Канон+ : РООИ «Реабилитация», 2014. 192 с.
22. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 94—96.
23. Степин В.С. Синергетика и системный анализ // Синергетическая парадигма. Когнитивно-коммуникативные стратегии современного научного познания. М., 2004. 559 с.
24. Антонова Е.Е. Правовое регулирование формирования и использования реестровой информации : дис. ... канд. юрид. наук.

25. Кузнецов П.У. Комплексный подход к правовому регулированию общественных отношений в области цифровой экономики // Российский юридический журнал. 2018. № 6 (123). С. 154—161.
26. Рожкова М.А. Является ли цифровое право отраслью права и ожидать ли появления Цифрового кодекса? // Хозяйство и право. 2020. № 4. С. 3—12.
27. Вайпан В.А. Понятие и правовая природа цифрового права // Право и бизнес. 2024. № 2. С. 10—17.
28. Рассолов И.М. Право и Интернет. Теоретические проблемы. 2-е изд., доп. М. : Норма, 2009. 383 с.

SECTION:
CONSTITUTIONAL LAW

THE TOPICALITY OF THE QUESTION OF CODIFYING LAWS REGULATING RELATIONS IN VIRTUAL SPACE

Elena Savchenko, Ph.D. (Law), Researcher at the Social Legislation Division of the Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russian Federation. ORCID: 0000-0001-8346-8829.

E-mail: elen_savchenko@bk.ru

Keywords: *information space, systemisation of legislation, laws and regulations, digital transformation, Internet, infrastructure, new information technologies, national projects.*

Abstract

Purpose of the study: determining the concept of virtual space, considering questions of the possibility of codifying laws regulating relations in virtual space.

Methods used in the study: classic general scientific and traditional methods of legal science.

Study findings: new federal digital transformation projects passed in 2025 makes topical the problems of codifying laws regulating relations in virtual space. The study resulted in conclusions about the development of just the Information Technology Law (Digital) Codex as a manifold codified regulation which would regulate, in a separate chapter, relations in virtual space. Among the tasks of codifying laws regulating relations in virtual space, there is the one of eliminating repetitions and gaps already abounding in laws regulating relations in virtual space.

References

1. Alekseev S.S. Obshchaia teoriia prava: v 2 t. T. I. M., 1981. 359 pp.
2. Poliakova T.A. Vliianie tsifrovoy 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.
3. Pravo i virtual'noe prostranstvo : monografiia. Otv. red. Iu.A. Tikhomirov. M. : Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve Rossiiskoi Federatsii, 2024. 176 pp.
4. Efimova L.G. Istochniki pravovogo regulirovaniia obshchestvennykh otnoshenii v kiberprostranstve. Lex russica. 2020. No. 3. Pp. 114–120.
5. Griбанov D.V. Pravovoe regulirovanie kiberneticheskogo prostranstva kak sovokupnosti informatsionnykh otnoshenii : dis. ... kand. iurid. nauk. Ekaterinburg, 2003.
6. Vaipan V.A. Istochniki tsifrovogo prava. Vestnik arbitrazhnoi praktiki. 2024. No. 1 (110). Pp. 3–29.
7. Tikhomirov Iu.A. Kreativnye regulatory v pravovom i virtual'nom prostranstve. Zhurnal rossiiskogo prava. 2023. T. 27. No. 3. Pp. 5–16.
8. Orlov S.V. Virtual'naia real'nost' kak iskusstvenno sozdannaia forma materii: struktura i osnovnye zakonomernosti razvitiia. Filosofii i gumanitarnye nauki v informatsionnom obshchestve. 2016. No. 1 (11). Pp. 16–31.
9. Rozhkova M.A. Virtual'naia real'nost' i Metavselennaia: predmet pravovogo issledovaniia. Zakon.ru. 2021. 12 ianvaria. URL: https://zakon.ru/blog/2022/1/12/virtualnaya_realnost_i_metavselennaya_predmet_ppravovogo_issledovaniya_virtual_reality_and_metaverse (data obrashcheniia: 05.02.2025).
10. Sinitsyn S.A. Lichnye neimushchestvennye prava i bezopasnost' cheloveka v virtual'nom prostranstve. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia. 2023. No. 1. Pp. 13–24.
11. Anisimova A.S. Mekhanizm pravovogo regulirovaniia internet-otnoshenii: problemy teorii i praktiki : dis. ... kand. iurid. nauk. Saratov : Saratovskaia gosudarstvennaia iuridicheskaiia akademiia, 2019.
12. Talapina E.V. Pravo na informatsiiu v svete teorii sub'ektivnogo publichnogo prava. Sravnitel'noe konstitutsionnoe obozrenie. 2016. No. 6 (115). Pp. 70–83.

13. Khusnutdinov A.I. Pravo na dostup v Internet v sisteme konstitutsionnykh prav i svobod : dis. ... kand. iurid. nauk. M., MGU, 2024.
14. Shcherbovich A.A. Realizatsiia konstitutsionnykh prav i svobod v Internetе. M. : TEIS, 2015. 147 pp.
15. Savchenko E.A. Pravovoe regulirovanie razreshitel'noi deiatel'nosti v sfere sviazi : dis. ... kand. iurid. nauk. Institut zakonodatel'stva i sravnitel'nogo pravovedeniia pri Pravitel'stve Rossiiskoi Federatsii. M., 2021. 168 pp.
16. Sistematzatsiia zakonodatel'stva v Rossiiskoi Federatsii. Pod red. A.S. Pigolkina. SPb. : Iuridicheskii tsentr Press, 2003. 380 pp.
17. Bratus' S.N. Vstupitel'naia stat'ia. Razvitie kodifikatsii sovetskogo zakonodatel'stva. M., 1968. 247 pp.
18. Mitskevich A.V. Nekotorye obshchie problemy sistematzatsii khoziaistvennogo zakonodatel'stva. Nauchnaia konferentsiia "Voprosy sistematzatsii khoziaistvennogo zakonodatel'stva v SSSR" : tez. dokl. i soobshchenii. 26–27 maia 1969 g. VNIISZ. M., 1969. 33 pp.
19. Abdieva D.A. Sistematzatsiia zakonodatel'stva v usloviakh perekhoda k novomu tekhnologicheskomu ukladu : dis. ... kand. iurid. nauk.
20. Bachilo I.L. Informatsionnoe pravo : uchebnik dlia vuzov. 5-e izd., pererab. i dop. M. : Iurait, 2023. 419 pp.
21. Kontseptsiiia Informatsionnogo kodeksa Rossiiskoi Federatsii. Pod red. I.L. Bachilo. M. : IGP RAN : Kanon+ : ROOI "Reabilitatsiia", 2014. 192 pp.
22. Khabrieva T.Ia., Chernogor N.N. Pravo v usloviakh tsifrovoy real'nosti. Zhurnal rossiiskogo prava. 2018. No. 1. Pp. 94–96.
23. Stepin V.S. Sinergetika i sistemnyi analiz. Sinergeticheskaia paradigma. Kognitivno-kommunikativnye strategii sovremennogo nauchnogo poznaniia. M., 2004. 559 pp.
24. Antonova E.E. Pravovoe regulirovanie formirovaniia i ispol'zovaniia reestrovoy informatsii : dis. ... kand. iurid. nauk.
25. Kuznetsov P.U. Kompleksnyi podkhod k pravovomu regulirovaniu obshchestvennykh otnoshenii v oblasti tsifrovoy ekonomiki. Rossiiskii iuridicheskii zhurnal. 2018. No. 6 (123). Pp. 154–161.
26. Rozhkova M.A. Iavlaietsia li tsifrovoe pravo otrasl'iu prava i ozhidat' li poiavleniia Tsifrovogo kodeksa? Khoziaistvo i pravo. 2020. No. 4. Pp. 3–12.
27. Vaipan V.A. Poniatie i pravovaia priroda tsifrovogo prava. Pravo i biznes. 2024. No. 2. Pp. 10–17.
28. Rassolov I.M. Pravo i Internet. Teoreticheskie problemy. 2-e izd., dop. M. : Norma, 2009. 383 pp.

АКТУАЛЬНЫЕ ВОПРОСЫ СИСТЕМАТИЗАЦИИ ПРАВОВЫХ АКТОВ, ОБЕСПЕЧЕНИЯ ЕДИНСТВА ПРАВОВОГО ПРОСТРАНСТВА, ПРАВОВОЙ ПОМОЩИ И ПРАВОВОГО ПРОСВЕЩЕНИЯ¹

Троян Н.А.²

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

Аннотация

Цель исследования: изучить актуальные вопросы систематизации законодательства РФ, выявить проблемы и концептуальные пути их решения.

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: обращено внимание на необходимость систематизации российского информационного законодательства, упорядочение действующих законов, нормативных правовых актов и приведение всех юридических норм в единую правовую систему. Основное внимание уделяется концептуальному подходу к созданию Информационного кодекса, а также рассмотрению различных мнений по поводу правового регулирования информационных отношений. Исследуется также текущее состояние правового регулирования, выявляются его противоречия и пробелы.

Выводы: на современном этапе необходимы научно-теоретические подходы, которые будут способствовать фундаментальной системе различных правовых конструкций, систематизировать правовые отношения, информационные процессы в рамках информационно-правового пространства, обеспечивающего взаимодействие информационного законодательства с различными отраслями права.

Научная новизна: в условиях цифровых технологий необходимо эффективное взаимодействие между государственными органами, образовательными учреждениями и общественными организациями, которые способны создать безопасную информационную среду, в которой граждане смогут осознанно воспринимать информацию. Выявлено, что в процессе цифровой трансформации современные технологии воздействуют на все сферы жизни общества, генерируя при этом различные вызовы и угрозы. В этой связи необходимо разработать современные подходы к противодействию этим вызовам.

DOI: 10.24412/1994-1404-2025-2-57-65

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

² **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

Введение

В условиях цифровизации развитие общества связано с цифровыми технологиями, являющимися определяющим фактором экономики данных и цифровой экосистемы, что позволяет выделить новый вектор развития права, новые правоотношения, формирующиеся под влиянием цифровых технологий³. В этой связи современные технологии оказывают существенное влияние на развитие системы законодательства в России. В целях защиты прав и свобод человека и гражданина, совершенствования правовой системы Российской Федерации, повышения эффективности государственного управления и деятельности органов публичной власти, обеспечения национального суверенитета Российской Федерации, защиты национальных интересов от внешних и внутренних угроз в правовой сфере, а также создания безопасной информационно-правовой среды остро необходима систематизация законодательства в Российской Федерации⁴. В связи с этим в процессе цифровой трансформации особую актуальность приобретает вопрос создания необходимых условий и возможностей для расширения доступа и получения гражданами, организациями, органами публичной власти и общественными объединениями официальной и достоверной правовой информации, которая приобретает характер стратегического ресурса в системе цифровизации управления и профессиональной деятельности [1, с. 134]. Поэтому на современном этапе необходимо формирование единого информационно-правового пространства Российской Федерации, обеспечивающего достоверную правовую информированность [2, с. 76] всех государственных и общественных структур, граждан и юридических лиц⁵. Безусловно, в процессе цифровизации важна согласованность правотворческой деятельности в режиме реального времени. В этой связи решение задач по систематизации правовых актов, поставленных президентом Российской Федерации, имеет не только теоретическое, но и стратегическое значение, а также является приоритетным для правотворческой деятельности и правоприменительной практики. Это становится ключевой составляющей информационной и национальной безопасности. В настоящее время активно решаются задачи по систематизации законодательства России, регулирующего цифровые отношения, что

приобретает особую значимость в контексте развития конституционно-правовых основ, требований и необходимости модернизации системы законодательства. Проблемы цифровизации сегодня находятся на острие общественного внимания. Поэтому необходимо уделить должное внимание современным вопросам, связанным с нанотехнологиями, биотехнологиями, генетическими экспериментами, когнитивными технологиями и трансформацией социальных технологий. Актуальность этих вопросов возрастает в условиях, когда возникают потенциальные риски и угрозы, а также важные задачи, связанные с этическими и правовыми аспектами⁶. В этой связи необходимы новые подходы для закрепления на законодательном уровне социальных гарантий и обязательств государства по их обеспечению, наличие государственно-правового механизма предупреждения, минимизации (устранения) рисков и угроз. Социальную безопасность следует отнести к приоритетному виду национальной безопасности, которая выступает фактором социальной устойчивости государства, детерминантой реализации прав и свобод человека и гражданина, индикатором уровня жизни населения страны, каждого индивида в условиях отсутствия опасности, угроз и рисков повседневной жизни, сохранения и развития человеческого потенциала, системы жизнеобеспечения людей [3].

Влияние цифровых технологий на правовое просвещение в правовом пространстве: традиционные ценности и правовая культура

В связи с этим следует отметить, что одним из приоритетных направлений государственной политики являются традиционные ценности и правовая культура, которые рассматриваются как основа российского общества и укрепления суверенитета России. Эти задачи относятся к стратегическому планированию в области национальной безопасности Российской Федерации. Государственная политика по сохранению и укреплению традиционных ценностей реализуется в сферах образования и воспитания, работы с молодежью, культуры, науки и других областях⁷. При этом традиционными ценностями являются нравственные ориентиры, формирующие мировоззрение граждан России. В рамках приоритетных направлений основными информационными инструментами для реализации государственной политики в сфере традиционных ценностей являются взаимодействие со средствами массовой ин-

³ Карцхия А.А. Гражданский оборот и цифровые технологии : монография. М. : Филинь, 2019.

⁴ Цифровая трансформация и защита прав граждан в цифровом пространстве. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. URL: <https://ifap.ru/pr/2021/n211213a.pdf> (дата обращения: 31.05.2025).

⁵ Методические рекомендации по определению нормативности актов субъектов Российской Федерации и муниципальных правовых актов в целях ведения федерального регистра нормативных правовых актов субъектов Российской Федерации, Федерального регистров муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации (утв. Минюстом России) // СПС «КонсультантПлюс».

⁶ Цифровая трансформация и защита прав граждан в цифровом пространстве. Доклад Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека. URL: <https://ifap.ru/pr/2021/n211213a.pdf> (дата обращения: 31.05.2025).

⁷ Указ Президента РФ от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru>, 20.02.2025.

формации, социальными сетями, цифровыми платформами и поисковыми системами с целью размещения подробной, объективной и достоверной информации о реализации государственной политики в этой сфере⁸. Нравственно-правовое воспитание, выстраиваемое на основе общечеловеческих ценностей, оказывает влияние на качественное содержание правовой практики. Сегодня, в современных условиях формирования новой архитектуры многополярного мира реализация стратегических целей научно-технологического развития России невозможна без учета достижений российской научной мысли, результатов эволюции духовно-нравственной культуры. В связи с этим в настоящее время большое значение приобретают фундаментальные работы, нацеленные на решение крупных научных задач, имеющих значимый характер и позволяющих выработать перспективные модели создания и использования накопленных человечеством передовых знаний для решения широкого комплекса проблем в области общественного развития и раскрытия потенциала личности в современном мире, укрепления государственного суверенитета, совершенствования механизмов управления социальными процессами [4]. Процесс правового воспитания должен органично включаться в систему общегражданского воспитания и базироваться на формировании нравственного и религиозного сознания, активной жизненной позиции, патриотизма и здорового образа жизни. Государство должно учитывать эти факторы при осуществлении своей законодательной власти. Не менее важным представляется духовно-нравственное воспитание молодежи и укрепление традиционных ценностей, которые реализуются в области образования, воспитания и работы с молодежью, а также в культуре, науке, межрелигиозных отношениях, средствах массовой информации, массовых коммуникациях и международном сотрудничестве. Сегодня особенно важно осмысливать социальные, культурные и технологические процессы и явления с непосредственным учетом традиционных ценностей и накопленного культурно-исторического опыта. Это позволяет эффективно реагировать на новые вызовы и угрозы в информационном пространстве [5, с. 33; 6]. В России остро стоят проблемы правового просвещения, связанные с повышением уровня правовой культуры населения в информационной сфере. Сегодня необходимо разработать новый комплексный подход к решению этой задачи и обеспечить обучение граждан современным правилам поведения для повышения информационной безопасности⁹. Стратегической целью государственной политики в области повышения культуры информационной безопасности граждан является формирование у них навыков проти-

водействия угрозам информационной безопасности, в том числе информационно-психологическим угрозам [7], что будет способствовать повышению общего уровня грамотности по вопросам информационной безопасности. Особое внимание необходимо уделять гражданам в возрасте до 18 лет: именно эта возрастная группа крайне уязвима к различным угрозам информационной безопасности, особенно к травле в цифровом пространстве, в силу своего возраста, отсутствия необходимых знаний в области информационной безопасности, а также свободного использования сети Интернет¹⁰. Именно поэтому крайне важно обеспечение безопасности несовершеннолетних в социальной среде современного информационного общества. Исходя из необходимости и важности вопроса, необходимы условия, способствующие формированию информационной культуры у ребенка, требующие обновленных подходов, которые позволят противостоять рискам и угрозам информационного пространства. Это также поможет выработать так называемый социальный иммунитет и устойчивость личности ребенка к информационным рискам [8, 9]. Сегодня является приоритетной задачей развитие информационной культуры, что будет способствовать новому подходу к образованию и формированию критического мышления и медиаграмотности у детей. Для обеспечения поставленных задач необходима активная вовлеченность родителей и педагогов в этот процесс. Взаимодействие между государственными органами, образовательными учреждениями и общественными организациями поможет создать безопасную среду, в которой дети смогут осознанно воспринимать информацию. Таким образом, формируя социальный иммунитет, мы не только сможем защитить несовершеннолетних, но и поможем им стать активными и ответственными участниками современного информационного общества.

Цифровая трансформация и её влияние на систематизацию законодательства в информационной сфере: проблемы и перспективы

Систематизация законодательства в информационной сфере в условиях цифровой трансформации представляет собой актуальную и многогранную задачу, необходимость гармонизации законов в информационной сфере. Стремительное развитие цифровых технологий, появление новых классов и типов технологий требует постоянной актуализации законодательства, учета технических изменений и цифровой трансформации складывающихся общественных отношений. Изменение требований, предъявляемых к цифровым технологиям, детерминирует необходимость пересмотра подходов к механизмам регулирования цифровых отношений, их сочетания и использования с учетом ряда новых условий. В этой связи важно разработать

⁸ Там же.

⁹ Распоряжение Правительства Российской Федерации от 22.12.2023 № 4088-р «О Концепции формирования и развития культуры информационной безопасности граждан РФ» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 29.05.2025).

¹⁰ Там же.

не только концептуальные подходы к регулированию цифровых отношений в целом, но и создать новые, гибкие подходы для решения конкретных случаев. На современном этапе в процессе развития цифровых технологий, учитывая состояние правового регулирования и выявление имеющихся противоречий, пробелов, слабой системной связи правовых актов и норм в пределах источников права этой отрасли, состояние механизмов взаимодействия информационного законодательства с другими отраслями права ставит ряд вопросов методологического и теоретического характера¹¹. В связи с этим формируются новые подходы к правовому регулированию общественных отношений. Следовательно, эти подходы должны быть интегрированы в действующий механизм правового регулирования, способствующий обеспечению эффективности действия современных правовых норм. Поэтому важное значение имеет ряд вопросов, связанных с приведением понятийного аппарата в непротиворечивое состояние в информационном законодательстве, а также проработка вопросов роли дефиниций, которые используются в законотворческой деятельности, поскольку они оказывают влияние на правоприменительную и судебную практику в сфере информационных отношений [12]. Очевидно, что создание множества автоматизированных информационно-правовых систем как в государственном, так и в частном секторах существенно упрощает процесс поиска и применения нормативных актов. Очевидно, что цифровые технологии сегодня играют ключевую роль в деятельности государственных органов, а также организаций и учреждений, обеспечивая эффективное межведомственное взаимодействие и документооборот. Они выступают гарантами высокого качества жизни граждан и способствуют реализации их конституционных прав и свобод [10]. В современных условиях возникла острая необходимость в систематизации российского законодательства. В связи с этим представляется важным упорядочение действующих законов и других нормативных актов, а также приведение всех юридических норм в соответствие друг с другом. Немаловажным является создание единого правового пространства, обеспечение доступа к актуальной и достоверной правовой информации, устранение устаревших и неэффективных норм, а также разрешение юридических коллизий и пробелов в действующем законодательстве. В правовом государстве правовая система представляет собой достаточно сложную конструкцию из-за множественности органов, принимающих правовые акты, а также значительного объема правовых актов, создаваемых правотворческими органами. Поэтому в условиях цифровизации в режиме реального времени крайне важна согласованность правотворческой деятельности для эффективного развития системы информационно-

го законодательства, а также для решения вопросов, требующих безотлагательного вмешательства. Важно, чтобы правовая система была взаимосвязанной, что, в свою очередь, будет способствовать решению актуальных проблем систематизации законодательства и планирования законопроектной деятельности. Сегодня для более глубокой, детальной проработки и эффективности систематизации информационного законодательства России необходимо обратить внимание не только на предметные области правового регулирования, но и сосредоточиться на выборе методов правового регулирования. При этом следует учитывать, что данная область является комплексной, как по предметным областям, так и по методам регулирования [11—13]. На наш взгляд, в режиме реального времени необходимо обратить пристальное внимание на связь информационного права с другими правовыми сферами. При этом должны использоваться существующие юридические конструкции, термины, отсылающие к сложившимся институтам различных отраслей права¹². Сегодня в связи с лавинообразным развитием цифровых технологий очевидным представляется принимать во внимание технические изменения, цифровую трансформацию и новые общественные отношения. В этой связи необходимы новые концептуальные и гибкие подходы к правовому регулированию. Представляется важной задачей создание структурированной и логичной системы нормативных правовых актов, которая будет отличаться полнотой, доступностью и удобством в решении методологических подходов, и проведение комплексных научных разработок в области информационной безопасности и формирования правового пространства. Поэтому значимы вопросы, связанные с формированием единого информационно-правового пространства с учетом вызовов и угроз. Т.А. Полякова отмечает, что «это не просто современный тренд, а жизненная потребность объединить усилия в области безопасности и формирования пространства доверия, защиты информационного и правового пространства, так как любая правовая система является, по сути, и информационной системой» [14, с. 28]. Резюмируя данные вопросы, необходимо отметить, что сегодня наблюдается недостаточно высокий уровень правового обеспечения информационной безопасности и противодействия киберпреступности, поэтому необходима тщательная научная проработка проблемных вопросов. Следует отметить, что внедрение цифровых технологий, цифрового взаимодействия требует новых научных подходов и правовых методов, механизмов государственного управления при обязательном соблюдении требований обеспечения информационной безопасности [15]. В первую очередь цифровая трансформация влияет на механизмы информационно-правового и электронно-

¹¹ Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М. : ИГП РАН : Канон+ : РООИ «Реабилитация», 2014. С. 25.

¹² Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М. : ИГП РАН : Канон+ : РООИ «Реабилитация», 2014. С. 27.

го взаимодействия между государством и обществом, информационная инфраструктура национальной системы является особенно актуальной, способствуя повышению правовой информированности и культуры граждан. Важно отметить, что вопросы, связанные с повышением культуры информационной безопасности и правового просвещения, отражены в ряде стратегических документов и имеют стратегический характер¹³. В правовых актах отражена необходимость интеграции информационных технологий в государственное управление и общественные процессы, что, в свою очередь, способствует более высокому уровню правовой информированности граждан и их активному участию в информационном взаимодействии. Таким образом, необходимо отметить, что влияние цифровых технологий на систему государственного управления не только способствует эффективности взаимодействия, но и повышает уровень просвещения и информированности граждан в области правовых норм и информационной безопасности.

Использование технологий искусственного интеллекта для систематизации информационного законодательства: актуальные вопросы и перспективы

Сегодня необходимо признать, что искусственный интеллект (ИИ) является одним из ключевых направлений и передовых научно-технических отраслей, влияющих на развитие технологий и систем в информационном обществе и экономике данных. В этой связи основное применение технологий и систем ИИ, согласно национальной государственной информационной политике, должно стать двигателем для решения актуальных задач приоритетных направлений развития информационного общества, цифровой экономики, цифрового государственного управления и информационной безопасности¹⁴. В качестве основных стратегических приоритетов развития информационного общества и государственного управления в условиях цифровой трансформации определена систематизация информационного законодательства, являющаяся

приоритетным направлением в реализации национальной программы «Экономика данных и цифровая трансформация государства», направленной на достижение национальной цели развития цифровой трансформации государственного и муниципального управления, экономики и социальной сферы за счет обеспечения кибербезопасности, бесперебойного доступа к сети Интернет, подготовки квалифицированных кадров для ИТ-отрасли, цифрового госуправления, развития отечественных цифровых платформ, программного обеспечения, перспективных разработок и ИИ¹⁵; планируется урегулировать сквозные технологии для различных отраслей законодательства, вопросы, касающиеся идентификации субъектов правоотношений в цифровой среде, электронный документооборот, оборот данных, персональных данных¹⁶. Сегодня современные технологии, безусловно, представляют широкие возможности для развития нового эффективного экономического уклада. Сквозные технологии, такие как большие данные, нейротехнологии, технологии искусственного интеллекта, квантовые технологии, блокчейн, беспилотный транспорт, облачные вычисления, цифровое моделирование, цифровая медицина, виртуальные среды общения и другие [16, 17], создают новые условия для всех участников общественных отношений и требуют осмысления новых явлений и феноменов с точки зрения существующего механизма правового регулирования [18]. Современное информационное общество уже немыслимо без социальных сетей и электронных сервисов, поисковых систем, сети Интернет, электронной торговли, цифровых и облачных платформ, а также цифровых технологий, блокчейн и удаленных сервисов, применяемых в самых разнообразных сферах жизнедеятельности [19]. В связи с этим для достижения устойчивого экономического и социального развития России, укрепления суверенитета в сфере государственного управления и цифровой экономики, а также повышения качества жизни граждан на основе традиционных духовно-нравственных ценностей и обеспечения информационной безопасности, необходимо реализовывать комплексные программы, направленные на развитие инфраструктуры, внедрение современных технологий и создание привлекательного инвестиционного климата. Важно отметить, что научные исследования в области информационно-правовых проблем развития правовой информации и информационных правовых систем проводились рядом ученых, среди которых следует отметить: А.Б. Венгерова, В.А. Копылова, И.Л. Бачило, В.Б. Исакова, П.У. Кузнецова, А.В. Морозова, Т.А. Полякову, Л.В. Филатову и многих других. Эти исследования являются ключевыми в процессе совершенствования правовых информационных систем в России. Необходимо отметить

¹³ Распоряжение Правительства Российской Федерации от 22.12.2023 № 4088-р «О Концепции формирования и развития культуры информационной безопасности граждан РФ» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 29.05.2025); Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 25.05.2025); Указ Президента Российской Федерации от 02.07.2021 № 400 «О стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 25.05.2025); Указ Президента Российской Федерации от 2 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 05.05.2025).

¹⁴ Право искусственного интеллекта : учебник / Под ред. А.В. Минбалева. Саратов : Амрит, 2024. С. 97.

¹⁵ Национальный проект «Экономика данных и цифровая трансформация государства». URL: <http://government.ru/rugovclassifier/923/about/> (дата обращения: 31.05.2025).

¹⁶ Там же.

также выдающихся ученых, занимающих особое место в становлении и развитии информационного права и правовой регламентации цифровизации. Среди них особое внимание следует уделить трудам И.Л. Бачило, научного сотрудника Института государства и права РАН¹⁷, представителей её исследовательской школы (Т.А. Полякова, В.Б. Наумов, Г.Г. Камалова, А.В. Минбалеев и др.), учёных академического института, авторов учебников и фундаментальные исследования А.В. Маликова, А.Н. Савенкова, А.А. Тедеева, А.В. Габова и др.

На современном этапе, в условиях цифровой трансформации, особенно актуальной становится необходимость обеспечения согласованности правотворческой деятельности в режиме реального времени. Сегодня следует признать, что в современном законодательстве России, к сожалению, отсутствует Информационный кодекс Российской Федерации и его законодательное закрепление. Разработка модели Информационного кодекса Российской Федерации важна и по той причине, что всё чаще поднимается вопрос о возможности создания Цифрового кодекса. Нам представляется, что принятие Цифрового кодекса на данном этапе является преждевременным. На данный момент не сформировано полноценное цифровое законодательство, не установлен единый понятийный аппарат в области цифровой среды, а также отсутствует согласованный подход к механизму регулирования цифровых отношений¹⁸. Поэтому сегодня в условиях цифровой трансформации крайне важно предложение научных концептуальных подходов, касающихся улучшения информационного законодательства, требуются новые научно-теоретические подходы, которые позволят разработать адекватную систему правовых механизмов, способствующих не только оптимизации информационных процессов, но и упорядочению правовых отношений в рамках информационного пространства. Это обеспечит взаимодействие информационного законодательства с различными отраслями права. А.В. Минбалеев считает, что «для решения возникших задач система правового регулирования цифровых технологий должна отвечать следующим критериям: возможности быстрой адаптации к меняющимся

условиям правовой деятельности, т. е. быть гибкой; быть гибридной — содержать в себе не только правовые механизмы регулирования, но и саморегулирования; должна основываться на технико-юридическом (технологическом) методе правового регулирования; должна сформироваться система представлений об объектах цифровых отношений, субъектах таких отношений и их прав; быть гибкой к имплементации международных правовых норм, в системе должна быть развита роль межотраслевых институтов, которые позволяют обеспечить взаимодействие норм внутри различных отраслей права» [20, с. 230]. Справедливое мнение по этому поводу высказывает В.И. Жуков: «Приведение законодательства в соответствие с потребностями цифровизации, «сквозных» информационных технологий и надёжного контроля за поддержанием глобальной информационной безопасности — одна из ключевых задач всех отраслей права. Время для внесения изменений в действующее законодательство и принятия локальных правовых актов пришло. Необходима разработка Информационного кодекса Российской Федерации и модернизация на его основе действующих сводов законов» [21, с. 139].

В заключение необходимо отметить, что в условиях цифровой трансформации необходимо создать актуальную законодательную базу, которая позволит эффективно регулировать использование цифровых технологий и облачных платформ. Для перехода общества к цифровым технологиям и достижения цифрового суверенитета необходимы развитие организационно-правовых механизмов, защищенность цифровых данных и формирование информационной безопасной цифровой среды, обладающей высоким уровнем цифровой зрелости. Следует отметить, что цифровая трансформация сегодня не только оптимизирует деятельность государственных органов, но и создает эффективные условия для динамичного и безопасного развития информационного общества в целом, способствуя улучшению качества жизни граждан, открывает новые возможности для государственных институтов, обеспечивая высокую степень взаимодействия и участия граждан в управлении. Для решения ключевых задач необходимо сохранить баланс между инновационными подходами и вопросами информационной безопасности. Важно также учитывать этические аспекты и права человека в условиях цифровизации, что будет способствовать созданию эффективной и устойчивой системы государственного управления, способной оперативно реагировать на современные вызовы и угрозы, а также удовлетворять растущие потребности общества.

¹⁷ Бачило И.Л. Информационное право. Основы практической информатики. М., 2001; Бачило И.Л. Информационное право. Роль и место в системе права Российской Федерации // Государство и право. 2001. № 2. С. 5—14; Бачило И.Л. Информационное право: учебник для вузов. М.: Высшее образование: Юрайт-Издат, 2009. 454 с. Концепция Информационного кодекса Российской Федерации / Под ред. И.Л. Бачило. М.: ИГП РАН: Канон+: РООИ «Реабилитация», 2014. С. 14.

¹⁸ Минбалеев А.В. Проблемы цифрового права: учебное пособие / Под ред. А.В. Минбалеева. Саратов: Амрита, 2022. 233 с.

Литература

1. 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.

2. Троян Н.А., Петровская О.В. Принцип достоверности при распространении и предоставлении информации с использованием искусственного интеллекта // Правовая информатика. 2023. № 2. С. 75—81.
3. Рыбаков О.Ю., Рыбакова О.С. Социальная безопасность в контексте национальной безопасности Российской Федерации // В сб.: Основные тенденции развития современного права: проблемы теории и практики. Материалы IV Всероссийской научно-практической конференции (с международным участием). Под ред. Р.Ф. Степаненко, С.Н. Тагаевой. 2020. С. 20—24.
4. Савенков А.Н. Философия права и становление российского государства цивилизации : монография. М. : Наука, 2024. 739 с.
5. Полякова Т.А., Троян Н.А. Концептуальные подходы к развитию системы правового обеспечения информационной безопасности несовершеннолетних в Российской Федерации: нужен ли Кодекс детства? // Мониторинг правоприменения. 2023. № 3 (48). С. 30—40.
6. Троян Н.А. К вопросу об оказании бесплатной юридической помощи в субъектах Российской Федерации // Мониторинг правоприменения. № 2 (35). 2020. С. 59—64.
7. Смирнов А.А. Проблемы формирования системы правового обеспечения информационно-психологической безопасности // Труды Института государства и права Российской академии наук. 2022. № 1 (205). С. 153—155.
8. Рыбакова О.С. Информационная безопасность несовершеннолетних / Безопасность детства: социальные проблемы и правовые способы их решения : монография / Под ред. О.Ю. Рыбакова. М. : Проспект, 2021. 424 с.
9. Дубень А.К. Информационная культура молодежи как правовой механизм обеспечения безопасности // Аграрное и земельное право. 2024. № 5 (233). С. 119—121.
10. Полякова Т.А., Троян Н.А. Актуальные проблемы систематизации законодательства России под влиянием цифровых технологий в период цифровой трансформации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2023. № 2. С. 25—33.
11. Полякова Т.А., Минбалеев А.В., Наумов В.Б. К вопросу о кодификации законодательства в условиях цифровой трансформации // Государство и право. 2024. № 1. С. 81—91.
12. Полякова Т.А., Минбалеев А.В., Кроткова Н.В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права // Государство и право. 2021. № 12. С. 97—108.
13. 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.
14. Полякова Т.А., Троян Н.А. Современные подходы к систематизации информационного законодательства России в условиях цифровизации: проблемы и перспективы развития // Мониторинг правоприменения. 2022. № 4 (45). С. 50—58. DOI: 10.21681/2226-0692-2022-4-50-58 .
15. Полякова Т.А., Минбалеев А.В., Троян Н.А. Формирование культуры информационной безопасности граждан Российской Федерации в условиях новых вызовов: публично-правовые проблемы // Государство и право. 2023. № 5. С. 131—144.
16. Карцхия А.А., Макаренко Д.Г. Правовые аспекты статуса и рисков искусственного интеллекта // В сб.: Труды X Междунар. науч.-техн. конф. «Безопасные информационные технологии» (3—4 декабря 2019 г.) / МГТУ им. Н.Э. Баумана (НИУ). М. : МГТУ, 2019. С. 167—171.
17. 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 .
18. Троян Н.А. Теоретико-правовые вопросы систематизации законодательства. Цифровой или Информационный кодекс сегодня необходим в России / Трансформация информационного права : монография / Отв. ред.: Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М. : ИГП РАН, 2023. 256 с.
19. Макаренко Д.Г. Механизмы формирования доверия общества к институтам государственной власти // Мониторинг правоприменения. 2021. № 2 (39). С. 21—26. DOI: 10.21681/2226-0692-2021-2-21-26 .
20. Механизмы и модели регулирования цифровых технологий / Под общ. ред. А.В. Минбалеева. М., 2020. 256 с.
21. Жуков В.И., Раттур М.В. Некоторые вопросы трансформации права в эпоху цифровизации: действующие нормы, отклонения и вектор развития // Государство и право. 2022. № 10. С. 129—140.

TOPICAL QUESTIONS OF SYSTEMATISING LEGAL REGULATIONS, SECURING A SINGLE LEGAL SPACE, LEGAL AID, AND RAISING LEGAL AWARENESS

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: digital sovereignty, reliable information, digital transformation, public administration, challenges, threats, legal regulation, knowledge intensive technologies, digital platforms.

Abstract

Purpose of the study: studying topical questions of systematising the laws of the Russian Federation, identifying problems and ways for solving them.

Methods used in the study: general scientific methods of analysis and synthesis as well as the system method allowing to analyse the state and problems of development of Russia's information technology laws in fields where digital technologies are used.

Study findings: attention is drawn to a need for systematising Russia's information technology laws, streamlining the current laws and legal regulations, and consolidating all legal instruments in a single legal system. The main focus is made on the conceptual approach to creating the Information Technology Law Codex as well as considering different opinions concerning legal regulation of information relations. The current state of legal regulation is also studied, and its gaps and contradictions are identified.

Conclusions: at the present stage, scholarly theoretical approaches are needed which would contribute to creating a fundamental system of different legal constructions, systematise legal relations, information processes within the framework of information and legal space securing interaction between information technology laws and different branches of law.

Research novelty: in the context of digital technologies, it is necessary to ensure an efficient interaction between government agencies, education institutions, and civil society organisations which are able to create a secure information environment where citizens can consciously perceive information. It is found that in the process of digital transformation modern technologies impact all spheres of life of the society generating thus different threats and challenges. Therefore, it is necessary to develop modern approaches for countering these challenges.

References

1. 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.
2. Troian N.A., Petrovskaia O.V. Printsip dostovernosti pri rasprostranении i predostavlenii informatsii s ispol'zovaniem iskusstvennogo intellekta. *Pravovaia informatika*. 2023. No. 2. Pp. 75–81.
3. Rybakov O.Iu., Rybakova O.S. Sotsial'naia bezopasnost' v kontekste natsional'noi bezopasnosti Rossiiskoi Federatsii. V sb.: *Osnovnye tendentsii razvitiia sovremennogo prava: problemy teorii i praktiki. Materialy IV Vserossiiskoi nauchno-prakticheskoi konferentsii (s mezhdunarodnym uchastiem)*. Pod red. R.F. Stepanenko, S.N. Tagaevoi. 2020. Pp. 20–24.
4. Savenkov A.N. *Filosofia prava i stanovlenie rossiiskogo gosudarstva tsivilizatsii* : monografiia. M. : Nauka, 2024. 739 pp.
5. Poliakova T.A., Troian N.A. Kontseptual'nye podkhody k razvitiu sistemy pravovogo obespecheniia informatsionnoi bezopasnosti nesovershennoletnikh v Rossiiskoi Federatsii: nuzhen li Kodeks detstva? *Monitoring pravoprimereniia*. 2023. No. 3 (48). Pp. 30–40.
6. Troian N.A. K voprosu ob okazanii besplatnoi iuridicheskoi pomoshchi v sub'ektakh Rossiiskoi Federatsii. *Monitoring pravoprimereniia*. No. 2 (35). 2020. Pp. 59–64.
7. Smirnov A.A. Problemy formirovaniia sistemy pravovogo obespecheniia informatsionno-psikhologicheskoi bezopasnosti. *Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk*. 2022. No. 1 (205). Pp. 153–155.

8. Rybakova O.S. Informatsionnaia bezopasnost' nesovershennoletnikh. Bezopasnost' detstva: sotsial'nye problemy i pravovye sposoby ikh resheniia : monografiia. Pod red. O.lu. Rybakova. M. : Prospekt, 2021. 424 с.
9. Duben' A.K. Informatsionnaia kul'tura molodezhi kak pravovoi mekhanizm obespecheniia bezopasnosti. Agrarnoe i zemel'noe pravo. 2024. No. 5 (233). S.119–121.
10. Poliakova T.A., Troian N.A. Aktual'nye problemy sistemizatsii zakonodatel'stva Rossii pod vlianiem tsifrovyykh tekhnologii v period tsifrovoi transformatsii. Vestnik Universiteta imeni O.E. Kutafina (MGIU). 2023. No. 2. Pp. 25–33.
11. Poliakova T.A., Minbaleev A.V., Naumov V.B. K voprosu o kodifikatsii zakonodatel'stva v usloviakh tsifrovoi transformatsii. Gosudarstvo i pravo. 2024. No. 1. Pp. 81–91.
12. Poliakova T.A., Minbaleev A.V., Krotkova N.V. Razvitie nauki informatsionnogo prava i pravovogo obespecheniia informatsionnoi bezopasnosti: formirovanie nauchnoi shkoly informatsionnogo prava. Gosudarstvo i pravo. 2021. No. 12. Pp. 97–108.
13. 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.
14. Poliakova T.A., Troian N.A. Sovremennye podkhody k sistemizatsii informatsionnogo zakonodatel'stva Rossii v usloviakh tsifrovizatsii: problemy i perspektivy razvitiia. Monitoring pravoprimeneniia. 2022. No. 4 (45). Pp. 50–58. DOI: 10.21681/2226-0692-2022-4-50-58 .
15. Poliakova T.A., Minbaleev A.V., Troian N.A. Formirovanie kul'tury informatsionnoi bezopasnosti grazhdan Rossiiskoi Federatsii v usloviakh novykh vyzovov: publichno-pravovye problemy. Gosudarstvo i pravo. 2023. No. 5. Pp. 131–144.
16. Kartskhiia A.A., Makarenko D.G. Pravovye aspekty statusa i riskov iskusstvennogo intellekta. V sb.: Trudy X Mezhdunar. nauch.-tekhn. konf. "Bezopasnye informatsionnye tekhnologii" (3–4 dekabria 2019 g.). MGTU im. N.E. Baumana (NIU). M. : MGTU, 2019. Pp. 167–171.
17. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatii kiberbezopasnosti v usloviakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti. 2019. No. 3 (31). Pp. 18–23. DOI: 10.21681/2311-3456-2019-3-18-23 .
18. Troian N.A. Teoretiko-pravovye voprosy sistemizatsii zakonodatel'stva. Tsifrovoi ili Informatsionnyi kodeks segodnia neobkhodim v Rossii. Transformatsiia informatsionnogo prava : monografiia. Otv. red.: T.A. Poliakova, A.V. Minbaleev, V.B. Naumov. M. : IGP RAN, 2023. 256 pp.
19. Makarenko D.G. Mekhanizmy formirovaniia doveriia obshchestva k institutam gosudarstvennoi vlasti. Monitoring pravoprimeneniia. 2021. No. 2 (39). Pp. 21–26. DOI: 10.21681/2226-0692-2021-2-21-26 .
20. Mekhanizmy i modeli regulirovaniia tsifrovyykh tekhnologii. Pod obshch. red. A.V. Minbaleeva. M., 2020. 256 pp.
21. Zhukov V.I., Rattur M.V. Nekotorye voprosy transformatsii prava v epokhu tsifrovizatsii: deistviushchie normy, otkloneniia i vektor razvitiia. Gosudarstvo i pravo. 2022. No. 10. Pp. 129–140.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ДЕЯТЕЛЬНОСТИ МИНЮСТА РОССИИ

Токолов А.В.¹

Ключевые слова: правовой анализ, инновационные подходы, методы системного анализа, информационное общество, Министерство юстиции, информационная база данных законодательных актов.

Аннотация

Цель работы: определить потенциал применения технологий искусственного интеллекта (ИИ) в формировании Свода законов в машиночитаемой форме.

Методы исследования: общенаучные методы системного анализа, аналогии, историзма, позволяющие провести анализ действующего законодательства в конкретном регистре нормативных правовых актов.

Результаты исследования: исследованы современные полномочия, а также перспективные направления развития системы правовой информации Министерства юстиции РФ. Особое внимание уделяется инновационному подходу, заключающемуся в активном применении передовых технологий ИИ. Отмечено, что посредством использования технологий ИИ, в соответствии с государственной программой «Юстиция», предусматривается возможность создания Свода законов Российской Федерации.

Технологии ИИ в деятельности Минюста РФ должны предоставлять возможности охватывать, обрабатывать и анализировать содержание баз данных правовых актов, принятых на федеральном, региональном и местном уровне.

Практическая значимость: результаты исследования могут быть использованы для разработки Свода законов Российской Федерации.

DOI: 10.24412/1994-1404-2025-2-66-71

Введение

Технологии искусственного интеллекта (ИИ), внедряемые в работу Министерства юстиции Российской Федерации (далее — Минюст России, Министерство юстиции), должны обладать высокой степенью точности и надежности, что позволит своевременно обнаруживать и устранять юридические несоответствия, способные влиять на правоприменительную практику и законность в стране.

Применяемыми в деятельности Минюста России технологиями ИИ должны выявляться коллизии, пробелы и противоречия, содержащиеся в нормативных правовых актах различной юридической силы.

ИИ должен осуществлять анализ опыта судебной деятельности и статистических данных по использованию определенных юридических механизмов правоприменения, что, в свою очередь, позволит обеспечить более высокий уровень правовой защиты и справедливости в обществе. При осуществлении государственной функции по контролю за использованием технологий ИИ в правовой сфере необходимо обеспечить раз-

работку рекомендаций для формирования правовых основ в рамках процессов совершенствования и принятия нового законодательства.

На этапе стремительного развития и формирования информационного общества в Российской Федерации наблюдается усиление влияния применения технологий ИИ в построении структуры доступа пользователей различных категорий к информационным ресурсам. Множество научных работ, посвященных изучению понятия ИИ, содержат рекомендации по совершенствованию подходов к правовому регулированию данного явления [1, 2]. По нашему мнению, ИИ представляет собой программный код, написанный по определенному авторскому алгоритму на языке программирования высокого уровня, функционирующий на компьютерно-технической платформе. Кроме того, ИИ способен адаптироваться к новым условиям, изменяя изначально заданные параметры и настройки в соответствии с меняющимися требованиями и задачами, что делает его незаменимым инструментом в современном мире.

¹ Токолов Александр Владимирович, кандидат юридических наук, доцент кафедры международного и публичного права Финансового университета при Правительстве Российской Федерации, г. Москва, Российская Федерация.
E-mail: altok40@mail.ru

Программный комплекс технологических решений обладает возможностью осуществлять сбор и накопление данных, совершенствоваться в процессе выработки решения, менять изначально заданные настройки [3].

Значение деятельности Министерства юстиции в эпоху информационно-технического прогресса сводится к предоставлению актуальной и точной правовой информации физическим и юридическим лицам, государственным органам и органам местного самоуправления. Это ключевое направление деятельности подразделений Минюста России. Эти инновационные подходы позволяют не только ускорить процесс обработки и анализа правовой информации, но и значительно расширить возможности для глубокого анализа различных аспектов законодательной деятельности и практики применения права. Применение технологий ИИ в работе Министерства юстиции способствует расширению и глубокой аналитике различных аспектов законотворческой и правоприменительной работы, повышению эффективности законотворческой деятельности, улучшению качества правоприменительной работы и, как следствие, повышению уровня правовой защищенности граждан и организаций.

Обсуждение

В 2023 году полномочия Министерства юстиции значительно изменились. Так, Указом Президента Российской Федерации от 13.01.2023 г. № 10² было утверждено Положение о Министерстве юстиции Российской Федерации, в соответствии с которым Министерство юстиции осуществляет ряд ключевых государственных функций, включая, в частности, систематизацию нормативных правовых актов. Считаем, что в ближайшее время перечень полномочий Минюста России будет существенно скорректирован путем добавления новых функций, задач и полномочий.

Государственная программа Российской Федерации «Юстиция», утвержденная постановлением Правительства Российской Федерации от 15.04.2014 № 312³, предполагает формирование широкого перечня информационно-правовых ресурсов, сервисов и инструментов, основанных на всестороннем использовании информационных систем и интеграции технологий ИИ.

Исследование функций и полномочий Министерства юстиции в качестве федерального органа исполнительной власти, унаследовавшего давние традиции систематизации правовых норм, наделило нас возможностью осуществить усилия в определении главен-

ствующей роли Министерства юстиции на протяжении продолжительного процесса развития государства. На всех этих исторических этапах и даже в сегодняшнее время процесс систематизации законодательства имеет вектор движения на формирование Свода законов. В нынешнее время для создания Свода законов Министерство юстиции России имеет возможности применения технологий ИИ.

Для реализации положений статьи 15 Конституции Российской Федерации был принят Указ Президента Российской Федерации от 14.02.1998 № 170 «О мерах по повышению эффективности работы, связанной с формированием Свода законов Российской Федерации»⁴. Минюст России (Крашенинников П.В.) подготовил и направил в Администрацию Президента проект структуры Свода законов Российской Федерации и другие необходимые материалы. Согласно приказу Минюста России главную роль в исполнении данного указа выполнял отдел Свода законов и систематизации федерального законодательства (Филатова Л.В.) Департамента правовой информатизации (Морозов А.В.) [4].

Необходимо отметить, что реализация проекта по формированию законодательства в машиночитаемом виде с применением технологий ИИ представляется возможной в обозримом будущем. Министерство юстиции обладает всеми необходимыми ресурсами для реализации данного проекта.

В структуре Министерства юстиции функционирует особое подразделение — Научный центр правовой информации, располагающий коллективом опытных профессионалов, современными технологиями, аналитическими инструментами и средствами обработки правовой информации. Информационные ресурсы Научного центра правовой информации обеспечены надлежащей защитой от информационных угроз [5].

Хотелось бы отметить, что информационной базой, необходимой для осуществления деятельности, направленной на создание Свода законов в машиночитаемой форме, необходимо считать Указ Президента Российской Федерации 20.05.2011 № 657 «О мониторинге правоприменения в Российской Федерации»⁵, в котором Министерству юстиции отведена значительная роль и даны существенные полномочия [6].

Министерство юстиции систематизирует нормативные правовые акты на федеральном, региональном и муниципальном уровнях. Процесс систематизации НПА предполагает взаимодействие Минюста России и публичных органов власти различного уровня.

² Указ Президента Российской Федерации от 13.01.2023 г. № 10 «Вопросы Министерства юстиции Российской Федерации» (в ред. Указа Президента РФ от 09.10.2023 № 750) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 04.06.2025).

³ Постановление Правительства Российской Федерации от 15.04.2014 г. № 312 «Об утверждении государственной программы Российской Федерации «Юстиция» (в ред. от 16.12.2021 № 2322) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

⁴ Указ Президента Российской Федерации от 14.02.1998 № 170 «О мерах по повышению эффективности работы, связанной с формированием Свода законов Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

⁵ Указ Президента Российской Федерации 20.05.2011 № 657 «О мониторинге правоприменения в Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

Возникает обоснованная потребность внедрить в деятельность по систематизации нормативных правовых актов Минюста России федеральную государственную информационную систему (ФГИС), состоящую из всех существующих и функционирующих на сегодняшний день баз данных правовой информации. Созданная ФГИС позволит использовать технологии ИИ в едином информационно-правовом пространстве.

На сегодняшний день отсутствует законодательное регулирование применения актуализированной версии нормативного правового акта. Нормативный правовой акт может иметь несколько версий: первоначальную, актуализированную и не вступившую в силу. Актуализированная и не вступившая в силу редакции нормативного правового акта носят исключительно информационный характер, в то время как официальный статус имеет только первоначальный текст документа, который был опубликован в официальной государственной информационной системе. Следует указать, что юридической силой обладает только актуализированная версия нормативного правового акта, чего нельзя сказать про первоначальную редакцию нормативного правового акта и про редакцию, не вступившую в законную силу.

Важно также отметить, что распоряжением Правительства Российской Федерации от 25.04.2006 № 584-р⁶ утвержден перечень регистров, реестров, классификаторов и номенклатур, отнесенных к учетным системам. В их число входит Единый регистр нормативных правовых актов Российской Федерации.

В свою очередь, это подтверждает необходимость создания ФГИС, объединяющей базы данных правовой информации. Информационные ресурсы указанной ФГИС позволяют в полной мере реализовывать принцип открытости, обеспечения реализации права на создание и распоряжение своей информацией для физических лиц, а также предоставления органам государственной власти соответствующей действующему законодательству правовой информации.

ФГИС, осуществляющая свою функциональную деятельность при помощи технологий ИИ, должна быть наделена инновационными техническими решениями, способными непрерывно анализировать, а также осуществлять контроль нормативных правовых актов с целью выявления коллизий и различных противоречий норм законодательства. ФГИС с применением технологий ИИ может выступить площадкой для интеллектуализации деятельности Минюста РФ по систематизации актов законодательства. Предназначением технологий ИИ в деятельности Минюста по систематизации актов законодательства является запуск механизма мониторинга правоприменительной практики [7].

⁶ Распоряжение Правительства Российской Федерации от 25.04.2006 № 584-р (в ред. постановления Правительства Российской Федерации от 08.12.2010 № 1002) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

Технологии ИИ в деятельности Минюста РФ должны предоставлять возможности охватывать, обрабатывать и анализировать содержание баз данных правовых актов, принятых на федеральном, региональном и местном уровне.

Технологиями ИИ, применяемыми в деятельности Минюста РФ, должны выявляться коллизии, пробелы и противоречия, содержащиеся в нормативных правовых актах различной юридической силы.

ИИ должен осуществлять анализ опыта судебной деятельности и статистических данных по использованию определенных юридических механизмов правоприменения. При осуществлении государственной функции по контролю за использованием технологий ИИ в правовой сфере, необходимо обеспечить разработку рекомендаций для формирования правовых основ в рамках процессов совершенствования и принятия нового законодательства [8].

Официальный портал правовой информации [9] должен состоять из баз данных правовой информации.

1. Государственный реестр нормативных правовых актов федеральных органов исполнительной власти ведется в соответствии с постановлением Правительства Российской Федерации от 13.08.1997 № 1009 «Об утверждении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации»⁷.

Процесс применения технологий ИИ в процессе регистрации нормативного документа, принятого федеральным исполнительным органом, включает в себя ряд мероприятий: проверку документа на соответствие действующему законодательству РФ; проведение антикоррупционной экспертизы, оценки на предмет наличия коррупционных рисков в нормативном правовом акте; разрешение на регистрацию документа, внесение в официальный реестр нормативных актов федеральных органов исполнительной власти.

2. Федеральный регистр нормативных правовых актов субъектов Российской Федерации (объемом около 1,5 млн документов) ведется в соответствии с Указом Президента Российской Федерации от 10.08.2000 № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации»⁸.

В развитие этого указа принято постановление Правительства Российской Федерации от 29.11.2000 № 904

⁷ Постановление Правительства Российской Федерации от 13.08.1997 № 1009 «Об утверждении правил подготовки нормативных правовых актов федеральных органов исполнительной власти и их государственной регистрации» (в ред. постановления Правительства Российской Федерации от 14.02.2023 № 218) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

⁸ Указ Президента Российской Федерации от 10.08.2000 № 1486 «О дополнительных мерах по обеспечению единства правового пространства Российской Федерации» (в ред. Указа Президента Российской Федерации от 26.12.2016 № 707) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

«Об утверждении положения «О порядке ведения федерального регистра нормативных правовых актов субъектов Российской Федерации»⁹. Считаю целесообразным отметить, что применение технологий ИИ при осуществлении правовой экспертизы для анализа содержания нормативного правового акта субъекта Российской Федерации территориальным органом Министерства юстиции Российской Федерации предоставит возможность значительно повлиять на качество принимаемых актов и укрепить не только уровень законодательства субъектов, но и повлиять на качество федерального законодательства.

3. Федеральный регистр муниципальных нормативных правовых актов (объемом около 13 млн документов) ведется в соответствии с постановлением Правительства Российской Федерации от 10.09.2008 № 657 «О ведении федерального регистра муниципальных нормативных правовых актов»¹⁰.

Сложившаяся на сегодняшний день проблема кадрового обеспечения современными специалистами, способными грамотно осуществлять действия по созданию и обновлению информационной базы данных законодательных актов на уровне муниципалитетов, сможет быть разрешена путем применения технологий ИИ как инновационных технологий в решении этой основной задачи государства. Использование ИИ для анализа законодательных актов с целью устранения конфликтов и разночтений будет способствовать улучшению качества разработки законов на муниципальном уровне.

Заключение

Федеральная государственная информационная система играет ключевую роль в обеспечении информационной безопасности государства в связи с кратно возросшими кибератаками, осуществляемыми на информационные ресурсы органов государственной власти, а также на информационную инфраструктуру раз-

личных организаций, занимающихся коммерческой реализацией правовых систем, которые также подвержены рискам финансово-экономических кризисов.

Министерство юстиции на сегодняшний день наделено основными необходимыми полномочиями, современными информационными технологиями, а также различными информационными ресурсами, способными в симбиозе с возможностями технологий ИИ создать машиночитаемый Свод законов РФ и выстроить механизм его обновления, способный отрегулировать эффективную систему качественного контроля за применением правовых норм, а также их дальнейший прогресс и будущую динамику развития во всех сферах деятельности.

В итоге необходимо отметить, что применение технологий ИИ для создания машиночитаемого свода законов РФ — важный и необходимый шаг, способный осуществить инновационный прорыв в процессе формирования единого информационного пространства в Российской Федерации на основе свода законов, обеспечения конституционного права на информацию и предоставления доступа к актуальным нормативным правовым актам в машиночитаемом формате, предоставления официального статуса актуализированным редакциям нормативных правовых актов в машиночитаемом виде.

Более мощные квантовые компьютеры, которые придут на смену ныне существующим классическим системам, будут объединять вычислительную мощность нескольких параллельно соединенных квантовых процессоров; такой компьютер работает на 105 кубитах и демонстрирует высокую скорость при выполнении сложных вычислений. Эти возможности смогут значительно повлиять на производительность систем в области ИИ, предоставляя им более широкий спектр возможностей для вычислительных задач высокой сложности и значительного объема. Минюсту России, несомненно, тоже придется применять эти системы для выполнения первоочередных задач.

Наряду с одной из основных задач Министерства юстиции по защите прав и свобод человека и гражданина вопрос систематизации законодательства и формирование свода законов в формате, область которого доступна для машинного чтения, где возможно применение технологий ИИ, также является ключевым. А те службы, которые входят в структуру Минюста России, используя инновационные решения в области применения технологий ИИ, также смогут осуществить качественный прорыв в решении ключевых задач, определенных государственной политикой.

⁹ Постановление Правительства Российской Федерации от 29.11.2000 № 904 «Об утверждении Положения «О порядке ведения федерального регистра нормативных правовых актов субъектов Российской Федерации» (в ред. постановления Правительства РФ от 26.03.2018 № 327) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

¹⁰ Постановление Правительства Российской Федерации от 10.09.2008 № 657 «О ведении федерального регистра муниципальных нормативных правовых актов» (в ред. постановления Правительства Российской Федерации от 20.11.2018 № 1391) // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru> (дата обращения: 21.11.2023).

Литература

1. Морозов А.В. Искусственный интеллект: понятие и особенности правового регулирования : монография. М. : ООО «Технолоджи-3000», 2021. 132 с.
2. Карцхия А.А. Искусственный интеллект как средство управления в условиях глобальных рисков // Мониторинг правоприменения. 2020. № 1 (34). С. 45—50. DOI: 10/21681/2226-0692-2020-1-45-50.

3. Семенов С.В. Анализ состояния правового регулирования в сфере деятельности систем искусственного интеллекта // Право и государство: теория и практика 2023. № 7 (223). С. 134—137.
4. Морозов А.В. История правовой информатизации Минюста России // Правовая информатика. 2020. № 2. С. 92—99.
5. 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.
6. Морозов А.В. История и перспективы развития системы мониторинга правоприменения Минюста России // Мониторинг правоприменения. 2020. № 2 (35). С. 11—18.
7. Карцхия А.А., Макаренко Д.Г. Правовые аспекты статуса и рисков искусственного интеллекта // Тр. X Междунар. науч.-техн. конф. «Безопасные информационные технологии» (3—4 декабря 2019 г.) / МГТУ им. Н.Э. Баумана (НИУ). М. : МГТУ, 2019. С. 167—171.
8. Морозов А.В. Бионические конструкции человеческого сознания как основа построения ЭВМ будущего // Будущее российского права: концепты и социальные практики. V Московский юридический форум. XIV Международная научно-практическая конференция (Кутафинские чтения) : материалы конференции: в 4 ч. Ч. 4. М. : РГ-Пресс, 2018. С. 82—89.
9. Модели правового регулирования в глобальном информационном обществе : монография / Под общ. ред. Т.А. Поляковой. Саратов : Амирит, 2020. 254 с.
10. Полякова Т.А., Минбалева А.В., Наумов В.Б. Правовое регулирование квантовых коммуникаций в России и в мире // Государство и право. 2022. № 5. С. 104—114.

SECTION:
CONSTITUTIONAL LAW

USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE WORK OF THE MINISTRY OF JUSTICE OF THE RUSSIAN FEDERATION

Aleksandr Tokolov, Ph.D. (Law), Associate Professor at the Department of International and Public Law of the Financial University under the Government of the Russian Federation, Moscow, Russian Federation.
E-mail: altok40@mail.ru

Keywords: legal analysis, innovative approaches, methods of system analysis, information society, Ministry of Justice, information database of legal regulations.

Abstract

Purpose of the study: determining the potential for artificial intelligence (AI) technologies in the forming of the Code of Laws in machine-readable form.

Methods used in the study: general scientific methods of system analysis, analogy, and historicism allowing to carry out an analysis of current laws and regulations in a specific register of legal regulations.

Study findings: the current powers of the Ministry of Justice of the Russian Federation as well as promising lines of development of its legal information system are studied. A special focus is made on the innovative approach consisting in actively using advanced AI technologies. It is noted that in accordance with the government programme “Justice”, using AI technologies would provide for the possibility to create the Code of Laws of the Russian Federation.

AI technologies used in the work of the Ministry of Justice of the Russian Federation should provide for possibilities to cover, process and analyse the content of databases of legal regulations passed at the federal, regional and local level.

Practical value: the results of the study can be used for developing the Code of Laws of the Russian Federation.

References

1. Morozov A.V. *Iskusstvennyi intellekt: poniatie i osobennosti pravovogo regulirovaniia* : monografiia. M. : OOO “Tekhnolodzhi-3000”, 2021. 132 pp.
2. Kartskhiia A.A. *Iskusstvennyi intellekt kak sredstvo upravleniia v usloviakh global’nykh riskov. Monitoring pravoprimeneniia*. 2020. No. 1 (34). Pp. 45–50. DOI: 10/21681/2226-0692-2020-1-45-50.

3. Semenov S.V. Analiz sostoiianiia pravovogo regulirovaniia v sfere deiatel'nosti sistem iskusstvennogo intellekta. *Pravo i gosudarstvo: teoriia i praktika* 2023. No. 7 (223). Pp. 134–137.
4. Morozov A.V. Istoriia pravovoi informatizatsii Miniusta Rossii. *Pravovaia informatika*. 2020. No. 2. Pp. 92–99.
5. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiiia kiberbezopasnosti v usloviakh tsifrovizatsii sistemy prava. *Voprosy kiberbezopasnosti*. 2019. No. 3 (31). Pp. 18–23. DOI: 10/21681/2311-3456-2019-3-18-23 .
6. Morozov A.V. Istoriia i perspektivy razvitiia sistemy monitoringa pravoprimeneniia Miniusta Rossii. *Monitoring pravoprimeneniia*. 2020. No. 2 (35). Pp. 11–18.
7. Kartskhiia A.A., Makarenko D.G. Pravovye aspekty statusa i riskov iskusstvennogo intellekta. *Tr. X Mezhdunar. nauch.-tekhn. konf. "Bezopasnye informatsionnye tekhnologii" (3–4 dekabria 2019 g.)*. MGTU im. N.E. Bauman (NIU). M. : MGTU, 2019. Pp. 167–171.
8. Morozov A.V. Bionicheskie konstruksii chelovecheskogo soznaniia kak osnova postroeniia EVM budushchego. *Budushchee rossiiskogo prava: kontsepty i sotsial'nye praktiki. V Moskovskii iuridicheskii forum. XIV Mezhdunarodnaia nauchno-prakticheskaiia konferentsiia (Kutafinskie chteniia) : materialy konferentsii: v 4 ch. Ch. 4. M. : RG-Press, 2018. Pp. 82–89.*
9. *Modeli pravovogo regulirovaniia v global'nom informatsionnom obshchestve : monografiia. Pod obshch. red. T.A. Poliakovoi. Saratov : Amirit, 2020. 254 pp.*
10. Poliakova T.A., Minbaleev A.V., Naumov V.B. *Pravovoe regulirovanie kvantovykh kommunikatsii v Rossii i v mire. Gosudarstvo i pravo*. 2022. No. 5. Pp. 104–114.

НОВЫЙ ВЕКТОР В РЕГУЛИРОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ: ПРОБЛЕМЫ И НЕОБХОДИМЫЕ ШАГИ ДЛЯ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ РУНЕТА

Шварц Л.В.¹

Ключевые слова: информация, идентификация, аутентификация, авторизация, информационная система, контроль доступа, пользователь, владелец информационного ресурса, новостной агрегатор, провайдер хостинга.

Аннотация

Цель работы: анализ законодательных новелл в сфере информационной безопасности, действие которых распространяется на способы авторизации пользователей на российских сайтах и деятельность провайдеров хостинга, освещение решаемых за счет настоящих перемен существующих проблем и возможных последствий принятых изменений.

Методы исследования: анализ, синтез, систематизация научных, а также нормативных правовых источников.

Результаты исследования: сформулирована авторская позиция о требуемых изменениях в законодательстве с точки зрения их прикладного применения для восполнения созданной законодателем правовой неопределенности в области информационной безопасности. Сделаны выводы о необходимости проработки существующих правовых понятий взамен включения нового понятия «авторизация пользователя», а также о пересмотре правового регулирования функционирования провайдеров хостинга в части переноса ответственности за действия пользователей на провайдеров, что фактически блокирует возможность нормальной работоспособности хостинга.

DOI: 10.24412/1994-1404-2025-2-72-78

Введение

Вопрос информационной безопасности на сегодняшний день приобрел национальный масштаб и является одним из актуальнейших аспектов борьбы с возможным негативным информационным воздействием, имеющим направленный и намеренный характер. Один из основополагающих документов, имеющий программный характер и на законодательном уровне регламентирующий эту борьбу, — Доктрина информационной безопасности, утвержденная Указом Президента РФ от 05.12.2016 № 646. Она декларирует необходимость обеспечения полноценного самостоятельного присутствия Российской Федерации в международном информационном поле и формирование механизма отбора каналов поставки достоверных данных и новостей, чтобы минимизировать риски и ущерб от дезинформационных вбросов и определить дальнейшее совершенствование правовых институтов с целью представления интересов населения и государства в коммуникационном пространстве. Как утверждает

В.Н. Лопатин, именно система информационной безопасности интегрирует все ключевые компоненты политики нацбезопасности в единое целое [1, с. 40—41]. При этом, исходя из Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 02.07.2021 № 400, в приоритете не просто обеспечение безопасного использования информационных технологий, но и создание для этого надлежащих условий (п. 57). Этот стратегический национальный приоритет развития созвучен Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Закон № 149-ФЗ), одно из положений которого устанавливает, что защита информации включает в себя в том числе и меры по реализации права на доступ к информации (ст. 16). Действительно, широкое использование информационных технологий, цифровизация различных сфер жизни общества привели к тому, что «информационная политика

¹ Шварц Лариса Владимировна, кандидат юридических наук, доцент, доцент кафедры гражданского и трудового права Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Санкт-Петербург, Российская Федерация.

E-mail: shvarts-lv@ranepa.ru

Российской Федерации является регулятором публичных и частных правоотношений, посредством чего реализуются стратегические задачи государства» [2, с. 55].

В конце 2023 года вступила в силу новая редакция Закона № 149-ФЗ, где уточняются требования, предъявляемые к владельцам российских информационных ресурсов, провайдером хостинга и новостным агрегаторам. Эта редакция подготовлена с учетом изменений, внесенных Федеральным законом от 31.07.2023 № 406-ФЗ «О внесении изменений в Федеральный закон „Об информации, информационных технологиях и о защите информации“ и Федеральный закон „О связи“» и Федеральным законом от 12.12.2023 № 588-ФЗ «О внесении изменения в статью 8 Федерального закона „Об информации, информационных технологиях и о защите информации“». По сути, происходит переностройка законодательства на решение задач, возникших среди прочего в связи с необходимостью информационной защиты россиян [3, с. 17].

Остановимся на двух ключевых моментах предстоящих изменений.

Способы авторизации на интернет-сайтах

Первое ключевое изменение коснулось ст. 8: в ней появился п. 10, обязывающий владельца сайта (программы, аккаунта, иного сетевого ресурса) авторизовывать пользователей одним из доступных в данный момент способов:

- через личный номер мобильной связи (при исключении обязанности соблюдения государственного порядка использования номера мобильной связи и отмене правила о заключении с мобильным оператором или поставщиком беспроводной связи договора об идентификации);
- через подтвержденную учетную запись абонента в Единой системе идентификации и аутентификации (ЕСИА, которой на данный момент является портал Госуслуг);
- через Единую биометрическую систему (ЕБС), хранящую такие персональные данные, как изображение лица и образец голоса человека;
- через иную систему, отвечающую установленным правовым нормам защиты информации и принадлежащую отечественному юридическому лицу или физическому лицу, имеющему только гражданство РФ.

В указанных выше случаях под российским юридическим лицом понимается юридическое лицо, находящееся под контролем РФ, субъекта РФ, муниципального образования, гражданина РФ, не имеющего гражданства другого государства, и (или) контролируемых ими совместно или по отдельности лиц. Под контролем, в свою очередь, понимается возможность определять решения, принимаемые указанным юридическим лицом, в силу наличия права прямо или косвенно распоряжаться более чем 50% общего количества голосов,

приходящихся на голосующие акции (доли), составляющие уставный капитал юридического лица.

Представители Государственной Думы РФ пояснили, что под «иной информационной системой» понимается ряд российских сервисов, таких как социальная сеть «ВКонтакте» или почтовый и поисковый сервис Mail.ru, не имеющих государственного или муниципального характера и созданных частными юридическими или физическими лицами².

Ограничение нужно будет соблюдать российским организациям и гражданам с интернет-бизнесом в РФ. Перечисленные способы авторизации распространяются на пользователей, которые находятся в России.

Так, 1 декабря 2023 года должен был вступить в силу запрет на регистрацию в Рунете с иностранной электронной почты. Планировалось, что нововведение распространится только на бизнес, осуществляемый на отечественных интернет-платформах, и указанные методы авторизации не коснутся международного интернет-бизнеса.

Если иностранные компании, сайтом которых пользуются россияне, находятся под контролем государственных органов РФ, то на них ограничение распространяется аналогично.

Автор приводимых в статье поправок депутат Государственной Думы Антон Вадимович Горелкин заверил, что данные изменения, призванные ограничить «использование для авторизации российских пользователей на информационных ресурсах, владельцами которых являются российские граждане и организации, иностранных систем, обеспечивающих такую авторизацию»³, обсуждались с представителями отечественного бизнеса разных уровней.

В тексте поправок не содержится сведений об ограничении способов регистрации новостных агрегаторов, включенных в реестры Роскомнадзора — федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Имеются в виду ресурсы с доступом более миллиона пользователей в сутки, такие как паблик «ВКонтакте», новостной агрегатор «Рамблер» и блогинг-платформа «Дзен», а также организаторы распространения информации — владельцы сайтов, соцсетей, мессенджеров и отзовиков.

Включенность всех вышеперечисленных субъектов в реестр Роскомнадзора обеспечивает их полную информационную прозрачность для органов государственной власти и контроля: ведомствам известны собственники этих ресурсов и инструментов распространения информации, способы связи с ними, сфера их ответственности (проще говоря, за что с них

²См., например, пояснения председателя Комитета Госдумы РФ по информационной политике Хинштейна А.Е. URL: <https://www.forbes.ru/tekhnologii/493489-duma-prinala-zakon-o-zaprete-na-registraciu-v-runete-s-zarubeznoj-elektronnoj-postoj> (дата обращения: 01.11.2024)

³России с 1 декабря вводится запрет на регистрацию в Рунете с иностранной электронной почты. URL: <https://habr.com/ru/news/751532/> (дата обращения: 02.11.2024).

спрашивать, кому направлять предписания и запросы, а также на кого накладывать штрафные санкции). Таким образом, новые поправки в закон затронут всех без исключения владельцев сайтов с пользовательской авторизацией⁴.

Сложность видится и в том, что деятельность большинства информационных систем носит трансграничный характер, поэтому правильно подмечено, что «национальные правила идентификации могут оказаться неэффективными» [4, с. 178].

В поправках к ФЗ «Об информации, информационных технологиях и о защите информации» и ФЗ «О связи» не предусмотрены санкции для владельцев интернет-ресурсов, которые не обеспечат возможность регистрации нужными способами. Видимо, меры ответственности будут прописаны в будущем после оценки правоприменительной практики [5, с. 12].

По замыслу разработчиков, новации затронут только сайты с регистрацией и аутентификацией пользователей — например, электронные торговые площадки, выступающие посредниками между продавцом и покупателем товара.

Согласно ст. 15.1 Закона № 149-ФЗ, при выявлении факта распространения сайтом или доменом информации о способах обхода установленных в РФ блокировок появляется основание для внесения такого ресурса в Единый реестр запрещенной информации Роскомнадзора. Однако запрет касается только любой рекламы способа обхода блокировок и никак не затрагивает само право пользователя применять инструменты безопасного соединения с общедоступной сетью, такие как VPN-сервисы⁵.

Тем, кто на момент принятия закона уже зарегистрированы на российских сайтах при помощи иностранной электронной почты, проходить аутентификацию заново не придется, т. е. обратной силы у закона не будет.

Итак, вводятся новые правила регистрации на интернет-площадках, которые уже прозвали Законом об авторизации. Система управления доступом к информации должна обеспечивать надежную и безопасную идентификацию и аутентификацию [6, с. 1], поскольку именно от эффективности этих процессов во многом зависит общая безопасность информационных систем.

Тем не менее пока что применение закона вызывает вопросы из-за неоднозначности трактовки некоторых его положений. Например, подпадают ли под действие вновь установленных правил сайты с подпиской на информационную рассылку или регистрацией пользователей на мероприятия через подтверждение адреса

электронной почты, в том числе и корпоративной? И что подразумевается под «авторизацией» — только первичная регистрация пользователя или любой его вход в аккаунт или систему?

Попробуем разобраться.

В первом случае проблема возникнет, если речь идет о регистрации новых пользователей с зарубежной почты, так как она будет находиться под запретом в целях сохранности персональных данных и снижения интеграции сервисов из недружественных стран в российские системы. Однако буквальных требований к стране регистрации почты в законе нет, если она используется в качестве логина. Физические лица, уже имеющие аккаунты в иностранных почтовых сервисах (Gmail, Microsoft и т. п.), могут продолжать пользоваться ими. Единственная ситуация, когда потребуются обязательный российский адрес электронной почты (e-mail) — при создании нового аккаунта на российском сайте. Естественно, никто не будет проверять, с помощью каких e-mail регистрируют блоги или малые инфосайты, так как это невозможно технически, как и нереально проверить документы на принадлежность системы регистрации корпоративного адреса российскому правовому полю.

Вместе с тем программисты советуют пользователям менять способы входа на сайты. Представляется, что во избежание сложностей лучше перейти на российские сервисы, как это сделали государственные служащие. Вероятнее всего, со временем интернет-площадки, отказавшиеся ввести регистрацию на базе российских «технологий единого входа», будут подвержены штрафным санкциям за несоблюдение требований по работе с персональными данными. Многие российские сайты уже убрали авторизацию через иностранные системы — к примеру, маркетплейс Ozon.

Что касается подписки на e-mail-рассылки, новые требования Закона № 149-ФЗ сработают, если форма регистрации совмещена с согласием на получение рекламных писем, так как e-mail будет использоваться для входа. Поэтому во всех остальных случаях пользователь вправе указать российский или иностранный адрес электронной почты, как посчитает нужным.

Во втором случае ситуация представляется сложнее в связи с тем, что зачастую «информационное законодательство не успевает за развитием информационно-коммуникационной сферы на базе электронной среды и оперирует устаревшими словами, а также тавтологичными, метафоричными и противоречивыми определениями легальных понятий» [7, с. 645].

Авторизация и аутентификация — это два совершенно разных процесса. Аутентификация нужна, чтобы проверить право доступа к данным, об авторизации же можно говорить только после получения доступа.

Стоит отметить, что в соответствии с требованиями ч. 1 ст. 16 Закона № 149-ФЗ защита информации, включая доступ к телекоммуникационным сетям, представляет собой принятие правовых, организационных

⁴ Установлен запрет регистрации на российских сайтах с помощью иностранных электронных почтовых сервисов. URL: https://admrebr.gosuslugi.ru/dlya-zhiteley/informatsiya-01/novosti_1309.html (дата обращения: 02.11.2024).

⁵ Данные о способах обхода блокировок станут основанием для включения сайта в реестр РКН. URL: <https://tass.ru/obschestvo/18326933> (дата обращения: 04.11.2024).

и технических мер. Идентификацию, аутентификацию и авторизацию пользователей относят к техническим мерам, дополняющим организационные меры и улучшающим общую защиту сайта [8, с. 414], создавая комплексную систему безопасности для серверных систем, защищающую данные от внутренних и внешних угроз [9, с. 447].

Проверка всегда начинается с идентификации, за ней идёт аутентификация и в конце авторизация. Все эти этапы помогают обезопасить важную информацию и защищают, например, персональные данные пользователей, деньги на подключенных к профилю счетах.

Идентификация — установление системой существования конкретного пользователя на основе предоставленных им определенных данных (например, номера телефона или логина).

Аутентификация — подтверждение пользователем своего права доступа в систему путем введения пароля, пин-кода, биометрии или другим предустановленным способом.

Авторизация — определение персональных привилегий и прав пользователя на данном ресурсе (например, просмотр и отправка электронной почты).

По тексту поправок речь идет о том, чтобы обязать владельцев сайтов проводить авторизацию, т. е. про действия внутри системы, так как авторизация — это элемент работы самой системы по определению набора прав в этой системе.

Представляется, что по замыслу инициаторов данных поправок речь все-таки идет об аутентификации, и названные мероприятия призваны контролировать доступ к информационной системе. Но если заменить термин «авторизация» на «аутентификацию», то не может быть использован четвертый способ регистрации пользователей — с использованием других систем, отвечающих требованиям о защите сведений, причем владеть этой системой должен российский гражданин либо человек без гражданства другой страны. Получается, что для того, чтобы иметь функции в одной информационной системе, необходимо получить разрешение в другой информационной системе. Таким образом, идентифицировать пользователей могут и частные информационные системы, но при условии наличия необходимой для этого инфраструктуры. Например, исходя из Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями, утвержденных постановлением Правительства РФ от 12 апреля 2018 г. № 447, доступ к негосударственной информационной системе обеспечивается с использованием подтвержденной учетной записи физического лица в федеральной государственной информационной системе с получением из нее набора сведений о заявителе (п. 5).

При этом многие авторы отмечают высокую степень риска от различного уровня использования сведений с информационных систем, принадлежащих частным лицам [10, с. 16].

К слову, утвержден и введен в действие приказом Росстандарта от 10.04.2020 № 159-ст «ГОСТ \ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения», в котором прописано, что в целях защиты информации решение о предоставлении доступа для использования информационных и вычислительных ресурсов средств вычислительной техники, а также ресурсов автоматизированных (информационных) систем основывается на результатах идентификации и аутентификации. Кстати, в Федеральном законе от 29.12.2022 № 572-ФЗ «Об использовании биометрических персональных данных» речь идет об осуществлении именно идентификации и аутентификации на основе биометрических персональных данных физических лиц.

Регулирование работы хостинг-провайдеров

Второе изменение, на которое необходимо обратить внимание, коснулось уже самих провайдеров в части утверждения новой ст. 10.2-1 Закона № 149-ФЗ. Напомним, что провайдер хостинга — это лицо, осуществляющее деятельность по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети Интернет. С 1 декабря 2023 года деятельность хостингов контролируется Роскомнадзором через учет определенных действий провайдера. Так, провайдер хостинга должен:

- уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций о начале такой деятельности;
- обеспечить соответствие защиты персональных данных требованиям, предъявляемым законом к данной деятельности;
- соблюдать требования к вычислительной мощности, установленные государственными органами, уполномоченными на ведение деятельности по обеспечению госбезопасности и правопорядка, для проведения мероприятий в целях реализации возложенных на них задач;
- предоставить вычислительные мощности для публикации данных в Интернете гражданам, обратившимся к провайдеру, только после прохождения идентификации и аутентификации.

Отметим, что вышеупомянутый государственный орган ведет Реестр хостингов, где хранит подробные сведения о них и об их действиях. В некоторых случаях Роскомнадзор вправе привлечь к ведению списка сторонние уполномоченные организации.

После 1 февраля 2024 года лица, которые не включены в Реестр, не могут оказывать услуги хостинга в России. Кроме того, с 1 сентября 2024 года операторы

государственных и муниципальных информационных систем могут пользоваться услугами хостинга только у провайдеров, не находящихся под иностранным контролем и размещающих технические средства хостинга в России.

Однако если ведомство обнаружит нарушение требований по защите данных, получив информацию от Федеральной службы безопасности РФ или подведомственных органов, то будет обязано выдать нарушителю предписание с указанием срока устранения недочетов. При этом максимальный срок исправления составляет 10 суток. Провайдер же, в свою очередь, обязан проинформировать государственный орган о выполнении обязательств в письменном виде. Если он не исправит ситуацию, отказавшись от принятия предложенных мер либо не оповестит о ликвидации ситуации, Роскомнадзор вправе исключить провайдера из соответствующего реестра.

Это буквально означает, что теперь тот, кто сдает свои вычислительные мощности в аренду, обязан с целью соблюдения требований по защите информации отслеживать действия своих клиентов и нести за них ответственность. Теперь будут блокироваться не пути, а сам ресурс, и обязанность эта возлагается на хостинг-провайдера. И если ранее не было законных оснований на разрыв экономических отношений, то согласно новым правилам (оказание услуг по предоставлению хостинга только компаниями из Реестра), Роскомнадзор полномочен исключать из данного Реестра, а за этим немедленно последует лишение лицензии.

Справедливости ради следует заметить, что согласно Федеральному закону от 12 декабря 2023 г. № 588-ФЗ «О внесении изменения в статью 8 Федерального закона „Об информации, информационных технологиях и о защите информации“» переход российских IT-компаний к авторизации через отечественные государственные сервисы перенесли на 2025 год. На сегодняшний день российские владельцы сайтов и программ могут проводить авторизацию через отдельную информационную систему, которая должна отвечать требованиям к защите информации и принадлежать владельцу ресурса или экономически значимой организации.

Решение об установлении переходного периода до 1 января 2025 г. для вступления вышеуказанных ограничений было принято с целью гарантии стабильного функционирования платформ и подготовки

их к переводу под российский контроль⁶. В понимании автора, вряд ли послабления в исполнении данных новелл позволят добиться единообразного толкования как понятия авторизации, так и нового порядка регистрации на российских сайтах, но хотя бы дадут время владельцам и провайдерам информационных ресурсов адаптироваться под новые правила.

Заключение

Таким образом, несмотря на вполне оправданные опасения относительно сложности перенесения технических категорий в правовые без потери качественной составляющей [11], для решения обозначенных стратегических задач следовало начать с фундаментальной работы по унификации нормативной правовой терминологии в сфере использования информационных технологий, на основе которой разработать юридический тезаурус, где закрепить также общие принципы идентификации и аутентификации, не углубляясь в подробную регламентацию авторизации. Исходя из реалий, справедливым будет отметить, что право как инструмент и средство управления процессами социума меняет свои формы, содержание, механизмы формирования и реализации, подвергаясь воздействию цифровых технологий [12, 13]. В части изменений правового регулирования деятельности хостинг-провайдеров попытка законодателя обеспечить выполнение правил информационной безопасности за счет агента, предоставляющего платформу для пользователей, размещающих на ней контент, содержание которого вне контроля провайдера, представляется нежизнеспособной правовой конструкцией, не приводящей к повышению уровня безопасности Рунета. Необходимо смена субъекта ответственности, а именно возложение ответственности на лиц, определяющих информационный контент, публикуемый на том или ином ресурсе, для существования которого хостинг-провайдеры предоставляют свои услуги. Настоящие изменения являются неэффективными и становятся очередной преградой для бизнеса из-за выбора тактики борьбы законодателя с нарушениями законодательства об информации.

⁶ Данные о способах обхода блокировок станут основанием для включения сайта в реестр РКН. URL: <https://tass.ru/obschestvo/18326933> (дата обращения: 04.11.2024).

Литература

1. Лопатин В.Н. Проблемы информационного права в цифровой экономике // Право и государство. 2019. № 1 (82). С. 40—56.
2. Дубень А.К. Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права // Вопросы безопасности. 2023. № 1. С. 51—56.
3. Цифровое право / А. Дюфло, Л.В. Андреева, В.В. Блажеев [и др.]; под общей редакцией В.В. Блажеева, М.А. Егоровой; Министерство науки и высшего образования Российской Федерации, Московский государственный юридический университет им. О.Е. Кутафина. Учеб. изд. М. : Проспект, 2020. 640 с.

4. Непомнящий П.А. Идентификация наследодателя цифровых прав // Гуманитарные, социально-экономические и общественные науки. 2024. № 6. С. 177—180. DOI: 10.24412/2220-2404-2024-6-16.
5. Ершова Е.А. Комментарий к Федеральному закону от 31 июля 2023 г. № 406-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и Федеральный закон «О связи» // Нормативные акты для бухгалтера. 2023. № 16. С. 12.
6. Бельский В.С., Герасимов И.Ю., Сабанов А.Г., Царегородцев К.Д. Анализ моделей идентификации и аутентификации // International Journal of Open Information Technologies. 2024. Т. 12. № 5. С. 1—14.
7. Нестеров А.В. Информационно-терминологические проблемы персональных данных в условиях цифровизации экономики // Россия: тенденции и перспективы развития : ежегодник. Материалы XX Национальной научной конференции с международным участием, Москва, 14—15 декабря 2020 г. Вып. 16. Ч. 1. М. : Институт научной информации по общественным наукам РАН, 2021. С. 645—648.
8. Матевосян Г.А. Системы обеспечения информационной безопасности в официальных сайтах образовательных организаций // Вестник науки. 2024. Т. 1. № 4 (73). С. 408—415.
9. Лисай В.Э. Безопасность в backend-разработке: современные методы защиты и шифрования данных // Вестник науки. 2024. Т. 3. № 4 (73). С. 437—449.
10. Антропов Д.В., Комаров С.И., Рассказова А.А. Обоснование приоритетности данных единого государственного реестра недвижимости перед данными иных информационных систем // Современные проблемы земельно-имущественных отношений, урбанизации территории и формирования комфортной городской среды : сборник докладов Международной научно-практической конференции, Тюмень, 28 октября 2022 года. Тюмень : Тюменский индустриальный университет, 2023. С. 13—18.
11. Щеглов Е.Н. Организационно-правовые аспекты авторизации пользователей для доступа к информационным системам с использованием сети Интернет // Полиция и общество: проблемы и перспективы взаимодействия. 2021. № 3. С. 205—210.
12. Хабриева Т.Я. Технологические революции и их проекция в праве // Вопросы истории. 2022. № 2-2. С. 256—270.
13. Хабриева Т.Я. Технологические императивы современного мира и право // Журнал зарубежного законодательства и сравнительного правоведения. 2023. Т. 19. № 1. С. 5—12. DOI: 10.12737/jzsp.2023.001.

SECTION:
CONSTITUTIONAL LAW

A NEW VECTOR IN REGULATING INFORMATION RESOURCES: PROBLEMS AND STEPS NEEDED FOR ENSURING THE SECURITY OF RUNET

Larisa Schwartz, Ph.D. (Law), Associate Professor at the Department of Civil and Labour Law of the Russian Presidential Academy of National Economy and Public Administration, Saint Petersburg, Russian Federation.

E-mail: shvarts-lv@ranepa.ru

Keywords: information, identification, authentication, authorisation, information system, access control, user, information resource owner, news aggregator, hosting provider.

Abstract

Purpose of the study: analysing legislative novelties in the information security field whose effect extends to ways of user authorisation on Russian websites and hosting provider activities, covering the existing problems that are being solved using the said changes in law and possible consequences of these changes.

Methods used in the study: analysis, synthesis, and systematisation of legal sources, scholarly as well as regulatory ones.

Study findings: the author's stance is worded on the required changes in law from the standpoint of applying them for filling in the legal uncertainty in the information security area created by the law makers. The following conclusions are made: an elaboration of existing legal notions is needed instead of introducing a new one, that is, "user authorisation", and legal regulation of hosting providers' operation to the extent of shifting the responsibility for users' actions to the provider should be reviewed since such a shift practically blocks the possibilities for normal hosting operation.

References

1. Lopatin V.N. Problemy informatsionnogo prava v tsifrovoi ekonomike. Pravo i gosudarstvo. 2019. No. 1 (82). Pp. 40–56.
2. Duben' A.K. Informatsionnaia bezopasnost' v sisteme natsional'noi bezopasnosti: aktual'nye problemy informatsionnogo prava. Voprosy bezopasnosti. 2023. No. 1. Pp. 51–56.
3. Tsifrovoe pravo. A. Diuflo, L.V. Andreeva, V.V. Blazheev [i dr.] ; pod obshchei redaktsiei V.V. Blazheeva, M.A. Egorovoi; Ministerstvo nauki i vysshego obrazovaniia Rossiiskoi Federatsii, Moskovskii gosudarstvennyi iuridicheskii universitet im. O.E. Kutafina. Ucheb. izd. M. : Prospekt, 2020. 640 pp.
4. Nepomniashchii P.A. Identifikatsiia nasledodatelia tsifrovyykh prav. Gumanitarnye, sotsial'no-ekonomicheskie i obshchestvennye nauki. 2024. No. 6. Pp. 177–180. DOI: 10.24412/2220-2404-2024-6-16 .
5. Ershova E.A. Kommentarii k Federal'nomu zakonu ot 31 iuliia 2023 g. No. 406-FZ "O vnesenii izmenenii v Federal'nyi zakon "Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii" i Federal'nyi zakon "O sviazi". Normativnye akty dlia bukhgaltera. 2023. No. 16. P. 12.
6. Bel'skii V.S., Gerasimov I.Iu., Sabanov A.G., Tsaregorodtsev K.D. Analiz modelei identifikatsii i autentifikatsii. International Journal of Open Information Technologies. 2024. T. 12. No. 5. Pp. 1–14.
7. Nesterov A.V. Informatsionno-terminologicheskie problemy personal'nykh dannykh v usloviakh tsifrovizatsii ekonomiki. Rossiia: tendentsii i perspektivy razvitiia : ezhegodnik. Materialy XX Natsional'noi nauchnoi konferentsii s mezhdunarodnym uchastiem, Moskva, 14–15 dekabria 2020 g. Vyp. 16. Ch. 1. M. : Institut nauchnoi informatsii po obshchestvennym naukam RAN, 2021. Pp. 645–648.
8. Matevosian G.A. Sistemy obespecheniia informatsionnoi bezopasnosti v ofitsial'nykh saitakh obrazovatel'nykh organizatsii. Vestnik nauki. 2024. T. 1. No. 4 (73). Pp. 408–415.
9. Lisai V.E. Bezopasnost' v backend-razrabotke: sovremennye metody zashchity i shifrovaniia dannykh. Vestnik nauki. 2024. T. 3. No. 4 (73). Pp. 437–449.
10. Antropov D.V., Komarov S.I., Rasskazova A.A. Obosnovanie prioritnosti dannykh edinogo gosudarstvennogo reestra nedvizhimosti pered dannymi innykh informatsionnykh sistem. Sovremennye problemy zemel'no-imushchestvennykh otnoshenii, urbanizatsii territorii i formirovaniia komfortnoi gorodskoi sredy : sbornik dokladov Mezhdunarodnoi nauchno-prakticheskoi konferentsii, Tiumen', 28 oktiabria 2022 goda. Tiumen' : Tiumenskii industrial'nyi universitet, 2023. Pp. 13–18.
11. Shcheglov E.N. Organizatsionno-pravovye aspekty avtorizatsii pol'zovatelei dlia dostupa k informatsionnym sistemam s ispol'zovaniem seti Internet. Politsiia i obshchestvo: problemy i perspektivy vzaimodeistviia. 2021. No. 3. Pp. 205–210.
12. Khabrieva T.Ia. Tekhnologicheskie revoliutsii i ikh proektsiia v prave. Voprosy istorii. 2022. No. 2-2. Pp. 256–270.
13. Khabrieva T.Ia. Tekhnologicheskie imperativy sovremennogo mira i pravo. Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia. 2023. T. 19. No. 1. Pp. 5–12. DOI: 10.12737/jzsp.2023.001 .

КВАНТОВОПОДОБНЫЕ ФЕНОМЕНЫ РАСПРОСТРАНЕНИЯ КОЛЛЕКТИВНЫХ ЭМОЦИЙ В СОЦИАЛЬНЫХ СЕТЯХ: МОДЕЛЬ, НАБОР ДАННЫХ И РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ

Гнидко К.О.¹, Лисов Д.Н.²

Ключевые слова: математическое моделирование, информационная безопасность, социальные сети, анализ тональности, коллективные эмоции, броуновское взаимодействие, большие языковые модели, интерференция.

Аннотация

Цель исследования: разработка математической модели распространения коллективных эмоций в социальных сетях; экспериментальная проверка гипотезы о возникновении квантовоподобных феноменов при много-агентном взаимодействии акторов массовой коммуникации посредством информационного поля.

Методы исследования: анализ тональности текстовых сообщений (сентимент-анализ) с использованием большой языковой модели; снижение размерности признакового пространства на основе метода главных компонент; статистическая обработка и визуализация данных.

Полученные результаты: разработана междисциплинарная математическая модель распространения коллективных эмоций в социальных сетях, основанная на концепции броуновского взаимодействия агентов. Модель учитывает эмоциональные состояния субъектов коммуникации через психологические переменные — валентность и эраузал, что позволяет моделировать динамику эмоций на индивидуальном и коллективном уровнях. Для экспериментальной проверки гипотезы о квантовоподобных феноменах проанализировано 2246 сообщений и 50326 комментариев из сообщества «Мировая политика» социальной сети «ВКонтакте» с декабря 2017 по июнь 2018 года. Результаты эксперимента показали, что взаимодействие агентов через информационное поле вызывает усиление или ослабление коммуникативной активности, проявляющееся в распределении эмоциональных параметров, схожем с интерференционной картиной. Установлена корреляция между «мотивационной силой» сообщений (лайки, репосты) и их эмоциональным тоном (валентность), что подтверждает наличие квантовоподобных эффектов, таких как интерференция и суперпозиция.

Научная новизна: представленная модель динамики коллективных эмоций в социальных сетях имеет междисциплинарный характер и учитывает современные результаты в области психологии и социологии, что отличает её от традиционных подходов, не рассматривающих нелинейные эффекты, обусловленные субъективными особенностями участников коммуникации. Впервые введена концепция «информационного поля» как среды, опосредующей взаимодействие агентов массовой коммуникации, что позволяет описывать наблюдаемые квантовоподобные феномены, такие как интерференция эмоциональных состояний субъектов массовой коммуникации. Авторский вклад включает разработку оригинального набора данных (эмоционально окрашенных текстовых сообщений и комментариев пользователей социальной сети), размещенного в открытом доступе, что обеспечивает воспроизводимость эксперимента и расширяет возможности для будущих исследований. Для получения количественных оценок тональности сообщений (сентимент-анализа), в отличие от предыдущих работ, использовавших наборы специализированных словарей, авторами применен алгоритм на основе большой языковой модели, что позволило более точно учесть контекст, сложные языковые конструкции, иронию и сарказм.

DOI: 10.24412/1994-1404-2025-2-79-94

¹ Гнидко Константин Олегович, доктор технических наук, доцент, заместитель руководителя группы Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Российская Федерация. ORCID: 0000-0002-8605-8865.

E-mail: gnidko.ko@talantiuspeh.ru

² Лисов Дмитрий Николаевич, младший научный сотрудник Научного центра информационных технологий и искусственного интеллекта, АНОО ВО «Университет «Сириус», Федеральная территория «Сириус», Российская Федерация. ORCID: 0000-0002-8214-4109.

E-mail: lisov.dn@talantiuspeh.ru

Введение

Моделирование процессов распространения информации в сетевых структурах является актуальной научно-технической задачей, имеющей высокую значимость для информационной безопасности. Исторические примеры подтверждают критическую важность изучения подобных механизмов. Так, анализ протестных движений в Сирии, Ливии, на территории Украины и в Республике Казахстан выявил значительное влияние социальных сетей на развитие так называемых «цветных революций» [1—3].

При этом особый интерес представляют процессы распространения в социальных сетях эмоционально окрашенных сообщений, поскольку именно они формируют повестку дня, мобилизуют группы пользователей и могут приводить к дестабилизации общественно-политической обстановки. Сообщения, вызывающие эмоциональный отклик [4], распространяются с большей скоростью и охватом, чем нейтральные сообщения. Это связано с тем, что пользователи склонны делиться информацией, вызывающей сильные эмоции, для выражения своей позиции или принадлежности к определенной группе.

Математические модели распространения информации, основанные на многоагентных системах и эпидемических моделях, позволяют не только предсказать динамику конфликта, но и выявить на ранних стадиях признаки его искусственного стимулирования через манипуляцию информационными потоками.

Таким образом, моделирование распространения эмоциональных сообщений в социальных сетях является не только важной научной задачей, но и критическим направлением обеспечения информационной безопасности, требующим дальнейшего изучения и внедрения.

Информационное взаимодействие субъектов коммуникации в онлайн-сообществах отличается от межличностного общения рядом ключевых особенностей. Наиболее значимые из них перечислены ниже.

1. В современных условиях субъектами массовой коммуникации могут быть не только пользователи-люди, но и агенты искусственного интеллекта, представленные, например, большими языковыми моделями.

2. Скорость реакции на стимулы и, соответственно, динамика эволюции эмоционального фона в средствах массовой коммуникации отличается от соответствующих показателей «традиционной» информационной среды. Часто в процессе коммуникации наблюдаются регулярные сдвиги по времени, связанные с периодичностью обновления того или иного информационного ресурса.

3. Существуют отличия в значении порогового уровня возбуждения, достигнув которого индивид принимает решение поделиться своей эмоцией с другими, а сама передача эмоционального состояния осуществляется, как правило, посредством размещения на информационном ресурсе текстового сообщения.

4. Анонимность общения в сети зачастую побуждает субъектов массовой коммуникации нарушать принятые в обществе нормы поведения и морали.

5. Теория слабых связей Грановеттера, многократно подтвержденная экспериментами [5, 6], подчеркивает влияние многочисленных связей малой силы, наблюдаемых между членами онлайн-сообществ, на скорость распространения информации. При этом поддержание виртуальных слабых связей требует от субъекта коммуникации существенно меньше усилий, чем поддержание сильных связей в реальной жизни.

6. Специфическим объектом исследования в рамках данной работы являются эмоционально окрашенные текстовые сообщения, которыми обмениваются участники массовой коммуникации. Количественная оценка эмоции, передаваемой в сообщении, может быть представлена в двумерном базисе, координатными осями которого являются знак (валентность) и интенсивность (эраузал), в терминах Дж. Рассела³ [7].

В современных информационных сообществах регулярно наблюдаются примеры спонтанного всплеска и постепенного угасания интереса большого количества людей к определенным явлениям, фактам и событиям реального и виртуального мира. Как правило, данные процессы следуют одному и тому же сценарию: пользователи средств массовой коммуникации реагируют на информационные поводы и, в зависимости от множества факторов (включая их личный жизненный опыт), начинают испытывать негативные или позитивные эмоции. Дальнейшее развитие сценариев в реальном мире определяется совокупностью начальных условий, действующих внешних сил и стохастических факторов, однако несомненна связь таких процессов с жизненно важными областями жизнедеятельности общества и государства: политической, социальной, экономической, что обуславливает высокую актуальность исследований в области моделирования названных процессов.

Исследователи в разных областях научного знания неоднократно обращали внимание на возможные аналогии между закономерностями, наблюдаемыми в процессе жизнедеятельности сложных социальных систем, и явлениями, происходящими в мире субатомных частиц. Так, например, И.М. Фейнберг и И.В. Гуревич в явном виде указывают на схожесть психологических процессов и квантовых феноменов микромира: «...может оказаться, что и в психологии, так же как и в микрофизике, существует интерференция амплитуд вероятностей»⁴. Предпосылки для выдвижения гипотезы о применимости математического аппарата

³ Russell J.A. A circumplex model of affect // Journal of Personality and Social Psychology. 1980. Vol. 39. No. 6. P. 1161–1178.

⁴ Гуревич И.В., Фейнберг В.В. Какие вероятности «работают» в психологии // Вероятностное прогнозирование в деятельности человека. М.: Наука, 1977. С. 9—21.

квантовой механики к моделированию психологических и социальных явлений содержатся в работах Р. Пенроуза (за нерациональное бессознательное поведение и эмоции человека «отвечают» квантовые процессы, происходящие в нано-структурах мозга), А.Ю. Хренникова [8, 9] (автоматические процессы в области бессознательного адекватно описываются тем же математическим аппаратом неархимедова анализа, что и квантовые процессы). Всестороннему анализу современных взглядов на глубокие взаимосвязи между феноменом сознания и квантовой механикой посвящен сборник [10].

В то же время некоторые известные модели, применяющие для описания поведения человека квантовоподобные формализмы, например, [11], позволяют формально описать динамику ментальных состояний, но не учитывают эффектов взаимодействия субъектов коммуникации в общей информационной среде. Модели, предложенные в работе [12], учитывают многоагентное взаимодействие, однако модель включает в себя всего один информационный повод.

Известные динамические модели индивидуальных и групповых психических процессов [13] в настоящее время не способны адекватно описать некоторые принципиально важные свойства эмоций, имеющие теоретическое обоснование и подтвержденные результатами экспериментальных исследований. Модели убеждения и распространения влияний [14, 15], в свою очередь, не учитывают относительно короткий срок существования эмоциональных состояний, их нерациональность, нелинейную зависимость от внешних и внутренних факторов, в том числе имеющих субъективную и стохастическую природу.

Отдельные вычислительные модели способны довольно точно воспроизводить динамику макроскопических показателей коллективных эмоций в онлайн-сообществах, однако практически непригодны для аналитической интерпретации полученных результатов. Кроме того, значительная часть таких моделей имеют исключительно умозрительный характер и основаны на гипотезах, не имеющих достаточно прочного теоретического обоснования в психологии и социологии. Частные модели, разработанные для конкретных событий (например, [16]) и онлайн-сообществ [17], имеют сильную привязку к моделируемым процессам либо механизмам информационного взаимодействия членов этих конкретных онлайн-сообществ и не обладают достаточным уровнем универсальности.

В рамках настоящего исследования была принята попытка устранить указанные противоречия и разработать модель процессов, происходящих при непрямом распространении эмоционально окрашенной информации в социальных сетях с учетом различных когнитивных состояний участников коммуникации и при различных информационных поводах. Дополнительной целью являлась проверка адекватности аналогии между эффектами, наблюдаемыми в ходе непрямого информационно-эмоционального взаимо-

действия пользователей социальных сетей, и интерференционной картиной, получаемой в ходе широко известного в квантовой физике эксперимента с двумя щелями.

Интерференция или эксперимент с двумя щелями, согласно Р. Фейнману, «заключает в себе сердце квантовой механики» и является квинтэссенцией принципа квантовой суперпозиции. Принцип интерференции как основной принцип волновой оптики впервые был сформулирован в 1801 году Т. Юнгом. Ученый так наглядно поясняет открытый им принцип (эксперимент, известный в наше время под названием «двухщелевой эксперимент Юнга»): «для получения эффектов наложения двух порций света необходимо, чтобы они исходили из одного источника и приходили в одну и ту же точку по разным путям, но по близким между собой направлениям». В рамках рассматриваемой аналогии интерференционная картина сложных коллективных эмоций формируется в результате прохождения одного и того же (априори эмоционально нейтрального) информационного сообщения, публикуемого в сообществе, через когнитивные каналы пользователей, опосредованно взаимодействующих между собой и оказывающих влияние на эмоциональное состояние других пользователей.

В ходе проведения экспериментального исследования были выполнены следующие основные этапы: получение доступа к сообщениям открытого сообщества социальной сети «ВКонтакте»; сбор и селекция исходных данных посредством официального программного интерфейса приложения (API) с применением функционально-ориентированного языка программирования высокого уровня Python; формирование априорного признакового пространства экспериментальной модели; выявление наиболее информативных признаков и значимых факторов с формированием ортогонального базиса некоррелированных главных компонент; статистическая обработка и визуализация результатов исследования.

В рамках частных сопутствующих подзадач разработаны специализированные программные модули сбора, обработки и визуализации данных из социальных сетей и сети Интернет.

Эмоциональные состояния субъектов коммуникации, описанные в координатном пространстве двух психологических переменных: валентности и эраузала [7], в рамках проведенного эксперимента интерпретировались как квантовые состояния, причём валентность соотносилась с координатой, а эраузал (энергетическая психологическая переменная) — с импульсом частицы. С квантовой точки зрения две данные переменные линейно независимы, то же справедливо для предлагаемой концепции представления эмоциональных состояний пользователей в момент отправки сообщений в координатах «валентность-эраузал».

Главными результатами экспериментального исследования являются полученные эмпирические распределения наблюдаемых признаков, характеризующие

состояния акторов социальной сети в процессе непрямого распространения эмоционально окрашенной информации в социальных сетях, а также их интерпретация, подтверждающая гипотезу о квантовоподобном характере непрямого взаимодействия акторов социальной сети. В частности, продемонстрирована аналогия феномена светоиндуцированной прозрачности, известного в квантовой оптике, с существенным ослаблением восприимчивости сетевого сообщества к эмоционально нейтральным сообщениям в результате сложного информационного взаимодействия между собой и сильным информационным полем.

Модель индивидуальных эмоциональных состояний субъектов массовой коммуникации

В основу исследования положены модели формального представления базовых эмоций в координатном пространстве «валентность-эраузал» Дж. Рассела, модель броуновского взаимодействия, а также технология автоматического анализа эмоциональной тональности текстов («сентимент-анализ») на основе передовой мультимодальной большой языковой модели (БЯМ) GPT-4o⁵.

Важным в контексте описываемой модели является обоснованное допущение о том, что эмоции индивидуальных акторов (агентов принятия решения) информационно-коммуникационного процесса транслируются обратно в средства массовой коммуникации и становятся, таким образом, достоянием всего сообщества пользователей информационного ресурса. Очевидно, однако, что пользователи обмениваются не самими эмоциями, а сообщениями, несущими определенную эмоциональную нагрузку и способными вызвать изменение эмоционального состояния у других пользователей, прочитавших данное сообщение. В зависимости от результата информационного воздействия, реципиент сообщения может либо принять решение включиться в коммуникацию и передать свое отношение (позитивное или негативное) другим пользователям, либо проигнорировать сообщение. При определенных условиях описанная модель коммуникации может наблюдаться в малых группах, однако чаще подобный сценарий наблюдается в онлайн-сообществах, насчитывающих тысячи пользователей. При этом субъекты коммуникации могут выражать свои эмоции однократно, регулярно-последовательно или спорадически. Возникающий при этом коллективный эмоциональный фон не всегда является однородным. Чаще наблюдается возникновение двух конкурирующих коллективных эмоций: «негативной» и «позитивной», что является отражением социокультурной неоднородности общества. Как правило, интенсивность обмена эмоциями угасает с течением времени, однако при срабатывании определенного триггера (внешнее событие или публи-

кация нового сообщения) может наблюдаться новый всплеск.

Пусть моделируемая система состоит из N взаимодействующих агентов. Броуновский агент может быть описан набором переменных состояния u_i^k , где $i = 1, \dots, N$ — номер агента, а k — номер соответствующей переменной. Переменные состояния могут быть представлены как внешними (то есть доступными для наблюдения) параметрами, так и внутренними степенями свободы, оценка которых возможна лишь по косвенным признакам. Значения переменных, как внешних, так и внутренних, могут изменяться с течением времени, либо вследствие внешних воздействий среды, либо в силу внутренней динамики. Таким образом, в наиболее общем виде динамика изменения переменных состояний может быть описана следующим уравнением:

$$\frac{du_i^k}{dt} = f_i^k + \mathcal{F}_i^{stoch}. \quad (1)$$

Уравнение (1) является отражением принципа причинности: любое изменение состояния агента во времени обусловлено воздействием некоторой совокупности факторов. Для концепции броуновского взаимодействия агентов за основу принято следующее допущение: всякое изменение состояния может быть описано как суперпозиция детерминированного и стохастического воздействия на агента i . Данное допущение, в свою очередь, базируется на гипотезе Ланжевена относительно описания броуновского движения.

Таким образом, совокупность ненаблюдаемых воздействий описывается обобщенным стохастическим компонентом $\mathcal{F}_i^{stoch}$, а совокупность детерминированных воздействий представлена компонентом f_i^k . При этом стохастическая составляющая вовсе не обязательно должна обладать характеристиками белого шума. Напротив, весьма вероятно присутствие и даже доминирование в ней окрашенных и мультипликативных шумов. Значимость влияния стохастической компоненты на конкретную переменную состояния может варьироваться для различных агентов. Влияние на неё могут оказывать как внешние параметры среды, так и внутренние степени свободы агента. Детерминированная составляющая f_i^k объединяет все поддающиеся наблюдению и моделированию факторы, которые способны вызвать изменение переменной состояния u_i^k . К ним может относиться взаимное влияние агентов друг на друга, имеющее нелинейный характер, поэтому в общем случае f_i^k может быть функцией от всех переменных состояния, описывающих любого агента, включая агента i .

Однако в соответствии с предложенной концепцией детерминированный компонент f_i^k должен позволять моделировать результат воздействия на агента со стороны внешней информационной среды, а также реакцию агента на поступившую информацию. Помимо этого, компонент f_i^k должен отражать внутреннюю динамику эмоций агента, заключающуюся в постепен-

⁵ Hello GPT-4o. URL: <https://openai.com/index/hello-gpt-4o/> (дата обращения: 04.01.2025).

ном затухании значений переменных состояния вследствие достижения эмоционального насыщения или истощения. Чтобы описать моделируемую многоагентную систему, нам необходимо в явном виде указать переменные состояния u_i^k и динамические законы их изменения с течением времени f_i^k . При этом следует подчеркнуть, что эмерджентность, проявляющаяся в возникновении феномена коллективных эмоций, порождается не на макроскопическом уровне, а исключительно на «микроскопическом» уровне индивидуальных агентов вследствие их многократного взаимодействия между собой. Для представления состояния агента i будем использовать две линейно независимые переменные: валентность $v_i(t)$ и эраузал $a_i(t)$, которые задают двумерное фазовое пространство (плоскость) эмоций. Значение валентности отражает позитивный или негативный характер эмоции, а эраузал — уровень активности (возбуждения), порождаемой конкретной эмоцией. Таким образом, эмоциональное состояние агента $e(t)$ в любой момент времени может быть указано парой координат на плоскости: $e(t) = v_i(t), a_i(t)$. Например, «восхищение» — это состояние, при котором значения эраузала и валентности положительны; «удовлетворённость» — комбинация положительной валентности и отрицательного эраузала; «депрессия» — крайнее проявление отрицательных значений эраузала и валентности; «раздражение» — сочетание отрицательной валентности и положительного эраузала и т. д. (рис. 1).



Рис. 1. Условное представление различных эмоциональных состояний в координатном пространстве «валентность-эраузал»

Подчеркнём, что обе переменные $e(t) = v_i(t)$, описывают внутреннюю динамику состояний агента, не доступны для непосредственного наблюдения и могут быть оценены только по косвенным признакам, например, посредством тестирования или психофизиологического обследования. В рамках разрабатываемой модели примем в качестве допущения, что при отсутствии внешних возбудителей эмоциональное состояние агента с течением времени стремится к нейтральному равновесному состоянию:

$$e_i(t) \xrightarrow{t \rightarrow \infty} 0, \text{ т. е. } v_i(t) \xrightarrow{t \rightarrow \infty} 0, a_i(t) \xrightarrow{t \rightarrow \infty} 0. \quad (2)$$

Тогда уравнение (1) может быть представлено в следующем виде:

$$\begin{cases} \dot{v}_i = -\gamma_{vi}v_i(t) + \mathcal{F}_v + A_{vi}\xi_v(t) \\ \dot{a}_i = -\gamma_{ai}a_i(t) + \mathcal{F}_a + A_{ai}\xi_a(t) \end{cases} \quad (3)$$

где коэффициенты γ_{vi} и γ_{ai} характеризуют скорость экспоненциального затухания значений валентности и эраузала соответственно для i -го агента при отсутствии внешних раздражителей; $\mathcal{F}_v$ и $\mathcal{F}_a$ — детерминированные компоненты динамики валентности и эраузала; $\xi_v(t)$ и $\xi_a(t)$ — стохастические значения валентности и эраузала; A_{vi} и A_{ai} — весовые коэффициенты, отражающие степень влияния стохастических факторов на значения валентности и эраузала i -го агента.

Конкретный вид аналитических выражений, моделирующих детерминированные компоненты $\mathcal{F}_v$ и $\mathcal{F}_a$, зависит от множества допущений, сделанных нами относительно как внешних факторов (таких, например, как процессы взаимодействия агентов и процедуры их доступа к информационному пространству), так и внутренних (уровень эмпатии агентов в сообществе, активность обмена информацией и прочее). Однако представляется справедливым, что в наибольшей степени данные компоненты должны зависеть от эмоциональных состояний самих агентов. Иными словами, те агенты, которые уже находятся в определённых эмоциональных состояниях, должны демонстрировать более сильную реакцию на эмоционально окрашенные сообщения (того же или противоположного знака), поступившие от других пользователей. Прежде чем подробно рассмотреть вид функций $\mathcal{F}_v$ и $\mathcal{F}_a$ рассмотрим описание информационной активности агентов.

В случае, если совокупное влияние детерминированной и стохастической компонент настолько мало, что им можно пренебречь, динамика эмоциональных состояний, определяемая (3), подразумевает наличие стационарного состояния $e_i(t) \xrightarrow{t \rightarrow \infty} 0$. Однако если агент получает из внешней среды эмоционально значимую информацию, то детерминистская и стохастическая компоненты уравнения (3) могут компенсировать естественное затухание абсолютных значений валентности и эраузала, а в ряде случаев приводят к их скачкообразному увеличению. В этом случае агент переходит в возбуждённое состояние, которое, однако, не является наблюдаемым до тех пор, пока агент не проявит данный факт посредством публикации сообщения в средствах массовой коммуникации.

Иными словами, гипотеза заключается в том, что агент косвенным образом демонстрирует текущее значение переменной валентности (т. е. своё позитивное или негативное отношение к чему-либо) лишь в тех случаях, когда значение эраузала превышает некоторое пороговое значение τ_i , индивидуальное для каждого

агента. В целях упрощения дальнейших рассуждений будем исходить из допущения, что если пороговое значение эраузала достигнуто, то агент в своем сообщении передаёт лишь часть информации о своём эмоциональном состоянии, а именно — знак валентности v_i (+1 или -1):

$$s_i(t + \Delta t) = \text{sign}(v_i(t))\Theta[a_i(t) - \tau_i], \quad (4)$$

где $\Theta[a_i(t)]$ — оператор Хевисайда от переменной эраузала, который принимает значение 1, если $a_i \geq 0$ и 0 — в остальных случаях.

Введённое допущение о бинарном характере проявляемых значений валентности не ведёт к потере общности следующих рассуждений и является необходимым только с практической точки зрения для упрощения построения базовой модели. Уравнение (4) также отражает тот факт, что агент не демонстрирует изменение своей валентности посредством публикации в средствах массовой коммуникации непосредственно в момент, когда значение эраузала превышает некое индивидуальное пороговое значение. Чаще между данным событием и публикацией сообщения наблюдается временная задержка Δt , которая может быть обусловлена такими причинами, как, например, отсутствие доступа к средствам передачи информации или высокая загруженность текущими делами. Очевидно, что должна существовать зависимость между субъективной значимостью эмоции и длительностью задержки (чем эмоции сильнее, тем меньше задержка). Исходя из результатов известных исследований по определению закона распределения времени задержки между возникновением потребности (постановкой задачи) и началом ее реализации в различных видах человеческой деятельности (например, при ответе на электронные письма), мы можем предположить, что случайная величина Δt распределена по степенному закону $P(\Delta t) \propto \Delta t^{-\alpha}$, где параметр α должен быть определен эмпирическим путем.

Из выражения (4) может быть получена оценка количества публикаций эмоционально окрашенных сообщений за данный промежуток времени как

$$N_s(t) = \sum_i \Theta[a_i(t) - \tau_i] \quad (5)$$

В случае непрерывного времени среднее количество таких сообщений за заданный интервал времени может быть получено в виде:

$$N_s(t) = \sum_i \Theta[a_i(t) - \tau_i] \quad (6)$$

Таким образом, уравнения 1—6 описывают внутреннюю динамику эмоций отдельного агента, которая приводит к внешне наблюдаемому проявлению эмоционального состояния через публикацию сообщения в сетевом сообществе. Для того, чтобы перейти к моделированию коллективных эмоций, необходимо формально описать процесс взаимодействия этого сообщения с другими агентами, действующими в общем информационном пространстве.

Динамическая модель коллективных эмоций

Будем исходить из допущения, что сообщения, имеющие позитивную или негативную эмоциональную окраску, формируют в соответствии со знаком своей валентности информационные поля $h_+(t)$ и $h_-(t)$. Совокупность этих полей h_+ образует коммуникационную среду, в которой происходит обмен эмоциональными сообщениями между авторами и читателями блогов, участниками форумов и т. д. Пусть публикация сообщения $s_i(t)$ каждым из агентов увеличивает значение h_+ или h_- на фиксированное значение s в промежутке времени t . Также примем, что значимость и мера влияния сообщения на других агентов убывает с течением времени (то есть, например, старые сообщения в блоге вызывают меньший эмоциональный отклик у подписчиков, чем недавно размещённые). Наконец, на динамику информационного поля могут оказывать влияние внешние факторы, имеющие в общем случае стохастическую природу. Тогда динамика количества сообщений, имеющих положительную и отрицательную окраску, в нашей модели может быть описана следующим аналитическим выражением

$$\dot{h}_{\pm} = -\gamma_{\pm}h_{\pm}(t) + sN_{\pm}(t) + I_{\pm}(t), \quad (7)$$

где $\gamma_{\pm}$ — коэффициент затухания эмоциональной значимости сообщения; $N_{\pm}(t)$ — совокупное количество агентов, оставивших положительные или отрицательные сообщения в промежуток времени t ; $I_{\pm}(t)$ — влияние стохастических факторов на соответствующее информационное поле. Схематичное изображение связей между основными элементами разработанной модели представлено на рис. 2.

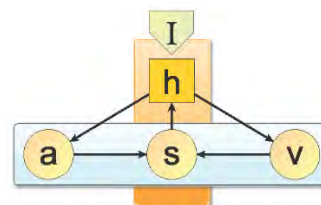


Рис. 2. Связи между основными элементами модели коллективных эмоций

Отметим, что представленную модель можно условно разделить на два слоя: внутренний слой, отражающий динамику изменения переменных агента (на рисунке изображен горизонтально) и внешний слой, описывающий непосредственно процесс коммуникации (изображен вертикально). На внутреннем слое психологические переменные (эразал и валентность) определяют наличие и знак тональности сообщения s , которое достигает внешнего слоя посредством публикации в информационном поле h . Поле h , в свою очередь, обладает собственной динамикой (см. (7)) и подвержено влиянию внешних стохастических факторов I . Замыкание причинно-следственных связей модели происходит за счет наличия обратного воздействия информационного поля h на валентность и эразал каждого агента.

Для того, чтобы модель приобрела завершённый вид, необходимо рассмотреть процесс воздействия информационного поля h на эмоциональное состояние агентов, то есть формально описать вид функций $\mathcal{F}_v$ и $\mathcal{F}_a$.

В контексте решаемой задачи наша гипотеза заключается в том, что эмерджентный феномен коллективных эмоций не может быть сведен к совокупности внутренних эмоциональных состояний агентов. Эмоциональное состояние одного агента может прямым или косвенным образом влиять на эмоциональные состояния других агентов, порождая весьма сложные картины взаимодействия.

В соответствии с предложенной гипотезой результат воздействия информационного поля зависит от знака текущего эмоционального состояния самого агента.

Так, например, если мы предположим, что агенты с положительной валентностью в основном реагируют на позитивный информационный контент (и наоборот), то выражение для $\mathcal{F}_v$ может быть представлено в следующем виде:

$$\mathcal{F}_v \propto \frac{r_i}{2} \{ (1 + r_i) f[h_+(t)] - (1 - r_i) f[h_-(t)] \}, \quad (8)$$

где $r_i = \text{sign}(v_i(t))$ и $f(h_{\pm}(t))$ — некоторые функции, зависящие от h_+ или h_- . Тогда при положительной валентности агента ($r_i(t) = +1$) выражение (8) сводится к $\mathcal{F}_v \propto f[h_+(t)]$, а при отрицательной валентности $r_i(t) = -1$ имеем $\mathcal{F}_v \propto f[h_-(t)]$.

При этом вполне очевидно, что сама функция должна иметь нелинейный характер. Для моделирования этой зависимости может быть использована полиномиальная функция вида:

$$f[h_{\pm}, v_i(t)] = h_{\pm}(t) \sum_{k=0}^n b_k v^k(t), \quad (9)$$

где коэффициенты b_k определяют вид функции. В рамках настоящего исследования они полагаются одинаковыми для положительных и отрицательных валентностей, хотя в общем случае могут принимать различные значения.

Представляется оправданным также применение для моделирования детерминированной составляющей эраузала и валентности сигмоиды (монотонно возрастающей всюду дифференцируемой S-образной нелинейной функции с насыщением). Существенным для нашей модели свойством сигмоиды является ее способность усиливать слабые сигналы и не насыщаться от сильных сигналов. Примером сигмоидальной функции активации может служить логистическая функция, задаваемая выражением:

$$y = \frac{1}{1 + e^{-\alpha x}} \quad (10)$$

где α — параметр наклона сигмоидальной функции активации. Изменяя этот параметр, можно построить функции с различной крутизной.

Как было сказано выше, эраузал как психологическая переменная отражает готовность проявлять активность в соответствии со значением переменной валентности. Если эраузал превышает некое пороговое значение, то агент выражает свои эмоции путем публикации сообщения. При этом сам факт выражения эмоций оказывает влияние на результирующее значение эраузала. В частности, будет логичным предположить, что после совершения акта коммуникации величина эраузала уменьшается или, в самом простом случае, возвращается к начальному значению.

Формальное описание динамики эраузала, таким образом, может быть условно разделено на два интервала: до достижения порога и после. Обозначим допороговую динамику в виде $\dot{a}$. Тогда выражение (3) для эраузала может быть представлено в виде:

$$\dot{a}_i = \dot{a}(t) \Theta[\tau_i - a_i(t)] - a_i(t) \Theta[a_i(t) - \tau_i] \quad (11)$$

До тех пор, пока $x = \tau_i - a_i(t) > 0$, $\Theta[x] = 1$, динамика эраузала определяется значением $\dot{a}$. Однако после достижения порогового значения $x \geq 0$, $\Theta[x] = 0$, $\Theta[-x] = 1$, значение эраузала возвращается к нулевому значению за счет слагаемого $-a_i(t)$.

Итоговый вид функции $\mathcal{F}_a$ для допороговых значений эраузала определяется принятыми нами гипотезами относительно характера изменения данной психологической переменной.

В частности, можно допустить, что изменение эраузала агентов пропорционально сумме сообщений позитивной и негативной тональности, размещенных в информационном поле h_+ , а также нелинейным образом зависит от текущего значения эраузала и не зависит от состояния валентности агента:

$$\mathcal{F}_a \propto [h_+(t) + h_-(t)] \sum_{k=0}^n d_k a^k(t) \quad (12)$$

С другой стороны, может быть рассмотрена модель, в рамках которой агенты реагируют на доступную информацию только в том случае, когда их значение эраузала положительно, поскольку отрицательные значения эраузала связаны с состояниями низкой активности (усталость, сонливость, депрессия, скука). В данном случае для описания эраузала может быть предложена линейная функция зависимости вида:

$$\mathcal{F}_a \propto [h_+(t) + h_-(t)] a(t) \Theta[a(t)]. \quad (13)$$

Однако наиболее правдоподобной нам представляется следующая гипотеза: агенты реагируют на размещенные в информационном поле сообщения определенной валентности в том случае, если их эраузал положителен, а значение внутренней переменной валентности агента противоположно по знаку валентности соответствующего информационного поля. Иными словами, внутренний протест и желание проявить активность в поддержку собственного мнения вызывает

post_id	date	from_id	text	likes	reposts	_of_coi	pos	neg	explanation
Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фи...	Фи...	Фильтр
1261198	2018-04-20...	-50377583	Балтфлот двинет в поход на Англию, ...	102	16	55	2	4	The text expresses aggressive and confrontational ...
1261223	2018-04-20...	-50377583	Самый опасный город для женщин ждет...	76	10	53	1	5	The text discusses the dangers that women face in...
1261235	2018-04-20...	-50377583	Космический майнстрим: технологии, ...	76	11	22	4	2	The text primarily conveys a positive sentiment ...
1261253	2018-04-20...	-50377583	Мировая отслеживает эту тему. Мы ...	52	2	12	5	2	The text expresses strong positive sentiment ...
1261265	2018-04-20...	-50377583	Немцы взмолились об отмене ...	109	13	32	3	4	The sentiment of the text is mixed, with elements ...
1261292	2018-04-20...	-50377583	Понтиак с топором войны ...	106	23	5	4	2	The text discusses Pontiac, a historical figure ...
1261316	2018-04-20...	-50377583	Безумная затея: экранопланы с ...	79	5	9	2	4	The text discusses screenoplanes with ...
1261332	2018-04-20...	-50377583	#ИсторияМП #ВОВ_МП	121	18	7	3	2	The text includes hashtags related to history and ...
1261343	2018-04-20...	-50377583	Русский ответ на американскую ...	93	10	17	1	4	The text discusses serious and grave topics ...
1261360	2018-04-20...	-50377583	иBloomberg: Израиль уничтожит все ...	141	13	58	1	4	The text primarily discusses geopolitical tension...
1261397	2018-04-20...	-50377583	Чем способен ответить американской ...	138	13	51	2	4	The text discusses military capabilities and ...
1261422	2018-04-20...	-50377583	Итальянская энергокомпания Eni не ...	92	4	2	3	2	The text expresses a neutral to slightly positive ...
1261438	2018-04-20...	-50377583	Нефть рвется вверх...	69	7	4	4	1	The text discusses an increase in oil prices and ...
1261451	2018-04-20...	-50377583	Асад отправил почтой императору ...	656	49	34	2	4	The text discusses actions taken by Assad regardi...
1261501	2018-04-20...	-50377583	Программа Littoral Combat Ship: ...	59	3	11	2	4	The text discusses the Littoral Combat Ship progr...

Рис. 3. Фрагмент таблицы *posts* базы данных SQLite, содержащей обработанные сообщения со страницы сообщества «Мировая политика» и результаты их сентимент-анализа

несогласие с превалирующей в информационном поле тональностью сообщений относительно обсуждаемого факта, объекта, явления или события:

$$\begin{cases} h_+(t)\Theta[a(t)] \sum_{k=0}^n d_k a^k(t), & \text{если } v(t) < 0 \\ h_-(t)\Theta[a(t)] \sum_{k=0}^n d_k a^k(t), & \text{если } v(t) \geq 0 \end{cases} \quad (13)$$

Схема проведения экспериментального исследования

Для обоснованного применения методов машинного обучения, интеллектуального анализа данных и сентимент-анализа в целях экспериментальной проверки выдвинутых гипотез требовалось обеспечить сбор 10^3 — 10^4 текстовых сообщений и комментариев к ним, публикуемых пользователями на страницах сообществ в социальных сетях. В качестве непосредственного объекта исследования была выбрана социальная сеть «ВКонтакте», доступ к которой осуществлялся посредством модуля (библиотеки) *vk* для языка программирования Python и официального API.

Всего по итогам проведения экспериментального исследования анализу подвергнуто 2246 сообщений и 50326 комментариев к ним с главной страницы сообщества «Мировая политика» с декабря 2017 по июнь 2018 года. Длина анализируемого текста для каждого сообщения или комментария ограничивалась 500 символами.

Для получения количественных оценок значений скрытых психологических переменных (валентности и эраузала) сообщений, оставляемых пользователями сообщества социальной сети на главной странице и в комментариях к публикациям, была применена технология сентимент-анализа на основе одной из наиболее эффективных мультимодальных языковых моде-

лей — GPT-4 Omni от компании OpenAI. Использование БЯМ, в отличие от наиболее распространенных методов сентимент-анализа, основанных на применении словарей, позволило учитывать контекст сообщений и такие традиционно сложные для анализа машинными методами особенности межличностной коммуникации, как ирония и сарказм. Предложенный подход также позволил отразить в количественной оценке валентности присутствующие в эмоционально окрашенных сообщениях специальные символы («смайлы»), выражающие отношение автора к обсуждаемой теме. Для оценивания валентности (положительной или отрицательной) была использована пятибалльная шкала, где оценка «-5» соответствует крайне негативному отношению пользователя, а «+5» — крайне позитивному.

Фрагмент таблицы *posts* базы данных, содержащей обработанные комментарии и результаты их сентимент-анализа, представлен на рис. 3.

Столбцы таблицы *posts* имеют следующие значения: *post_id* — уникальный идентификационный номер сообщения сообщества; *date* — дата и время публикации сообщения; *from_id* — уникальный идентификационный номер отправителя сообщения; *text* — текст сообщения, очищенный от xml и html тегов; *likes* — количество «лайков», собранных сообщением; *reposts* — количество репостов; *number_of_comments* — количество комментариев к сообщению; *pos* — количественная оценка позитивной составляющей тональности сообщения (по шкале от 1 до 5), вычисленная на основе применения БЯМ GPT-4 Omni; *neg* — количественная оценка негативной составляющей тональности сообщения (по шкале от 1 до 5); *explanation* — сгенерированное БЯМ текстовое пояснение к результатам сентимент-анализа.

Фрагмент таблицы *comments* базы данных, содержащей обработанные комментарии и результаты их сентимент-анализа, представлен на рис. 4.

Столбцы таблицы *comments* имеют следующие значения: *comment_id* — уникальный идентификационный номер комментария; *to_post_id* — уникальный идентификационный номер сообщения, к которому

⁶ URL: https://vk.com/world_policy

comment_id	to_post_id	from_user_id	date	text	likes	pos	neg	explanation
Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фи...	Фи...	Фи...	Фильтр
1320390	1320353	334162241	2018-06-10 20:01:06	[id208328721 Артур], подробнее про ...	5	1	4	The text expresses a somber and ...
1320389	1320316	484731702	2018-06-10 20:01:02	[id696822 Дмитрий], да пусть ...	0	2	5	The text expresses a clear negative...
1320386	1320353	119660675	2018-06-10 20:00:55	[id208328721 Артур], статистику ...	8	1	4	The text expresses frustration and ...
1320385	1320353	159471791	2018-06-10 20:00:31	Им надо больше учений проводить, ...	1	2	4	The text expresses a sense of ...
1320384	1320353	163471571	2018-06-10 20:00:00	[id34516363 Федор], 😊😊😊	0	5	1	The text contains positive emojis ...
1320383	1320353	34516363	2018-06-10 19:59:26	[id163471571 Ирина], я не причем, ...	1	1	4	The text contains a reference to ...
1320381	1320353	163471571	2018-06-10 19:58:17	Хочется плескаться в ладоши...	0	5	1	The phrase 'Хочется плескаться в ...
1320379	1320316	238192922	2018-06-10 19:57:44	Свой дурак куда проблемней уминого ...	6	2	4	The text expresses a sentiment that...
1320380	1320209	441199915	2018-06-10 19:57:44	[id64322708 Болеслав], ну и чего - ...	0	1	4	The text expresses frustration or ...
1320378	1320316	484731702	2018-06-10 19:57:25	[id259872739 Виталий], какой ты ...	3	2	4	The text primarily conveys a mockin...
1320376	1320316	696822	2018-06-10 19:57:21	[id259872739 Виталий], это же юмор!...	4	3	4	The text has a humorous tone at the...
1320377	1320353	163471571	2018-06-10 19:57:21	[id34516363 Федор], блеск!!!👍👍👍	0	5	1	The text expresses a strong positiv...
1320375	1320316	44573392	2018-06-10 19:55:43	Теперь Истоники придётся дружить с ...	2	2	4	The text expresses a mix of ...
1320374	1320316	153788741	2018-06-10 19:55:22	Виталий, это вроде сарказм был)	5	2	3	The text appears to imply a ...
1320373	1320353	426225431	2018-06-10 19:55:09	Как говорят янки, сопутствующие ...	0	4	2	The text conveys a somewhat ...
1320371	1320209	215421875	2018-06-10 19:53:17	[id51004419 Константин], на душу ...	0	2	2	The text expresses a neutral ...

Рис. 4. Фрагмент таблицы comments базы данных SQLite, содержащей обработанные комментарии пользователей и результаты их sentiment-анализа

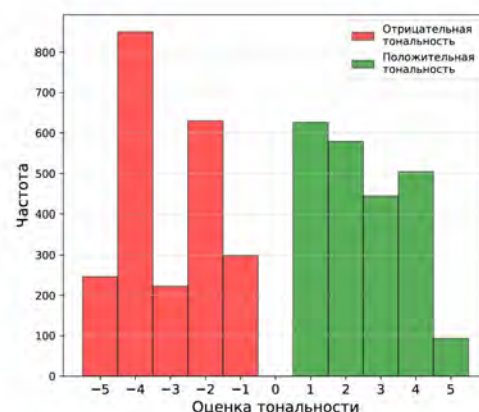
адресован комментарий; from_user_id — уникальный идентификационный номер отправителя комментария; date — дата и время публикации комментария; text — текст комментария, очищенный от xml и html тегов; likes — количество «лайков», полученных комментарием; pos — количественная оценка позитивной составляющей тональности комментария (по шкале от 1 до 5), вычисленная на основе применения БЯМ GPT-4 Omni; neg — количественная оценка негативной составляющей тональности комментария (по шкале от 1 до 5); explanation — сгенерированное БЯМ текстовое пояснение к результатам sentiment-анализа.

Необходимо особо отметить, что для каждого сообщения одновременно оценивались обе составляющие тональности сообщения: позитивная и негативная, что является отражением эллиптичности естественного языка и невозможности точно зафиксировать эмоциональное состояние как в результате внешнего наблюдения, так и в результате рефлексии (например, словосочетание «геройская смерть» несет в себе как негативную (смерть), так и позитивную (геройская) компоненты. Вне контекста практически невозможно дать точную оценку тональности данного сообщения одной переменной). Текстовые комментарии, сгенерированные БЯМ и добавленные в столбец explanation, позволяют провести контроль качества sentiment-анализа и могут служить основой для дальнейших исследований, направленных на повышение качества распознавания большими языковыми моделями эмоциональной тональности семантически сложных текстовых сообщений на русском языке.

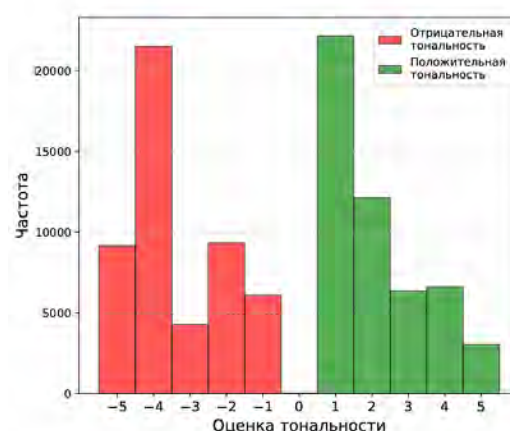
Результаты экспериментального исследования

В результате обработки полученных экспериментальных данных установлено, что в содержании сообщений и комментариев к ним преобладает отрица-

тельная тональность, что может объясняться сложной международной политической обстановкой в рассматриваемый временной период (рис. 5).



а) Гистограмма тональностей сообщений



б) Гистограмма тональностей коммент

Рис. 5. Гистограмма тональности сообщений (а) и комментариев к ним (б)

Далее для анализа корреляционных зависимостей между полученными числовыми характеристиками и обоснованного сокращения размерности признакового пространства к данным таблицы posts применен метод главных компонент (МГК). При этом осуществлена проверка на выполнение необходимых условий применения МГК: все признаки должны быть количественными, поэтому матрица исходных данных составлена из столбцов (5—9 таблицы posts); число наблюдений должно быть не менее чем в два раза больше числа переменных; выборка должна быть однородна;

исходные переменные должны быть распределены симметрично.

Для обеспечения выполнения последнего условия для данных выполнена процедура стандартизации данных (приведение к центрированным нормированным значениям) по формуле: $Z = \frac{x - \bar{x}}{\sigma}$, где $\bar{x}$ — выборочное среднее, σ — оценка среднеквадратического отклонения. Строкам матрицы исходных данных соответствовали наблюдения, столбцам — переменные. Полученная по итогам вычислений матрица коэффициентов (факторных нагрузок) представлена в табл. 1.

Таблица 1

Матрица факторных нагрузок метода главных компонент

Исходные переменные	Главные компоненты				
	1	2	3	4	5
likes	0.5803	0.3387	-0.2101	-0.1037	0.7026
reposts	0.5427	0.4008	-0.227	0.0775	-0.698
number_of_comments	0.1249	0.3573	0.9256	-0.0071	0.0003
pos	0.4301	-0.537	0.1547	0.7070	0.0542
neg	-0.41	0.5555	-0.1538	0.6953	0.1275

Столбцам матрицы факторных нагрузок соответствуют главные компоненты (в порядке значимости вклада в описываемую дисперсию), строкам — исходные переменные. Полученный базис является строго ортогональным (в чем можно убедиться путем умножения полученной матрицы нагрузок на себя же транспонированную, получив единичную матрицу) и нормированным. Полученная матрица оценок (координаты исходных наблюдений в ортогональном базисе полученных главных компонент) имеет размерность 2246×5 и не приводится в целях экономии места.

Процентный вклад главных компонент в описание суммарной дисперсии выглядит следующим образом: 1-я — 40,1%; 2-я — 34,9%, 3-я — 17,4%; 4-я — 4,18%; 5-я — 3,4%. Из анализа матрицы факторных нагрузок очевидно, что для первой главной компоненты максимальный вклад вносят исходные переменные № 1 («лайки») и № 2 («репосты»). Для второй ГК основной вклад вносят переменные № 4 (оценка позитивной тональности) и № 5 (оценка негативной тональности). Для третьей ГК наибольший по абсолютному значению вклад вносит переменная № 3 (количество комментариев). Таким образом, может быть сделан следующий вывод: первая главная компонента, которая в ходе проводимого эксперимента проявляется в количестве «лайков» и «репостов», характеризует

«побудительную силу» или «импульс» анализируемого текстового сообщения. Вторая главная компонента, в свою очередь, отвечает за эмоциональную окраску или «валентность», что полностью соответствует принятой в психологии системе координат «валентность-эраузал», в которой может быть описано любое психоэмоциональное состояние индивида — от депрессии до эйфории.

Представим наглядно полученные главные компоненты и исходные переменные в новом базисе (рис. 6). Стрелками на рис. 6 показаны исходные 5 параметров («лайки», «репосты», комментарии, позитивная и негативная оценки тональности соответственно) в новом ортонормированном базисе 3-х главных компонент. Каждая отдельная точка представляет публикацию на стене сообщества. Хорошо заметно, что исходные признаки («лайки» и «репосты») сильно коррелированы и являются проявлением одного и того же скрытого фактора — «побудительной силы» или «импульса» сообщения.

Трехмерная гистограмма, отображающая количественное соотношение пар полученных экспериментальным путем оценок «эмоциональных» и «энергетических» параметров для 50326 комментариев акторов сообщества «Мировая политика» социальной сети «ВКонтакте», представлена на рис. 7.

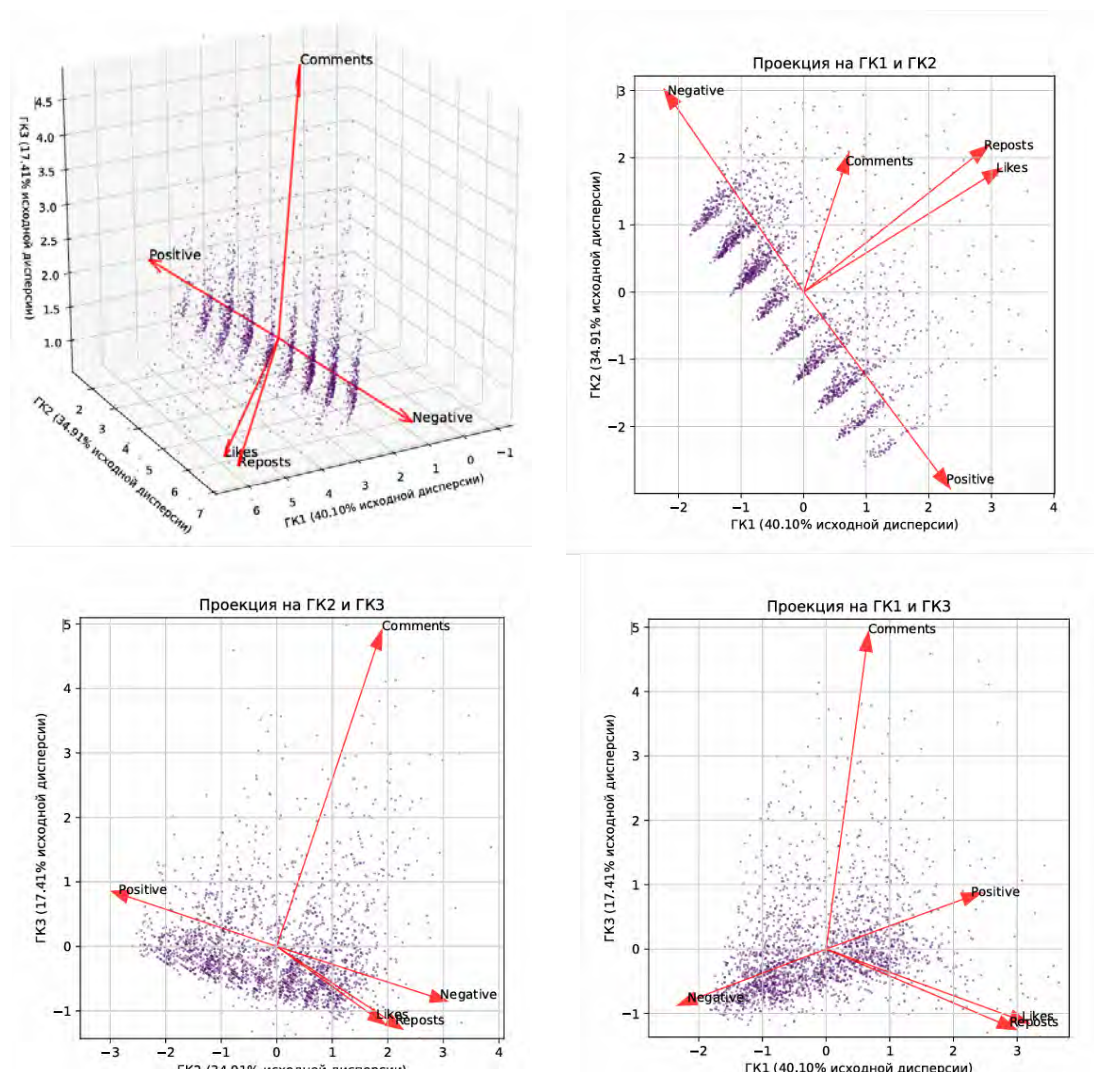


Рис. 6. Исходные переменные в новом ортогональном базисе главных компонент

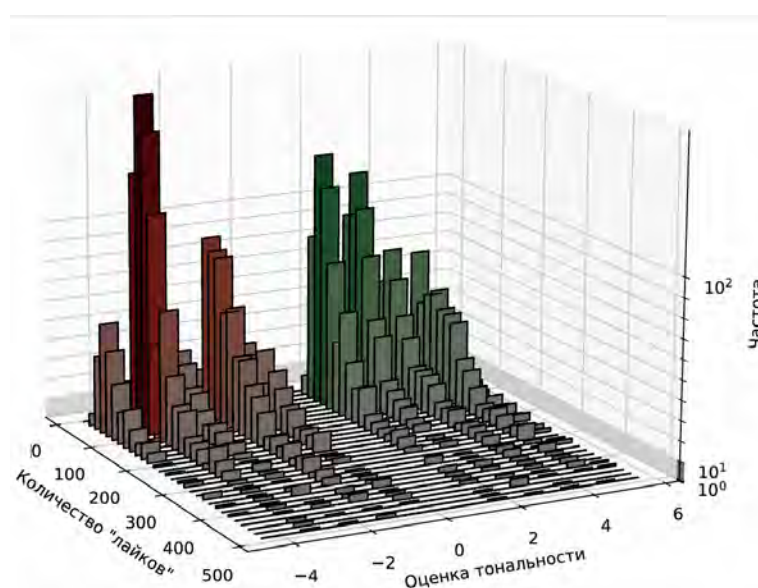


Рис. 7. Количественное соотношение пар полученных экспериментальным путем оценок «эмоциональных» и «энергетических» параметров для 2246 постов социальной сети

Обсуждение полученных результатов

Визуализация результатов экспериментального исследования продемонстрировала расслоение анализируемых текстовых сообщений как по тональности (эмоциональной окраске) (главная компонента № 2), так и по «побудительной силе» (главная компонента № 1). Важным свойством наблюдаемого расслоения и кластеризации является наличие «интерференционной картины», образованной взаимным усилением и ослаблением когнитивных эмоциональных состояний акторов сети.

Продemonстрированные на рис. 6 и 7 распределения соотносятся с результатами, известными в квантовой оптике. В результате непрямого взаимодействия и при условии наличия сильного информационного поля, формирующего контекст восприятия, пользователи социальных сетей склонны игнорировать нейтрально окрашенные сообщения. Такие сообщения не вызывают соответствующего эмоционального отклика (не поглощаются средой) и не побуждают акторов к публикации собственных сообщений (не порождают вторичного излучения). Вместе с тем в работе [18] рассматривается явление электромагнитно-индуцированной прозрачности, при котором квантовая интерференция появляется вследствие воздействия на два верхних уровня трехуровневой атомной системы сильным когерентным полем. Среда становится прозрачной при воздействии сильного когерентного поля, то есть поглощение почти отсутствует там, где показатель преломления равен единице. В рассматриваемой аналогии, при воздействии сильного «когерентного» информационного поля с околонулевой эмоциональной окраской поглощение и испускание «квантов» эмоционально окрашенных сообщений акторами прекращается, информационная среда становится «прозрачной».

Таким образом, в проведенном нами экспериментальном исследовании информационное поле (размещаемые на странице социальной сети новости на тему мировой политики) воздействует на акторов социальной сети, изначально находящихся в различных эмоциональных состояниях, характеризующихся квантовоподобной суперпозицией мнений. Эмоциональные состояния пользователей в рамках проведенного эксперимента могут быть рассмотрены в качестве аналогов квантовых состояний, причем валентность соотносится с координатой, а эраузал (энергетическая психологическая переменная) — с импульсом частицы. С квантовой точки зрения две данные переменные линейно независимы, то же самое справедливо для полученного ортогонального базиса главных компонент.

Взаимодействие акторов посредством публикации комментариев и непрямого обмена эмоциями приводит к взаимному усилению или ослаблению восприимчивости к эмоционально окрашенным сообщениям в определенных диапазонах тональности, что непосредственно

может быть соотнесено с наблюдаемой интерференционной картиной в пространстве главных компонент и может быть источником усиления или ослабления (на более глобальном уровне) распространения информации в сети Интернет.

Данные исследования могут иметь большой практический интерес в связи с концепцией так называемого социального лазера, заключающейся в усилении информации в социальных сетях благодаря эффектам информационной накачки. Данные исследования требуют проведения дополнительных исследований по распространению информации в сложных сетевых структурах.

Выводы

В работе представлена модель, которая позволяет формировать проверяемые гипотезы относительно условий, при которых возникают и протекают процессы коллективного проявления эмоций в сети. В качестве отправной точки для разработки модели использованы результаты, полученные в области психологии, в частности, метод описания состояний психики испытуемого в системе координат, задаваемой двумя психологическими переменными: валентностью и эраузалом.

Второй важной составной частью проведенного исследования является формальное описание обмена эмоциями между агентами. Моделирование процесса эмоциональной коммуникации имеет большую значимость для задач исследования онлайн-сообществ, в которых агенты не общаются лично, а опосредованно взаимодействуют путем размещения сообщений в блогах, на форумах и т. д. При этом в процессе коммуникации могут возникать временные задержки, а сам электронный ресурс посредством модерирования сообщений может выступать в качестве активного участника коммуникации.

Информация, размещаемая на ресурсе агентами, в основном имеет вид текстовых сообщений и становится доступной для всех членов сообщества одновременно сразу же после опубликования на ресурсе. Следовательно, ресурс обеспечивает между всеми агентами информационное взаимодействие, весьма сходное с взаимодействием, которое обеспечивается самосогласующимся (средним) полем. Для учета эффекта взаимодействия агентов в информационной среде введено понятие поля коммуникации.

Формально описав динамику информационных процессов, происходящих в данном поле, также анализируем децентрализованную генерацию в различные моменты времени сообщений, имеющих различную эмоциональную окраску (как позитивную, так и негативную), «старение» эмоциональной информации (снижение эффекта воздействия эмоционально значимой информации с течением времени), распределение информации между агентами, для которого также могут быть применены допущения, относящиеся к другим (не самосогласующимся) типам полей.

Третьей особенностью разработанной модели является учет зависимости воздействия эмоционально окрашенной информации на агентов от их собственного эмоционального состояния. Сформулирована и обоснована гипотеза о наличии нелинейной обратной связи между количеством доступной информации и индивидуальным состоянием агента, описываемым парой психологических переменных — валентностью и эраузалом. Данный подход позволяет выдвигать различные экспериментально проверяемые гипотезы касательно результирующего воздействия на агента.

Разработанный формальный математический аппарат позволяет не только описывать, но и прогнозировать динамику развития коллективных эмоций в сетевых сообществах.

К достоинствам разработанной модели относится возможность применения к полученным аналитическим выражениям известного математического аппарата теории идентификации и технической диагностики для оценивания интервалов параметров модели, при которых в сетевых сообществах возникает эффект коллективных эмоций. В частности, в рамках разработанной аналитической модели могут быть описаны условия для возникновения поляризованного эмоционального фона с бимодальным законом распределения или сценариев, при которых агенты выражают свои эмоции либо единообразно (например, отзыв на товар или услугу), либо неоднократно (например, во время дискуссии на форумах).

Полученные аналитическим путем теоретические закономерности в дальнейшем могут быть скорректированы с учетом полученных эмпирических данных в ходе параметрической идентификации.

Таким образом, разработанная модель многоагентного броуновского информационного взаимодействия между субъектами коммуникации в сетевых сообществах позволяет формально описывать и прогнозировать динамику развития коллективных эмоций, а также объединить результаты экспериментальных исследований по регистрации психофизиологической реакции испытуемых на эмоционально значимую информацию с закономерностями, полученными в ходе анализа больших массивов эмоционально окрашенных сообщений пользователей информационных сетей, и определить параметры модели для различных сценариев

развития ситуации. Полученные результаты позволяют повысить наблюдаемость информационной среды и достоверность моделирования прогноза ее состояния к заданному моменту времени в будущем.

Кроме того, в работе представлены результаты оригинального экспериментального исследования по проверке гипотезы о квантовоподобных свойствах процессов непрямого распространения информации в социальных сетях с учетом когнитивных процессов их акторов.

Эксперимент «пассивного» типа выполнен посредством ретроспективного анализа текстовых сообщений и комментариев пользователей на странице сообщества «Мировая политика» социальной сети «ВКонтакте». В выборку включены более 2000 публикаций и более 50000 комментариев пользователей. Для автоматизированной оценки тональности текстовых сообщений использован авторский программный модуль на основе большой языковой модели.

По итогам проведенного эксперимента может быть сделан вывод о квантовоподобном (волновом) характере распространении информации в социальных сетях. Он непосредственно связан с наблюдаемой интерференционной картиной в пространстве параметров, описывающих эмоциональные состояния акторов сети. При этом валентность соотнесена с координатой, а «побуждающая сила», выраженная в количестве «лайков» и «репостов» — с импульсом частицы. С квантовой точки зрения, две данные переменные линейно независимы, то же справедливо для полученной ортогональной системы координат в базисе вычисленных главных компонент.

Для удобства последующего анализа, обеспечения воспроизводимости полученных результатов эксперимента и возможного применения собранных исходных данных в последующих исследовательских проектах данные и результаты их первичной обработки сохранены в базе данных формата SQLite, доступной для исследователей⁷ на правах лицензии Apache 2.0.

Исследование выполнено за счет гранта Российского научного фонда (проект № 25-11-20034).

⁷greeny598/vk_social_network_sentiment Datasets at Hugging Face.
URL: https://huggingface.co/datasets/greeny598/vk_social_network_sentiment (дата обращения: 12.01.2025).

Литература

1. Ахременко А.С., Стукал Д.К., Петров А.П. Сеть или текст? Факторы распространения протеста в социальных медиа: теория и анализ данных // Полис. Политические исследования. 2020. С. 73—91. DOI: 10.17976/jpps/2020.02.06 .
2. Давыдова М.А. Протестная активность и акторы политической мобилизации в социальных медиа Республики Казахстан в январе 2022 года // Среднерусский вестник общественных наук. 2024. № 4. С. 141—159. DOI: 10.22394/2071-2367-2024-19-4-141-159 .
3. Малькевич А.А. Роль социальных сетей в протестном политическом участии граждан. // Управленческое консультирование. 2020. № 1. С. 35—42. DOI: 10.22394/1726-1139-2020-1-35-42 .

4. McLoughlin K.L. et al. Misinformation exploits outrage to spread online. *Science*. 2024. Vol. 386. № 6725. P. 991–996. DOI: 10.1126/science.adl2829 .
5. Rajkumar K. et al. A causal test of the strength of weak ties. *Science*. 2022. Vol. 377. № 6612. P. 1304–1310. DOI: 10.1126/science.abl4476 .
6. Wang D., Uzzi B. Weak ties, failed tries, and success. *Science*. 2022. Vol. 377. № 6612. P. 1256–1258. DOI: 10.1126/science.add0692 .
7. Mohammad S.M. Sentiment analysis: Automatically detecting valence, emotions, and other affectual states from text. *Emotion measurement*: Elsevier, 2021. P. 323–379. DOI: 10.1016/B978-0-12-821124-3.00011-9 .
8. Khrennikov A. On Applicability of Quantum Formalism to Model Decision Making: Can Cognitive Signaling Be Compatible with Quantum Theory? *Entropy*. 2022. Vol. 24. № 11. P. 1592. DOI: 10.3390/e24111592 .
9. Khrennikov A.Y. Open quantum systems in biology, cognitive and social sciences. *Springer Nature*, 2023. DOI: 10.1007/978-3-031-29024-4 .
10. *Consciousness and Quantum Mechanics*. Ed. by S. Gao. Oxford, New York: Oxford University Press, 2022. 536 pp.
11. Гнидко К.О., Ломако А.Г. Оценивание уровня контаминации сознания в ультраметрическом пространстве состояний р-адической модели поведения субъекта // *Известия высших учебных заведений. Приборостроение*. 2016. № 9 (59). С. 729—734. DOI: 10.15622/SP.44.5 .
12. Wei X., Gong H., Song L. Product diffusion in dynamic online social networks: A multi-agent simulation based on gravity theory. *Expert Systems with Applications*. 2023. Vol. 213. P. 119008. DOI: 10.1016/j.eswa.2022.119008 .
13. Treur J., Ments L.V. Mental Models and Their Dynamics, Adaptation, and Control: A Self-Modeling Network Modeling Approach. *Springer Nature*, 2022. 616 pp. DOI: 10.1007/978-3-030-85821-6 .
14. Liu P., Li Y., Wang P. Opinion dynamics and minimum adjustment-driven consensus model for multi-criteria large-scale group decision making under a novel social trust propagation mechanism. *IEEE Transactions on Fuzzy Systems*. 2022. Vol. 31. № 1. P. 307–321. DOI: 10.1109/TFUZZ.2022.3186172 .
15. Ishii A., Okano N. Sociophysics approach of simulation of mass media effects in society using new opinion dynamics. *Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys)*. Vol. 3. Springer, 2021. P. 13–28. DOI: 10.1007/978-3-030-55190-2_2 .
16. Metzler H. et al. Collective emotions during the COVID-19 outbreak. *Emotion*. 2023. Vol. 23. № 3. P. 844–858. DOI: 10.1037/emo0001111 .
17. Paletz S.B. et al. Emotional content and sharing on Facebook: A theory cage match. *Science Advances*. 2023. Vol. 9. № 39. P. eade9231. DOI: 10.1126/sciadv.ade9231 .
18. Zhu L., Dong L. Electromagnetically induced transparency metamaterials: theories, designs and applications. *Journal of Physics D: Applied Physics*. 2022. Vol. 55. № 26. P. 263003. DOI: 10.1088/1361-6463/ac60cc .

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

QUANTUM-LIKE PHENOMENA IN THE PROPAGATION OF COLLECTIVE EMOTIONS IN SOCIAL NETWORKS: MODEL, DATASET, AND EXPERIMENTAL RESEARCH RESULTS

Konstantin Gnidko, Dr.Sc. (Technology), Associate Professor, Deputy Head of Group at the Research Centre for Information Technology and Artificial Intelligence of the Autonomous Non-Profit Educational Organisation of Higher Education “Universitet Sirius” (Sirius University), Sirius Federal Territory, Russian Federation. ORCID: 0000-0002-8605-8865.

E-mail: gnidko.ko@talantiuspeh.ru

Dmitrii Lisov, Junior Researcher at the Research Centre for Information Technology and Artificial Intelligence of the Autonomous Non-Profit Educational Organisation of Higher Education “Universitet Sirius” (Sirius University), Sirius Federal Territory, Russian Federation. ORCID: 0000-0002-8214-4109.

E-mail: lisov.dn@talantiuspeh.ru

Keywords: mathematical modelling, information security, social networks, sentiment analysis, collective emotions, Brownian interaction, large language models, interference.

Abstract

Purpose of the study: development of a mathematical model for the propagation of collective emotions in social networks; experimental validation of the hypothesis regarding the emergence of quantum-like phenomena in multi-agent interactions among mass communication actors mediated by an informational field.

Methods used in the study: sentiment analysis of textual messages using a large language model; dimensionality reduction of the feature space based on the principal component analysis (PCA) method; statistical processing and data visualization.

Study findings: an interdisciplinary mathematical model for the spread of collective emotions in social networks has been developed, based on the concept of Brownian agent interaction. The model accounts for the emotional states of communication subjects through psychological variables, valence and arousal, enabling the simulation of emotional dynamics at both individual and collective levels. To experimentally test the hypothesis of quantum-like phenomena, 2,246 posts and 50,326 comments from the "World Politics" community on the VKontakte social network (December 2017 to June 2018) were analyzed. The experimental results demonstrated that agent interactions through the informational field lead to amplification or suppression of communicative activity, manifesting in a distribution of emotional parameters resembling an interference pattern. A correlation was established between the "motivational force" of messages (likes, reposts) and their emotional tone (valence), confirming the presence of quantum-like effects such as interference and superposition.

Research novelty: the proposed model of collective emotional dynamics in social networks is interdisciplinary and incorporates contemporary findings in psychology and sociology, distinguishing it from traditional approaches that neglect nonlinear effects arising from the subjective characteristics of communication participants. For the first time, the concept of an "informational field" is introduced as a medium mediating interactions among mass communication agents, allowing for the description of observed quantum-like phenomena, such as the interference of emotional states in mass communication subjects. The author's contribution includes the development of an original dataset (emotionally charged textual posts and user comments from a social network), made publicly available to ensure reproducibility and facilitate future research. Unlike previous studies relying on specialized sentiment dictionaries, the authors employed a large language model-based algorithm for quantitative sentiment analysis, improving accuracy in accounting for context, complex linguistic structures, irony, and sarcasm.

References

1. Akhremenko A.S., Stukal D.K., Petrov A.P. Set' ili tekst? Faktory rasprostraneniia protesta v sotsial'nykh media: teoriia i analiz dannykh. Polis. Politicheskie issledovaniia. 2020. Pp. 73–91. DOI: 10.17976/jpps/2020.02.06 .
2. Davydova M.A. Protestnaia aktivnost' i aktory politicheskoi mobilizatsii v sotsial'nykh media Respubliki Kazakhstan v ianvare 2022 goda. Srednerusskii vestnik obshchestvennykh nauk. 2024. No. 4. Pp. 141–159. DOI: 10.22394/2071-2367-2024-19-4-141-159 .
3. Mal'kevich A.A. Rol' sotsial'nykh setei v protestnom politicheskom uchastii grazhdan. Upravlencheskoe konsul'tirovanie. 2020. No. 1. Pp. 35–42. DOI: 10.22394/1726-1139-2020-1-35-42 .
4. McLoughlin K.L. et al. Misinformation exploits outrage to spread online. Science. 2024. Vol. 386. № 6725. P. 991–996. DOI: 10.1126/science.adl2829 .
5. Rajkumar K. et al. A causal test of the strength of weak ties. Science. 2022. Vol. 377. № 6612. P. 1304–1310. DOI: 10.1126/science.abl4476 .
6. Wang D., Uzzi B. Weak ties, failed tries, and success. Science. 2022. Vol. 377. № 6612. P. 1256–1258. DOI: 10.1126/science.add0692 .
7. Mohammad S.M. Sentiment analysis: Automatically detecting valence, emotions, and other affectual states from text. Emotion measurement: Elsevier, 2021. P. 323–379. DOI: 10.1016/B978-0-12-821124-3.00011-9 .
8. Khrennikov A. On Applicability of Quantum Formalism to Model Decision Making: Can Cognitive Signaling Be Compatible with Quantum Theory? Entropy. 2022. Vol. 24. № 11. P. 1592. DOI: 10.3390/e24111592 .
9. Khrennikov A.Y. Open quantum systems in biology, cognitive and social sciences. Springer Nature, 2023. DOI: 10.1007/978-3-031-29024-4 .
10. Consciousness and Quantum Mechanics. Ed. by S. Gao. Oxford, New York: Oxford University Press, 2022. 536 pp.
11. Gnidko K.O., Lomako A.G. Otsenivanie urovnia kontaminatsii soznaniia v ul'trametricheskom prostranstve sostoianii p-adicheskoi modeli povedeniia sub'ekta. Izvestiia vysshikh uchebnykh zavedenii. Priborostroenie. 2016. No. 9 (59). Pp. 729–734. DOI: 10.15622/SP.44.5 .
12. Wei X., Gong H., Song L. Product diffusion in dynamic online social networks: A multi-agent simulation based on gravity theory. Expert Systems with Applications. 2023. Vol. 213. P. 119008. DOI: 10.1016/j.eswa.2022.119008 .
13. Treur J., Ments L.V. Mental Models and Their Dynamics, Adaptation, and Control: A Self-Modeling Network Modeling Approach. Springer Nature, 2022. 616 pp. DOI: 10.1007/978-3-030-85821-6 .
14. Liu P., Li Y., Wang P. Opinion dynamics and minimum adjustment-driven consensus model for multi-criteria large-scale group decision making under a novel social trust propagation mechanism. IEEE Transactions on Fuzzy Systems. 2022. Vol. 31. № 1. P. 307–321. DOI: 10.1109/TFUZZ.2022.3186172 .

15. Ishii A., Okano N. Sociophysics approach of simulation of mass media effects in society using new opinion dynamics. Intelligent Systems and Applications: Proceedings of the 2020 Intelligent Systems Conference (IntelliSys). Vol. 3. Springer, 2021. P. 13–28. DOI: 10.1007/978-3-030-55190-2_2 .
16. Metzler H. et al. Collective emotions during the COVID-19 outbreak. Emotion. 2023. Vol. 23. № 3. P. 844–858. DOI: 10.1037/emo0001111 .
17. Paletz S.B. et al. Emotional content and sharing on Facebook: A theory cage match. Science Advances. 2023. Vol. 9. № 39. P. eade9231. DOI: 10.1126/sciadv.ade9231 .
18. Zhu L., Dong L. Electromagnetically induced transparency metamaterials: theories, designs and applications. Journal of Physics D: Applied Physics. 2022. Vol. 55. № 26. P. 263003. DOI: 10.1088/1361-6463/ac60cc .

МЕТОД ОЧИСТКИ ОБУЧАЮЩЕЙ ВЫБОРКИ ДЛЯ ЗАДАЧ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ЧЕРЕЗ ОБНАРУЖЕНИЕ АНОМАЛИЙ

Арустамян А.Б.¹, Цирлов В.Л.², Шишкин И.И.³

Ключевые слова: медицинская аналитика, обработка данных, алгоритмы классификации, оптимизация моделей, анализ выбросов, предсказательные системы, датасет обработки, устойчивость моделей, экспериментальная оценка.

Аннотация

Цель работы: анализ и разработка метода очистки обучающей выборки для моделей машинного обучения посредством обнаружения аномалий с использованием алгоритма Isolation Forest (IsFo).

Метод исследования: применение алгоритма IsFo для выявления и фильтрации аномальных данных в медицинском датасете COVID-19. Проведена предобработка данных, включая кодирование категориальных признаков и стандартизацию, а также симуляция аномалий путем искажения меток и добавления шума. Настроены гиперпараметры алгоритма для оптимизации F1-меры, после чего выполнена фильтрация аномалий и оценка качества классификации с использованием многослойного перцептрона.

Результаты исследования: алгоритм IsFo эффективно выявляет аномалии, обнаружив 324 из 342 искаженных точек с минимальными ложными срабатываниями (19). Точность классификации на исходных данных составила 85%, на искаженных — снизилась до 78%, а после фильтрации восстановилась до 83%. Тестирование на реальных данных подтвердило сохранение качества модели (82%). Метод повышает надежность моделей, но требует настройки гиперпараметров и может быть менее эффективен при целенаправленных атаках или высокоразмерных данных.

Практическая ценность: показана перспективность алгоритма IsFo для медицинской аналитики, однако для сложных случаев рекомендуется комбинирование с другими методами.

DOI: 10.24412/1994-1404-2025-2-95-102

Введение

В последние десятилетия модели машинного обучения стали неотъемлемой частью множества критически важных систем, включая финансовый сектор, здравоохранение, автономные транспортные средства, системы информационной безопасности и многие другие области [1, 2]. Они позволяют автоматизировать сложные процессы, анализировать огромные объемы данных и принимать решения, которые ранее требовали значительных человеческих ресурсов. Благодаря этим возможностям машинное обучение стало ключевым инструментом для решения сложных задач в различных отраслях промышленности и науки.

Однако широкое применение делает их чувствительными к качеству входных данных. Наличие ано-

мальных или искаженных данных в тренировочных наборах может существенно повлиять на точность и надежность моделей, приводя к ухудшению их производительности. Аномалии способны кардинально изменить поведение модели, вызывая значительное снижение ее эффективности и точности прогнозов, что особенно критично для систем, где точность и надежность предсказаний имеют решающее значение, например, в медицинской диагностике, в системах принятия финансовых решений и др. [3—6].

Основная проблема заключается в том, что аномальные данные могут выглядеть как корректные, но содержать скрытые искажения, влияющие на производительность модели и корректность прогнозов.

¹ **Арустамян Александр Борисович**, магистрант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, Российская Федерация.

E-mail: s.arustamian@yandex.ru

² **Цирлов Валентин Леонидович**, кандидат технических наук, доцент, генеральный директор АО «НПО «Эшелон», г. Москва, Российская Федерация. ORCID: 0000-0003-2657-4179.

E-mail: v.tsirlov@npo-echelon.ru

³ **Шишкин Иван Ильич**, магистрант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана, г. Москва, Российская Федерация.

E-mail: super.vansha2013@yandex.ru

Искажения могут проявляться в различных формах: от случайного шума в обучающем наборе до добавления ложных данных, имитирующих нормальные, наличия небольших наборов данных, вызывающих в модели поведение, не соответствующее реальности [7]. Сложность обнаружения этих аномалий стандартными методами обработки данных делает их трудными для устранения [8].

Для выявления и устранения аномалий в данных разрабатываются различные методы, среди которых одним из ключевых подходов является обнаружение и фильтрация аномальных записей [9]. Алгоритм Isolation Forest зарекомендовал себя как эффективный метод для обнаружения и устранения искаженных данных. Его суть заключается в изоляции аномалий посредством построения алгоритма случайного леса, что позволяет эффективно обрабатывать большие и сложные наборы данных без необходимости делать предположения об их распределении. Этот метод особенно полезен в задачах, где аномалии составляют небольшой процент от общего объема данных, но могут существенно влиять на результаты модели [10—15].

В данной работе исследуются возможности и эффективность применения алгоритма Isolation Forest для обнаружения и устранения аномальных данных в моделях машинного обучения. В рамках экспериментов были проведены тесты на реальных медицинских данных, направленные на оценку эффективности Isolation Forest в различных условиях наличия аномалий, а также на анализ восстановления показателей точности и других метрик после фильтрации аномальных данных.

Обзор основных типов аномалий в данных машинного обучения

Модели машинного обучения чрезвычайно чувствительны к различным типам аномалий в данных, которые представляют собой наблюдения, существенно отличающиеся от основной массы данных, и могут приводить к непредсказуемым последствиям при обучении моделей [2]. Эти отклонения способны не только исказить результаты прогнозов, но и снижать общую надежность систем, что особенно критично в таких областях, как медицина, финансы и кибербезопасность, где ошибки могут иметь серьезные последствия. Основные типы аномалий включают следующие категории.

- Случайный шум в данных: введение случайного шума в тренировочный набор данных является одной из наиболее распространенных форм аномалий. Такой шум может возникать из-за ошибок измерения, передачи данных или случайных сбоев в оборудовании, что приводит к снижению отношения «сигнал/шум» и ухудшению способности модели выделять значимые паттерны. Для борьбы с этим эффектом применяются предварительная фильтрация данных, использование алгоритмов, устойчивых к шуму, а также регулярная проверка качества источников информации, что

помогает минимизировать влияние случайных факторов.

- Ошибки в метках классов: ошибочное присвоение меток классов предполагает неверное обозначение категории, к которой принадлежит объект. Например, в задаче классификации «спам/не спам» сообщение, являющееся спамом, может быть ошибочно помечено как «не спам», что снижает качество модели и ее способность правильно классифицировать данные. Такие ошибки особенно опасны в задачах бинарной классификации, где даже небольшое количество неправильно размеченных примеров может существенно повлиять на производительность модели. Поскольку ошибки в метках обычно затрагивают лишь малую часть данных, их обнаружение традиционными методами очистки становится сложной задачей, требующей применения специализированных подходов.
- Скрытые зависимости и корреляции: существование скрытых или неожиданных зависимостей между признаками может вводить модель в заблуждение. Например, в данных могут присутствовать ложные корреляции, которые не отражают реальную причинно-следственную связь и создают иллюзию значимых паттернов. Такие аномалии могут привести к тому, что модель будет учиться на искаженных закономерностях, что ухудшает ее способность к обобщению на новых данных и снижает предсказательную силу. Для выявления скрытых зависимостей необходим тщательный анализ данных, включающий визуализацию корреляционных матриц и использование методов обнаружения аномалий, таких как Isolation Forest.
- Выбросы в значениях признаков: выбросы представляют собой значения признаков, выходящие за пределы нормального диапазона. Они могут возникать из-за ошибок ввода данных, неисправности оборудования или редких событий, таких как экстремальные природные явления. Наличие выбросов искажает статистические характеристики данных, смещает средние значения и дисперсию, что может существенно влиять на обучение модели, особенно если алгоритм чувствителен к масштабу признаков [1]. Методы обработки выбросов включают их удаление, замену на медианные значения или использование робастных алгоритмов, адаптированных к наличию экстремальных точек.
- Структурные аномалии в данных: структурные аномалии связаны с нарушением ожидаемой структуры данных, например, наличием пропусков значений, некорректным форматированием или несоответствием типов данных. Эти проблемы могут существенно затруднять процесс обработки и анализа данных, приводя к сбоям в работе модели и снижению ее точности. Для их обна-

ружения и устранения применяются методы проверки целостности данных, включая заполнение пропусков с использованием интерполяции или статистических методов, а также преобразование форматов для обеспечения совместимости.

- Синтетические или дублирующие данные: наличие синтетических или дублирующих записей в наборе данных может серьезно исказить результаты обучения модели [4]. Синтетические данные, созданные без учета реальных распределений, или дубликаты могут привести к переобучению модели, когда она начинает чрезмерно подстраиваться под искусственные паттерны, а также к смещению оценок, что снижает обобщающую способность. Выявление таких аномалий требует анализа уникальности записей с использованием хэш-функций или методов дедупликации, а также проверки источников данных на предмет их достоверности.
- Контекстные аномалии: контекстные аномалии возникают, когда данные являются аномальными только в определенном контексте. Например, высокая температура может быть нормальной для южных регионов, но аномальной для северных территорий, что требует учета географического или временного контекста. Такие аномалии сложно обнаружить без дополнительной информации, например, метаданных или исторических данных, и они могут существенно влиять на точность моделей, работающих с временными рядами или географическими наборами данных. Решение этой проблемы часто требует интеграции контекстного анализа в процесс обучения.
- Аномалии, связанные с изменением распределения данных: изменение распределения данных во времени, известное как дрейф данных, может привести к тому, что модель, обученная на старых данных, станет менее эффективной. Это особенно актуально для моделей, работающих в реальном времени, где характеристики данных могут меняться из-за сезонных факторов, изменений в поведении пользователей или внешних воздействий. Обнаружение данного типа аномалий требует постоянного мониторинга модели с использованием контрольных метрик, а также периодического обновления ее на новых данных для адаптации к текущим условиям. Этот процесс может включать переобучение или использование адаптивных алгоритмов, способных автоматически корректировать параметры в зависимости от изменений.

Каждый из описанных типов аномалий представляет собой уникальный и сложный вызов для обеспечения качества данных в моделях машинного обучения. Эти проблемы подчеркивают необходимость разработки эффективных методов обнаружения и обработки аномалий, которые могли бы минимизировать их негативное влияние на производительность систем. В этом

контексте алгоритм Isolation Forest выступает как перспективный инструмент для выявления различных видов аномалий данных, предлагая автоматизированный подход к их изоляции и устранению. Каждая из описанных атак представляет собой уникальный и сложный вызов для защиты моделей машинного обучения, требующий не только технических, но и стратегических решений. Эти угрозы подчеркивают необходимость разработки эффективных методов обнаружения и нейтрализации «отравленных» данных, где Isolation Forest демонстрирует значительный потенциал для защиты моделей от различных видов атак, особенно в условиях ограниченных ресурсов и высоких требований к скорости обработки.

Isolation Forest как метод выявления аномалий

Алгоритм Isolation Forest основан на предположении, что аномальные объекты легче изолировать от остального набора данных [16]. Аномалии обычно занимают периферийные области распределения, имеют низкую плотность и отличаются по характеристикам от основной массы. Обычные объекты скрыты в плотных кластерах и требуют большего числа разбиений для изоляции. Этот принцип делает Isolation Forest эффективным для обнаружения аномалий в высокомерных данных без необходимости предполагать какое-либо распределение данных.

Вот основные этапы работы алгоритма.

- Формирование случайных разбиений: на каждом этапе построения дерева случайным образом выбирается признак и точка разделения, создавая случайные гиперплоскости, разделяющие пространство данных [16]. Этот подход позволяет эффективно находить редкие и удаленные объекты, которые могут быть аномалиями.
- Построение деревьев изоляции: деревья строятся с целью максимальной изоляции каждого объекта. Чем меньше шагов требуется для изоляции объекта, тем выше вероятность, что он является аномалией. Аномалии обычно находятся на периферии распределения, упрощая их отделение от остальных.
- Оценка глубины объекта в дереве: для каждого объекта рассчитывается глубина изоляции в дереве. Средняя глубина вычисляется по всем деревьям, и чем меньше средняя глубина, тем выше вероятность аномальности объекта. Нормальные объекты требуют большего числа разбиений для изоляции.
- Агрегация оценок по деревьям: для получения надежной оценки аномальности алгоритм использует множество деревьев. Итоговая оценка рассчитывается на основе средней глубины изоляции объекта во всех деревьях леса. Это повышает устойчивость результатов и снижает влияние случайных факторов.

- Расчет индекса аномальности: на основании средней глубины изоляции формируется индекс аномальности. Чем выше индекс, тем более вероятно, что объект является аномалией. Это позволяет ранжировать объекты по степени их аномальности и принимать решения о их исключении из обучающего набора.

Isolation Forest помогает снизить вероятность включения искаженных данных в тренировочный набор, обеспечивая более устойчивую и надежную работу модели. Он показал высокую эффективность в условиях, когда аномальные данные составляют лишь небольшой процент от общего объема. Благодаря своей масштабируемости и эффективности алгоритм широко применяется в различных областях, включая финансовые мошенничества, обнаружение сетевых вторжений и анализ медицинских данных.

Постановка и реализация задачи

Обработка больших объемов медицинской информации сопряжена с риском наличия искаженных или ошибочных записей, способных повлиять на результаты анализа и снизить эффективность предсказаний моделей. Такие искажения, известные как «отравление данных», представляют угрозу для целостности аналитических процессов в критически важных системах.

В исследовании использовался датасет COVID-19 Outcomes by Vaccination Status – Historical, предоставляющий статистические данные о заболеваемости, госпитализациях и смертности от COVID-19 в Чикаго, классифицированные по статусу вакцинации. Задача заключалась в применении алгоритма Isolation Forest для выявления и устранения аномальных записей, возникающих из-за ошибок в сборе данных или неправильной интерпретации. Такие аномалии могут существенно исказить выводы, сделанные на основе данных, особенно в таких чувствительных областях, как здравоохранение.

Основная цель заключалась в тестировании устойчивости модели к аномалиям данных и демонстрации эффективности работы алгоритма Isolation Forest. Моделирование аномалий проводится аналогично тем, что описаны в исследовании [3]. Для этого были выполнены следующие задачи.

1. Предобработка данных.

На первом этапе происходит загрузка и подготовка данных. Используется массив данных с различными признаками и целевой переменной — результата лечения, наблюдения. Выполняется очистка от пропусков, а также преобразование категориальных признаков в числовые с помощью LabelEncoder. Далее данные стандартизируются с помощью StandardScaler, чтобы привести их к единому масштабу.

2. Симуляция искажения данных.

Чтобы протестировать устойчивость модели к искажениям, в коде реализована функция симуляции ано-

малий, заключающимся в преднамеренном искажении части данных.

Искажения проводятся следующим образом:

- Выбирается 10% случайных точек из всего набора данных,
- Метки целевой переменной (y) для этих точек заменяются случайными значениями из диапазона возможных меток. Это симулирует ситуацию, когда злоумышленник меняет метки, вводя в заблуждение модель.
- Признаки (X) также подвергаются искажению, добавляется случайный шум, используя нормальное распределение с математическим ожиданием 0 и стандартным отклонением 5. Это делает данные менее предсказуемыми и затрудняет их классификацию.

3. Настройка Isolation Forest.

После создания аномальных данных используется алгоритм Isolation Forest для выявления отклонений. Алгоритм строит деревья, где каждое разбиение представляет собой случайный выбор признака и значения. Точки данных, которые изолируются на малой глубине дерева, считаются аномальными, так как они отличаются от основной массы данных.

Проводится настройка гиперпараметров Isolation Forest, таких как количество деревьев ($n_estimators$), количество выборок ($max_samples$), доля аномальных данных ($contamination$) и количество признаков для разбиений ($max_features$). Путём перебора комбинаций этих параметров определяется наилучшая конфигурация, обеспечивающая максимальную F1-меру — показатель, учитывающий как точность, так и полноту обнаружения аномалий.

4. Обнаружение и фильтрация аномалий.

После настройки Isolation Forest модель применяется к измененным данным. Алгоритм предсказывает, какие точки данных являются аномальными, и они удаляются из набора данных. Таким образом, создаётся отфильтрованный набор данных.

5. Оценка удаления аномалий.

Для оценки эффективности работы Isolation Forest проводится анализ, сколько из введенных искажений было успешно обнаружено и сколько ложных срабатываний (удалений нормальных данных) произошло. Это позволяет оценить качество работы алгоритма по следующим показателям:

- Количество обнаруженных аномалий — число точек, которые были успешно идентифицированы как атакованные.
- Ложные срабатывания — случаи, когда нормальные данные ошибочно классифицируются как аномалии.

6. Оценка модели классификации.

На следующем этапе проводится обучение и оценка модели классификации (многослойного перцептрона, MLPClassifier) на следующих трёх различных наборах данных.

- Исходные данные (без искажений) — для базовой оценки модели.
- Искажённые данные — для проверки, насколько сильно искаженные данные влияют на результаты классификации.
- Отфильтрованные данные — для анализа, насколько хорошо фильтрация аномалий с помощью Isolation Forest помогает восстановить качество модели.

Основные метрики для оценки включают средне-квадратичную ошибку (MSE), среднюю абсолютную ошибку (MAE), точность (accuracy), F1-меру, точность (precision) и полноту (recall).

7. Итоговая оценка модели после фильтрации.

Последним этапом является проверка модели, обученной на отфильтрованных данных, на реальных данных. Это позволяет оценить, насколько улучшилось качество классификации после удаления аномалий. Оцениваются те же метрики, что и на предыдущих этапах.

Обзор результатов эксперимента

Для оценки качества удаления аномалий подсчитывается количество корректно обнаруженных искажений, а также количество ложных срабатываний, то есть случаев, когда нормальные данные ошибочно классифицируются как аномалии. В эксперименте было введено 342 искажённые точки, из которых алгоритм успешно обнаружил 324, допустив всего 19 ложных срабатываний [17]. Были выявлены лучшие гиперпараметры для модели Isolation Forest (см. рис. 1).

```
Лучшие параметры IsolationForest:
Contamination: 0.1
Max Features: 1.0
Max Samples: 0.8
Num_estimators: 200
Лучший F1 Score для обнаружения аномалий: 0.9460
Количество введенных аномалий (искаженных меток): 342
Количество корректно обнаруженных искажений: 324
Количество ложных срабатываний (случайных удалений): 19
```

Рис. 1. Параметры настройки модели Isolation Forest

Следующий этап — это оценка модели классификации на трёх различных наборах данных: исходных (чистых), искажённых и отфильтрованных. На исходных данных модель показывает высокие результаты: точность около 85%, что свидетельствует о хорошем качестве классификации (см. рис. 2).

Однако на искажённых данных результаты значительно ухудшаются: точность падает до 78%, увеличивается количество ошибок, особенно при классификации второго класса. Это указывает на то, что измененные данные отрицательно влияют на качество модели, снижая её способность правильно классифицировать объекты (см. рис. 3).

Результаты на исходных данных:

Метрики для исходных данных:
MSE: 0.3338, MSA: 0.2114, Accuracy: 0.8499, F1 Score: 0.8496
Precision: 0.8546, Recall: 0.8499

Отчет о классификации:

	precision	recall	f1-score	support
0	0.95	0.85	0.90	237
1	0.82	0.94	0.88	227
2	0.79	0.76	0.77	222
accuracy			0.85	686
macro avg	0.85	0.85	0.85	686
weighted avg	0.85	0.85	0.85	686

Рис. 2. Результаты работы алгоритма классификации на исходных данных

Результаты на искажённых данных:

Метрики для искажённых данных:
MSE: 0.4431, MSA: 0.2915, Accuracy: 0.7843, F1 Score: 0.7853
Precision: 0.7869, Recall: 0.7843

Отчет о классификации:

	precision	recall	f1-score	support
0	0.86	0.82	0.84	237
1	0.79	0.79	0.79	232
2	0.70	0.73	0.71	217
accuracy			0.78	686
macro avg	0.78	0.78	0.78	686
weighted avg	0.79	0.78	0.79	686

Рис. 3. Результаты работы алгоритма классификации на искаженных данных

После фильтрации искажённых данных с помощью Isolation Forest результаты классификации заметно улучшаются. Точность возрастает до 83%, а F1-мера приближается к значениям, полученным на исходных данных. Это демонстрирует, что удаление аномалий позволяет восстановить качество модели, приближая её к уровню классификации на чистых данных (см. рис. 4).

Результаты на отфильтрованных данных:

Метрики для отфильтрованных данных:
MSE: 0.3436, MSA: 0.2301, Accuracy: 0.8266, F1 Score: 0.8276
Precision: 0.8421, Recall: 0.8266

Отчет о классификации:

	precision	recall	f1-score	support
0	0.90	0.90	0.90	193
1	0.92	0.72	0.81	212
2	0.71	0.87	0.78	212
accuracy			0.83	617
macro avg	0.84	0.83	0.83	617
weighted avg	0.84	0.83	0.83	617

Рис. 4. Результаты работы алгоритма классификации на отфильтрованных данных

Наконец, проводится тестирование модели, обученной на отфильтрованных данных, на реальных (чистых) данных, чтобы проверить, не ухудшится ли её качество из-за фильтрации. Результаты показывают, что точность остаётся на уровне 82%. Это подтверждает, что фильтрация аномалий с помощью Isolation Forest не только помогает улучшить устойчивость модели к искажениям, но и не сильно снижает её качество на новых, неискорженных данных (см. рис. 5).

Метрики для модели, обученной на отфильтрованных данных, на реальных данных:
MSE: 0.3848, MSA: 0.2507, Accuracy: 0.8163, F1 Score: 0.8179
Precision: 0.8325, Recall: 0.8163

Отчет о классификации:

	precision	recall	f1-score	support
0	0.89	0.90	0.89	237
1	0.92	0.71	0.80	227
2	0.69	0.83	0.75	222
accuracy			0.82	686
macro avg	0.83	0.82	0.82	686
weighted avg	0.83	0.82	0.82	686

Матрица ошибок:
[[213 3 21]
[1 162 64]
[25 12 185]]

Рис. 5. Результаты работы классификатора, обученного на отфильтрованных данных

Выводы

Применение алгоритма Isolation Forest позволило эффективно обнаружить и удалить искажённые

данные, восстановив метрики модели. Однако его использование требует учёта ряда факторов и ограничений.

Результаты Isolation Forest зависят от гиперпараметров: `contamination`, `max_features`, `max_samples` и `n_estimators`. Они подбирались для оптимизации F1-меры, но могут потребовать пересмотра для других данных во избежание переобучения или пропуска аномалий. Алгоритм хорошо справляется со случайными искажениями, но его эффективность снижается при целенаправленных атаках, маскирующих аномалии под нормальные точки. Это требует дополнительной настройки параметров.

Проблема ложных срабатываний, когда нормальные данные удаляются вместе с аномальными, в данном эксперименте была минимальной, но может усиливаться при низком количестве аномалий или схожих характеристиках нормальных и аномальных точек. Эффективность алгоритма также снижается при обработке данных высокой размерности, что может потребовать понижения размерности.

При целенаправленных атаках с качественным маскированием искажений Isolation Forest теряет способность их обнаруживать. В таких случаях необходимы дополнительные методы, например, комбинирование алгоритмов или гибридные модели. В реальных условиях, где искажения более разнородны, производительность алгоритма может отличаться, что требует адаптации подхода.

Литература

1. Безопасность России. Правовые, социально-экономические и научно-технические аспекты / Анищенко А.В., Артемьев В.Б., Бондарева М.К. и др. / Под. ред. Махутова Н.А. Тематический блок «Национальная безопасность». Системная инженерия в проблемах национальной безопасности. М.: МГОФ «Знание», 2025. 898 с.
2. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Зегжда Д.П., Александрова Е.Б., Калинин М.О. и др. М.: Горячая линия — Телеком, 2021. 560 с.
3. Горбачев А.А., Максимов Р.В. Проблема маскирования и применения технологий машинного обучения в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 37—49. DOI: 10.21681/2311-3456-2023-5-37-49.
4. Костогрызов А.И., Нистратов А.А. Анализ угроз злоумышленной модификации модели машинного обучения для систем с искусственным интеллектом // Вопросы кибербезопасности. 2023. № 5 (57). С. 9—24. DOI: 10.21681/2311-3456-2023-5-9-24.
5. 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: 10.21681/2311-3456-2024-1-24-37.
6. Марков А.С. О сертификации систем искусственного интеллекта по требованиям безопасности информации // В сб.: Кибернетика и информационная безопасность «КИБ-2024»: сборник научных трудов II Всероссийской научно-технической конференции. М., 2024. С. 18—21.
7. Biggio B., Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84 (2018): 317—331.
8. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
9. Сухов А.В., Конюшев В.В. Системный анализ аномальных событий в информационном пространстве // Правовая информатика. 2024. № 1. С. 58—67. DOI: 10.24412/1994-1404-2024-1-58-67.
10. Гурина Л.А., Томин Н.В. Интеллектуальные методы обеспечения кибербезопасности мультиагентных систем управления микросетями // Вопросы кибербезопасности. 2024. № 6 (64). С. 53—64. DOI: 10.21681/2311-3456-2024-6-53-64.

11. Дубинин А.Ю. Исследование набора признаков для построения цифрового профиля пользователя удалённых подключений (на основе данных межсетевого экрана) // Безопасность информационных технологий. 2024. Т. 31. № 1. С. 120—134.
12. Калинин А.О., Голуб С.А., Коркин И.Ю., Пятаковский Д.Н. Обнаружение программ-шифровальщиков на основе данных механизма трассировки событий и применения метода машинного обучения // Безопасность информационных технологий. 2022. Т. 29. № 3. С. 82—93.
13. Сухов А.В., Конюшев В.В. Идентификация сингулярных последовательностей признаков аномальных событий в информационном пространстве // Правовая информатика. 2023. № 2. С. 26—33. DOI: 10.24412/1994-1404-2023-2-26-33.
14. Шелухин О.И., Полковников М.В. Исследование алгоритма Isolation Forest при бинарной классификации сетевых аномалий // В сб.: Безопасные информационные технологии : сборник трудов X Международной научно-технической конференции. 2019. С. 387—393.
15. Liu T., Zhou Zh., Yang L. Layered isolation forest: a multi-level subspace algorithm for improving isolation forest. Neurocomputing. 2024. Vol. 581. P. 127525.
16. Liu B., Lyu L., Chen H. A taxonomy and survey of data poisoning attacks. Computers & Security. 2020. Vol. 92. P. 101746. DOI: 10.1016/j.cose.2020.101746.
17. Арустамян А.Б., Цирлов В.Л., Шишкин И.И. Обнаружение и фильтрация аномалий в моделях машинного обучения для противодействия атакам отравления данных // В сб.: Кибернетика и информационная безопасность «КИБ-2024» : сборник научных трудов II Всероссийской научно-технической конференции. М., 2024. С. 74—75.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

A METHOD OF CLEARING THE TRAINING DATASET FOR MACHINE LEARNING MODEL TASKS BY ANOMALY DETECTION

Aleksandr Arustamian, master's student at the Information Security Department of the Bauman Moscow State Technical University, Moscow, Russian Federation.

E-mail: s.arustamian@yandex.ru

Valentin Tsirlov, Ph.D. (Technology), Associate Professor, Director-General of the AO (JSC) NPO Echelon, Moscow, Russian Federation. ORCID: 0000-0003-2657-4179.

E-mail: v.tsirlov@npo-echelon.ru

Ivan Shishkin, master's student at the Information Security Department of the Bauman Moscow State Technical University, Moscow, Russian Federation.

E-mail: super.vansha2013@yandex.ru

Keywords: *medical analytics, data processing, classification algorithms, model optimisation, emissions analysis, predictive systems, processing dataset, model stability, experimental evaluation.*

Abstract

Purpose of the work: analysing and developing a method for clearing the training dataset for machine learning model tasks by detecting anomalies using the Isolation Forest (IsFo) algorithm.

Methods used in the study: using the IsFo algorithm for detecting and filtering anomalous data in the COVID-19 medical dataset. Data preprocessing including category feature coding and standardisation was carried out, as well as a simulation of anomalies by distorting labels and adding noise. Algorithm hyperparameters are tuned for optimising the F1 measure, then anomalies filtering is performed and classification quality is evaluated using a multi-layer perceptron.

Study findings: the IsFo algorithm efficiently detects anomalies: 324 out of 342 distorted points were found, with a minimum number of false positives (19). The classification accuracy for the original data was 85%, for the distorted data it decreased to 78% and, after filtering, recovered to 83%. Testing using real data confirmed the preservation of the quality of the model (82%). The method improves the models reliability, but it requires hyperparameter tuning and may be less efficient for targeted attacks or high-dimensional data.

Practical value: the viability of the IsFo algorithm for medical analytics is shown, however, for complex cases it is recommended to use the algorithm in combination with other methods.

References

1. Bezopasnost' Rossii. Pravovye, sotsial'no-ekonomicheskie i nauchno-tekhnicheskie aspekty. Anishchenko A.V., Artem'ev V.B., Bondareva M.K. i dr. Pod. red. Makhutova N.A. Tematicheskii blok "Natsional'naia bezopasnost'". Sistemnaia inzheneriia v problemakh natsional'noi bezopasnosti. M. : MGOF "Znanie", 2025. 898 pp.
2. Kiberbezopasnost' tsifrovoi industrii. Teoriia i praktika funktsional'noi ustoichivosti k kiberatakam. Zegzhda D.P., Aleksandrova E.B., Kalinin M.O. i dr. M. : Goriachaia liniia – Telekom, 2021. 560 pp.
3. Gorbachev A.A., Maksimov R.V. Problema maskirovaniia i primeneniia tekhnologii mashinnogo obucheniia v kiberprostranstve. Voprosy kiberbezopasnosti. 2023. No. 5 (57). Pp. 37–49. DOI: 10.21681/2311-3456-2023-5-37-49 .
4. Kostogryzov A.I., Nistratov A.A. Analiz ugroz zloumyshlennoi modifikatsii modeli mashinnogo obucheniia dlia sistem s iskusstvennym intellektom. Voprosy kiberbezopasnosti. 2023. No. 5 (57). Pp. 9–24. DOI: 10.21681/2311-3456-2023-5-9-24 .
5. Kotenko I.V., Saenko I.B., Lauta O.S., Vasil'ev N.A., Sadovnikov V.E. Ataki i metody zashchity v sistemakh mashinnogo obucheniia: analiz sovremennykh issledovani. Voprosy kiberbezopasnosti. 2024. No. 1 (59). Pp. 24–37. DOI: 10.21681/2311-3456-2024-1-24-37 .
6. Markov A.S. O sertifikatsii sistem iskusstvennogo intellekta po trebovaniyam bezopasnosti informatsii. V sb.: Kibernetika i informatsionnaia bezopasnost' "KIB-2024": sbornik nauchnykh trudov II Vserossiiskoi nauchno-tekhnicheskoi konferentsii. M., 2024. Pp. 18–21.
7. Biggio B., Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition 84 (2018): 317–331.
8. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviia sredstv zashchity informatsii. M. : Radio i sviaz', 2012. 192 pp.
9. Sukhov A.V., Koniushchev V.V. Sistemnyi analiz anomal'nykh sobytii v informatsionnom prostranstve. Pravovaia informatika. 2024. No. 1. Pp. 58–67. DOI: 10.24412/1994-1404-2024-1-58-67 .
10. Gurina L.A., Tomin N.V. Intellektual'nye metody obespecheniia kiberbezopasnosti mul'tiagentnykh sistem upravleniia mikrosetiami. Voprosy kiberbezopasnosti. 2024. No. 6 (64). Pp. 53–64. DOI: 10.21681/2311-3456-2024-6-53-64 .
11. Dubinin A.Iu. Issledovanie nabora priznakov dlia postroeniia tsifrovogo profilia pol'zovatel'ia udalennykh podkliuchenii (na osnove dannykh mezhsetevogo ekrana). Bezopasnost' informatsionnykh tekhnologii. 2024. T. 31. No. 1. Pp. 120–134.
12. Kalinkin A.O., Golub S.A., Korkin I.Iu., Piatovskii D.N. Obnaruzhenie programm-shifroval'shchikov na osnove dannykh mekhanizma trassirovki sobytii i primeneniia metoda mashinnogo obucheniia. Bezopasnost' informatsionnykh tekhnologii. 2022. T. 29. No. 3. Pp. 82–93.
13. Sukhov A.V., Koniushchev V.V. Identifikatsiia singuliarnykh posledovatel'nostei priznakov anomal'nykh sobytii v informatsionnom prostranstve. Pravovaia informatika. 2023. No. 2. Pp. 26–33. DOI: 10.24412/1994-1404-2023-2-26-33 .
14. Shelukhin O.I., Polkovnikov M.V. Issledovanie algoritma Isolation Forest pri binarnoi klassifikatsii setevykh anomalii. V sb.: Bezopasnye informatsionnye tekhnologii : sbornik trudov X Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii. 2019. Pp. 387–393.
15. Liu T., Zhou Zh., Yang L. Layered isolation forest: a multi-level subspace algorithm for improving isolation forest. Neurocomputing. 2024. Vol. 581. P. 127525.
16. Liu B., Lyu L., Chen H. A taxonomy and survey of data poisoning attacks. Computers & Security. 2020. Vol. 92. P. 101746. DOI: 10.1016/j.cose.2020.101746 .
17. Arustamian A.B., Tsirlov V.L., Shishkin I.I. Obnaruzhenie i fil'tratsiia anomalii v modeliakh mashinnogo obucheniia dlia protivodeistviia atakam otravleniia dannykh. V sb.: Kibernetika i informatsionnaia bezopasnost' "KIB-2024": sbornik nauchnykh trudov II Vserossiiskoi nauchno-tekhnicheskoi konferentsii. M., 2024. Pp. 74–75.

МОДЕЛЬ ОЦЕНКИ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНОЙ СИТУАЦИИ

Лубенцов А.В.¹

Ключевые слова: сложная система, анализ эффективности, интервальная оценка, эффективность процессора.

Аннотация

Цель работы: приведен системный анализ вопросов проектирования сложных информационных систем (СИС) и оценки эффективности функционирования СИС как интегральной эффективности составляющих элементов.

Методика: предлагается методология декомпозиции СИС, оценка модели интеграционного обобщения кластерных оценок. Используется модель многоуровневой системы интервальной оценки индексов.

Полученные результаты: разработанные методики применяются для оценки эффективности процессоров, используемых в СИС. Приведены графические представления результатов расчетов и выводы о применимости и эффективности методики.

DOI: 10.24412/1994-1404-2025-2-103-111

Актуальность оценки эффективности процессоров

Процессоры, или центральные процессорные устройства (ЦП), являются основными компонентами любых сложных информационных систем (СИС), будь то сеть, персональный компьютер, ноутбук или сервер. Эффективность процессора напрямую влияет на производительность системы в целом, что делает оценку его эффективности одной из ключевых задач как для производителей, так и для конечных пользователей.

Постановка задачи

В данной статье будут подробно рассмотрены актуальность оценки эффективности процессоров, методы оценки, а также влияние этих показателей на выбор процессора для различных задач. Предложена методика анализа обобщенной эффективности процессоров, проведен сравнительный анализ этой методики с реальными показателями быстродействия.

Влияние эффективности на производительность системы

Эффективность процессора определяет, насколько быстро и качественно система справляется с выполнением заданий. В процессе работы ЦП выполняет множество операций, от обработки данных до выполнения сложных вычислений. При этом на производительность влияет не только тактовая частота, но и архитектура процессора, его энергопотребление, кэш-память и другие характеристики.

При выборе процессора пользователи часто сталкиваются с множеством моделей и конфигураций. Понимание того, как оценивать эффективность процессора, позволяет сделать более обоснованный выбор. От правильного выбора зависит не только скорость работы программ, но и общий пользовательский опыт, включая время загрузки ОС и программ, качество воспроизведения мультимедиа и высоких нагрузок в играх.

¹ **Лубенцов Александр Витальевич**, кандидат географических наук, кандидат географических наук, доцент Воронежского института Федеральной службы исполнения наказаний России, г. Воронеж, Российская Федерация. ORCID: 0000-0003-0239-4843, SPIN-код: 6530-4715.

E-mail: lubensov@mail.ru

Архитектура процессора

Архитектура процессора — основа его работы. Разные архитектуры процессоров могут значительно отличаться в плане производительности при равной тактовой частоте. Например, архитектура x86 имеет свою специфику, которая может влиять на скорость обработки операций. Контроллер памяти, количество ядер и потоков, поддержка технологий виртуализации и других особенностей также важны при оценке.

Недавние тенденции в разработке процессоров показывают, что многие производители стали делать акцент на многоядерности. Это позволяет одновременно обрабатывать несколько потоков информации, что особенно полезно для многозадачных операций. Процессоры с высокой многоядерностью демонстрируют преимущества в задачах, связанных с обработкой видео, 3D-рендерингом и научными расчетами.

Энергопотребление и теплоотведение

Еще одним важным аспектом оценки эффективности процессора является его энергопотребление и способность к теплоотведению. Современные процессоры должны обеспечивать высокую производительность при минимальном потреблении энергии. Это особенно важно для мобильных устройств, таких как ноутбуки и планшеты, где продолжительность работы от аккумулятора играет ключевую роль.

Эффективные процессоры способны выполнять больше операций на каждый ватт потребляемой энергии, что делает их более привлекательными с точки зрения экологии и экономии. Процессоры нового поколения используют технологии, позволяющие им переключаться между различными режимами работы, подстраиваясь под текущие нагрузки и тем самым снижая общее энергопотребление.

Методы оценки эффективности процессоров

Существует ряд методов оценки эффективности процессоров, которые варьируются от простых до сложных. К ним относятся использование бенчмарков, тестирование в реальных условиях и анализ стендовых систем.

Бенчмарки

Бенчмарки — это стандартные тесты, которые позволяют количественно оценить производительность процессоров. Они могут измерять различные аспекты работы ЦП, включая скорость выполнения операций с плавающей точкой, эффективность работы с целыми числами и обработку многопоточных задач.

Существует множество доступных бенчмарков, среди которых наиболее популярными являются Cinebench, Geekbench и 3DMark. Каждый из них имеет свои особенности и подходит для различных сценариев использова-

ния. Например, Cinebench, основанный на рендеринге 3D-сцен, может дать представление о производительности в задачах, связанных с графикой.

Тестирование в реальных условиях

Помимо бенчмарков, тестирование в реальных условиях также представляет собой важный метод оценки. Это позволяет фактически проверить, как процессор будет работать в условиях, приближенных к обычному использованию. В рамках такого тестирования могут использоваться ресурсоемкие приложения, такие как видеоредакторы и игры.

Такое тестирование полезно, поскольку даже высокие рейтинги в бенчмарках не всегда отражают реальную производительность в конкретных сценариях. Например, процессор может отлично справляться с тестами на производительность с плавающей точкой, но оказывать недостаточное влияние на производительность в многопоточных задачах.

Подбор процессора для задач

При выборе процессора важно учитывать, какие задачи будут выполняться. Разные виды деятельности требуют разных ресурсов, и поэтому одним пользователям понадобятся мощные многоядерные процессоры, тогда как другим достаточно более простых моделей.

Для моделирования технических/физических процессов

Моделирующие процессоры должны обеспечивать высокую производительность в многопоточных задачах, так как современные модели описания процессов часто используют несколько ядер для обработки различных игровых механик. Такие процессоры, как Intel Core i7 и AMD Ryzen 7, зарекомендовали себя как отличные варианты для моделирования технических/физических процессов благодаря своей высокой тактовой частоте и большому количеству ядер.

Для работы с графикой и видео

Пользователи, занимающиеся видеомонтажом или 3D-рендерингом, также должны обращать внимание на количество ядер и потоков, а также на поддержку параллельных вычислений. Процессоры с большими объемами кэш-памяти и высокой пропускной способностью памяти помогут значительно ускорить выполнение сложных вычислительных задач.

Для офисной работы

Для офисных задач, таких как работа с документами и электронными таблицами, подойдет процессор начального уровня. Здесь важнее низкое энергопотребление и достаточно хорошая производительность для

выполнения базовых операций. Такие модели, как Intel Core i3 или AMD Ryzen 3, могут удовлетворить эти потребности с минимальными затратами.

Будущее оценки эффективности процессоров

По мере развития технологий и роста требований к вычислительным системам, актуальность оценки эффективности процессоров будет сохраняться. Появление новых архитектур и технологий, таких как квантовые вычисления, замедляет старение традиционных процессоров и повышает требования к их производительности.

Новые технологии

Одной из перспективных технологий является искусственный интеллект, который уже сейчас активно используется для оптимизации работы процессоров. Ожидается, что будущие процессоры будут более адаптивными и смогут самостоятельно регулировать свою производительность в зависимости от выполняемых задач.

Критерии оценки

С изменением технологий будут возникать и новые критерии оценки производительности процессоров. Параметры, связанные с производительностью на ватт и другими метриками, будут иметь всё большее значение. Оценка не будет сводиться только к тактовой частоте и количеству ядер.

Математические модели оценки эффективности процессоров

Математические модели являются мощным инструментом для оценки эффективности процессоров. Эти модели помогают исследовать и предсказывать, как различные факторы влияют на производительность, энергопотребление и стоимость вычислительных систем. В данной статье мы подробно рассмотрим существующие математические модели, их применение и недостатки, а также актуальность выбранных подходов в современном мире компьютерных технологий.

Рассмотрим самую общую формулу производительности:

$$\text{Производительность} = \frac{\text{количество инструкций}}{\text{время выполнения}}$$

Понятно, что производительность процессора может измеряться количеством проведенных операций/инструкций в секунду.

Рассмотрим формулу более подробно. Для этого введем в нее параметр внутренней скорости процессора — тактовую частоту.

$$\text{Производительность} = \left(\frac{\text{количество инструкций}}{\text{количество тактов}} \right) \times \left(\frac{\text{количество тактов}}{\text{время выполнения}} \right)$$

Основным аспектом производительности вычислительных устройств является разделение на два ключевых показателя: первое — это количество инструкций, которые процессор обрабатывает за один такт (англ. Instructions Per Cycle, IPC), а второе — частоту тактовой скорости. Следовательно, для повышения эффективности работы необходимо либо увеличивать частоту процессора, либо оптимизировать его так, чтобы за один такт обрабатывалось больше инструкций. Однако, учитывая, что достижение большей частоты стало существенно ограничено, актуальной задачей становится разработка методов повышения IPC — увеличения числа инструкций, выполняемых за один такт.

Основы математических моделей в вычислительной технике

Математические модели используются для описания и анализа систем, основанных на математических уравнениях и алгоритмах. В контексте процессоров такие модели позволяют предсказать, как изменения в архитектуре, размерах кеша, частоте работы или других характеристиках компонентов могут повлиять на общую производительность системы.

Роль математических моделей в оценке процессоров

Производительность процессора оценивается по множеству критериев, включая тактовую частоту, количество ядер, архитектуру, кэш-память и энергопотребление. Математические модели помогают:

- определить оптимальные архитектурные решения: они позволяют оценить, какие изменения в дизайне процессора приведут к самым значительным улучшениям производительности;
- сравнить производительность различных процессоров: с помощью моделей можно провести анализ и сопоставить, как различные процессоры ведут себя под нагрузкой;
- прогнозировать потребление энергии: эффективное управление потреблением энергии становится все более важным, особенно в контексте мобильных и встраиваемых систем.

Оценка стоимости-эффективности: модели жизненного цикла процессора позволяют понять, какой продукт является наиболее выгодным к покупке в долгосрочной перспективе.

Типы математических моделей для оценки эффективности процессоров

Существует несколько основных типов математических моделей, которые используются для оценки производительности процессоров.

Модели производительности

Наиболее распространенными являются модели производительности. Они основаны на различных метриках, таких как время выполнения алгоритма или количество операций, выполненных за единицу времени. Одной из популярных моделей производительности является модель IPC, которая вычисляет количество выполненных инструкций за тактовый цикл процессора.

Кроме того, важным показателем является тактовая частота.

Эта модель позволяет разработчикам и инженерам быстро оценить, как увеличение тактовой частоты или IPC может повлиять на общую производительность устройства. Однако стоит отметить, что увеличение тактовой частоты не всегда линейно увеличивает производительность, поскольку могут возникать проблемы с перегревом и энергопотреблением.

Модели энергопотребления

Энергопотребление процессора также важно для его оценки. Прямое влияние на абстрактную производительность оказывает и архитектурное проектирование, и программное обеспечение. Модели энергопотребления обычно включают следующие компоненты:

- динамическое потребление: зависит от количества выполняемых операций и частоты работы,
- статическое потребление: связано с потерями энергии из-за утечек в транзисторах.

Простым и предпочтительным методом определения общей потребляемой теплоотводящей мощности для системы состоит в сложении TDP (термальной проекции) центрального процессора и видеокарты с последующим умножением полученного значения на коэффициент 1,5. Здесь TDP представляет собой критический показатель — это расчетная тепловая мощность компонента, для которой должна быть спроектирована система охлаждения, обеспечивая безопасную и надежную работу устройства.

Таким образом, понимание того, как различные архитектурные решения влияют на энергопотребление, становится критически важным для устойчивого дизайна процессоров в условиях растущих энергозатрат.

Модели стоимости

Для более глубокого анализа процессов полезно использовать модели, которые оценивают не только производительность, но и стоимость. Они могут учитывать различные факторы, такие как

- цена компонентов: сколько стоит процессор, материнская плата, оперативная память и т. д.,
- техническое обслуживание: расходы на эксплуатацию и поддержку.

Модель стоимости может быть представлена в виде:
стоимость = стоимость приобретения + стоимость эксплуатации

Согласование стоимостных моделей с производительностью и энергопотреблением позволяет выделить наиболее эффективные процессоры на рынке.

Интерпретация и применение математических моделей

Создание и использование математических моделей предполагает правильную интерпретацию и применение полученных данных. Тщательный анализ моделей позволяет:

- оптимизировать архитектуру процессоров;
- оценивать влияние новых технологий, таких как увеличение числа ядер или внедрение новых материалов, на производительность;
- настроить программное обеспечение для более эффективного использования аппаратного обеспечения.

Примеры практического применения

Рассмотрим несколько случаев практического применения математических моделей для оценки процессоров.

- Разработка новых архитектур: при проектировании новых процессоров, таких как архитектура ARM, используются модели, позволяющие максимально увеличить производительность при минимальном энергопотреблении. Специалисты тестируют различные варианты конфигурации и выбирают оптимальное решение.
- Обновление существующих систем: компании, обновляющие свои вычислительные системы, используют модели, чтобы определить, какие компоненты стоит заменить для достижения максимальной производительности. Например, обновление кеша может значительно улучшить общую производительность системы.
- Исследование новых технологий: когда разрабатываются новые технологии, такие как 3D-структуры транзисторов, используются модели для прогнозирования, как эти новшества могут повлиять на производительность. Это помогает инвесторам, производителям и исследователям принимать обоснованные решения.

Ограничения и недостатки математических моделей

Несмотря на свою полезность, математические модели имеют ряд ограничений и недостатков.

- Сложность вычислений

Некоторые модели могут быть очень сложными и требовать значительных вычислительных ресурсов для их решения. Это может ограничивать их применение в реальных системах, особенно когда необходимо быстро получать результаты.

- Приблизительность результатов

Модели, использующие упрощенные предположения, могут давать приблизительные результаты, которые не всегда отражают действительность. Для достижения точных оценок требуется комплексный подход, использующий как количественные, так и качественные методы.

– Изменчивость факторов

Факторы, влияющие на производительность процессоров, со временем меняются. Новые технологии, такие как квантовые вычисления, изменяют всю парадигму проектирования процессоров. Таким образом, модели, основанные на устаревших подходах, могут быть менее актуальными.

Будущее математических моделей в оценке процессоров

Интересно отметить, что в последние годы происходит интеграция методов машинного обучения и искусственного интеллекта в математические модели оценки производительности процессоров. Эти технологии могут значительно повысить точность прогноза, учитывая большое количество переменных и сложных взаимосвязей.

Анализ существующих моделей

Теме эффективности сложных систем и ее конкретных элементов посвящено большое количество работ, начиная с монографий и учебников Плетнева И.Л., Рембеза А.И., Виноградова В.А., Хачатурова Т.С. и других. В последнее время вопросам эффективности сложных технических и информационных систем уделяется немало внимания.

Например, в работе [1] дана стройная система классификации процессоров, но нет иерархизации по эффективности. В работе [2] дана модель оценки эффективности функционирования рабочих приложений, но привязки к тандему «приложение — процессор» не приводится. В связи с этим появилась возможность предложить методику оценки эффективности функционирования процессоров как ядра сложной информационно-технической системы.

Практическое моделирование

Оценка эффективности сложных технических систем (СТС) и их элементов является критически важной задачей, требующей комплексного подхода. Для обеспечения точного и надёжного анализа был осуществлён отбор четырёх процессоров промышленного класса, каждый из которых обладал уникальной архитектурой и набором технических характеристик. Эти данные, необходимые для исследования, были систематизированы в табл. 1, которую предполагается дополнить в рамках реального эксперимента. Выбор различных архитектур, например, x86, ARM, RISC-V или специализированных процессоров типа

FPGA или ASIC, позволяет продемонстрировать влияние архитектурных решений на производительность в рамках конкретных задач, реализуемых в моделируемой СТС. Синтез алгоритма производительности проводился на основе моделей, разработанных в [3-5], при этом важно отметить, что эффективность моделирования зависит не только от выбранных процессоров, но и от точности и адекватности самих моделей. Например, модели, основанные на стохастических процессах, могут более точно отражать реальную работу системы, чем детерминированные модели. Выбор модели определяется целями исследования и характером задачи. Общая схема моделирования, описанная в [6], вероятно, включает в себя различные уровни абстракции, от уровня отдельных компонентов до уровня всей системы. Это позволяет анализировать взаимодействие разных подсистем и определять узкие места. Для оценки эффективности используется многоуровневая система индексов, которая учитывает как количественные, так и качественные показатели. Структура этой системы должна быть четко определена и документирована. Композитная структура модели представлена на рис. 1. К примеру, индексы могут включать в себя время отклика, пропускную способность, надежность, энергопотребление и другие критерии, релевантные для данной СТС. Критически важным аспектом является определение веса каждого индекса. Простой арифметический подход может быть недостаточно точным. Поэтому используется метод, учитывающий коэффициент вариации, который позволяет учесть разброс значений и их статистическую значимость. Для уменьшения влияния случайных факторов на результаты, измерения повторяются несколько раз, а полученные данные подвергаются статистической обработке. Для оценки достоверности результатов используется пороговое значение интервала, определяющее границы приемлемой ошибки. Это позволяет отсеивать выбросы и уменьшать влияние шумов. Кроме того, для устранения неточностей в данных и экспертных оценках применяется метод взвешенного среднего. Вес каждого критерия определяется на основе его значимости для функционирования системы. Интервал параметров веса и надежности/достоверности представлен на рис. 2 и 3. Анализ чувствительности позволяет определить, какие параметры системы наиболее сильно влияют на ее эффективность. Этот анализ помогает сосредоточить усилия на оптимизации критических компонентов. Полученные результаты моделирования используются для создания нелинейной модели оптимизации, которая позволяет найти наилучшие параметры системы для достижения максимальной эффективности. Оптимизация может проводиться с использованием различных алгоритмов, таких как генетические алгоритмы, метод градиентного спуска или симплекс-метод. Выбор алгоритма зависит от сложности модели и ограничений.

Параметры, влияющие на эффективность процессоров

	Виды параметров	Intel Xeon W-1270E	Intel Core i7-10700E	Intel Core i7-11850HE	AMD Ryzen Embedded V2748
1	Контроллер ОЗУ MHz	2933,00	2933,00	3200,00	4266,00
2	Частота MHz	3400,00	2900,00	2600,00	2900,00
3	Авторагон MHz	4800,00	4500,00	4700,00	4250,00
4	Кеш L1, kb	512,00	512,00	448,00	512,00
5	Кеш L2, kb	2048,00	2048,00	10240,00	4096,00
6	Кеш L3, kb	16384,00	16384,00	24576,00	8192,00
7	Техпроцесс nm	14,00	14,00	10,00	7,00
8	TDP w	80,00	65,00	35,00	45,00
9	3DMark 06 CPU	28533,83	25139,17	25125,38	26658,55
10	WinRAR	15571,41	13718,88	13689,30	10920,14
11	X264 HD 4.0 Pass 1	541,91	477,44	477,18	420,25
12	PassMarc	18635,00	16418,00	16409,00	16706,00
13	Cinebench R11,5	21,92	19,31	19,28	18,62

Анализ результатов

На рис. 4 представлено сравнительное влияние рассмотренных параметров на итоговую эффективность процессоров. На рис. 5 представлено официальное

быстродействие рассматриваемых процессоров, представленное независимыми экспертами и характеризующее эффективность в процессе проведения вычислительных операций.

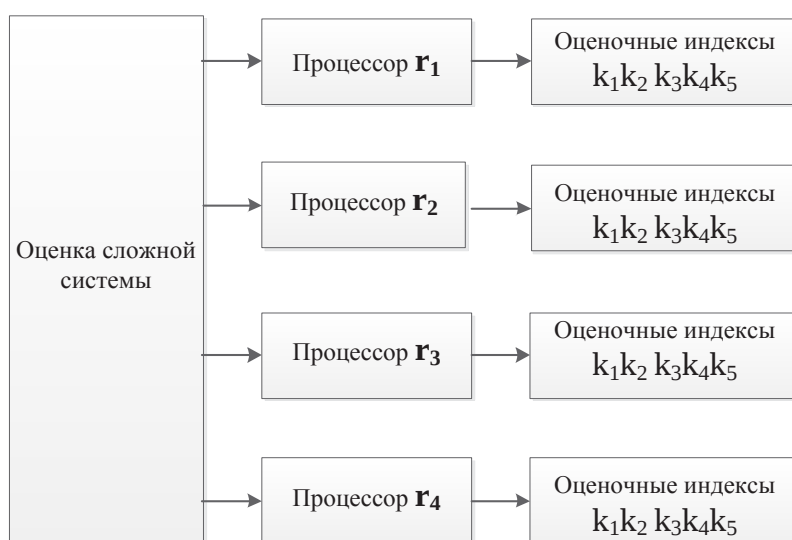


Рис. 1. Общая структура модели оценки эффективности сложной системы

Сравнивая эти две диаграммы, можно определить влияние каждого из рассматриваемых параметров

на итоговую эффективность или производительность анализируемых процессоров.

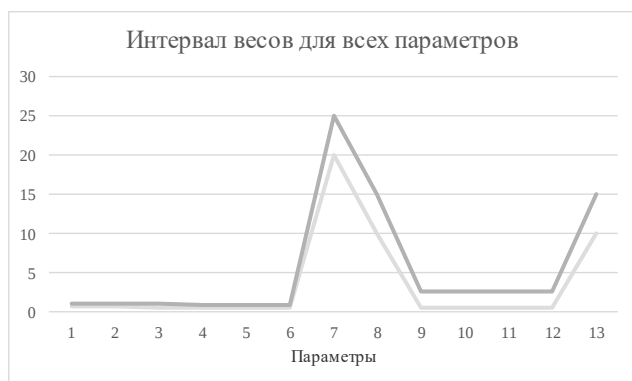


Рис. 2. Интервал весов для 13 параметров всех процессоров

Можно определить, что из технических параметров процессоров наибольшее влияние на производительность оказывает кэш 3 уровня, так как не связан с ядрами процессора и используется для передачи информации между ядрами, хранения информации, и обеспечивает эффективность всего чипа.

Из тестов наиболее качественно оценивает эффективность 3DMark 06 CPU и PassMarc.

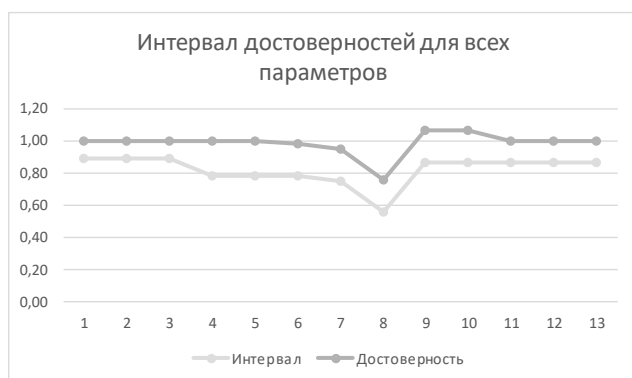


Рис. 3. Интервал достоверностей для параметров всех процессоров

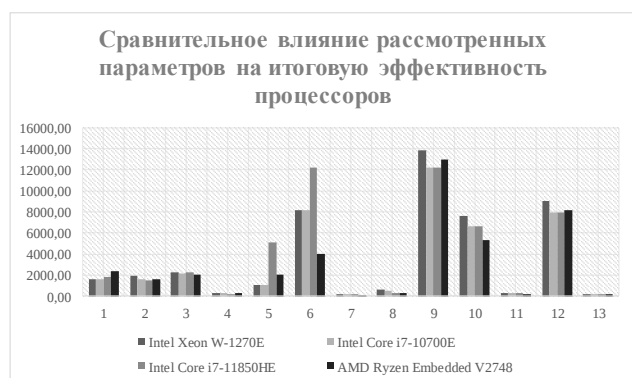


Рис. 4. Сравнительное влияние рассмотренных параметров на итоговую эффективность процессоров

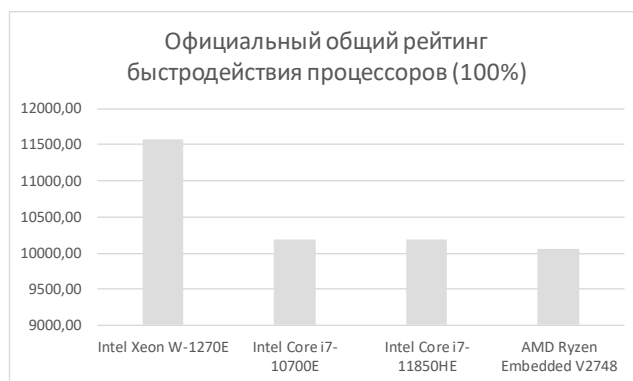


Рис. 5. Официальное быстродействие рассматриваемых процессоров

Заключение

Актуальность оценки эффективности процессоров неоспорима. Процессоры становятся все более сложными, и их производительность является ключевым фактором в выборе оборудования для конкретных задач. Понимание различных методов оценки, включая бенчмарки и тестирование в реальных условиях, позволяет пользователям принимать обоснованные решения при выборе процессоров. В будущем эта оценка станет еще более важной, с учетом роста использования искусственного интеллекта и новых технологий. Процессоры продолжают эволюционировать, и их эффективность будет оставаться в центре внимания.

Математические модели оценки эффективности процессоров являются жизненно важным инструментом для разработчиков, инженеров и исследователей в области вычислительных технологий. Они позволяют анализировать и предсказывать производительность, энергопотребление и стоимость, что критично для достижения устойчивости и эффективности в быстро меняющемся мире технологий. Однако важно помнить о их ограничениях и стремиться к использованию современных методов и технологий, которые могут повысить точность и надежность этих оценок.

В заключение: комплексная оценка эффективности сложных систем требует многоступенчатого подхода, включающего выбор адекватных моделей, определение релевантных индексов эффективности, учет достоверности данных, а также применение методов статистического анализа и оптимизации. Результаты такого анализа позволяют разработать эффективные стратегии технического совершенствования и обслуживания системы, обеспечивая ее бесперебойную и эффективную работу. Предложенная методика обсуждалась на научно-практических конференциях и ее варианты были опубликованы в научных журналах [7—12]. Дальнейшие исследования могут быть направлены на разработку более совершенных методов оценки и учет новых факторов, влияющих на производительность систем.

Расчетная модель реализована в среде Excel и может быть использована для анализа эффективности любых сложных систем: например, информационных, технических, комплексных систем безопасности.

Литература

1. Даулетмуратова Р.А. Особенности интегральных схем и микропроцессорных устройств // Евразийский журнал математической теории и компьютерных наук. 2024. № 3. С. 24—28.
2. Алиева М.Ф. Оценка производительности мобильных приложений / М.Ф. Алиева, В.К. Давтян, С.В. Коцур // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023. № 2 (321). С. 74—83.
3. Лубенцов А.В. Системный анализ оптимизации в модели управленческих решений комплексной системы безопасности / А.В. Лубенцов, О.А. Андреева // Вестник Воронежского института ФСИН России. 2022. № 2. С. 103—111.
4. Лубенцов А.В. Использование каскадного метода анализа иерархий для оценки эффективности комплексной системы безопасности // Вестник Воронежского института ФСИН России. 2022. № 4. С. 113—118.
5. Лубенцов А.В. Системный анализ и синтез методов поддержки принятия решений при построении комплексной системы безопасности // Вестник Воронежского института ФСИН России. 2023. № 1.
6. Лубенцов А.В. Системный анализ модели получения характеристик эффективности комплексной системы безопасности // Моделирование, оптимизация и информационные технологии. 2023. № 11 (1). С. 1—8. DOI: 10.26102/2310-6018/2023.40.1.030.
7. 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.
8. Лубенцов А.В. Синтез иерархической многоуровневой модели параметров для оценки эффективности системы защиты информации в условиях нечетких данных // Известия высших учебных заведений. Электроника. 2024. Т. 29. № 2. С. 236—248.
9. Лубенцов А.В. Моделирование оценки эффективности производительности контроллеров СКУД / Лубенцов А.В., Кобзистый С.Ю. // ВИ ФСИН РФ : труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2023. Т. 1. С. 191—195.
10. Лубенцов А.В. Синтез интервальных оценок для построения модели оценки эффективности сложных систем // ВИ ФСИН РФ : труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2023. Т. 1. С. 171—175.
11. Лубенцов А.В. Синтез модели комбинирования интервальных оценок для анализа эффективности сложных систем // ВИ ФСИН РФ : труды международной конференции «Техника и безопасность объектов уголовно-исполнительной системы». 2023. Т. 1. С. 175—179.
12. Лубенцов А.В. Комплексные системы безопасности: системный анализ, архитектура, управление жизненным циклом / А.В. Лубенцов, А.В. Душкин. Воронеж : Научная книга, 2022. 254 с.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

A MODEL FOR EVALUATING THE EFFICIENCY OF OPERATION OF COMPUTING SYSTEMS IN AN EMERGENCY

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: complex system, efficiency analysis, interval estimation, processor efficiency.

Abstract

Purpose of the study: a system analysis of questions of designing complex information systems (CIS) and evaluating the operation of a CIS as an integrated efficiency of its components is presented.

Methodology used: a CIS decomposition methodology, an evaluation of integrative generalisation of cluster estimates is proposed. The model of multi-level interval estimation of indices is used.

Study findings: the developed methodologies are applied for evaluating the efficiency of processors used in CISs. Diagrams of calculation results are given, and conclusions regarding the applicability and efficiency of the methodology are presented.

References

1. Dauletmuratova R.A. Osobennosti integral'nykh skhem i mikroprotssessornykh ustroystv. Evraziiskii zhurnal matematicheskoi teorii i komp'iuternykh nauk. 2024. No. 3. Pp. 24–28.
2. Alieva M.F. Otsenka proizvoditel'nosti mobil'nykh prilozhenii. M.F. Alieva, V.K. Davtian, S.V. Kotsur. Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki. 2023. No. 2 (321). Pp. 74–83.
3. Lubentsov A.V. Sistemnyi analiz optimizatsii v modeli upravlencheskikh reshenii kompleksnoi sistemy bezopasnosti. A.V. Lubentsov, O.A. Andreeva. Vestnik Voronezhskogo instituta FSIN Rossii. 2022. No. 2. Pp. 103–111.
4. Lubentsov A.V. Ispol'zovanie kaskadnogo metoda analiza ierarkhii dlia otsenki effektivnosti kompleksnoi sistemy bezopasnosti. Vestnik Voronezhskogo instituta FSIN Rossii. 2022. No. 4. Pp. 113–118.
5. Lubentsov A.V. Sistemnyi analiz i sintez metodov podderzhki priniatiia reshenii pri postroenii kompleksnoi sistemy bezopasnosti. Vestnik Voronezhskogo instituta FSIN Rossii. 2023. No. 1.
6. Lubentsov A.V. Sistemnyi analiz modeli polucheniia kharakteristik effektivnosti kompleksnoi sistemy bezopasnosti. Modelirovanie, optimizatsiia i informatsionnye tekhnologii. 2023. No. 11 (1). Pp. 1–8. DOI: 10.26102/2310-6018/2023.40.1.030 .
7. Lubentsov A.V. Sintez metoda otsenki effektivnosti sistemy informatsionnoi bezopasnosti. Izvestiia vysshikh uchebnykh zavedenii. Elektronika. 2024. T. 29. No. 1. Pp. 118–129. DOI: 10.24151/1561-5405-2024-29-1-118-129 . EDN: UJNZBJ.
8. Lubentsov A.V. Sintez ierarkhicheskoi mnogourovnevoi modeli parametrov dlia otsenki effektivnosti sistemy zashchity informatsii v usloviakh nechetkikh dannykh. Izvestiia vysshikh uchebnykh zavedenii. Elektronika. 2024. T. 29. No. 2. Pp. 236–248.
9. Lubentsov A.V. Modelirovanie otsenki effektivnosti proizvoditel'nosti kontrollerov SKUD. Lubentsov A.V., Kobzisty S.Iu. VI FSIN RF : trudy mezhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob"ektov ugovolno-ispolnitel'noi sistemy". 2023. T. 1. Pp. 191–195.
10. 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 ugovolno-ispolnitel'noi sistemy". 2023. T. 1. Pp. 171–175.
11. Lubentsov A.V. Sintez modeli kombinirovaniia interval'nykh otsenok dlia analiza effektivnosti slozhnykh sistem. VI FSIN RF : trudy mezhdunarodnoi konferentsii "Tekhnika i bezopasnost' ob"ektov ugovolno-ispolnitel'noi sistemy". 2023. T. 1. Pp. 175–179.
12. Lubentsov A.V. Kompleksnye sistemy bezopasnosti: sistemnyi analiz, arkhitektura, upravlenie zhiznennym tsiklom. A.V. Lubentsov, A.V. Dushkin. Voronezh : Nauchnaia kniga, 2022. 254 pp.

ПОНЯТИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ: ТЕХНИЧЕСКИЕ И НОРМАТИВНО-ПРАВОВЫЕ АСПЕКТЫ

Метельков А.Н.¹

Ключевые слова: система, информация, структура, информационная технология, персонал, правовая модель, процесс.

Аннотация

Цель работы: обоснование понятийного элементного состава в правовой модели информационной системы (ИС), объективно связанной с существующими организационно-техническими процессами. Правовая модель может существенно отличаться от аналитических и технических схем и представлений о ее внутренней структуре.

Методы исследования: структурный анализ понятия, сравнительный анализ источников права и взглядов технических специалистов на включение непосредственно в состав исследуемого понятия ИС субъекта права.

Результаты исследования: раскрыто содержание понятия «информационная система». Анализ действующего законодательства и существующих в научной и учебной литературе различных точек зрения специалистов на понятие ИС приводит к выводу об отсутствии субъекта как составляющего элемента в законодательной модели понятий «информационная система» и «информационная технология». Выделение субъекта права как самостоятельной биосоциальной системы из элементов технической системы позволяет на практике конкретизировать подход к защите информации и дифференцировать усилия для обеспечения информационной безопасности на решение поставленных задач в условиях интенсивного использования злоумышленниками методов социальной инженерии и убедительных сценариев их реализации для проникновения в компьютерные сети и критическую инфраструктуру.

DOI: 10.24412/1994-1404-2025-2-112-118

Введение

Коммуникационные и информационные технологии становятся частью современных управляющих систем и всё больше проникают в жизнь общества и государства, что порождает не только организационно-технические, но и «правовые проблемы в сфере сдерживания киберугроз» [11, с. 3] в критической инфраструктуре. Например, агрессивные кибератаки в одной из целевых для злоумышленников электроэнергетической системе направлены «на срыв технологических операций и могут привести к разрушению системной инфраструктуры, травмам и гибели людей...»². Информационные технологии (ИТ) играют

определяющую роль в информационном обществе. Проникновение ИТ практически во все сферы «деятельности, регулируемые правом, ведет к появлению новых правовых отношений и новых предметов регулирования» [4, с. 4].

В условиях бурного развития новых технологий в связи с усложнением задач в сфере обеспечения информационной безопасности (ИБ) возникла потребность в уточнении взглядов на содержание правового термина «информационная система» (ИС). В условиях цифровой трансформации осмысление содержания ИС имеет не только теоретическую направленность, но и способствует углублению понимания и приращению знаний о составе объектов защиты информации в практической деятельности [2, 9].

² Папков Б.В., Куликов А.Л., Осокин В.Л. Киберугрозы и кибератаки в электроэнергетике : учебное пособие. Н. Новгород: НИУ РАНХиГС, 2017. С. 6.

¹ Метельков Александр Николаевич, кандидат юридических наук, доцент кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-6113-8981.

E-mail: metelkov5178@mail.ru

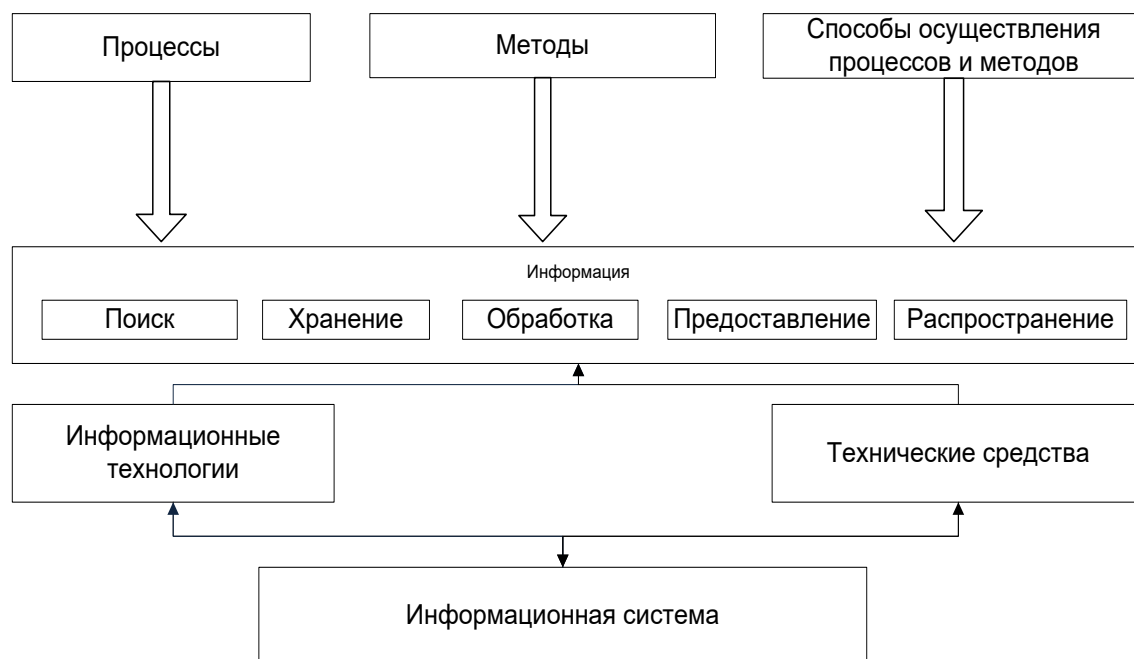


Рис. 1. Схема ИС согласно Закону № 149

Обсуждение

В научной литературе ИС трактуется и как техническая система, реализованная с применением информационных и телекоммуникационных технологий, и как социально-техническая, и как социальная система, а также концептуальная система, интегрирующая эти подходы [7]. В числе компонентов ИС исследователи и технические специалисты обычно выделяют аппаратное и программное обеспечение, базы данных, человеческие ресурсы, процессы (процедуры).

Впервые нормативно-правовое понятие ИС было использовано в Законе РФ от 20 февраля 1995 г. «Об информации, информатизации и защите информации» и рассматривалось в качестве массива документов и ИТ без участия человека. Дальнейшее развитие это понятие получило в Федеральном законе РФ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» (Закон № 149), в котором оно раскрывается как «совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств»³. На рис. 1 представлена соответствующая схема ИС. В действующем законе сохранился правовой подход об исключении человека из элементов системы.

Это утверждение опосредованно доказывается через анализ определения оператора ИС, которым может быть только эксплуатирующее ИС юридическое лицо или гражданин, то есть юридическое лицо, являюще-

еся в качестве субъекта права юридической фикцией, и человек выводятся за границы понятия ИС. Серьезным подтверждением бессубъектности правовых элементов, составляющих содержание ИС, является установление законодателем обязанности соблюдать ряд требований законодательства РФ владельцем информационной системы (ст. 10.2-2 Закона № 149). Рассмотрим эту правовую норму подробнее.

Для проведения анализа сделаем допущение от противного. Допустим, что в состав ИС, например, через понятие ИТ, входит субъект — физическое или юридическое лицо. В этом случае, рассуждая логически, получается, что владелец ИС окажется владельцем физического лица, например, если обслуживающий эту систему персонал включить в ее состав. Очевидно, что с правовой точки зрения в цивилизованном мире это выглядит некорректно. Современный человек в правовом отношении вышел из состояния рабства, правовая сущность которого в гражданском праве Древнего Рима заключалась в отождествлении раба с вещью. В определении государственных ИС обеспечения градостроительной деятельности, создаваемых и эксплуатируемых в соответствии с требованиями Градостроительного кодекса РФ (ст. 56), указывается, что к ним относятся ИС, содержащие сведения, документы, материалы о развитии территорий, их застройке, существующих и планируемых к размещению объектах капитального строительства и иные необходимые для осуществления градостроительной деятельности сведения. Удивительно, но для целей Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Россий-

³ Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в ред. от 23 ноября 2024 г.) // Собрание законодательства РФ. 2006. № 31. Ч. 1. Ст. 3448.

ской Федерации» (Закон № 259) под узлами ИС понимаются «пользователи информационной системы...» [8]. Пользователи ИС ассоциируются с широким кругом субъектов. Таким образом, пользователи как субъекты включаются в состав ИС, становясь неотъемлемым элементом ИС, своеобразными «рабами» системы, что противоречит определению ИС, данному в базовом Законе № 149. Парадокс заключается в том, что Закон № 149 в понятие ИС явно не включает человека, а Закон № 259 считает пользователей узлами ИС, что противоречит доминирующим в технике взглядам на понимание узла ИС. При этом понятие «информационная система» в Законе № 259, как прямо указано в нем, используется в значении, определенном Законом № 149. Узлы ИС обязаны только обеспечивать соответствие порядка выпуска электронных данных (цифрового кода или обозначения) и осуществления в их отношении действий по внесению или изменению записей в такую ИС ее правилам [13, с. 37]. Включая человека в состав ИС, невольно возникает вопрос о расширении объекта технической защиты данных в ИС, так как регулятором, ФСТЭК России, в число установленных ведомственным приказом от 11 февраля 2013 г. № 17 объектов защиты в ИС, антропологический элемент обоснованно не включается. Несмотря на то, что внутренний фактор является одним из наиболее опасных с точки зрения формирования и реализации угроз безопасности информации, к его защите надо подходить в первую очередь с использованием нетехнических методов.

В официальных документах Содружества Независимых Государств (СНГ) понятие ИС рассматривается и как совокупность документов, средств, а также как имущественный комплекс (см. таблицу 1).

В стандартах ИС определяется применительно к сферам деятельности и трактуется как система обработки и распространения информации, предполагающая наличие человеческих, технических, финансовых и других организационных ресурсов (ISO/IEC 2382:2015), «организующая обработку информации о предметной области и ее хранение» (ГОСТ 33707-2016), «предназначенная для представления, хранения, обработки, поиска, распространения и передачи по каналам связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» и как совокупность «содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» (ГОСТ Р 51583-2014)⁴. В формулировке термина «информационно-вычислительная система» (ИВС) также отсутствует субъект (ГОСТ Р 53622-2009)⁵. В то же время система, согласно документу Национального института стандартов и технологий США NIST SP 800-66 Rev. 1, объединяет не только аппаратное и программное обеспечение, информацию, данные, приложения, средства связи, но и людей.

Исследование понятия ИС и составляющих ее элементов способствует раскрытию содержания ИБ. Ввиду высокой цифровизации и специфики применения цифровых систем исходным критерием разбиения на группы является «признак автономности...». По наличию связи «человек-машина» системы разделяют на автоматические — функционирующие без участия челове-

⁴ ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М. : Стандартинформ, 2018.

⁵ ГОСТ Р 53622-2009 ИТ. Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность доку-

Таблица 1

Понятие ИС в документах СНГ

Составные элементы понятия ИС	Официальный документ СНГ
а) организационно упорядоченная совокупность документов (массивов документов); б) ИТ; в) информационные процессы	Соглашение о свободном доступе и порядке обмена открытой научно-технической информацией государств-участников СНГ (утв. Решением глав правительств, г. Москва, 11.09.1998)
а) организационно упорядоченная совокупность средств; б) технологические действия; в) информационные процессы	Модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности» (приложение к постановлению МПА СНГ от 28.11.2014 № 41-15)
Имущественный комплекс, включающий следующие элементы: а) техническое оборудование б) программное обеспечение (включая информацию, средства ее предоставления и организацию).	Решение Совета глав правительств СНГ «О Стратегии сотрудничества государств-участников СНГ в сфере информатизации и Плана действий по реализации Стратегии сотрудничества государств-участников СНГ в сфере информатизации на период до 2010 года» от 24.11.2006

ка и «автоматизированные — включающие человека и H2M связи» [5, с. 53]. Д.П. Зегжда представляет ИС в виде сложной иерархической структуры, состоящей «из дискретных моделей... между которыми установлена архитектура логических, семантических, сигнальных связей» [5, с. 89]. Под ИС специалисты также понимают компьютерную сеть, включающую программные, аппаратные и информационные ресурсы, а также «персонал, поддерживающий их согласованное функционирование» [10, с. 8].

Определения ИС, отражающие социально-технический подход, описывают динамичные социально-технические процессы взаимодействия человека и технической системы. В работе Singh A. et al.⁶, по мнению индийских исследователей, ИС охватывает не только комплекс программного и аппаратного обеспечения, информацию, но и людей и необходимые для использования данных процедуры в качестве внутри- и вне-организационного ресурса. В представлении редакционной команды Indeed Editorial Team, отраженном на ее сайте, модель ИС объединяет людей (например, программистов, специалистов по ИТ, сотрудников службы поддержки, системных аналитиков), которых нельзя исключать из описания ИС. Однако с точки зрения защиты информации в законодательное определение ИС включать людей (пользовательский и обслуживающий персонал) как элемент такой системы, по нашему мнению, будет методически неправильно. Очевидно, что с любой вычислительной задачей без самого простого включения электропитания для начала работы или ликвидации последствий успешной кибератаки сама ИС без участия человека в большинстве случаев не справится [7, 9]. Поэтому человека в этом контексте следует концептуально рассматривать как социально-биологическую систему, взаимодействующую с «железом», программами и технологиями. Такой подход делает предметным построение системы защиты информации, придает ей конкретную практическую направленность.

Очевидно, любая теория, отрасль права и практика базируются на строгом понятийном аппарате. Поэтому с точки зрения защиты информации важно понять социально-техническое содержание термина ИС. Современные определения обычно основаны на онтологической позиции, в которой люди и технологии по своей сути разделены. ИС предназначена «для хранения, обработки, поиска, распространения, передачи и предоставления информации» [12, с. 18]. Эта же концепция реализована в действующем законодательстве [8] посредством установления трехэлементного состава (информация, технические средства, ИТ) понятия ИС. Проанализируем поэлементно содержание этих компонентов на предмет возможного присутствия какого-либо субъекта права. Очевидно, что в собственном смысле

в информацию и технические средства (средства компьютерной и коммуникационной техники) субъект в современном его понимании не входит. В примечании к статье 272 УК РФ компьютерная информация рассматривается только как сведения, «представленные в форме электрических сигналов»⁷. Если рассуждать от противного и включать субъект как компонент ИС, то, исходя из доктринального определения термина «силы обеспечения информационной безопасности»⁸, сотрудники (работники), должностные лица государственных органов и их подразделений, а также органов местного самоуправления и организаций, уполномоченные законодателем на решение задач по обеспечению ИБ конкретных ИС, будут также являться элементами ИС. Очевидно, такой исход не выдерживает критики.

Доктринальное понимание обеспечения ИБ, в отличие от защиты информации, определенной в Законе № 149, предусматривает реализацию более широкого набора различных взаимоувязанных мер, не только правовых, организационных и технических. Прерогатива осуществления специальных (разведывательных, контрразведывательных, оперативно-розыскных), «научно-технических, информационно-аналитических, кадровых, экономических и иных мер»⁹ по противодействию информационным угрозам и ликвидации их последствий законодателем, как правило, возлагается не на всех, а только на определённый круг субъектов права.

Мысль о включения информации в цепь производства информационного продукта принадлежит В.М. Глушкову. В 1982 г. известный ученый предложил в определение ИТ включить «процессы, где основной перерабатываемой продукцией является информация»¹⁰. В научной и учебной технической литературе существуют полярные взгляды на субъектный состав ИТ. В научной литературе ИС рассматриваются не только как сложные объекты, состоящие из технологических и социальных элементов, но и как объекты, формирующие синергетические явления, которые могут возникать при взаимодействии различных элементов. Такие подходы требуют от исследователей одновременного рассмотрения социальных и технических аспектов функционирования технологических и социальных компонентов. В ряде работ непосредственно в состав ИС включают и субъектов. В одном из широких по содержанию определений М.Р. Коголовский включает «системный персонал»¹¹. Таких субъектов в опре-

⁶ Singh A. et al. Information Security: Components and Techniques. MS International Journal of Advanced Research in Computer Science and Software Engineering. 2014; 4(1):1072-1077.

⁷ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 28 декабря 2024 г.) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

⁸ Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

⁹ Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

¹⁰ Глушков В.М. Основы безбумажной информатики. М. : Наука, 1987. С. 334.

¹¹ Коголовский М.Р. Перспективные технологии информационных систем. М. : ДМК Пресс, 2003.

делении ИС Н.А. Гайдамакин называет «функционально-определенной группой работников»¹². Ряд авторов полагают, что ИС не включают субъектов права, другие придерживаются противоположной точки зрения. Например, авторы авторитетного учебного пособия в общей схеме обеспечения ИБ (см. рис. 2) в качестве структурных блоков ИТ включают информацию, технические средства и людей¹³. Энциклопедический подход к ИС включает «компьютерное и коммуникационное оборудование, программное обеспечение, информационные ресурсы»¹⁴. Однако понятия «оператор» и «владелец (собственник)» не являются тождественными.

Статья 14 Закона № 149, именуемая «Государственные информационные системы», определяет, по крайней мере, владельца (собственника) информационных систем в государственном секторе общественных отношений в лице государства [14].

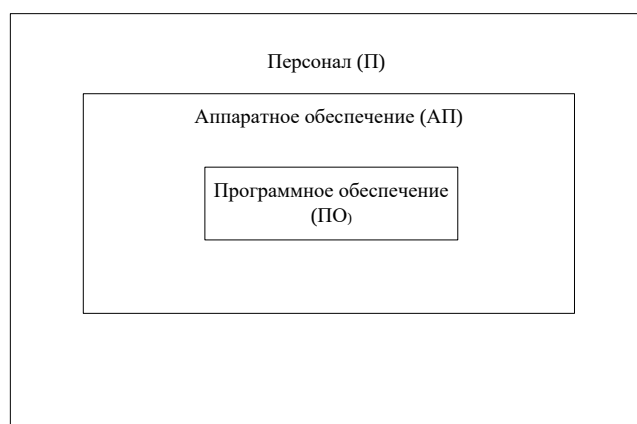


Рис.2. Фрагмент «Модели ИБС»

ИС рассматривают также и как среду работы ИТ [6, с. 95], и как «совокупность организационных, технических, программных и информационных средств, объединенных в единую систему с целью сбора, хранения, обработки и выдачи необходимой информации, предназначенной для обеспечения функционирования объекта деятельности»¹⁵, и как организационно упорядоченную «совокупность программно-аппаратных и других вспомогательных средств...» [6, с. 487] с поддержкой интерфейса с пользователями системы, и как систему обработки информации совместно с соответствующими организационными ресурсами (челове-

ческими, техническими, финансовыми и т. д.), которая «обеспечивает и распространяет информацию»¹⁶.

В широком смысле теоретически возможно включение субъектов в ИТ. Однако в правовом отношении считаем нецелесообразным включать людей в состав понятий ИТ и ИС. Участие человека предопределяет особенности защиты информации в автоматизированных ИС, так как человек является субъектом доступа и его наличие формирует потенциальные угрозы в первую очередь социального, а не узкотехнического характера, что отражается в моделях нарушителя и угроз безопасности информации. При этом, безусловно, человек оказывает воздействие на информационные процессы, информацию и технические средства. Включение в набор элементов ИС человека приводит к растворению биосоциальной системы в технической системе, что запутывает доктринальную модель обеспечения ИБ и затрудняет использование сил обеспечения ИБ. Субъект в системе «человек — машина» в этом случае раздваивается: с одной стороны, он является представителем сил обеспечения, с другой — элементом технической ИС, автоматизирующей какие-либо процессы. При таком подходе существенно затуманивается и усложняется концептуальная и правовая модель обеспечения ИБ.

Субъект сам по себе является сложной социальной системой и носителем информации, в том числе защищаемой. Злоумышленники, манипулируя социально-психологическими свойствами человека, часто сравнительно легко получают доступ к такой информации. Метод социальной инженерии как совокупность способов и приемов реализации компьютерных атак или несанкционированного доступа к информации и ИС без использования технических средств или в сочетании с ними основан на эксплуатации особенностей психики и человеческих слабостей. Он является весьма эффективным в реализации различных криминальных сценариев.

Методологически с точки зрения правовой и технической защиты информации целесообразно отдельно рассматривать субъекты права, с одной стороны, и информацию, информационные технологии и технические средства — с другой, даже если они интегрированы в организм человека-киборга. В противном случае понятие ИС становится синонимичным понятию автоматизированной системы (АС). Анализ состава понятия «автоматизированная система», определенного в ГОСТ Р 59853-2021, подтверждает мысль о том, что ИТ и персонал включены в качестве самостоятельных элементов в это понятие. В состав ИТ входят как технические средства, так и методы передачи информации (например, канал связи, компьютерная сеть); часто используют термин «информационно-коммуникационная технология» [1].

Заключение

¹² Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс : учебное пособие. М. : Гелиос АРВ, 2002. С. 12—13.

¹³ Когаловский М.Р. Перспективные технологии информационных систем. М. : ДМК Пресс, 2003.

¹⁴ Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс : учебное пособие. М. : Гелиос АРВ, 2002. С. 12—13.

¹⁵ Малюк А.А., Горбатов В.С. [и др.] Введение в информационную безопасность : учебное пособие для вузов. М. : Горячая линия — Телеком, 2018. С. 14.

¹⁶ Большая российская энциклопедия. М. : Большая российская энциклопедия, 2008. Т. 11. С. 487.

В настоящее время широкое распространение получили технологии распределенных систем, глобальных, региональных и локальных компьютерных сетей, стремительно развиваются технологии электронной коммерции, облачные технологии и туманные вычисления, технологии дополненной и виртуальной реальности. Экспоненциальный рост объемов информации привел к созданию и использованию технологий data mining, применению искусственного интеллекта (нейронных сетей) для решения широкого спектра задач.

В результате анализа различных подходов к наполнению содержательными элементами понятия ИС отражения в российском законодательстве структуры правового понятия ИС в части включения в его состав субъекта права. Такой подход законодателя размывает объективные процессы в социотехнической системе, обрабатывающей данные с помощью компьютерной техники и средств телекоммуникаций, с тем или иным участием субъекта.

Литература

1. Акопян Б.К., Григорьева Н.Н. Системный анализ информационных и технических систем: лаб. практикум. СПб. : ГУАП, 2023. 55 с.
2. Бурый А.С., Усцелемов В.Н. Развитие систем поддержки принятия решений на основе прецедентов в распределенных информационных структурах // Правовая информатика. 2024. № 1. С. 88—95.
3. Гончаров В.В., Гончаров А.В., Мишенина О.В. Моделирование обнаружения информационных атак на основе теории конечных автоматов // Правовая информатика. 2023. № 1. С. 41—51. DOI: 10.21681/1994-1404-2023-1-41-51.
4. Запольский С.В., Исаков В.Б. Новые актуальные основания модернизации в сфере информационного права // Правовая информатика. 2013. № 1. С. 4—12.
5. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак : монография. СПб. : Политех-Пресс, 2022. 490 с.
6. Кузнецова О.Д., Кумратова А.М., Курносоева Н.С. Автоматизированные информационные системы для увеличения эффективности работы предприятия // Цифровизация экономики: направления, методы, инструменты : сборник материалов III Всероссийской научно-практической конференции. Краснодар, 2021. С. 94—97.
7. Ловцов Д.А., Бурый А.С. Кибербезопасность: основные тенденции в обеспечении // Правовая информатика. 2024. № 2. С. 23—34. DOI: 10.21681/1994-1404-2024-2-23-34.
8. Метельков А.Н. Парадокс узлов: защита информации и право цифровой валюты // Защита информации. Инсайд. 2021. № 6. С. 4—12.
9. Метельков А.Н. Техническое регулирование информационной безопасности «безопасного города»: гармонизация подходов // Правовая информатика. 2024. № 3. С. 58—67. DOI: 10.24412/1994-1404-2024-3-58-67.
10. Олифер В.Г., Олифер Н.А. Безопасность компьютерных сетей. М. : Горячая линия — Телеком, 2020. 644 с.
11. Себекин С.А. Генезис и развитие стратегий сдерживания киберугроз в США, КНР и России (1990-е — 2014 гг.) : автореф. дис. ... канд. историч. наук: 07.00.03 / Сергей Александрович Себекин. Иркутск, 2020. 26 с.
12. Торба О.И., Торба Д.О., Коваленко Ю.И., Тараскин М.М. Правовое нормативное обеспечение управления проектами в области информационной безопасности : монография. М. : Русайнс, 2022. 520 с.
13. Тутынин И.Б., Химичева О.В. Применение мер уголовно-процессуального принуждения при расследовании преступлений, совершенных с использованием криптовалюты : монография. М. : Юрлитинформ, 2022. 144 с.
14. Яковец Е.Н. Некоторые аспекты организационно-правовой защиты информационно-телекоммуникационных систем // Проблемы правовой и технической защиты информации. 2022. № 10. С. 94—105.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

THE CONCEPT OF INFORMATION SYSTEM: TECHNICAL AND LEGAL ASPECTS

Aleksandr Metel'kov, Ph.D. (Law), Associate Professor at the Department of Applied Mathematics and Information Technologies Security of the Saint Petersburg University of the State Fire Service of the Ministry of Emergency Situations of the Russian Federation, Saint Petersburg, Russian Federation. ORCID: 0000-0002-6113-8981.

Keywords: system, information, structure, information technology, personnel, legal model, process.

Abstract

Purpose of the study: justifying the conceptual element composition in the legal model of an information system (IS) which is related to current organisational and technological processes. The legal model can have considerable differences from analytical and technical schemes and understanding of the IS internal structure.

Methods used in the study: concept structure analysis, comparative analysis of legal sources and views of technical specialists as regards including the legal subject IS in the structure of the concept under study.

Study findings: the content of the concept of IS is expounded. An analysis of the current laws and regulations as well as of different stances of specialists on the concept of IS which can be found in scholarly and teaching literature leads to the conclusion that the legal model of the concepts of 'information system' and 'information technology' lacks the subject as a constituting element. Singling out the subject of law as an independent bio-social system from the elements of a technical system allows to make more specific and practical both the approach to information protection and the efforts aimed at ensuring information security, in the context of extensive use by malefactors of social engineering methods and convincing scenarios of their implementation for penetrating computer networks and critical infrastructure.

References

1. Akopian B.K., Grigor'eva N.N. Sistemnyi analiz informatsionnykh i tekhnicheskikh sistem: lab. praktikum. SPb. : GUAP, 2023. 55 pp.
2. Buryi A.S., Ustselemonov V.N. Razvitie sistem podderzhki priniatiia reshenii na osnove pretsedentov v raspredelennykh informatsionnykh strukturakh. Pravovaia informatika. 2024. No. 1. Pp. 88–95.
3. Goncharov V.V., Goncharov A.V., Mishenina O.V. Modelirovanie obnaruzheniia informatsionnykh atak na osnove teorii konechnykh avtomatov. Pravovaia informatika. 2023. No. 1. Pp. 41–51. DOI: 10.21681/1994-1404-2023-1-41-51.
4. Zapol'skii S.V., Isakov V.B. Novye aktual'nye osnovaniia modernizatsii v sfere informatsionnogo prava. Pravovaia informatika. 2013. No. 1. Pp. 4–12.
5. Zegzhda D.P. Teoreticheskie osnovy kiberustoiichivosti i praktika prognosticheskoi zashchity ot kiberatak : monografiia. SPb. : Politekh-Press, 2022. 490 pp.
6. Kuznetsova O.D., Kumratova A.M., Kurnosova N.S. Avtomatizirovannye informatsionnye sistemy dlia uvelicheniia effektivnosti raboty predpriiatiia. Tsifrovizatsiia ekonomiki: napravleniia, metody, instrumenty : sbornik materialov III Vserossiiskoi nauchno-prakticheskoi konferentsii. Krasnodar, 2021. Pp. 94–97.
7. Lovtsov D.A., Buryi A.S. Kiberbezopasnost': osnovnye tendentsii v obespechenii. Pravovaia informatika. 2024. No. 2. Pp. 23–34. DOI: 10.21681/1994-1404-2024-2-23-34.
8. Metel'kov A.N. Paradoks uzlov: zashchita informatsii i pravo tsifrovoy valiuty. Zashchita informatsii. Insaidd. 2021. No. 6. Pp. 4–12.
9. Metel'kov A.N. Tekhnicheskoe regulirovanie informatsionnoi bezopasnosti "bezopasnogo goroda": garmonizatsiia podkhodov. Pravovaia informatika. 2024. No. 3. Pp. 58–67. DOI: 10.24412/1994-1404-2024-3-58-67.
10. Olifer V.G., Olifer N.A. Bezopasnost' komp'iuternykh setei. M. : Goriachaia liniia – Telekom, 2020. 644 pp.
11. Sebekin S.A. Genezis i razvitie strategii sderzhivaniia kiberugroz v SShA, KNR i Rossii (1990-e – 2014 gg.) : avtoref. dis. ... kand. istorich. nauk: 07.00.03. Sergei Aleksandrovich Sebekin. Irkutsk, 2020. 26 pp.
12. Torba O.I., Torba D.O., Kovalenko Iu.I., Taraskin M.M. Pravovoe normativnoe obespechenie upravleniia proektami v oblasti informatsionnoi bezopasnosti : monografiia. M. : Rusains, 2022. 520 pp.
13. Tutynin I.B., Khimicheva O.V. Primenenie mer ugolovno-protssessual'nogo prinuzhdeniia pri rassledovanii prestuplenii, sovershennykh s ispol'zovaniem kriptovaliuty : monografiia. M. : Iurlitinform, 2022. 144 pp.
14. Iakovets E.N. Nekotorye aspekty organizatsionno-pravovoi zashchity informatsionno-telekommunikatsionnykh sistem. Problemy pravovoi i tekhnicheskoi zashchity informatsii. 2022. No. 10. Pp. 94–105.

ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРАВА НА ДОСТУП К ИНФОРМАЦИИ В УСЛОВИЯХ РАЗВИТИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА¹

Герашенко А.И.², Беда А.А.³

Ключевые слова: чат-бот, цифровой помощник, достоверность информации, генеративность, датификация, цифровизация, информирование.

Аннотация

Цель статьи: выявление проблемных аспектов реализации права на доступ к информации — в публичном и частном смыслах — в условиях развития технологий искусственного интеллекта (ИИ), имитирующих когнитивные функции человека и получающих при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их.

Методы исследования: общенаучные (анализ, синтез, обобщение, сравнение) и специальные юридические методы (формально-юридический, сравнительно-правовой, казуальный).

Результаты исследования: аргументированная доктринальная позиция авторов о том, что право на доступ к информации в условиях появления технологий ИИ активно развивается и нарушается. Предлагается предусмотреть в праве на доступ к информации право субъекта информационных правоотношений на выбор источника достоверной информации: «цифрового помощника», основанного на моделях ИИ, или человека, обладателя предоставляемой информации. В текущих условиях правоотношения между обращающимся и государственными и частными «цифровыми помощниками» должны строиться на принципе свободы выбора формы обращения.

Практическая ценность: предлагается применять презумпцию достоверности информации, генерируемой «цифровыми помощниками», при определении обращающегося за информацией субъекта права в качестве «слабой стороны правоотношений». Предлагается также внедрить правовой инструмент информирования такого лица об особенностях функционирования «цифрового помощника» и правовую возможность обращения к владельцу «цифрового помощника» или его полномочному представителю в случае, если у обращающегося субъекта есть сомнения в достоверности информации, полученной от «цифрового помощника».

DOI: 10.24412/1994-1404-2025-2-119-131

Введение

Право на доступ к информации как фундаментальное конституционное право человека активно трансформируется с началом эпохи цифровизации, стадии развития информационного общества, для которого характерны явления «цифровизации» (в узком смысле), «датификации», и «генеративности» [1, с. 144]. В рамках настоящей статьи, согласно доктринальным подходам, под цифровизацией понимается перевод аналоговых технологических процессов в цифровой вид по модели двоичного кода «1», «0». Под датификацией — перевод информации в цифровой формат и её преобразование в система-

тизированные совокупности данных — базы данных. Под генеративностью — применение технологий с целью интерпретации и создания мультимодальных данных на уровне, сопоставимом с результатами интеллектуальной деятельности человека или превосходящем их [8, с. 6]. Указанные явления во взаимосвязи расширяют потенциал реализации субъектами права на доступ к информации, но вместе с тем порождают вопросы

- (1) о достоверности информации и
- (2) о квалификации источника информации получателем информации как субъекта права, в то время как

¹ Исследование выполнено за счет гранта Российского научного фонда № 25-18-00698, URL: <https://rscf.ru/project/25-18-00698/>

² **Герашенко Алёна Игоревна**, преподаватель департамента права цифровых технологий и биоправа НИУ ВШЭ, комплаенс-менеджер департамента информационной безопасности АО «Т-банк», г. Москва, Российская Федерация.
E-mail: agerashchenko@hse.ru

³ **Беда Александр Артёмович**, студент 4 курса факультета права НИУ ВШЭ, г. Москва, Российская Федерация.
E-mail: abeda@edu.hse.ru

источником информации выступает автоматизированная информационная технология.

При этом второй вопрос затрагивает не только аспекты правового регулирования создания и предоставления информации, но также аспекты искусственной этики, которая на текущий момент находится в стадии становления [1, с. 9].

Указанные выше вопросы связаны с применением технологий искусственного интеллекта (ИИ), которые, как отмечают А.А. Карцхия и Г.И. Макаренко, «моделируют когнитивные функции человека и позволяют компьютерам и машинам выполнять такие задачи, как <...> принятие решений, понимание и воспроизведение естественного языка» [10, с. 4]. Настоящее исследование посвящено проблемам реализации права на доступ к информации в условиях внедрения технологий ИИ в государственные и частные чат-боты.

Право на доступ к информации в Российской Федерации и за рубежом

Право на доступ к информации нашло свое закрепление в нормативных правовых актах разного уровня — от Всеобщей декларации прав человека, принятой Генеральной Ассамблеей ООН 10 декабря 1948 г., и Международного пакта о гражданских и политических правах, принятого резолюцией Генеральной Ассамблеи 16 декабря 1966 года, до национальных законодательств стран — участниц Организации Объединенных Наций. Исследователь Н. Канакши из Индии пишет, что тот факт, что 132 государства декларировали данное право, подтверждает его международное, глобальное признание [24, с. 1718].

В Российской Федерации право на доступ к информации было закреплено в ст. 29 Конституции РФ и ст. 8 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — ФЗ об информации). Ст. 8 ФЗ об информации неоднократно оценивалась на соответствие Конституции РФ Конституционным Судом РФ⁴. В ФРГ в ст. 5 Основного закона ФРГ закреплена свобода выражения мнений и свободный

доступ к информации⁵. Общий регламент ЕС по защите данных (GDPR⁶) и Федеральный закон о защите данных (Bundesdatenschutzgesetz, BDSG⁷) регулируют доступ к персональным данным и к информации об обработке персональных данных. В Конституции Индии закреплена свобода слова и выражения мнения (ст. 19(1)(a)), наряду с правом свободных невооруженных собраний (ст. 19(1)(b)), правом объединений (ст. 19(1)(c)) и правом на свободное передвижений по территории Индии (ст. 19(1)(d)⁸). Верховный суд Индии неоднократно признавал, что данная статья воплощает фундаментальное право на доступ к информации (и на распространение информации)⁹. С целью кодификации и защиты этого права парламент Индии принял Закон о праве на информацию 2005 года¹⁰. В ряде других государств есть отдельные права на доступ к информации и доступе к информации о деятельности органов власти¹¹.

Так, право на доступ к информации может пониматься в широком смысле, как «возможность получения информации и ее использования»¹² вне зависимости от источника и характера такой информации, и в узком смысле, как возможность получения информации о деятельности исключительно органов власти. В рамках настоящей статьи право на доступ к информации рассматривается в широком смысле согласно ч. 1 ст. 8 ФЗ об информации, в соответствии с которой граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных ФЗ об информации и иными федеральными законами Российской Федерации.

⁵ Grundgesetz für die Bundesrepublik Deutschland. URL: <https://www.gesetze-im-internet.de/gg/BJNR000010949.html> (дата обращения: 03.06.2025).

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата обращения: 03.06.2025).

⁷ Федеральный закон Германии о защите данных (Bundesdatenschutzgesetz, BDSG): в ред. от 20 ноября 2019 г. // Gesetze im Internet. URL: https://www.gesetze-im-internet.de/englisch_bdsdg/ (дата обращения: 03.06.2025).

⁸ Конституция Индии, принята 26 ноября 1949 г. // Government of India. Ministry of Law and Justice. URL: <https://legislative.gov.in/constitution-of-india> (дата обращения: 03.06.2025).

⁹ Secretary, Ministry of Information & Broadcasting, Government of India v. Cricket Association of Bengal, 1995 AIR 1236, 1995 SCC (2) 161 (Supreme Court of India) // Indian Kanoon. URL: <https://indiankanoon.org/doc/539407/> (дата обращения: 04.06.2025).

¹⁰ Right to Information Act, 2005 // RTI Portal, Government of India. URL: <https://legalaffairs.gov.in/sites/default/files/rti-act-2005.pdf> (дата обращения: 04.06.2025).

¹¹ Freedom of Information Act (FOIA), 1966 (Закон о свободе информации, 1966 г., США) // U.S. Department of Justice. URL: <https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf> (дата обращения: 04.06.2025).

¹² Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

⁴ См. например: определение Конституционного Суда РФ от 26.11.2018 № 3087-О «Об отказе в принятии к рассмотрению жалобы гражданина К. на нарушение его конституционных прав пунктом 1 статьи 3 и частью 1 статьи 8 Федерального закона «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс» (дата обращения: 03.06.2025); определение Конституционного Суда РФ от 23.06.2016 № 1230-О «Об отказе в принятии к рассмотрению жалобы гражданина Чернякова Василия Петровича на нарушение его конституционных прав частью 3 статьи 8 и пунктом 4 части 1 статьи 10 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации», частью 1 статьи 8 Федерального закона «Об информации, информационных технологиях и о защите информации», а также пунктом 1 статьи 1 Закона Российской Федерации «О защите прав потребителей» // СПС «КонсультантПлюс» (дата обращения: 03.06.2025).

Особенности развития права на доступ к информации в условиях эпохи цифровизации

В эпоху цифровизации право на доступ к информации как базовое право отрасли информационного права активно развивается и зачастую нарушается. Это происходит

во-первых, вследствие увеличения источников информации: информационных технологий, информационных систем и обладателей информации;

во-вторых, из-за неправомерных действий обладателей информации, связанных как с обработкой такой информации, так и с использованием информационных технологий и информационных систем; и

в-третьих, по причине отставания правового регулирования новых информационных технологий от развития таких технологий.

Одной из наиболее масштабируемых информационных технологий сегодня является технология искусственного интеллекта. Субъекты — физические и юридические лица, использующие данную технологию — находятся только в процессе познания её особенностей, что приводит к частым нарушениям обработки информации, в т.ч. ограниченного доступа, при тестировании и развитии ИИ, а также при использовании ИИ для цели предоставления информации.

Основы правового регулирования ИИ закладываются в Указе Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждена национальная стратегия развития ИИ на период до 2030 г.¹³ (далее — Национальная стратегия развития искусственного интеллекта на период до 2030 года), а также законодательством об экспериментальном правовом режиме (прекращает действие в июле 2025 года)¹⁴. В 2024 году был разработан также ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022) «Национальный стандарт Российской Федерации. Искусственный интеллект. Концепции и терминология искусственного интеллекта»¹⁵, который может быть применим разработчиками технологий ИИ на добровольной основе или императивной, если это предписано федеральным законодательством.

¹³ Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства РФ, 14.10.2019, № 41, ст. 5700.

¹⁴ Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ, 27.04.2020, № 17, ст. 2701.

¹⁵ ГОСТ Р 71476-2024 (ИСО/МЭК 22989:2022). Национальный стандарт Российской Федерации. Искусственный интеллект. Концепции и терминология искусственного интеллекта (утв. и введен в действие Приказом Росстандарта от 28.10.2024 № 1550-ст.) // М.: ФГБУ «Институт стандартизации», 2024.

Упомянутые источники регулирования в совокупности с рядом рекомендательных актов формируют отечественную правовую модель регулирования ИИ [9, с. 8—9]. Заложенные основы должны учитываться при регулировании правоотношений в различных отраслях права с учетом специального законодательства данной отрасли.

Использование ИИ в предоставлении информации

Трансформация общества приводит к созданию новых информационных технологий, которые, в свою очередь, способствуют возникновению новых рисков и вопросов к сущностному содержанию данного права. Генеративные модели ИИ, способные предоставлять информацию на основе запросов [9, с. 6], становятся «посредником» в процессе предоставления информации одним субъектом права, предоставляющим информацию, другому субъекту права, получающему информацию.

Для определения возникающих рисков и разработки путей их решения необходимо для начала очертить рамки исследуемых технологий. Современное общество информации и знаний все больше отдает предпочтение системам «управления информацией», которые включают в себя совершенно разные технологии: большие данные (big data), технологии ИИ, машинное обучение, способы упрощения и удешевления обработки информации и работы технологий ИИ, такие как «промт тюнинг» (prompt tuning) или LoRA (адаптация низкого ранга), и многие другие [20, с. 173, 177—178]. Юридическая классификация технологий представлена в пп. «б» п. 5 Национальной стратегии развития искусственного интеллекта на период до 2030 года, в соответствии с которой к технологиям ИИ относятся: компьютерное зрение, обработка естественного языка, распознавание и синтез речи, интеллектуальная поддержка принятия решений, перспективные методы искусственного интеллекта.

Многие применимые технологии можно разделить на (1) используемые при организации внутренней работы и (2) для внешних взаимодействий. К первым относятся такие технологии, как машинное обучение и нейронные сети, необходимые для оптимизации работы компаний, например, в процессах сбора, хранения и обработки информации. Они используются для принятия управленческих решений и координации работы при разработке сложных проектов [10, с. 75—76]. В рамках использования ИИ во внутренних (корпоративных) отношениях выделяются такие риски, как информационная безопасность системы, изменение структуры подотчетности, распределение ответственности за решения принятые ИИ или с помощью анализа больших данных и др. [5, с. 183—184].

Текущее исследование сосредоточено на использовании информационных технологий во внешних взаимодействиях. В качестве внешних взаимодействий можно считать

(1) отношения, которые возникают у юридических лиц с третьими лицами [15],

(2) отношения публичных органов власти с физическими и юридическими лицами (противопоставляются отношениям внутри органа или между госорганами) и

(3) отношения физических лиц с третьими лицами.

В качестве применимых во внешних отношениях технологий выделяют ИИ, машинное обучение и глубокое обучение¹⁶.

ИИ — статистическая технология, которая позволяет имитировать процесс мышления человека для решения разноплановых задач. Её примером можно считать большие языковые модели (LLM) — технологию ИИ, используемую для восприятия человеческого языка и предоставления ответов в форме, которую может понять человек.

Машинное обучение (ML) и глубокое обучение (DL) — это методы совершенствования работы моделей ИИ, которые позволяют обучить ИИ выполнять разноплановые задачи на основе предоставленных данных [23, с. 685—695].

Обе технологии применяются для оптимизации человеческой деятельности (представителя юридического лица, государственного органа) в общении с третьими лицами. В процессе такого общения технология самообучается и/или собирает статистические данные о собеседнике и его запросах, которые в дальнейшем могут быть применимы для составления статистики и определения таких показателей, как целевая аудитория, часто задаваемые вопросы и т. д.

Использование подобных технологий связано с рядом рисков, в том числе в сфере информационных правоотношений. Так, обращающееся лицо может воспринимать общение с LLM как взаимодействие с представителем компании или государственного органа, следовательно, опираться на её ответы при принятии юридически значимых решений, вроде купли товара или услуги или сбора перечня документов, необходимых для получения государственной услуги. Современные LLM могут предоставлять неправильные ответы, что может быть связано как с общей особенностью технологии — галлюцинации LLM [28, с. 3—4], так и с неясно сформулированным запросом (промптом) [26].

Остается не разрешенной и проблема ответственности за ответ, полученный от LLM. Как поступить добросовестному обращающемуся, который опирался на ответ, но при этом был введен в заблуждение относительно качества товара или ему было отказано в предоставлении государственной услуги, по причине недостаточности пакета документов?

Данный риск связан со (1) сбором информации об обращающемся и (2) его запросом. С одной стороны, данная информация необходима для дальнейшего

совершенствования работы LLM посредством машинного и глубокого обучения. С другой стороны, использование технологий DL позволяет раскрывать новые грани субъекта персональных данных, т. е. определять его [7], путем сопоставления в т.ч. обезличенных данных.

Исходя из всех высказанных опасений, возникает также вопрос, может ли обращающийся посредством реализации права на доступ к информации выбрать, с кем ему общаться: с технологией или представителем-человеком. При ответе на данный вопрос необходимо учитывать баланс прав и интересов как обращающегося, так и лица, использующего технологию ИИ при осуществлении своей профессиональной деятельности или деятельности государственного служащего.

ИИ как инструмент стороны информационных правоотношений

Современная юридическая наука не признает в моделях и системах ИИ субъекта права и правоотношений, т. к. данные информационные технологии не наделены признаками правосубъектности (правоспособность, дееспособность и деликтоспособность) [9, с. 87—92]. Однако нынешний пользовательский опыт складывается таким образом, что среднестатистическому человеку не всегда понятно, кто является его собеседником: человек или модель ИИ (чат-бот или «цифровой помощник», основанные на данной технологии) [24, с. 8]. «Запутанность» связана с существом новой технологии, которая отражена в Национальной стратегии развития искусственного интеллекта на период до 2030 года. Согласно Стратегии, под искусственным интеллектом понимается «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их».

Рассмотрим следующую ситуацию: физическое лицо обращается в компанию или к публичному субъекту через сайт в сети Интернет для получения информации. Перед тем как переключиться на сотрудника компании или служащего органа, лицу предлагается адресовать свой вопрос «цифровому помощнику».

В одном случае система может предложить пользователю выбрать из списка часто задаваемых вопросов интересующий его вопрос и дать ответ по заранее подготовленному шаблону; иллюстрирующий пример — робот Максим¹⁷, «цифровой помощник» на Едином портале государственных услуг (далее — Госуслуги). Однако в таком случае с наибольшей долей вероятности мы не можем говорить о применении технологий ИИ в режиме реального времени.

¹⁶ AI vs. machine learning vs. deep learning vs. neural networks: What's the difference? // IBM. URL: <https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks> (дата обращения: 27.05.2025).

¹⁷ Робот Максим // Официальный сайт Единого портала государственных услуг. URL: <https://www.gosuslugi.ru/newsearch> (дата обращения: 28.05.2025).

Иной случай, когда у обращающегося субъекта есть возможность задать произвольный вопрос (сформулированный самостоятельно) и получить ответ, подготовленный «цифровым помощником». Примером такой технологии является чат-бот с «цифровым помощником» Миа18 от ООО «Т2 Мобайл».

На данном этапе необходимо определиться, что из себя представляет сущность «цифрового помощника». Легального закрепления понятий «цифровой помощник», «ИИ-ассистент» или «чат-бот» в отечественном законодательстве нет (далее данные понятия будут рассматриваться как синонимичные). В доктрине предлагается следующее определение: чат-бот — это компьютерная программа, которая ведет разговор с помощью слуховых или текстовых методов. Чат-боты, или виртуальные собеседники, используются в диалоговых системах для различных практических целей, включая обслуживание клиентов или сбор информации [17, с. 72].

Зарубежная научная литература предлагает следующее определение: ИИ-ассистент — искусственный агент с интерфейсом на естественном языке, функцией которого является планирование и выполнение последовательностей действий от имени пользователя в одной или нескольких областях и в соответствии с ожиданиями пользователя [22].

Понятие «чат-бот», изначально предложенное М.Л. Молдином¹⁹, на данный момент раскрывается следующим образом: компьютерная программа, которое посредством ИИ общается с пользователем с помощью текстовых или звуковых методов. Чат-бот может анализировать вопросы пользователей, оформлять ответы на основе изученных баз данных, а также вести беседу с пользователем, имитируя человеческое общение [27, с. 1—6].

Следовательно, в предложенном нами случае можно говорить о технологии LLM, особенности работы которой заключаются в статистическом прогнозировании ответа исходя из ранее полученного в процессе обучения опыта. При этом LLM могут быть как универсальными, т. е. выполнять широкий спектр задач от ответа на вопросы до перевода текста и формирования резюме, так и специализированными, например, отвечать на вопросы по конкретно определенной теме.

Основываясь на предложенных определениях и исходя из пп. 2 ст. 2 ФЗ об информации, чат-бот можно квалифицировать в качестве информационной технологии, т. е. как метод поиска, сбора, хранения, обработки, предоставления, распространения информации, а его функции — предоставление или распространение информации в смысле п. 8 и 9 ст. 2 ФЗ об информации. Критерием разграничения данных информационных действий является круг лиц, которые получают инфор-

мацию: соответственно определенный при предоставлении и неопределенный при распространении [19]. Однако при использовании чат-бота в сети Интернет функции сложно разграничить, т. к. обращаться может как идентифицированный, так и анонимный пользователь (т. е. пользователь вне авторизованной зоны). В данном случае можно воспользоваться решением, предложенным А.И. Савельевым: если пользователь анонимный или зарегистрированный, но регистрация доступна неограниченному кругу лиц, то можно говорить о распространении информации. В тех случаях, когда регистрация предоставляется ограниченному кругу лиц, например клиентам банка в мобильном приложении (в авторизованной зоне), то чат-бот осуществляет предоставление информации²⁰.

К вопросу о наделении «цифрового помощника» статусом «обладателя информации»

При анализе функций, выполняемых чат-ботом и имитирующих мышление и коммуникативную деятельность человека, возникает вопрос: возможно ли наделение статусом «обладателя информации» по смыслу ст. 6 ФЗ об информации? Ответ на этот вопрос скорее отрицательный. Согласно разъяснениям Конституционного Суда Российской Федерации (далее — КС РФ), данным в постановлении КС РФ от 26.10.2017 № 25-П²¹, данное понятие раскрывает правовой статус лица, правомочного в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами. Факт возможности предоставления доступа к информации не означает приобретение статуса обладателя информации. Так, КС РФ разъяснил, что доступ к информации со стороны правообладателя информационной системы не означает, что он может реализовывать правомочия, доступные обладателю информации, при этом наделение субъекта правами и обязанностями, вытекающими из статуса обладателя информации, должно определяться из существа правоотношений [8].

Технология чат-ботов подразумевает обучение на основе баз данных и предоставление или распространение информации, содержащейся в векторных базах данных. При этом права и обязанности правообладателя шире описанных действий. «Цифровой помощник» не может отказать в предоставлении информации и делегировать её распространение. Его функционал ограничивается предоставлением или распространением информации и сбором данных

²⁰ Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный). М.: Статут, 2015.

²¹ Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // СПС «КонсультантПлюс» (дата обращения: 03.06.2025).

¹⁸ Чат. Официальное приложение t2. Новый уровень от ООО «Т2 Мобайл» (дата обращения: 28.05.2025).

¹⁹ Mauldin M. L. Chatterbots, tinymuds, and the turing test: Entering the Loebner prize competition // AAAI. 1994. Т. 94. С. 16—21.

об обращающемся (не только о его личности, но и о характере вопроса, удовлетворенности ответом и другой информации, которая в последующем позволит или собрать статистические данные, или улучшить технологию посредством машинного и глубокого обучения).

К вопросу о наделении «цифрового помощника» статусом «представителя»

Можно ли наделить чат-бот статусом представителя согласно абз. 2 п. 1 ст. 182 Гражданского кодекса Российской Федерации²² (далее — ГК РФ)? При анализе применения норм о представительстве в цифровой среде ученые исходят из классических условий для наличия представительства из обстановки [11], а именно из совокупности:

- 1) поведения представляемого;
- 2) поведения представителя;
- 3) добросовестных ожиданий третьего лица²³.

Анализ наличия данных условий в рассматриваемом примере приводит нас к следующим выводам. В процессе взаимодействия с чат-ботом можно видеть наличие как минимум двух условий: действия представляемого явно свидетельствуют о том, что он доверил чат-боту предоставление информации, и третье лицо добросовестно может ожидать предоставления интересующей его информации от «цифрового помощника». При этом второе условие — поведение представляемого — является не соблюденным в силу того факта, что третье лицо оценивает поведение представителя исходя из его волеизъявлений (волеизъявление о том, что сделка заключается не от имени представителя, а от имени представляемого)²⁴. Современные LLM и чат-боты, которые их используют, не способны к разумной деятельности и формированию собственных волеизъявлений. Выдаваемые ответы, хоть и не шаблонны и могут имитировать человеческую речь, являются результатом деятельности человека по программированию технологии и следствием вычислительной деятельности программного обеспечения [6, с. 27—31].

Таким образом, «цифровой помощник» или чат-бот представляет собой информационную технологию, осуществляющую функции предоставления или распространения информации по запросу пользователя. На современном этапе в наделении субъектным статусом «представителя» данной технологии должно быть отказано в силу уровня ее развития.

Способ преодоления риска восприятия чат-бота как живого человека

Способ преодоления риска восприятия чат-бота как живого человека должен быть построен на принципе транспарентности. Владельцу «цифрового помощника» необходимо предусмотреть информирование обращающегося о том, что он общается не с человеком, а с технологией LLM, и что предоставляемые ему ответы являются результатом её работы. Простота реализации данного способа может позволить без значительных последствий для оборота предусмотреть возможность для дальнейшего внедрения в российское законодательство обязанности владельцев «цифровых помощников» информировать обращающихся посредством использования дисклеймера и (или) иного визуального, текстуального или аудиального способа. Данное информирование может быть подобно уже существующей в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» обязанности оператора персональных данных информировать субъекта персональных данных о том, как и для каких целей обрабатываются его персональные данные (посредством публикации политики обработки персональных данных, сбора согласий на обработку персональных данных)²⁵.

Достоверность информации, предоставляемой чат-ботом

Для урегулирования данного риска необходимо определиться с понятием «достоверность». Несмотря на распространенное употребление принципа или требования достоверности в отечественном законодательстве, конкретного определения или критериев, которые говорят об отнесении информации к достоверной, нет [13, с. 207—210].

Так, исследователи принципа достоверности в информационном праве обращаются к толкованию слова «достоверность», данному в толковых словарях, используют требования, которые содержатся в федеральных законах, подзаконных актах и других источниках [14, с. 46—50].

Некоторые доктриналоги исходят из принципа, что «достоверность информации исходит из ее проверяемости», т. е. предоставляемая информация должна проверяться пользователями перед тем, как будет воспринята и использована²⁶. Однако использование такого подхода обременительно для обращающегося, что в конечном счете может привести к полному отказу от использования чат-ботов. Такое событие вызовет не-

²² Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ, 05.12.1994, № 32, ст. 3301.

²³ Егоров А.В., Папченкова Е.А., Ширвиндт А.М. Представительство: исследование судебной практики. М.: Статут, 2016. С. 62.

²⁴ Егоров А.В., Папченкова Е.А., Ширвиндт А.М. Указ. соч. С. 64.

²⁵ Ст. 9, 18, 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3451.

²⁶ См., например: Fallis D. On verifying the accuracy of information: Philosophical perspectives. 2004.

гативные последствия для рынка, который уже сейчас активно использует технологию в различных сферах²⁷.

Достоверность — одно из ключевых требований к информации в современном обществе, что связано с постоянным потоком информации («информационным шумом»). Обеспечение достоверности сочетается с такими критериями, как своевременность, использование информации из официальных источников и соблюдение прав и свобод человека и гражданина [17].

К информации, которая предоставляется или распространяется, может быть предъявлено несколько требований режима достоверности: соблюдение или обязанности достоверности, или принципа достоверности [18, с. 49—50]. Обязанность достоверности является более узкой по сравнению с принципом достоверности. Первая следует из указания закона к определенным субъектам обеспечивать достоверность информации, второй представляет собой общий принцип информационного права.

Согласно ч. 9 ст. 14 ФЗ об информации, специализированные государственные органы обязаны обеспечить достоверность информации, содержащейся в государственных информационных системах. Обязанность обеспечения достоверности содержится в ч. 11 ст. 18.1 Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе»²⁸ и накладывается на оператора рекламных данных, рекламодателя и иных указанных в законе лиц. Согласно п. 1 ст. 10 Закона РФ от 07.02.1992 № 2300-1 «О защите прав потребителей»²⁹ (далее — ЗоЗПП) изготовитель (исполнитель, продавец) обязан обеспечить достоверную информацию о товарах (работах, услугах), обеспечивающую возможность их правильного выбора.

На владельце «цифрового помощника» лежит обязанность обеспечить предоставление или распространение достоверной информации посредством данной технологии в случае указания закона о соблюдении обязанности достоверности самим владельцем технологии. Например, продавец обязан обеспечить предоставление достоверной информации «цифровым помощником» о продаваемом товаре. В иных случаях предоставляемая или распространяемая чат-ботами информация должна соответствовать принципу достоверности. Так, если пользователь задает вопрос об истории компании, то продавец должен обеспечить соблюдение принципа достоверности при ответе «цифрового помощника».

Так как в основе LLM лежит обучение, то владельцу чат-бота следует своевременно проводить обновление своей модели, чтобы его «цифровой помощник» предоставлял достоверную информацию. Современные тех-

нологии способствуют удешевлению этих процессов посредством новых методов, таких как prompt tuning или LoRA, т. к. при их использовании не требуется полное переобучение модели.

Представляется верным закрепить презумпцию достоверности информации, которая предоставляется обращающемуся лицу чат-ботом. Данная презумпция подразумевает, что добросовестное третье лицо будет защищено, если оно при формировании своего поведения опиралось на информацию, полученную от «цифрового помощника». При этом такие пользователи должны квалифицироваться как слабая сторона возникающих правоотношений [3, с. 93].

Ответственность за информацию, предоставленную «цифровым помощником»

Разграничение обязанности достоверности и ответственности принципу достоверности имеет значение для определения правовых последствий для лица, которое их нарушает. Так, несоблюдение обязанности достоверности является прямым нарушением указания закона и должно влечь наступление ответственности, которая предусмотрена данным законом. Например, в силу п. 2 ст. 12 ЗоЗПП продавец (исполнитель), чат-бот которого не предоставил покупателю полную и достоверную информацию о товаре (работе, услуге), несет ответственность, предусмотренную данным законом, за недостатки товара (работы, услуги), возникшие после его передачи потребителю вследствие отсутствия у него такой информации.

В случае отхода от принципа достоверности следует говорить о нарушении именно принципа информационного права, что ведет к различным правовым последствиям, первостепенным из которых является ограничение распространения такой информации. В случае наступления убытков или реальной общественной опасности должны применяться соответствующие нормы гражданского или уголовного законодательства [4, с. 12—13]. В примере с продавцом, если информация об истории компании в ответе чат-бота нарушает принцип достоверности, то она надлежит удалению (если, например, она сохраняется в разделе «Часто задаваемые вопросы цифровому помощнику»), также видится верным направление регулятором предписания владельцу технологии о корректировке работы чат-бота. Схожий порядок взаимодействия владельцев чат-ботов, пользователей и регулятора содержится в AI Act³⁰.

Так как LLM проходят обучение на данных, которые предоставляются компанией или публичным образованием, то за все последствия недостатков их обучения и за информацию, которая предоставляется,

²⁷ См. подробнее: Исследование чат-ботов. Naumen, 2024. URL: <https://naumenresearch.ru/retail-chat-bots-2024/> (дата обращения: 28.05.2025).

²⁸ Федеральный Закон от 13.03.2006 № 38-ФЗ «О рекламе» // Собрание законодательства РФ, 20.03.2006, № 12, ст. 1232.

²⁹ Закон РФ от 07.02.1992 № 2300-1 «О защите прав потребителей» // Российская газета, № 8, 16.01.1996.

³⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 // Официальный сайт EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689> (дата обращения: 29.05.2025).

должно нести лицо, имеющее контроль над данной технологией и владеющее базами данных, используемых LLM.

Возможность выбора общения с «цифровым помощником», функционирующим на базе ИИ, или с человеком

Исходя из определения права на доступ к информации физические и юридические лица вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований закона. При этом, как было отмечено ранее, на некоторых субъектах лежит обязанность предоставления информации, в том числе достоверной информации. В частности, это государственные органы и исполнители (в трактовке ЗоЗПП). Однако применение технологии чат-ботов происходит, в том числе, и такими лицами.

Для начала следует разграничить субъектов, к которым может быть обращен запрос через чат-бот, на государственные (муниципальные) и частные субъекты, по причине различного законодательного регулирования.

Цифровой помощник органа власти

В отношении предоставления информации государственными (муниципальными) органами действует специальный Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»³¹ (далее — ФЗ об обращениях граждан). Согласно его положениям, пользователь информации может направить обращение в государственные органы и получить ответ или мотивированный отказ в ответе. Начиная с прошлого десятилетия, обращение граждан в государственные органы происходит через сеть Интернет, в том числе посредством направления электронных обращений [8]. Возможность направления электронных обращений предусмотрена п. 1 ст. 4 и ч. 3 ст. 7 ФЗ об обращениях граждан.

К обращениям граждан, в том числе в электронном формате, предъявляются обязательные требования, которые включают в себя указание фамилии, имени и отчества, а также электронной почты или адреса личного кабинета на портале Госуслуг (далее — ЛК Госуслуг). Исходя из указанных требований, квалифицировать вопрос, который задает обращающийся к «цифровому помощнику», как обращение видится невозможным, если он задается без регистрации, т. е. за пределами авторизованной зоны. Если же регистрация, которая подразумевает указание ФИО и адреса электронной почты/ЛК Госуслуг, была произведена, то можно говорить о соблюдении формальных критериев и квалифи-

кации такого вопроса как обращения. При этом должен соблюдаться еще один критерий — регистрация обращения.

Законодательство также содержит требования к ответу государственного органа: сущностные требования (объективное, всестороннее и своевременное рассмотрение) и формальные (подпись должностного лица). Стандартный ответ, который предоставляет чат-бот, не соответствует данным требованиям, если он не подписывается должностным лицом или руководителем органа.

Соблюдение сущностного критерия также ставится под вопрос, т. к. всестороннее рассмотрение зависит от уровня развития LLM, используемой в «цифровом помощнике», а объективность ответов чат-ботов ставится специалистами по этике в текущих реалиях под сомнение и является высокорискованным фактором [30] (например, AI Act относит системы ИИ, которые используются для оценки возможности предоставления услуг тем или иным лицам, к высокорискованным системам ИИ).

Так как ответ «цифрового помощника» является результатом поиска, обработки, анализа, представления информации из общедоступных баз данных государственных органов, то видится возможным применить регулирование, аналогичное применяемому к таким базам данных. Согласно постановлению Правительства РФ от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» в форме открытых данных»³², часть информации о деятельности государственных органов является обязательно общедоступной и определяется перечнями общедоступной информации. Иная информация, не вошедшая в перечни, является общедоступной по указанию закона, решению самого органа, органа, обеспечивающего эксплуатацию (ведение) государственной информационной системы с учетом методических указаний Министерства экономического развития Российской Федерации по согласованию с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Федеральной службой безопасности Российской Федерации.

Исходя из вышесказанного, ответы «государственных» чат-ботов можно квалифицировать как общедоступную информацию. К таким технологиям должно применяться общее регулирование из ст. 7 ФЗ об информации и специальное регулирование информации, предоставляемой государственными органами, из ч. 2—9 ст. 8 ФЗ об информации.

³¹ Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // Парламентская газета, № 70-71, 11.05.2006.

³² Постановление Правительства РФ от 10.07.2013 № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» // Собрание законодательства РФ, 29.07.2013, № 30 (часть II), ст. 4107.

Отдельно стоит остановиться на предоставлении услуг посредством «цифровых помощников». Данные правоотношения регулируются Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»³³ (далее — ФЗ о государственных услугах). Основываясь на принципах предоставления государственных и муниципальных услуг, правах заявителей и обязанностях представителей услуг, государственные услуги должны предоставляться в электронном и иных форматах по выбору заявителя, кроме случаев, предусмотренных законом (услуги предоставляются только в электронном формате) — ч. 6 ст. 4, п. 3 ч. 1 ст. 5 и п. 2 ч. 1 ст. 3 ФЗ о государственных услугах. Законодатель исходит из возможности выбора заявителями формы получения государственных услуг. Предоставление услуг посредством чат-ботов должно рассматриваться как самостоятельный формат предоставления услуги, т. к. такое представление не является в полной мере предоставлением услуги в электронном формате, исходя из сущности данных правоотношений. Поэтому у заявителей при обращении должна быть возможность выбора формы получения услуги: в электронном формате, в письменной форме, посредством личного или коллективного обращения, посредством чат-бота или в иной форме.

Как справедливо отмечается в доктрине, новые редакции ФЗ о государственных услугах изменили возможность выбора формы предоставления услуг, поставив в приоритет получение услуг в электронном формате [16, 20]. Но т. к. предоставление услуг в электронной форме и посредством «цифрового помощника» выступают как самостоятельные формы, данные изменения не должны повлиять на возможность заявителей выбрать альтернативную чат-боту форму получения государственной услуги.

Таким образом, отношения между обращающимися и «государственным» чат-ботами по общему правилу должны регулироваться нормами информационного права об общедоступной информации и информации, предоставляемой государственными органами. Для реализации прав граждан на обращение к государственным органам им в обязательном порядке должна предоставляться возможность оформления обращения по правилам ФЗ об обращениях граждан и иных норм законодательства, т. е. в обход чат-бота и посредством иных форм обращения. Аналогичное регулирование касается предоставления услуг посредством «цифровых помощников». Правоотношения между обращающимися и «государственными» «цифровыми помощниками» должны строиться на принципе свободы выбора формы обращения.

«Цифровой помощник» юридического лица

Возвращаясь к вопросу возможности выбрать источник получения информации при взаимодействии с чат-ботами частных субъектов, следует отметить, что информация может выступать объектом публичных, гражданских и иных правоотношений, согласно ч. 1 ст. 5 ФЗ об информации. Не уделяя много внимания научной дискуссии о возможности квалификации информации как объекта гражданских правоотношений при отсутствии ее в ст. 128 ГК РФ, отметим, что значительная часть отечественных правоведов выступают за наделение ее таким свойством [9, с. 30—40].

При этом обладатель информации, коим в нашем примере является владелец чат-бота, волен самостоятельно определять порядок предоставления и распространения информации. Являясь предпринимателем, владелец чат-бота также вправе самостоятельно решать способ ведения предпринимательской деятельности (ч. 1 ст. 34, ч. 1 ст. 8 Конституции РФ и п. 1 ст. 1 ГК РФ), следовательно, он может самостоятельно определить режим общения с контрагентами при условии соблюдения прав и свобод граждан, требований и ограничений национального законодательства.

Как отмечается в Информации КС РФ о защите предпринимательства: «экономическая свобода реализуется в границах, которые установлены законом, при этом что за предпринимателями всегда остается выбор юридических условий и принятие объективных рисков, связанных с конкретной хозяйственной деятельностью... Оправданность публичного вмешательства в осуществление предпринимательской деятельности обусловлена задачей поддержания баланса между конституционными ценностями, затрагиваемыми в рамках соответствующих правоотношений, пределы же такого вмешательства определяются принципом соразмерности (пропорциональности)»³⁴. Исходя из вышесказанного, предприниматель вправе установить возможность общения контрагентов только с цифровыми помощниками, однако в тех случаях, когда обращение касается прав и интересов обращающихся, им должна предоставляться возможность задать вопрос непосредственно владельцу чат-бота или его полномочному представителю. Т. к. для полной реализации права на получение информации (например, информации о товаре) обращающему может потребоваться задать ряд дополнительных вопросов, т. е. получить полную и достоверную информацию.

Следует также отметить, что в тех случаях, когда закон предписывает владельцу чат-бота обязанность предоставить информацию, при этом указывая форму предоставления информации, очевидно, что пре-

³³ Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Собрание законодательства РФ, 02.08.2010, № 31, ст. 4179.

³⁴ Информация «Конституционно-правовая защита предпринимательства: актуальные аспекты (на основе решений Конституционного Суда Российской Федерации 2018—2020 годов)» (одобрено решением Конституционного Суда РФ от 17.12.2020) // СПС «КонсультантПлюс» (дата обращения: 01.06.2025).

доставление информации безальтернативно только цифровым помощником является нарушением прямого указания закона. Например, если информация об организации перевозок пассажиров на внутреннем водном транспорте будет предоставляться только посредством ответа от чат-бота, то это будет нарушать п. 2 ст. 99 Кодекса внутреннего водного транспорта Российской Федерации от 07.03.2001 № 24-ФЗ³⁵, т. к. такая информация должна располагаться в местах обслуживания пассажиров, в том числе в местах продажи билетов, и должна быть представлена в наглядной и доступной форме.

Заключение

Активное внедрение технологий ИИ в информационные технологии по типу «чат-бот» или «цифровой помощник» не позволяет квалифицировать технологию ИИ ни как обладателя информации по смыслу ФЗ об информации, ни как представителя по смыслу ГК РФ. В текущих реалиях развития технологий ИИ ей отказывается в правосубъектности.

Ответственность за достоверность информации, генерируемой технологией ИИ и предоставляемой субъектам права, должна распределяться между обладателем информации и технологии ИИ или между обладателем информации и разработчиком технологии ИИ. Чтобы снизить вероятность совершения не-

корректных юридических действий обращающимися, получившими недостоверную информацию, ошибочно сгенерированную технологией ИИ, без ущерба для развития указанной технологии, владельцам информации и разработчикам технологии ИИ *предлагается* предоставлять обращающимся возможность выбора источника получаемой информации — или «цифрового помощника», или владельца «цифрового помощника»/его полномочного представителя.

Эта возможность должна быть реализована технологически при соблюдении презумпции достоверности информации, предоставляемой обращающемуся с помощью «цифрового помощника».

Техническая реализация данной возможности должна также сопровождаться информационным сообщением для обращающегося. Формирование требований к такому сообщению может осуществляться по аналогии с требованиями к информированию субъекта персональных данных об обработке его персональных данных. Например, в сообщении может быть отражаться информация о том,

- (1) кто является владельцем данной технологии,
- (2) какие сведения собираются с помощью данной технологии,
- (3) какие есть требования к запросам в данной технологии,
- (4) какой предусмотрен порядок обращения к владельцу «цифрового помощника»/его полномочного представителя, в случае если у обращающегося есть сомнения в достоверности информации, полученной от ИИ-технологии.

³⁵ Кодекс внутреннего водного транспорта Российской Федерации от 07.03.2001 № 24-ФЗ // Российская газета, № 50-51, 13.03.2001.

Литература

1. Батурин Ю.М. О построении стандартов искусственной этики роботов // Социология науки и технологий. 2024. № 4. С. 7—21.
2. Бухт Р., Хикс Р. Определение, концепция и измерение цифровой экономики // Вестник международных организаций. 2018. Т. 13. № 2. С. 143—172.
3. Волос А.А. Категория «слабая сторона гражданского правоотношения» в условиях цифровизации // Право. Журнал Высшей школы экономики. 2024. № 3. С. 84—105.
4. Жарова А.К. Информация, не соответствующая действительности с точки зрения различных отраслей права // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. Т. 45. № 2. С. 8—16.
5. Зуб А.Т., Петрова К.С. Искусственный интеллект в корпоративном управлении: возможности и границы применения // Государственное управление. Электронный вестник. 2022. № 94. С. 173—187.
6. Калятин В.О. Определение субъекта прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта // Право. Журнал Высшей школы экономики. 2022. № 4. С. 24—50.
7. Карасев А.Т., Кожевников О.А., Мещерягина В.А. Цифровизация правоотношений и ее влияние на реализацию отдельных конституционных прав граждан в Российской Федерации // Антиномии. 2019. № 3. С. 99—119.
8. Карлаш Д.С. Субъекты отношений по использованию больших данных в предпринимательской деятельности: понятие и правовой статус // Предпринимательское право. 2023. № 3. С. 56—62.
9. Карцхия А.А., Макаренко Г.И. Правовые проблемы применения искусственного интеллекта в России // Правовая информатика. 2024. № 1. С. 4—19.
10. Кресс В.В. Информация как объект гражданских прав // Актуальные проблемы российского права. 2024. Т. 19. № 5. С. 30—40.
11. Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79—102.
12. Мейрияни М., Деи Леонарда В., Видхья А. Большие данные, машинное обучение, искусственный интеллект и блокчейн в корпоративном управлении // Форсайт. 2023. № 4. С. 69—78. DOI: 10.17323/2500-2597.2023.4.69.78.

13. Папченкова Е.А. Действия под чужим аккаунтом: применение норм о представительстве в сети Интернет // Закон. 2020. № 10. С. 34—49.
14. Петровская О.В. Принцип достоверности информации и его реализация в информационном обществе: теоретико-правовые проблемы // Право и государство: теория и практика. 2020. № 3 (183). С. 207—211.
15. Петровская О.В. Принципы достоверности в информационном праве в условиях цифровой трансформации // Мониторинг правоприменения. 2021. № 3 (40). С. 46—50. DOI: 10.21681/2226-0692-2021-3-46-50.
16. Современное корпоративное право: актуальные проблемы теории и практики : монография / О.А. Беляева, С.А. Бурлаков, М.М. Вильданова и др.; отв. ред. О.В. Гутников. М. : ИЗИСП : Статут, 2021. 528 с.
17. Терещенко Л.К. Реестровая модель оказания государственных и муниципальных услуг // Журнал российского права. 2021. № 7. С. 110—120.
18. Троян Н.А., Петровская О.В. Принцип достоверности при распространении и предоставлении информации с использованием искусственного интеллекта // Правовая информатика. 2023. № 2. С. 75—81. DOI: 10.21681/1994-1404-2023-2-75-81.
19. Усольцева Н.А., Усольцев Ю.М. Чат-бот как элемент правовой реальности // Юридическая наука. 2020. № 9. С. 72—75.
20. Устюжанина Е.В. Принцип достоверности информации: постановка проблемы // Электронное приложение к Российскому юридическому журналу. 2017. № 4. С. 47—52.
21. Чурилов А.Ю. Комментарий к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (постатейный). М. : Юстицинформ, 2024. 404 с.
22. Швабауэр А.В. Кардинальное изменение правил оказания госуслуг и конституционные права граждан // Государственная власть и местное самоуправление. 2021. № 10. С. 3—7.
23. Al Mansoori S., Salloum S.A., Shaalan K. The impact of artificial intelligence and information technologies on the efficiency of knowledge management at modern organizations: a systematic review. Recent advances in intelligent systems and smart applications. 2020. Pp. 163–182.
24. Gabriel I. et al. The ethics of advanced AI assistants. arXiv preprint arXiv:2404.16244. 2024. 267 pp. URL: <https://arxiv.org/pdf/2404.16244> (data obrashcheniia: 13.06.2025).
25. Janiesch C., Zschech P., Heinrich K. Machine learning and deep learning. Electronic markets. 2021. Vol. 31. Pp. 685–695.
26. Jones C.R., Bergen B.K. Large language models pass the turing test. arXiv preprint arXiv:2503.23674. 2025. 32 pp. URL: <https://arxiv.org/pdf/2503.23674> (data obrashcheniia: 13.06.2025).
27. Kanakshi N. Right To Information in the Digital Age: A Comparative Analysis. International Journal of Law Management & Humanities, Vol. 7, Iss 6. 2024. Pp. 1717–1727.
28. Salinas A., Morstatter F. The butterfly effect of altering prompts: How small changes and jailbreaks affect large language model performance. arXiv preprint arXiv:2401.03729. 2024. 24 pp. URL: <https://arxiv.org/abs/2401.03729> (data obrashcheniia: 05.06.2025).
29. Skrebeca J. et al. Modern development trends of chatbots using artificial intelligence (AI). 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE, 2021. Pp. 1–6.
30. Yao J.Y. et al. LLM lies: Hallucinations are not bugs but features as adversarial examples. arXiv preprint arXiv:2310.01469. 2023. 18 pp. URL: <https://arxiv.org/abs/2310.01469> (data obrashcheniia: 05.06.2025).

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

PROBLEMS OF EXERCISING THE RIGHT TO ACCESS TO INFORMATION IN THE CONTEXT OF DEVELOPMENT OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Alena Gerashchenko, Lecturer at the School of Digital Law and Bio-Law of the Higher School of Economics University, Compliance Manager at the Information Security Department of the AO (JSC) "T-Bank", Moscow, Russian Federation.

E-mail: agerashchenko@hse.ru

Aleksandr Beda, 4th year student at the Faculty of Law of the Higher School of Economics University, Moscow, Russian Federation.

E-mail: abeda@edu.hse.ru

Keywords: chatbot, digital assistant, information reliability, generativity, datafication, digitalisation, informing.

Abstract

Purpose of the study: identifying problems aspects of exercising the right to access to information (public and private law aspects) in the context of development of artificial intelligence (AI) technologies mimicking human cognitive functions and yielding results comparable with the results of human intellectual activity or exceeding them in performing specific tasks.

Methods used in the study: general scientific (analysis, synthesis, generalisation, comparison) and special legal methods (the formal legal, comparative legal, and casual ones).

Study findings: the authors' well-argued doctrinal stance that the right to access to information, in the context of emerging AI technologies, is actively developing and is violated. It is proposed to provide, in the right to access to information, for the right of the subject of information legal relations to choose the source of reliable information: a digital assistant based on AI models or a human owner of the required information. Under the current conditions, the legal relations between the person applying for information and government as well as private 'digital assistants' should be based on the principle of free choice of form of application.

Practical value: it is proposed to apply the presumption of reliability of information generated by 'digital assistants' when defining the subject of law applying for information as the "weaker party in legal relations". It is also proposed to implement a legal tool for informing such persons about the specific features of operation of the 'digital assistant' and to provide for a legal possibility to apply to the owner of the 'digital assistant' or his/her authorised representative if the applicant doubts the reliability of information obtained from the 'digital assistant'.

References

1. Baturin Iu.M. O postroenii standartov iskusstvennoi etiki robotov. Sotsiologiya nauki i tekhnologii. 2024. No. 4. Pp. 7–21.
2. Bukht R., Khiks R. Opredelenie, kontseptsii i izmerenie tsifrovoy ekonomiki. Vestnik mezhdunarodnykh organizatsii. 2018. T. 13. No. 2. Pp. 143–172.
3. Volos A.A. Kategorii "slabaia storona grazhdanskogo pravootnosheniia" v usloviakh tsifrovizatsii. Pravo. Zhurnal Vysshei shkoly ekonomiki. 2024. No. 3. Pp. 84–105.
4. Zharova A.K. Informatsiia, ne sootvetstvuiushchaia deistvitel'nosti s tochki zreniia razlichnykh otraslei prava. Trudy po intellektual'noi sobstvennosti (Works on Intellectual Property). 2023. T. 45. No. 2. Pp. 8–16.
5. Zub A.T., Petrova K.S. Iskusstvennyi intellekt v korporativnom upravlenii: vozmozhnosti i granitsy primeneniia. Gosudarstvennoe upravlenie. Elektronnyi vestnik. 2022. No. 94. Pp. 173–187.
6. Kaliatin V.O. Opredelenie sub'ekta prav na rezul'taty intellektual'noi deiatel'nosti, sozdannye s ispol'zovaniem iskusstvennogo intellekta. Pravo. Zhurnal Vysshei shkoly ekonomiki. 2022. No. 4. Pp. 24–50.
7. Karasev A.T., Kozhevnikov O.A., Meshcheriagina V.A. Tsifrovizatsiia pravootnoshenii i ee vliianie na realizatsiiu ot-del'nykh konstitutsionnykh prav grazhdan v Rossiiskoi Federatsii. Antinomii. 2019. No. 3. Pp. 99–119.
8. Karlash D.S. Sub'ekty otnoshenii po ispol'zovaniiu bol'shikh dannykh v predprinimatel'skoi deiatel'nosti: poniatie i pravovoi status. Predprinimatel'skoe pravo. 2023. No. 3. Pp. 56–62.
9. Kartskhiia A.A., Makarenko G.I. Pravovye problemy primeneniia iskusstvennogo intellekta v Rossii. Pravovaia informatika. 2024. No. 1. Pp. 4–19.
10. Kress V.V. Informatsiia kak ob'ekt grazhdanskikh prav. Aktual'nye problemy rossiiskogo prava. 2024. T. 19. No. 5. Pp. 30–40.
11. Laptev V.A. Poniatie iskusstvennogo intellekta i iuridicheskaya otvetstvennost' za ego rabotu. Pravo. Zhurnal Vysshei shkoly ekonomiki. 2019. No. 2. Pp. 79–102.
12. Meiriiani M., Dezi Leonarda V., Vidkh'ia A. Bol'shie dannye, mashinnoe obuchenie, iskusstvennyi intellekt i blokchein v korporativnom upravlenii. Forsait. 2023. No. 4. Pp. 69–78. DOI: 10.17323/2500-2597.2023.4.69.78.
13. Papchenkova E.A. Deistviia pod chuzhim akkauntom: primeneniie norm o predstavitel'stve v seti Internet. Zakon. 2020. No. 10. Pp. 34–49.
14. Petrovskaia O.V. Printsip dostovernosti informatsii i ego realizatsiia v informatsionnom obshchestve: teoretiko-pravovye problemy. Pravo i gosudarstvo: teoriia i praktika. 2020. No. 3 (183). Pp. 207–211.
15. Petrovskaia O.V. Printsipy dostovernosti v informatsionnom prave v usloviakh tsifrovoy transformatsii. Monitoring pravoprimeneniia. 2021. No. 3 (40). Pp. 46–50. DOI: 10.21681/2226-0692-2021-3-46-50.
16. Sovremennoe korporativnoe pravo: aktual'nye problemy teorii i praktiki : monografiia. O.A. Beliaeva, S.A. Burlakov, M.M. Vil'danova i dr.; otv. red. O.V. Gutnikov. M. : IZiSP : Statut, 2021. 528 pp.
17. Tereshchenko L.K. Reestrovaia model' okazaniia gosudarstvennykh i munitsipal'nykh uslug. Zhurnal rossiiskogo prava. 2021. No. 7. Pp. 110–120.
18. Troian N.A., Petrovskaia O.V. Printsip dostovernosti pri rasprostranenii i predostavlenii informatsii s ispol'zovaniem iskusstvennogo intellekta. Pravovaia informatika. 2023. No. 2. Pp. 75–81. DOI: 10.21681/1994-1404-2023-2-75-81.

19. Usol'tseva N.A., Usol'tsev Iu.M. Chat-bot kak element pravovoi real'nosti. Iuridicheskaya nauka. 2020. No. 9. Pp. 72–75.
20. Ustiuzhanina E.V. Printsip dostovernosti informatsii: postanovka problemy. Elektronnoe prilozhenie k Rossiiskomu iuridicheskomu zhurnalu. 2017. No. 4. Pp. 47–52.
21. Churilov A.Iu. Kommentarii k Federal'nomu zakonu ot 27.07.2006 No. 149-FZ "Ob informatsii, informatsionnykh tekhnologiiakh i o zashchite informatsii" (postateinyi). M. : Iustitsinform, 2024. 404 pp.
22. Shvabauer A.V. Kardinal'noe izmenenie pravil okazaniya gosuslug i konstitutsionnye prava grazhdan. Gosudarstvennaya vlast' i mestnoye samoupravlenie. 2021. No. 10. Pp. 3–7.
23. Al Mansoori S., Salloum S.A., Shaalan K. The impact of artificial intelligence and information technologies on the efficiency of knowledge management at modern organizations: a systematic review. Recent advances in intelligent systems and smart applications. 2020. Pp. 163–182.
24. Gabriel I. et al. The ethics of advanced AI assistants. arXiv preprint arXiv:2404.16244. 2024. 267 pp. URL: <https://arxiv.org/pdf/2404.16244> (data obrashcheniya: 13.06.2025).
25. Janiesch C., Zschech P., Heinrich K. Machine learning and deep learning. Electronic markets. 2021. Vol. 31. Pp. 685–695.
26. Jones C.R., Bergen B.K. Large language models pass the turing test. arXiv preprint arXiv:2503.23674. 2025. 32 pp. URL: <https://arxiv.org/pdf/2503.23674> (data obrashcheniya: 13.06.2025).
27. Kanakshi N. Right To Information in the Digital Age: A Comparative Analysis. International Journal of Law Management & Humanities, Vol. 7, Iss 6. 2024. Pp. 1717–1727.
28. Salinas A., Morstatter F. The butterfly effect of altering prompts: How small changes and jailbreaks affect large language model performance. arXiv preprint arXiv:2401.03729. 2024. 24 pp. URL: <https://arxiv.org/abs/2401.03729> (data obrashcheniya: 05.06.2025).
29. Skrebeca J. et al. Modern development trends of chatbots using artificial intelligence (AI). 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS). IEEE, 2021. Pp. 1–6.
30. Yao J.Y. et al. LLM lies: Hallucinations are not bugs but features as adversarial examples. arXiv preprint arXiv:2310.01469. 2023. 18 pp. URL: <https://arxiv.org/abs/2310.01469> (data obrashcheniya: 05.06.2025).

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: СИСТЕМЫ ФИЗИЧЕСКОЙ ЗАЩИТЫ, НОРМАТИВНО-ПРАВОВАЯ ОСНОВА

Муравьев А.Г.¹, Шифрин Б.М.²

Ключевые слова: физическая защита, критическая информационная инфраструктура, несанкционированный доступ.

Аннотация

Цель работы: проведение исследования современного состояния нормативно-правовой основы регулирования создания систем физической защиты (СФЗ) объектов критической информационной инфраструктуры (ОКИИ).

Методы исследования: методы анализа, сравнения, обобщения, структурной декомпозиции из теории системного анализа, анализ методов создания СФЗ в составе комплекса средств защиты информации (СЗИ) ОКИИ.

Результаты исследования: проведен анализ действующих нормативных документов, регламентирующих обеспечение безопасности ОКИИ и рассмотрены различные современные подходы по созданию СФЗ. Формирование объективных оценок позволяет понять современное состояние правовых основ, применяемых при создании (совершенствовании) СФЗ комплексных СЗИ и поставить задачи по совершенствованию нормативно-правовой базы для более эффективного решения задач по обеспечению безопасности критической информационной инфраструктуры РФ.

Практическая полезность: представлена оценка состояния современного нормативно-правового регулирования при создании СФЗ ОКИИ.

DOI: 10.24412/1994-1404-2025-2-132-139

Введение

На современном этапе ни одна компания не обходится без надёжной информационной инфраструктуры. Технологические разработки заметно влияют на производительность бизнеса, касаясь и государственных учреждений. Однако высокие достижения в технологиях привлекают не только ответственные компании. Печально, но преступные группировки и террористические организации также используют новации для реализации своих пагубных целей.

Согласно данным Positive Technologies, в первые три квартала 2019 года было зарегистрировано 167 кибернападений на государственные учреждения. Для сопоставления: в аналогичный период 2018 года их зафиксировали 133 [1].

Не следует забывать о печально известном инциденте в Иране, произошедшем в сентябре 2010 года. Кибератака StuxNet привела к выходу из строя цен-

трифуг на атомной станции [2]. Случай стал знаковым и продемонстрировал, как информационная угроза способна ставить под угрозу национальную безопасность.

В 2020 году кибератаки принесли российской экономике ущерб в 3,5 трлн рублей [3]. Ситуация ухудшилась: по итогам третьего квартала 2022 года количество DDoS-атак на отечественные компании возросло до 46 в неделю — на 46% больше по сравнению с началом года. За первую половину года злоумышленники похитили данные свыше 13 млн пластиковых карт, причинив ущерб не менее чем на 4,5 млрд рублей [4].

Темы информационной безопасности вызывают активные обсуждения в разных странах. В частности, в обновлённой Национальной стратегии кибербезопасности США 2023 года основное внимание уделено защите критически важной инфраструктуры [5]. Это яв-

¹ **Муравьев Александр Георгиевич**, аспирант кафедры автоматизации, метрологии и управления в технических системах Института технологических машин и транспорта леса Санкт-Петербургского государственного лесотехнического университета им. С.М. Кирова, г. Санкт-Петербург, Российская Федерация. ORCID: 0009-0008-4901-9112.
E-mail: muravyev_a_g@mail.ru

² **Шифрин Борис Маркович**, кандидат технических наук, доцент кафедры автоматизации, метрологии и управления в технических системах Института технологических машин и транспорта леса Санкт-Петербургского государственного лесотехнического университета им. С.М. Кирова, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0001-5377-741X.
E-mail: shifrinb@mail.ru

Annexes

Tier performance: Global

Tier 1 – Role-modelling (score of 95-100)

Australia	Ghana	Morocco	Singapore
Bahrain	Greece	Netherlands (Kingdom of the)	Slovenia
Bangladesh	Iceland	Norway	Spain
Belgium	India	Oman	Sweden
Brazil	Indonesia	Pakistan	Tanzania
Cyprus	Italy	Portugal	Thailand
Denmark	Japan	Qatar	Türkiye
Egypt	Jordan	Korea (Republic of)	United Arab Emirates
Estonia	Kenya	Rwanda	United Kingdom
Finland	Luxembourg	Saudi Arabia	United States
France	Malaysia	Serbia	Viet Nam
Germany	Mauritius		

Tier 2 – Advancing (score of 85-95)

Albania	Ecuador	Mexico	Switzerland
Austria	Georgia	Philippines	Togo
Azerbaijan	Hungary	Poland	Uruguay
Benin	Ireland	Romania	Uzbekistan
Canada	Israel	Russian Federation	Zambia
China	Kazakhstan	Slovakia	
Croatia	Lithuania	South Africa	
Czech Republic	Malta	Sri Lanka	

Рис. 1. Группы T1, T2 Глобального индекса кибербезопасности в 2024 году

ным образом подчеркивает необходимость внедрения прочной системы противодействия киберугрозам.

Согласно данным Глобального индекса кибербезопасности 2024 года, подготовленного Международным союзом электросвязи (МСЭ), Россия попадает в категорию T2 (развивающаяся) (рис. 1). Это указывает на необходимость дальнейшего повышения потенциала в киберзащите для эффективного реагирования на стремительно эволюционирующие угрозы³.

26 июля 2017 года в силу вступил Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации». Цель документа — охрана информационных систем, автоматизированных управляющих систем и телекоммуникационных сетей, относящихся к критической инфраструктуре. Закон ставит задачу обеспечить безопасность, надёжность и устойчивую работу указанных объектов⁴.

³ URL: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024>

⁴ Федеральный закон № 187 от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» (в ред. Федерального закона от 10.07.2023 № 312-ФЗ) // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

Субъекты критической информационной инфраструктуры (КИИ) обязаны следовать установленным требованиям федерального органа, отвечающего за безопасность критически важных объектов. Эти требования распространяются на основные предприятия, жизненно важные для функционирования государства и общества. Согласно законодательным нормам, субъекты КИИ должны осуществлять комплекс обязательных мероприятий, в частности, следующих.

Важным шагом считается проведение мероприятий по категоризации объектов КИИ и создание системы обеспечения безопасности значимых объектов данной инфраструктуры. Необходимо установить сотрудничество с профильными органами для быстрой реакции на инциденты в области информационной безопасности, затрагивающие объекты КИИ.

Привлечение внимания к основным секторам экономики также не остаётся без внимания: наука, транспорт, связь, энергетика, государственная регистрация прав на недвижимое имущество и сделок с ним, финансовый рынок и банковская сфера, топливно-энергетический комплекс, атомная энергетика, оборонная и ракетно-космическая отрасль, в дополнение к горнодобывающей, металлургической и химической промышленности.

Субъектами КИИ признаются российские юридические лица, в том числе коммерческие и некоммерческие организации, индивидуальные предприниматели, а также собственники или арендаторы информационных систем, телекоммуникационных сетей и автоматизированных систем управления, играющие ключевую роль в обеспечении безопасности и устойчивости органов государственной власти и местного самоуправления.

Классификация объектов КИИ требует строгого соблюдения установленного порядка категоризации. Эффективный выбор категории является залогом безопасности данных⁵.

Объекты, имеющие высокий уровень значимости, подлежат строгим условиям безопасности. Тем не менее подобные критерии вполне допустимо применять к менее важным объектам КИИ. В результате важно принимать во внимание все нюансы их охраны⁶.

Специфика охраны ключевых объектов, работающих с данными, требует комплексного подхода, включающего новейшие технологии защиты, стратегические меры по снижению рисков и систематические

проверки. Указанные меры способствуют повышению уровня безопасности и надежности критически важной информации. Данные, относящиеся к государственной тайне, подлежат строгому регулированию в соответствии с российским законодательством. Обработка такого рода информации должна строго соответствовать действующим нормативам в сфере персональных данных. Даже если сведения не относятся к категории государственной тайны, к ним тем не менее применяются требования, касающиеся защиты данных в государственных системах.

Организация систем безопасности значимых объектов КИИ

Согласно приказу ФСТЭК России № 235 от 21 декабря 2017 года, для защиты значимых объектов разрабатываются специализированные системы безопасности⁷.

Системы обязаны обеспечивать комплексный подход, включая технические, правовые и организационные мероприятия, а их главная цель — защита информации.

При разработке системы безопасности КИИ необходимо принимать во внимание следующие важнейшие элементы.

- При исследовании классификации следует принимать во внимание, что объекты распределяются по трем категориям значимости, а также могут быть признаны освобожденными от такой оценки⁸.
- На следующем этапе необходимо провести анализ уязвимостей и создать модель угроз для системы информационной безопасности. Главные требования к системам выполнения защиты информации можно разделить на несколько ключевых аспектов.
- Первое правило охватывает защиту конфиденциальности — шифрование и аутентификация обеспечивают безопасность данных от несанкционированного вмешательства. Далее следует вопрос целостности данных, гарантирующий актуальность информации и её защиту от искажений; внедрение системы контроля версий и методов выявления изменений вносит значимый вклад в достижение этой цели. Третий аспект — доступность — подразумевает возможность пользова-

⁵ Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 19.09.2024) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

⁶ Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (рег. в Минюсте России 26.03.2018 № 50524). URL: <https://fstec.ru/dokumenty/vsedokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239> (дата обращения: 16.02.2025).

⁷ Приказ ФСТЭК России от 21.12.2017 № 235 (ред. от 20.04.2023) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (рег. в Минюсте России 22.02.2018 № 50118) // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

⁸ Постановление Правительства РФ от 08.02.2018 № 127 (ред. от 19.09.2024) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

телей запрашивать информацию в любое время. Эффективное резервное копирование и продуманный сетевой дизайн обеспечивают непрерывный доступ к материалам. Управление правами доступа критически важно. Ограничение доступа для отдельных групп пользователей снижает риск утечки информации. Не стоит забывать о гарантии бесперебойной работы систем: мониторинг и резервирование данных помогают поддерживать функционирование без сбоев. Удаленный контроль соблюдения законодательства предотвращает неприятности юридического характера. Выполнение вышеозначенных требований существенно минимизирует риск утечек и потерь информации.

Меры по охране объектов информатизации складываются в единую систему, задачей которой является защита информационных ресурсов. К основным этапам разработки относятся следующие.

1. Внедрение системы информационной защиты, предполагающей использование технических средств наряду с учётом человеческого фактора.

2. Анализ эффективности и соответствия действующему законодательству подразумевает учет стандартов защиты информации. Средства защиты информации (СЗИ) представляют собой совокупность мероприятий, базирующихся на разнообразных методах и технологиях охраны. При этом необходимо строгое соблюдение норм и правил, изложенных в нормативных документах⁹.

Защита информации представляет собой совокупность мер и технологических решений, ориентированных на охрану данных от угроз, вызванных как природными, так и антропогенными факторами. В отношении КИИ используются меры, установленные приказом ФСТЭК России от 25.12.2017 № 239¹⁰.

Общие требования к построению СЗИ информационных систем отражены в приказе ФСТЭК № 17¹¹.

Ключевые аспекты данного документа включают следующие положения:

- критерии классификации информационных систем;
- организационно-управленческие процедуры;

- средства обеспечения безопасности;
- методы управления доступом;
- оценку эффективности проведенных мероприятий по защите;
- планирование и обеспечение поддержки мер защиты на необходимом уровне.

Анализ угроз безопасности информации охватывает оценку применения методов, которые могут использовать злоумышленники, как внешние, так и внутренние. Решение многих задач безопасности связано с обнаружением уязвимостей в системе. Важно осознать, каким образом угроза может проявляться и какие последствия возникают при нарушении трех составляющих безопасности: конфиденциальности, целостности и доступности информации.

ФСТЭК РФ использует уникальную базу данных, предназначенную для анализа рисков и угроз безопасности информации. Этот инструмент существенно улучшил защиту данных¹².

Текущие методы разработки систем защиты информации основываются на сочетании различных методов и инструментов, способствующем достижению требуемого уровня безопасности защищаемых объектов.

Защита критически важных объектов требует внедрения многоуровневой системы безопасности данных. Комплексная система защиты информации подразумевает объединение всех компонентов, процессов и условий, обеспечивающих сохранность данных [6]. Система физической защиты информации (СФЗ) является важным звеном системы, направленным на охрану объектов и информационных систем.

Физическая безопасность КИИ служит основой защиты от несанкционированного доступа к ресурсам и системам [7]. Согласно ГОСТ Р 50922-96 физическая защита информации обозначает комплекс мероприятий, нацеленных на охрану объектов информации от несанкционированного проникновения. В состав этого комплекса входят организационные и технические меры, которые защищают объекты от вторжений и обеспечивают сохранение информации.

Система информационного устройства для выполнения физической защиты охватывает разнообразные элементы: временные, пространственные и режимные параметры. Необходимо произвести анализ ограниченной пространственной среды для функционирования объекта защиты.

К числу объектов защиты информации примыкают: охраняемые территории, здания и сооружения, предназначенные помещения, а также информационные ресурсы и данные, ассоциированные с объектом информатизации¹³.

⁹ Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст) // СПС «Гарант» (дата обращения: 16.02.2025).

¹⁰ Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 28.08.2024) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (рег. в Минюсте России 26.03.2018 № 50524). URL: <https://fstec.ru/dokumenty/vsedokumenty/prikazy/prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239> (дата обращения: 16.02.2025).

¹¹ Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (рег. в Минюсте России 31.05.2013 № 28608). URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения: 16.02.2025).

¹² Банк данных угроз безопасности информации. URL: <https://bdu.fstec.ru/threat> (дата обращения: 16.02.2025).

¹³ ГОСТ Р 50922 — 2006 Защита информации. Основные термины и определения. URL: https://rogosts.ru/file/gost/01/040/gost_r_50922-2006.pdf (дата обращения: 16.02.2025).

СФЗ выступает как ключевой элемент системы безопасности информационных систем. Она предназначена для защиты от угроз, возникающих как по причине природных явлений, так и в результате человеческой деятельности. СФЗ разрабатывается с целью эффективного обнаружения и устранения угроз, например, попыток несанкционированного доступа к охраняемой инфраструктуре с намерением хищения информации или оборудования.

Природные катастрофы, например, наводнения и пожары, причиняют серьезные убытки. Чтобы снизить ущерб от подобных угроз, следует осуществлять строгий мониторинг доступа к объектам КИИ.

Согласно Методическим указаниям¹⁴, несанкционированный доступ к контролируемой зоне происходит при наличии сотрудников КИИ без требуемых разрешений и перемещении машин или оборудования. Субъекты КИИ обязаны обеспечивать физическую безопасность своих объектов, систем защиты информации и местонахождения, чтобы предотвратить несанкционированный вход¹⁵.

ФСТЭК предложила комплекс требований к обеспечению защиты информации, обязательный к учету в процессе проектирования федеральной системы. В первую очередь следует создать контролируемую зону, оборудованную стационарными техническими средствами, предназначенными для обработки и защиты данных¹⁶.

Физическая охрана и контроль доступа к закрытым помещениям с техникой и СЗИ крайне необходимы. Предотвращение неразрешённого доступа станет вероятным при выполнении следующих условий:

- разработка ясных инструкций для работников, имеющих дело с технологическим оборудованием и работающих в контролируемых зонах;
- регулярный мониторинг доступа к системам обработки и защиты информации;
- внедрение системы контроля доступа, основанной на строгих методах, с целью снижения вероятности утечек и повышения надёжности охраняемых мер.

Организациям необходимо обеспечить контроль за физическим доступом к техническим средствам (ТС) и системам защиты информации. Важно фиксировать, кто и в какое время получает доступ к указанным объектам. В соответствии с требованиями ГОСТ Р 51241-2008 внедрение автоматизированных систем контроля

и управления доступом (СКУД) выступает необходимым условием для качественного учёта и мониторинга доступа.

Организациям настоятельно рекомендуется установить видеонаблюдение, фиксирующее все входы и выходы в зоны с транспортными средствами и защитными системами. Это намерение способствует укреплению безопасности и оперативному реагированию на потенциальные угрозы¹⁷.

Установка СКУД способствует идентификации и аутентификации пользователей, а также мониторингу их доступа к информационным ресурсам. Такая мера считается основополагающей для повышения уровня безопасности.

Необходимо обеспечить защиту оборудования от воздействия внешней среды. Следует учесть влияние окружающей среды, возможные отключения электричества и трудности с поддержанием оптимального температурного режима. Кроме того, строгое соблюдение норм пожарной безопасности поможет предотвратить возникновение чрезвычайных ситуаций¹⁸.

Для выполнения задач по защите информации в составе СФЗ выделяются подсистемы:

- физические преграды;
- тревожная сигнализация;
- контроль и управление доступом;
- телевизионное наблюдение;
- охранное освещение;
- противопожарная автоматика;
- связь;
- система сбора и обработки информации.

Нынешние СФЗ в России формируются, учитывая исторический опыт и особенности отдельных секторов. Заметное внимание уделяется ядерной безопасности, где способы физической защиты достигли высокой степени развития. Важно отметить, что в этой сфере отсутствуют жизненно необходимые подсистемы, среди которых пожарная автоматика и охранное освещение.

В сфере противокриминальной безопасности термин «физическая защита» не столь часто употребляется. Однако основные принципы и охранные методы остаются схожими, с применением аналогичных технических средств.

В данной работе проанализируем компоненты, определяющие структуру СФЗ, и их практическое использование.

7 декабря 2023 года Федеральная служба по экологическому, технологическому и атомному надзору ут-

¹⁴ Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК 11.02.2014). URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-11-fevralya-2014-g> (дата обращения: 16.02.2025).

¹⁵ Там же.

¹⁶ Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (рег. в Минюсте России 31.05.2013 № 28608). URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения: 16.02.2025).

¹⁷ ГОСТ Р 51241-2008. Национальный стандарт Российской Федерации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний (утв. и введен в действие Приказом Ростехрегулирования от 17.12.2008 № 430-ст) // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

¹⁸ Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.08.2024) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (рег. в Минюсте России 31.05.2013 № 28608). URL: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения: 16.02.2025).

вердила приказ № 440, в рамках которого была учреждена СФЗ ЯО. Обязанности этой службы включают¹⁹:

- анализ слабых мест объектов;
- анализ воздействия незаконных действий на средства охраны.

Классификация объектов физической защиты предполагает рассмотрение зданий и сооружений. Определяются зоны с ограниченным доступом, а также устанавливаются охраняемые объекты. Охранные средства размещаются по утверждённым местам.

Изучение эффективности СФЗ включает анализ разнообразных моделей с целью нахождения оптимального охранного решения. Важным аспектом является рассмотрение концепций, способствующих разработке действенной охранной системы.

В России противокриминальная защита осуществляется вневедомственной охраной Национальной гвардии. Работы проводятся в соответствии с Методическими рекомендациями Р 093-2024.

Оценка объекта охраны требует внимания к ряду факторов. В первую очередь следует рассмотреть степень ценности объекта, а также наличие материальных и культурных ценностей. Эти критерии обеспечивают определение уровня угрозы и выбор наиболее подходящей категории охраны. Классификация объектов варьируется от высокозащищённых, уровня А1, до объектов с минимальным уровнем охраны, Б2.

Теперь следует подготовить перечень действий, необходимых для защиты объекта. Разработка блокировочных схем и составление технического задания для проектировщиков занимают ключевое место в создании систем защиты информации. На данный момент стоит подчеркнуть отсутствие строгих норм, регламентирующих создание СЗИ в составе системы защиты информации. Этот пробел в документации отрицательно отражается на безопасности системы защиты информации, открывая злоумышленникам возможность использования физических методов против защищаемых объектов.

Современные вызовы ставят перед нами задачу усиления защиты данных. Одним из основных направ-

лений станет внедрение способов анализа информации и всех аспектов информатизации. Такой подход позволит адекватно оценивать значимость объектов и их активов. Благодаря ему охрана будет более результативной; мы сможем определить, что требует первоочередного внимания в защите.

Установление категории охраняемого объекта станет ключевым этапом в формировании охранной системы. На основании этой категории разрабатываются мероприятия безопасности и устанавливаются уровни защиты. Нормативы ГОСТ Р 50776-95 содержат ясные рекомендации о классификации объектов и мерах, подлежащих применению. Этот подход обеспечит эффективную и комплексную защиту информации²⁰.

Категория объектов охраны — это всеобъемлющая характеристика состояния, обременённого культурной, экономической или иной ценностью. Основными критериями служат состояние накопленных материальных и нематериальных ценностей, оценка потенциального ущерба от правонарушений и сложности осуществления охраны.

В современных условиях категорирование объектов КИИ становится необходимостью. Процедура не сводится к формальным действиям: она играет ключевую роль в оценке информационных систем. На основе полученных результатов формируются точные рекомендации по составу и структуре СЗИ для каждого отдельного объекта.

Заключение

В Российской Федерации нет формализованных научных методик для установления критериев физической защиты объектов КИИ. В результате разработки адекватных защитных решений оказываются затруднительными. В итоге владельцы этих систем сталкиваются с угрозой недостаточной безопасности или, напротив, вынуждены тратить бюджетные средства на избыток защитных мер.

¹⁹ Приказ Ростехнадзора от 07.12.2023 № 440 «Об утверждении федеральных норм и правил в области использования атомной энергии „Требования к физической защите ядерных материалов, ядерных установок и пунктов хранения ядерных материалов“ (НП-083-23)» (рег. в Минюсте России 20.03.2024 № 77568) // СПС «Консультант-Плюс» (дата обращения: 16.02.2025).

²⁰ ГОСТ Р 50776-95 (МЭК 60839-1-4:1989). Государственный стандарт Российской Федерации. Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию (принят и введен в действие Постановлением Госстандарта РФ от 22.05.1995 № 256) (ред. от 13.12.2011) // СПС «КонсультантПлюс» (дата обращения: 16.02.2025).

Литература

1. Долгиева Д.М.Г. Законодательство о безопасности критической информационной инфраструктуры Российской Федерации // Актуальные научные исследования в современном мире. 2021. № 5-6 (73). С. 70—76. EDN: KIFJDL.
2. W. Duo, M. Zhou, A. Abusorrah. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, Vol. 9, No. 5, pp. 784–800, May 2022. DOI: 10.1109/JAS.2022.105548.
3. Волхонский В.В. К вопросу единства терминологии в задачах физической защиты объектов / В.В. Волхонский, С.Л. Малышкин // Информационно-управляющие системы. 2013. № 5 (66). С. 61—68. EDN: RFLKID.

4. Перминова Я.А. Анализ основных нормативных документов по обеспечению безопасности критической информационной инфраструктуры Российской Федерации / Я.А. Перминова, А.К. Урсегов // Научный аспект. 2023. Т. 7. № 6. С. 887—893. EDN: WWDMTT.
5. Родионов М.А. Защита критической информационной инфраструктуры как необходимое условие обеспечения экономической безопасности России / М.А. Родионов, Е.Ю. Егоров // Экономика и бизнес: теория и практика. 2024. № 3-2 (109). С. 77—81. DOI: 10.24412/2411-0450-2024-3-2-77-81 . EDN: AKQGAD.
6. Штоль В.В. Информационно-коммуникационные технологии и информационная безопасность России / В.В. Штоль, А.Г. Задохин // Обозреватель. 2022. № 5-6 (388-389). С. 66—78. DOI: 10.48137/2074-2975_2022_5_6_66 . EDN: LTISSH.
7. Локнов А.И. Особенности реализации угроз безопасности информации на значимом объекте критической информационной инфраструктуры и меры по его защите / А.И. Локнов, Е.А. Симакова // Региональная информатика и информационная безопасность : сборник трудов Санкт-Петербургской международной конференции, Санкт-Петербург, 25—27 октября 2023 г. Санкт-Петербург : Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2023. С. 185—188. EDN: GZTGSZ.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

CRITICAL INFORMATION INFRASTRUCTURE SECURITY: PHYSICAL PROTECTION SYSTEMS, LEGAL FOUNDATION

Aleksandr Murav'ev, Ph.D. student at the Department of Automation, Metrology, and Management in Technical Systems of the Institute of Technological Machines and Forest Transportation of the Saint Petersburg State Forest Technical University, Saint Petersburg, Russian Federation. ORCID: 0009-0008-4901-9112.

E-mail: muravyev_a_g@mail.ru

Boris Shifrin, Ph.D. (Technology), Associate Professor at the Department of Automation, Metrology, and Management in Technical Systems of the Institute of Technological Machines and Forest Transportation of the Saint Petersburg State Forest Technical University, Saint Petersburg, Russian Federation. ORCID: 0000-0001-5377-741X.

E-mail: shifrinb@mail.ru

Keywords: physical protection, critical information infrastructure, unauthorised access.

Abstract

Purpose of the work: studying the modern state of legal foundations for regulating the creation of physical protection systems (PhPS) for objects of critical information infrastructure (OCII).

Methods used in the study: analysis, comparison, generalisation, structural decomposition from the system analysis theory, analysis of methods for creating PhPS being a part of an information protection means (IPM) complex for OCII.

Study findings: an analysis of current legal regulations governing ensuring the security of OCII is carried out, and different modern approaches for creating PhPS are considered. Forming objective assessments allows to understand the modern state of legal foundations for creating (improving) PhPS of integrated IPM and pose the problems of improving the legal foundation for more efficiently solving tasks of ensuring the security of the critical information infrastructure of the Russian Federation.

Practical value: an assessment of the modern state of legal regulation of creating PhPS for OCII is given.

References

1. Dolgieva D.M.G. Zakonodatel'stvo o bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii. Aktual'nye nauchnye issledovaniia v sovremennom mire. 2021. No. 5-6 (73). Pp. 70–76. EDN: KIFJDL.
2. W. Duo, M. Zhou, A. Abusorrah. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, Vol. 9, No. 5, pp. 784–800, May 2022. DOI: 10.1109/JAS.2022.105548 .
3. Volkhonskii V.V. K voprosu edinstva terminologii v zadachakh fizicheskoi zashchity ob'ektov. V.V. Volkhonskii, S.L. Malyshkin. Informatsionno-upravliaiushchie sistemy. 2013. No. 5 (66). Pp. 61–68. EDN: RFLKID.

4. Perminova I.A. Analiz osnovnykh normativnykh dokumentov po obespecheniiu bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii. I.A. Perminova, A.K. Ursegov. Nauchnyi aspekt. 2023. T. 7. No. 6. Pp. 887–893. EDN: WWDMTT.
5. Rodionov M.A. Zashchita kriticheskoi informatsionnoi infrastruktury kak neobkhodimoe uslovie obespecheniia ekonomicheskoi bezopasnosti Rossii. M.A. Rodionov, E.Iu. Egorov. Ekonomika i biznes: teoriia i praktika. 2024. No. 3-2 (109). Pp. 77–81. DOI: 10.24412/2411-0450-2024-3-2-77-81 . EDN: AKQGAD.
6. Shtol' V.V. Informatsionno-kommunikatsionnye tekhnologii i informatsionnaia bezopasnost' Rossii. V.V. Shtol', A.G. Zadokhin. Obozrevatel'. 2022. No. 5-6 (388-389). Pp. 66–78. DOI: 10.48137/2074-2975_2022_5-6_66 . EDN: LTISSH.
7. Loknov A.I. Osobennosti realizatsii ugroz bezopasnosti informatsii na znachimom ob'ekte kriticheskoi informatsionnoi infrastruktury i mery po ego zashchite. A.I. Loknov, E.A. Simakova. Regional'naia informatika i informatsionnaia bezopasnost': sbornik trudov Sankt-Peterburgskoi mezhdunarodnoi konferentsii, Sankt-Peterburg, 25–27 oktiabria 2023 g. Sankt-Peterburg : Sankt-Peterburgskoe Obshchestvo informatiki, vychislitel'noi tekhniki, sistem svyazi i upravleniia, 2023. Pp. 185–188. EDN: GZTGSZ.

ПРОГНОЗНАЯ МОДЕЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ¹

Авраменко В.С.², Саенко И.Б.³, Котенко И.В.⁴

Ключевые слова: безопасность информации, прогнозирование, показатель защищенности, машинное обучение, оценка точности.

Аннотация

Цель работы: разработка прогнозной модели защищенности информации в инфокоммуникационных системах (ИКС) на основе рекуррентных нейронных сетей, обеспечивающей высокую точность прогнозов значений показателей защищенности информации.

Методы исследования: системный анализ, классификация, моделирование, машинное обучение с помощью искусственных нейронных сетей.

Результаты исследования: разработана прогнозная модель защищенности информации в ИКС на основе рекуррентной нейронной сети; проведена экспериментальная оценка точности прогнозирования защищенности информации; обоснована целесообразность использования комплексных показателей защищенности информации в качестве прогнозных величин и рекуррентных нейронных сетей для прогнозирования их значений.

Практическая ценность: уточнены концептуальные положения по прогнозированию защищенности информации в ИКС.

DOI: 10.24412/1994-1404-2025-2-140-147

Введение

Проблема защиты информации в инфокоммуникационных системах (ИКС) относится к классу постоянных, требует регулярного исследования с учетом изменений в защищаемой системе и ландшафта угроз безопасности информации. В настоящее время публикуемые статистические данные свидетельствуют о росте количества компьютерных инцидентов безопасности в ИКС различного назначения, в том числе относящихся к объектам критической инфраструктуры. Помимо традиционных факторов, связанных с появлением новых уязвимостей, средств и технологий реализации компьютерных атак, в том числе и с использованием технологий искусственного интеллекта [1], увеличение количества атак обусловлено сложившейся геополитической обстановкой.

Следует отметить, что объектом компьютерных атак становятся и модели машинного обучения, все чаще используемые в различных сферах деятельности, что требует разработки и внедрения соответствующих методов и технологий защиты [2—4]. В целом ситуация характеризуется значительным повышением нагрузки на системы защиты информации в ИКС, необходимостью привлечения дополнительных сил и средств для обработки возрастающего количества инцидентов безопасности и реагирования на них. В таких условиях возрастает актуальность задачи прогнозирования угроз безопасности информации и уровня защищенности информации в ИКС в целом с целью своевременного проведения мероприятий по предотвращению перехода ИКС в незащищенное состояние.

¹ Работа выполнена при частичной финансовой поддержке бюджетной темы FFZF-2025-0016.

² **Авраменко Владимир Семенович**, кандидат технических наук, доцент, профессор Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-2452-0380.
E-mail: vsavr@yandex.ru

³ **Саенко Игорь Борисович**, доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0002-9051-5272.
E-mail: ibsaen@comsec.spb.ru

⁴ **Котенко Игорь Витальевич**, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), заслуженный деятель науки РФ, г. Санкт-Петербург, Российская Федерация. ORCID: 0000-0001-6859-7120.

E-mail: ivkote@comsec.spb.ru

В системах защиты информации ИКС функция прогнозирования защищенности информации в автоматическом режиме практически не реализуется. Основными причинами проблемы прогнозирования защищенности информации является недостаточно высокая результативность прогнозных аналитических и статистических моделей защищенности и низкий уровень автоматизации существующих решений по прогнозированию защищенности.

Одним из путей решения повышения эффективности прогнозирования защищенности информации в ИКС является применение технологий машинного обучения, в частности, — рекуррентных нейронных сетей, хорошо зарекомендовавших себя в задачах прогнозирования временных последовательностей в различных предметных областях [5, 6].

Данная работа посвящена исследованию возможностей рекуррентных нейронных сетей для повышения точности прогнозирования уровня защищенности информации в ИКС. Новизна работы заключается в применении рекуррентных нейронных сетей для прогнозирования комплексных показателей защищенности информации, в отличие от известных, совместно учитывающих зависимости процессов нарушений безопасности и восстановления защищенности информации.

Обзор исследований

Исследования в области применения технологий искусственного интеллекта для решения задач защиты информации, в том числе для прогнозирования уязвимостей, атак, угроз и состояния защищенности информации в ИКС, ведутся достаточно активно. В частности, в [7] рассматривается влияние архитектуры искусственной нейронной сети на эффективность обнаружения сетевых атак, обсуждаются преимущества и недостатки различных архитектур, а также проблемы, связанные с их использованием. В [8] предложена модель прогнозирования ситуации на основе темпоральной сверточной сети, которая фокусируется на проблеме долгосрочного прогнозирования временных рядов. В [9] представлен обзор методов прогнозирования в области защиты информации, обсуждается задача прогнозирования следующего шага или намерения злоумышленника, предсказания предстоящих кибератак и прогнозирования безопасности всей сети. В [10] предлагается метод прогнозирования сетевой безопасности, основанный на модели LSTM-XGBoost, в котором модель сети LSTM используется для прогнозирования сетевых вторжений, а XGBoost применяется для оценки ситуации на основе прогнозируемых данных. В [11] рассматривается методика прогнозирования показателей защищенности информации в автоматизированных системах на основе статистических методов. В [12] для прогнозирования безопасности защищенных систем предлагается нейро-нечеткая сеть, обеспечивающая возможность использования слабо формализованных данных и обучение в режиме реального време-

ни. В [13] предложен метод прогнозирования ситуации безопасности в программно-определяемой сети. В [14] исследованы методы предотвращения, прогнозирования и распознавания угроз информационной безопасности, которые направлены на снижение ущерба из-за недостатков существующих подходов управления рисками. В [15] для прогнозирования атак UDP-flood используются модели экспоненциального сглаживания и нейросетевого прогнозирования. В [16] обсуждается прогнозирование и распознавание намерений при многоэтапной или постоянной сетевой атаке. В [17] предложены стохастические модели прогнозирования ущерба от инцидентов безопасности в информационных системах, учитывающие статистику временных и объемных характеристик ущерба. В [18] представлен метод прогнозирования рисков сетевой информационной безопасности, основанный на сверточной нейронной сети. В [19] описаны взаимоувязанные модели и методы, систематизированные для использования при планировании и реализации стандартизованных процессов системной инженерии. Их применение позволяет осуществлять анализ влияния защищенности информации в терминах прогнозируемых рисков. В [20] исследуется влияние функции потерь в нейронных сетях на эффективность прогнозирования и производится сравнение статистических методов и нейронных сетей при прогнозировании осведомленности о ситуации сетевой безопасности. Делается вывод, что нейронные сети более точны для прогнозирования ситуации в области сетевой безопасности. В [21] предложена модель прогнозирования инцидентов информационной безопасности на основе метода ближайшего соседа.

Таким образом, обзор исследований показывает, что прогнозирование защищенности информации является актуальной задачей защиты информации в ИКС, для решения которой используются как традиционные статистические методы, так и методы машинного обучения с использованием нейронных сетей. Предлагаемый в работе подход к прогнозированию отличается применением рекуррентных нейронных сетей для прогнозирования значений комплексных показателей защищенности информации в ИКС в целом.

Концептуальные положения по прогнозированию защищенности информации в ИКС

Под прогнозом защищенности информации в ИКС понимается предположение о возможных состояниях защищенности ИКС в будущем и (или) о путях и сроках перехода в эти состояния. Прогнозирование защищенности информации может выполняться как отдельная функция управления защитой и (или) частная функция планирования, контроля (мониторинга) защищенности. Целью прогнозирования защищенности информации в ИКС является получение оценок состояния защищенности информации ИКС в будущем для обеспечения своевременного проведения мероприятий

упреждающего характера на возможное нарушение защищенного состояния ИКС. Прогнозировать защищенность целесообразно как при проектировании ИКС, так и в ходе ее функционирования.

Методы и модели прогнозирования защищенности определяются задачами защиты информации в ИКС, полнотой и степенью неопределенности имеющейся информации о состоянии защищенности в прошлом, условиями функционирования ИКС, требованиями к показателям эффективности прогнозирования. По характеру информации, на основе которой осуществляется прогнозирование защищенности, можно выделить фактографические, экспертные и комбинированные методы. При наличии достоверных статистических данных для прогнозирования защищенности целесообразно использовать фактографические методы, основанные на анализе динамических (временных) рядов характеристик (параметров) защищенности информации.

Эффективность прогнозирования защищенности определяется точностью, оперативностью и ресурсоемкостью прогнозирования. На точность прогноза в первую очередь влияют выбранные методы прогнозирования, а также данные из источников, которые должны быть достоверны, сопоставимы, представительны, однородны и устойчивы. Такими источниками могут быть различного рода журналы событий аппаратных и программных средств построения ИКС и средств защиты информации, консолидированные данные из собственных и внешних центров мониторинга информационной безопасности, информация об уязвимостях и компьютерных атаках как из публичных, так и из собственных источников, заключения экспертов.

Ключевой задачей прогнозирования является разработка прогнозной модели защищенности. Под прогнозной моделью защищенности ИКС понимается модель системы защиты информации ИКС, исследование которой позволяет получить совокупность данных о возможных состояниях защищенности ИКС в будущем и (или) путях и сроках их осуществления.

В общем виде прогнозная модель защищенности информации в ИКС по аналогии с классическими моделями имеет следующий вид:

$$y_3(t) = tr(t) + S(t) + I(t) + \varepsilon \quad (1)$$

где $y_3(t)$ — прогнозное значение характеристики или показателя защищенности, $tr(t)$ — тренд, представляющий собой плавно изменяющуюся составляющую, отражающую влияние оказывающих долговременное воздействие факторов на процессы защиты информации; $S(t)$ — циклическая составляющая, отражающая регулярную повторяемость процессов защиты во времени (в течение года, недели, суток и др.); $I(t)$ — интервенции (резкие изменения уровня защищенности под влиянием факторов, которые практически сложно локализовать во времени с точки зрения возможности предвидения); ε — нерегулярная составляющая.

При отсутствии объективных предпосылок для цикличности основных процессов защиты и непредвиденных воздействий может использоваться упрощенная прогнозная модель защищенности:

$$y_3(t) = tr(t) + \varepsilon \quad (2)$$

Для формирования прогноза защищенности как случайного нестационарного процесса необходимо произвести декомпозицию исходного процесса на регулярную (тренд) и нерегулярную составляющие. Тренд описывает устойчивые тенденции изменения значений показателей защищенности информации. Нерегулярная составляющая характеризует случайную непрогнозируемую часть и возможные отклонения фактических значений показателей защищенности от тренда. Выделенный в результате декомпозиции тренд может в дальнейшем использоваться в качестве основы прогнозной модели защищенности.

Прогнозная модель защищенности должна обеспечить требуемую точность и достоверность прогноза, но при этом минимизировать значения показателей оперативности и ресурсоемкости прогнозирования.

В качестве показателя точности прогноза комплексных показателей защищенности может использоваться средняя абсолютная ошибка прогноза в процентах (Mean Absolute Percentage Error, MAPE).

В качестве показателя оперативности прогноза защищенности целесообразно использовать время, затраченное на разработку прогноза. С учетом направленности исследования на реализацию прогнозирования защищенности ИКС в автоматизированном режиме в качестве показателя ресурсоемкости может применяться коэффициент использования вычислительных ресурсов, отражающий загруженность процессора и оперативной памяти. Могут использоваться также финансово-экономические показатели.

Другой вариант постановки задачи на прогнозирование защищенности может быть сформулирован следующим образом: прогнозная модель должна обеспечить максимально возможную точность прогноза при заданных ограничениях на значения показателей оперативности и ресурсоемкости прогнозирования. При определении требований к оперативности прогноза следует учитывать время, необходимое на анализ результатов прогнозирования и проведение мероприятий по реагированию.

Можно выделить два основных направления решения задачи разработки прогнозной модели значений показателей защищенности информации в рамках модели временных рядов: на основе

- статистических моделей (регрессии, экспоненциального сглаживания и т. д.) и
- структурных моделей (цепи Маркова, классификационные деревья, нейронные сети и другие).

С учетом результатов исследований в данной области перспективным направлением решения задачи прогнозирования показателей защищенности информации в ИКС является использование рекуррентных нейронных сетей.

Прогнозная модель защищенности информации на основе рекуррентных сетей

Первоочередной задачей прогнозирования защищенности информации в ИКС является определение целей прогнозирования и прогнозируемых показателей защищенности. В интересах управления защитой информации в ИКС могут использоваться прогнозы как единичных, так и комплексных показателей защищенности информации. В качестве единичных могут использоваться такие показатели, как интенсивность появления уязвимостей, интенсивность нарушений безопасности информации, величина ущерба, интенсивность восстановления защищенности информации. Но для прогнозирования уровня защищенности информации в ИКС в целом целесообразно использовать комплексные показатели защищенности информации, учитывающие характеристики как процесса нарушения безопасности, так и восстановления защищенного состояния. В частности, в качестве прогнозной величины может быть использован коэффициент защищенности информации K_3 , определяемый следующим образом:

$$K_3 = \frac{\mu_{вз}}{\lambda_{нб} + \mu_{вз}} \quad (3)$$

где $\lambda_{нб}$ — интенсивность нарушений безопасности в ИКС; $\mu_{вз}$ — интенсивность восстановления защищенности информации в ИКС.

Показатель $\mu_{вз}$ отражает возможности системы защиты информации по восстановлению защищенности информации, включающее задачи обнаружения и диагностирования нарушений безопасности, а также реагирования на них.

Более точно оценить защищенность информации в ИКС возможно при учете процессов нарушения безопасности и восстановления защищенности для каждого защищаемого ресурса ИКС. При наличии возможности восстановления защищенности только одного ресурса для расчета коэффициента защищенности информации в ИКС может использоваться следующая формула:

$$K_3 = 1 / \sum_{i=0}^{N_{зр}} A_{N_{зр}}^i \left(\frac{\lambda_{нб,i}}{\mu_{вз,i}} \right)^i \quad (4)$$

где $N_{зр}$ — количество защищаемых ресурсов в ИКС; $A_{N_{зр}}^i = \frac{N_{зр}!}{(N_{зр}-i)!}$ — число размещений из $N_{зр}$ по i .

При условно неограниченных возможностях по восстановлению защищенности ресурсов расчетное выражение следующее:

$$K_3 = \prod_{i=1}^{N_{зр}} \frac{\mu_{вз,i}}{\lambda_{нб,i} + \mu_{вз,i}} \quad (5)$$

Из известных апробированных моделей машинного обучения для прогнозирования защищенности целесообразно использовать рекуррентные нейронные сети (Recurrent Neural Network, RNN), хорошо зарекомендовавшие себя в задачах прогнозирования временных рядов. Наиболее распространенными являются RNN Элмана, LSTM-сети и Gated Recurrent Units (GRU) [5]. Ос-

новным преимуществом сетей LSTM и GRU является решение проблемы исчезающего градиента, характерной для простейшей рекуррентной нейронной сети. В [5] показано, что в задачах прогнозирования временных рядов LSTM демонстрирует более высокую точность, чем GRU и RNN Элмана. Но для относительно небольших наборов данных или коротких последовательностей GRU может быть более эффективна, чем LSTM, так как способна обучаться на таких данных с меньшими вычислительными затратами без потери в точности.

Обобщенная прогнозная модель защищенности включает наборы нейронных сетей для прогнозирования единичных показателей защищенности и блок расчета прогнозных значений комплексного показателя защищенности (рис. 1).



Рис. 1. Прогнозная модель защищенности информации в ИКС на основе рекуррентных сетей

На входы рекуррентных сетей подаются последовательности значений интенсивностей нарушений безопасности $\lambda_{нб}$ и интенсивностей восстановления защищенности $\mu_{вз}$ для каждого i -го защищаемого ресурса, рассчитываемых на основе исходных статистических данных. На выходе рекуррентных сетей формируются прогнозные значения единичных показателей защищенности. Далее рассчитываются прогнозные значения комплексного показателя защищенности $\bar{K}_3$.

Пример прогнозирования защищенности информации в ИКС

Для прогнозирования показателей защищенности информации была создана система LSTM-сетей с использованием языка программирования Python и общедоступных библиотек.

Для прогнозирования интенсивности нарушений безопасности в качестве входных данных для нейросетей использовались временные ряды интенсивностей нарушений безопасности, построенные на основе статистических данных за несколько лет, полученных из базы данных уязвимостей National Vulnerability Database (NVD).

Для обучения нейросети и прогнозирования защищенности информации в ИКС необходимо использовать статистические данные о функционировании системы защиты. В наихудшем для системы защиты информации случае, когда нарушитель имеет высокую квалификацию, постоянно отслеживает появление но-

вых уязвимостей, а также имеет возможность оперативно использовать их для реализации нарушения безопасности, интенсивность нарушений безопасности соответствует интенсивности появления уязвимостей.

Исходя из принятого допущения, в качестве примера были построены динамические (временные) ряды интенсивностей нарушений безопасности для ОС Linux (ядро Debian) на основе данных за несколько лет, полученных из базы данных NVD. Построенные временные ряды соответствовали типовым интервалам планирования защиты информации в ИКС (неделя, месяц и год). Далее была проведена подготовка данных, включающая выявление повторяющихся и незаполненных значений, аномалий и выбросов, нормализацию данных.

Для обучения LSTM-сети использовался алгоритм обратного распространения ошибки.

В ходе испытания программного макета автоматизированной системы прогнозирования защищенности информации в ИКС на выходе нейросетей формировались прогнозные значения интенсивности нарушений безопасности $\lambda_{нб,t}$ с заданным прогнозным периодом. В контрольном примере прогнозирования защищенности было сделано допущение о неизменности значения интенсивности восстановления защищенности в исследуемый период функционирования (структура и характеристики системы защиты не изменяются).

Оценка интенсивности восстановления защищенности была получена на основе статистической обработки данных о возможностях системы защиты типовой ИКС. Далее рассчитывались прогнозные значения комплексного показателя защищенности информации по формуле (3).

Аналогичный эксперимент был также проведен для прогнозной модели на основе GRU-сетей.

В качестве показателя точности прогноза защищенности использовалась средняя абсолютная процентная ошибка прогноза, рассчитываемая по формуле

$$MAPE = \frac{1}{n} \sum_{t=1}^n \frac{|e_t|}{x_t} \cdot 100, \quad (8)$$

где $e_t = x_t - \bar{x}_t$ — ошибка прогноза; x_t — фактическое значение; $\bar{x}_t$ — прогнозное значение; n — количество прогнозных значений.

Для сравнительного анализа методов прогнозирования на основе рекуррентных сетей и традиционных статистических методов прогнозирования были рассчитаны прогнозные значения показателей защищенности на основе методов скользящего среднего и экспоненциального сглаживания с использованием тех же исходных данных, что и для нейросетей.

Результаты оценки точности прогнозов представлены в таблице 1.

Таблица 1

Результаты оценки точности прогнозов защищенности

Используемый метод прогнозирования	MAPE (%)		
	на 1 год	на 1 месяц	на 1 неделю
На основе LSTM-сети	4,6	6,8	10,4
На основе GRU-сети	5,3	7,7	11,2
Скользящего среднего	8,5	17,53	21,2
Экспоненциального сглаживания	26,3	32,7	40,9

По результатам сравнительного анализа методов прогнозирования защищенности информации, представленных в таблице 1, можно сделать вывод о том, что метод прогнозирования на основе LSTM-сети точнее, чем на основе GRU-сети, и существенно точнее классических статистических методов прогнозирования. Также очевидна закономерность увеличения точности прогноза с увеличением прогнозного периода.

Для достижения максимальной точности прогноза за защищенности информации в ИКС и наличии достаточно полных и достоверных исходных данных за длительные периоды времени предпочтительным представляется использование LSTM-сетей. В условиях ограниченности статистических данных о функционировании ИКС данных в прошлом или жестких ограничений на вычислительные ресурсы целесообразно использовать GRU-сети.

Программное средство прогнозирования защищенности информации в ИКС на основе рекуррентных

сетей может использоваться как администраторами безопасности ИКС для обеспечения упреждающего оперативного реагирования, так и сотрудниками, ответственными за организацию защиты информации в ИКС, при долгосрочном планировании защиты информации. В качестве исходных данных для прогнозирования могут использоваться как имеющиеся статистические данные о процессах защиты в ИКС, так и данные об уязвимостях и угрозах из внешних источников информации.

Заключение

Использование представленной прогнозной модели защищенности информации на основе рекуррентных сетей может использоваться как разработчиками системы защиты информации ИКС, так и должностными лицами по защите информации ИКС на стадии эксплуатации для обеспечения своевре-

менного проведения мероприятий упреждающего характера по поддержанию требуемого уровня защищенности. При этом разработка и внедрение автоматизированной системы прогнозирования защищенности информации не требует существенных затрат.

Дальнейшие исследования направлены на повышение эффективности прогнозирования защищенности за счет более детального учета в прогнозной модели защищенности характеристик процессов нарушения безопасности информации, структуры и характеристик системы защиты информации, повышения степени автоматизации процесса прогнозирования.

Рецензент: Липатников Валерий Алексеевич, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, старший научный сотрудник научно-исследовательского центра Военной академии связи имени Маршала Советского Союза С.М. Буденного, г. Санкт-Петербург, Россия.
E-mail: lipatnikovanl@mail.ru

Литература

1. Намиот Д.Е. О кибератаках с помощью систем искусственного интеллекта // International journal of open information technologies. 2024. Т. 12. № 9. С. 132—141.
2. 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—38. DOI: 10.21681/2311-3456-2023-6-2-19.
3. Kotenko I., Saenko I., Laut O., Vasiliev N., Iatsenko D. Attacks Against Machine Learning Systems: Analysis and GAN-based Approach to Protection. Proceedings of the 7th International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. Springer, Cham. 2023. Pp. 49–59. DOI: 10.1007/978-3-031-43792-2_5.
4. Zhou Sh., Liu Ch., Ye D., Zhu T., Zhou W., Yu Ph.S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 2022. Vol. 55. No. 8. Article 163. 39 p. DOI: 10.1145/3547330.
5. Hewamalage H., Bergmeir C., Bandara K. Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. International Journal of Forecasting. 2021. Vol. 37. No. 1. Pp. 388–427. DOI: 10.1016/j.jforecast.2020.06.008.
6. Kotenko I., Laut O., Kribel K., Saenko I. LSTM Neural Networks for Detecting Anomalies Caused by Web Application Cyber Attacks. Frontiers in Artificial Intelligence and Applications. Vol. 337: New Trends in Intelligent Software Methodologies, Tools and Techniques. 2021. Pp. 127–140. DOI: 10.3233/FAIA210014.
7. Xoliyarov F.T., Gulomov S.R., Bozorov S.M. The Impact of Artificial Neural Network Architecture on Network Attack Detection. The International Conference on Future Networks and Distributed Systems (ICFNDS '23). 2023. 9 p. DOI: 10.1145/3644713.3644792.
8. Yin K., Yang Y., Yao C., Yang J. Long-Term Prediction of Network Security Situation Through the Use of the Transformer-Based Model. IEEE Access. 2022. Vol. 10. Pp. 56145–56157. DOI: 10.1109/ACCESS.2022.3175516.
9. Liu H., Jiang R., Zhou B., Rong X., Li J., Li A. A Survey of Cyber Security Approaches for Prediction. 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC). 2021. Pp. 439–444. DOI: 10.1109/DSC53577.2021.00069.
10. Gao F., Xia J., Wu D., Wang W., Wang C., Song C. Network security situation prediction based on LSTM. 2023 2nd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE). 2023. Pp. 350–354. DOI: 10.1109/CBASE60015.2023.10439145.
11. Авраменко В.С. Методика прогнозирования защищенности информации в инфокоммуникационных системах // Перспективные направления развития отечественных информационных технологий. Материалы VI межрегиональной научно-практической конференции. 2020. С. 235—236.
12. Sklyarov V. Forecasting Performance of Security Information for Protected Systems Based on Hybrid Artificial Neural Networks. Proceedings of the 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). 2020. Pp. 1–3. DOI: 10.1109/FarEastCon50210.2020.9271334.
13. Sheng M., Liu H., Yang X., Wang W., Huang J., Wang B. Network Security Situation Prediction in Software Defined Networking Data Plane. Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). 2020. Pp. 475–479. DOI: 10.1109/AEECA49918.2020.9213592.
14. Grishaeva S.A., Borzov V.I. Information Security Risk Management. Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020. Pp. 96–98. DOI: 10.1109/ITQMIS51053.2020.9322901.
15. Тумбинская М.В., Волков В.В., Загидуллин Б.Г. Применение статистических методов для прогнозирования UDP-FLOOD атак // Вестник Дагестанского государственного технического университета. Технические науки. 2020. Т. 47. № 2. С. 108—122. DOI: 10.21822/2073-6185-2020-47-2-108-122.

16. Buchta R., Gkoktsis G., Heine F., Kleiner C. Advanced Persistent Threat Attack Detection Systems: A Review of Approaches, Challenges, and Trends. *Digital Threats*. 2024. Vol. 5. No. 4. Article 39. Pp. 1–37. URL: <https://doi.org/10.1145/3696014>
17. Saurenko T.N., Anisimov V.G., Anisimov E.G., Kasatkin V.V., Los' V.P. Information Security Incident Forecasting. *Automatic Control and Computer Sciences*. 2021. Vol. 55. No. 8. Pp. 903–907. DOI: 10.3103/S0146411621080277 .
18. Li W. Prediction and Analysis of Network Information Security Risk Based on Convolutional Neural Network. 2021 4th International Conference on Information Systems and Computer Aided Education (ICISCAE 2021). 2021. Pp. 2819–2823. DOI: 10.1145/3482632.3487522 .
19. Костогрызлов А.И. О моделях и методах вероятностного анализа защиты информации в стандартизованных процессах системной инженерии // Вопросы кибербезопасности. 2022. № 6(52). С. 71—82. DOI: 10.21681/2311-3456-2022-6-71-82 .
20. Staňa R., Pekarčík P., Gajdoš A., Sokol P. Network Security Situation Awareness Forecasting Based on Neural Networks. *Theory and Applications of Time Series Analysis and Forecasting. ITISE 2021. Contributions to Statistics*. 2023. Pp. 255–270. DOI: 10.1007/978-3-031-14197-3_17 .
21. Беляева Т.А., Микрюков А.А. Нейросетевое прогнозирование инцидентов информационной безопасности // Международный студенческий научный вестник. 2023. № 6. С. 30—36.

SECTION:

INFORMATION AND AUTOMATED SYSTEMS AND NETWORKS

A PROGNOSTIC MODEL OF INFORMATION PROTECTION IN INFORMATION COMMUNICATION SYSTEMS BASED ON A RECURRENT NEURAL NETWORK

Vladimir Avramenko, Ph.D. (Technology), Associate Professor, Professor at the Military Academy of the Signal Corps, Saint Petersburg, Russian Federation. ORCID: 0000-0002-2452-0380.
E-mail: vsavr@yandex.ru

Igor' Saenko, Dr.Sc. (Technology), Professor, Principal Researcher at the Laboratory for Computer Security Problems of the Saint Petersburg Federal Research Centre of the Russian Academy of Sciences, Saint Petersburg, Russian Federation. ORCID: 0000-0002-9051-5272.
E-mail: ibsaen@comsec.spb.ru

Igor' Kotenko, 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, Honoured Figure of Science of the Russian Federation, Saint Petersburg, Russian Federation. ORCID: 0000-0001-6859-7120.
E-mail: ivkote@comsec.spb.ru

Keywords: information security, forecasting, protection indicator, machine learning, accuracy evaluation.

Abstract

Purpose of the study: developing a prognostic model of information protection in information communication systems (ICS) based on recurrent neural networks which ensures a high accuracy of forecasts for the values of information protection indicators.

Methods used in the study: system analysis, classification, modelling, machine learning using artificial neural networks.

Study findings: a prognostic model of information protection in ICS based on a recurrent neural network was developed. An experimental evaluation of accuracy for information protection forecasting was carried out. A justification was given for the advisability of using integrated information protection indicators as prognostic values, and recurrent neural networks for forecasting their values.

Practical value: conceptual provisions for information protection forecasting in ICS were made more specific.

References

1. Namiot D.E. O kiberatakakh s pomoshch'iu sistem iskusstvennogo intellekta. *International journal of open information technologies*. 2024. T. 12. No. 9. Pp. 132–141.

2. Kotenko I.V., Saenko I.B., Laut 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. 24–38. DOI: 10.21681/2311-3456-2023-6-2-19 .
3. Kotenko I., Saenko I., Laut O., Vasiliev N., Iatsenko D. Attacks Against Machine Learning Systems: Analysis and GAN-based Approach to Protection. Proceedings of the 7th International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. Springer, Cham. 2023. Pp. 49–59. DOI: 10.1007/978-3-031-43792-2_5 .
4. Zhou Sh., Liu Ch., Ye D., Zhu T., Zhou W., Yu Ph.S. Adversarial Attacks and Defenses in Deep Learning: From a Perspective of Cybersecurity. ACM Computing Surveys. 2022. Vol. 55. No. 8. Article 163. 39 p. DOI: 10.1145/3547330.
5. Hewamalage H., Bergmeir C., Bandara K. Recurrent Neural Networks for Time Series Forecasting: Current status and future directions. International Journal of Forecasting. 2021. Vol. 37. No. 1. Pp. 388–427. DOI: 10.1016/j.ijforecast.2020.06.008 .
6. Kotenko I., Laut O., Kribel K., Saenko I. LSTM Neural Networks for Detecting Anomalies Caused by Web Application Cyber Attacks. Frontiers in Artificial Intelligence and Applications. Vol. 337: New Trends in Intelligent Software Methodologies, Tools and Techniques. 2021. Pp. 127–140. DOI: 10.3233/FAIA210014 .
7. Xoliyarov F.T., Gulomov S.R., Bozorov S.M. The Impact of Artificial Neural Network Architecture on Network Attack Detection. The International Conference on Future Networks and Distributed Systems (ICFNDS '23). 2023. 9 p. DOI: 10.1145/3644713.3644792 .
8. Yin K., Yang Y., Yao C., Yang J. Long-Term Prediction of Network Security Situation Through the Use of the Transformer-Based Model. IEEE Access. 2022. Vol. 10. Pp. 56145–56157. DOI: 10.1109/ACCESS.2022.3175516 .
9. Liu H., Jiang R., Zhou B., Rong X., Li J., Li A. A Survey of Cyber Security Approaches for Prediction. 2021 IEEE 6th International Conference on Data Science in Cyberspace (DSC). 2021. Pp. 439–444. DOI: 10.1109/DSC53577.2021.00069 .
10. Gao F., Xia J., Wu D., Wang W., Wang C., Song C. Network security situation prediction based on LSTM. 2023 2nd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE). 2023. Pp. 350–354. DOI: 10.1109/CBASE60015.2023.10439145 .
11. Avramenko V.S. Metodika prognozirovaniia zashchishchennosti informatsii v infokommunikatsionnykh sistemakh. Perspektivnye napravleniia razvitiia otechestvennykh informatsionnykh tekhnologii. Materialy VI mezhr regional'noi nauchno-prakticheskoi konferentsii. 2020. C. 235–236.
12. ISklyarov V. Forecasting Performance of Security Information for Protected Systems Based on Hybrid Artificial Neural Networks. Proceedings of the 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon). 2020. Pp. 1–3. DOI: 10.1109/FarEastCon50210.2020.9271334 .
13. Sheng M., Liu H., Yang X., Wang W., Huang J., Wang B. Network Security Situation Prediction in Software Defined Networking Data Plane. Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA). 2020. Pp. 475–479. DOI: 10.1109/AEECA49918.2020.9213592 .
14. Grishaeva S.A., Borzov V.I. Information Security Risk Management. Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). 2020. Pp. 96–98. DOI: 10.1109/ITQMIS51053.2020.9322901 .
15. Tumbinskaia M.V., Volkov V.V., Zagidullin B.G. Primenenie statisticheskikh metodov dlia prognozirovaniia UDP-FLOOD atak. Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. Tekhnicheskie nauki. 2020. T. 47. No. 2. Pp. 108–122. DOI: 10.21822/2073-6185-2020-47-2-108-122 .
16. Buchta R., Gkoktsis G., Heine F., Kleiner C. Advanced Persistent Threat Attack Detection Systems: A Review of Approaches, Challenges, and Trends. Digital Threats. 2024. Vol. 5. No. 4. Article 39. Pp. 1–37. URL: <https://doi.org/10.1145/3696014>
17. Saurenko T.N., Anisimov V.G., Anisimov E.G., Kasatkin V.V., Los' V.P. Information Security Incident Forecasting. Automatic Control and Computer Sciences. 2021. Vol. 55. No. 8. Pp. 903–907. DOI: 10.3103/S0146411621080277 .
18. Li W. Prediction and Analysis of Network Information Security Risk Based on Convolutional Neural Network. 2021 4th International Conference on Information Systems and Computer Aided Education (ICISCAE 2021). 2021. Pp. 2819–2823. DOI: 10.1145/3482632.3487522 .
19. Kostogryzov A.I. O modeliakh i metodakh veroiatnostnogo analiza zashchity informatsii v standartizovannykh protsessakh sistemnoi inzhenerii. Voprosy kiberbezopasnosti. 2022. No. 6(52). Pp. 71–82. DOI: 10.21681/2311-3456-2022-6-71-82 .
20. Staňa R., Pekarčík P., Gajdoš A., Sokol P. Network Security Situation Awareness Forecasting Based on Neural Networks. Theory and Applications of Time Series Analysis and Forecasting. ITISE 2021. Contributions to Statistics. 2023. Pp. 255–270. DOI: 10.1007/978-3-031-14197-3_17 .
21. Beliaeva T.A., Mikriukov A.A. Neurosetevoe prognozirovanie intsidentov informatsionnoi bezopasnosti. Mezhdunarodnyi studencheskii nauchnyi vestnik. 2023. No. 6. Pp. 30–36.

Над номером работали:

<i>Начальник РИО</i>	<i>Ю.В. Матвиенко</i>
<i>Шеф-редактор</i>	<i>Г.И. Макаренко</i>
<i>Редактор-переводчик</i>	<i>Т.В. Галатонов</i>
<i>Дизайн обложки</i>	<i>Н.Г. Шабанова</i>
<i>Верстка</i>	<i>Н.Г. Шабанова</i>
