

DIGITAL TECHNOLOGIES AND LAW

Как цитировать: Цифровые технологии и право: сборник научных трудов IV Международной научно-практической конференции (г. Казань, 19 сентября 2025 г.) / под ред. И. Р. Бегешева, Е. А. Громовой, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2024. EDN: RPTUQB. http://dx.doi.org/10.21202/978-5-8399-0904-5_4 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

For citation: Digital Technologies and Law: collection of scientific papers of the IV International Scientific and Practical Conference (Kazan, 2025, September 19) / I. R. Begishev, E. A. Gromova, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2024. EDN: RPTUQB. http://dx.doi.org/10.21202/978-5-8399-0904-5_4 – 1 CD-ROM. – Title from the title screen. – Text: electronic.



ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
IV Международной научно-практической конференции

19 сентября 2025 г.

г. Казань

В шести томах

Том 4



DIGITAL TECHNOLOGIES AND LAW

Collection of scientific articles
of the IV International Scientific and Practical Conference

2025, September 19

Kazan

In 6 volumes

Volume 4

УДК 004:34(063)
ББК 67с51я43
Ц75

Издается по решению редакционно-издательского совета
Казанского инновационного университета имени В. Г. Тимирязова

Рецензенты:

А. К. Жарова, доктор юридических наук, доцент, директор Центра исследований киберпространства, ассоциированный член Международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам» Национального исследовательского университета «Высшая школа экономики»;

К. А. Пономарева, доктор юридических наук, доцент, ведущий научный сотрудник Центра налоговой политики Научно-исследовательского финансового института Министерства финансов Российской Федерации, профессор кафедры правового обеспечения рыночной экономики Высшей школы правоведения Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации;

Е. А. Рускевич, доктор юридических наук, доцент, профессор кафедры уголовного права Московского государственного юридического университета имени О. Е. Кутафина;

К. Л. Томашевский, доктор юридических наук, профессор, заместитель декана юридического факультета по научной работе, профессор кафедры гражданского и предпринимательского права Казанского инновационного университета имени В. Г. Тимирязова;

Ю. С. Харитонова, доктор юридических наук, профессор, руководитель Центра правовых исследований искусственного интеллекта и цифровой экономики, профессор кафедры предпринимательского права Московского государственного университета имени М. В. Ломоносова

Ц75 Цифровые технологии и право: сборник научных трудов IV Международной научно-практической конференции (г. Казань, 19 сентября 2025 г.) / под ред. И. Р. Бегешева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. – Казань: Изд-во «Познание» Казанского инновационного университета, 2026. 401 с. EDN: RPTUQB. http://dx.doi.org/10.21202/978-5-8399-0904-5_4 – 1 CD-ROM. – Загл. с титул. экрана. – Текст: электронный.

ISBN 978-5-8399-0910-6

ISBN 978-5-8399-0907-6 (Vol. 4)

Системные требования: операционные системы Linux, Windows; 120 Мб; 16 Мб; PDF Reader; дисковод CD-ROM, мышь.

Вошедшие в сборник научные труды приурочены к IV Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 19 сентября 2025 г. в Казани в рамках Международного форума Kazan Digital Week 2025, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

На конференции обсуждался широкий спектр теоретико-методологических, практико-ориентированных, междисциплинарных и отраслевых вопросов, касающихся приоритетов развития правового регулирования цифровых технологий, нормативного контроля над цифровой средой, перспектив влияния права на формирование и развитие новых общественных отношений.

Научные труды представленного тома систематизированы по современным трендам развития цифровых технологий в системе правовых отношений и подготовлены студентами и магистрантами: рассматриваются вопросы правового регулирования квантовых технологий как инструмента обеспечения национальной безопасности и технологического суверенитета, постквантовой криптографии, а также иные молодежные исследования в области взаимодействия цифровых технологий и права.

Нашедшие отражение в многотомном издании идеи и предложения в своей совокупности являются ключом к пониманию интеллектуальной карты смыслов, которые будут интересны ученым-правоведам и экспертам в области цифровых технологий, практикующим юристам, представителям правотворческих и правоприменительных органов, государственным служащим и участникам реального сектора экономики, включая разработчиков и производителей продуктов на основе достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0910-6
ISBN 978-5-8399-0907-6 (Vol. 4)

© Авторы статей, 2026
© Казанский инновационный университет
имени В. Г. Тимирязова, 2026

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов IV Международной научно-практической конференции
19 сентября 2025 г.
г. Казань

В шести томах
Том 4

Под редакцией И. Р. Бегешева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой

Электронное издание

Главный редактор Г. Я. Дарчинова; редакторы: Г. А. Тарасова, Е. А. Маннапова;
технические редакторы: О. А. Аймурзаева, С. Р. Каримова; дизайн обложки: Г. И. Загреддинова

Дата подписания к использованию: 07.07.2026. Объем издания 4,7 Мб. Тираж 11 экз. Заказ № 12/2026
ISBN 978-5-8399-0910-6

Издательство Казанского инновационного университета им. В. Г. Тимирязова
420111, г. Казань, ул. Московская, 42 Тел. (843) 231-92-90, E-mail: zaharova@ieml.ru 7



Reviewers:

A. K. Zharova, Dr. Sci. (Law), Associate Professor, Director of the Center for Cyberspace Research, Associate Member of the International Scientific and Educational Center “UNESCO Chair in Copyright, Related, Cultural and Information Rights” of the National Research University Higher School of Economics;

K. A. Ponomareva, Dr. Sci. (Law), Associate Professor, Leading Researcher of Centre for Taxation Policy of Scientific-research Institute of the Russian Ministry of Finance, Professor of the Department of Legal Provision of Market Economy, Higher School of Legal Studies, Russian Presidential Academy of National Economy and Public Administration;

E. A. Russkevich, Dr. Sci. (Law), Associate Professor, Professor of the Department of Criminal Law of the Moscow State Law University named after O. E. Kutafin;

K. L. Tomashevsky, Dr. Sci. (Law), Professor, Deputy Dean of the Faculty of Law for Research, Professor of the Department of Civil and Business Law of the Kazan Innovation University named after V. G. Timiryasov;

Yu. S. Kharitonova, Dr. Sci. (Law), Professor, Head of the Center for Legal Research of Artificial Intelligence and Digital Economy, Professor of the Department of Business Law at Lomonosov Moscow State University

Digital Technologies and Law: collection of scientific papers of the IV International Scientific and Practical Conference (Kazan, 2025, September 19) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 4. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2026. EDN: RPTUQB. http://dx.doi.org/10.21202/978-5-8399-0904-5_4 – 1 CD-ROM. – Title from the title screen. – Text: electronic.

ISBN 978-5-8399-0910-6

ISBN 978-5-8399-0907-6 (Vol. 4)

System requirements: Linux, Windows operation systems; 120 Mb; 16 Mb; PDF Reader; CD-ROM, mouse.

The scientific works included in the collection are tied with the 4th International scientific-practical conference “Digital Technologies and Law”, which was held on September 19, 2025 in Kazan as part of Kazan Digital Week 2025 International Forum, organized by the Russian Government jointly with the Republic of Tatarstan Cabinet of Ministers.

The conference discussed a wide range of theoretical and methodological, practice-oriented, interdisciplinary and sectoral issues related to the priorities in the legal regulation of digital technologies, regulatory control over the digital environment, and prospective impact of law on the formation and development of new public relations.

The scientific works in this volume are systematized according to modern trends in the development of digital technologies within the system of legal relations. They were prepared by students and undergraduates on the issues of legal regulation of quantum technologies as a tool for ensuring national security and technological sovereignty, post-quantum cryptography, as well as other spheres of interaction between digital technologies and law.

The ideas and proposals reflected in the multi-volume publication are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies, practicing lawyers, lawmakers and law-enforcers, government officials and participants in the real sector of the economy. These include developers and manufacturers of products based on digital technologies, young researchers – students, undergraduates, and postgraduates, to all those interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0910-6

ISBN 978-5-8399-0907-6 (Vol. 4)

© Authors of articles, 2026

© Kazan Innovative University

named after V. G. Timiryasov, 2026

Scientific publication

DIGITAL TECHNOLOGIES AND LAW

Collection of scientific papers of the IV International Scientific and Practical Conference

2025 September 19
Kazan

In 6 volumes
Volume 4

I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.)

Electronic publication

Editor-in-Chief G. Ya. Darchinova; editors: G. A. Tarasova, E. A. Mannapova;
technical editors: O. A. Aimurzaeva, S. A. Karimova; cover designer G. I. Zagretdinova

Date of signing for usage: 07.07.2026. Volume of the publication 4,7 Mb. Number of copies: 11. Order No. 12/2026
ISBN 978-5-8399-0910-6

Poznaniye Publishing House of Kazan Innovative University named after V. G. Timiryasov
42 Moskovskaya Str., 420111 Kazan, Russian Federation; Tel. +7 (843) 231-92-90; E-mail: zaharova@ieml.ru



Редакторы:

И. Р. Бегишев, доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова;

Е. А. Громова, доктор юридических наук, доцент, заместитель директора Юридического института по международной деятельности, профессор кафедры гражданского права и гражданского судопроизводства Южно-Уральского государственного университета (национального исследовательского университета);

М. В. Залоило, кандидат юридических наук, ведущий научный сотрудник отдела теории права и междисциплинарных исследований законодательства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации;

И. А. Филипова, кандидат юридических наук, доцент, доцент кафедры трудового и экологического права Национального исследовательского Нижегородского государственного университета имени Н. И. Лобачевского;

А. А. Шутова, кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса Казанского инновационного университета имени В. Г. Тимирязова

Editors:

I. R. Begishev, Dr. Sci. (Law), Associate Professor, Honored Lawyer of the Republic of Tatarstan, Chief Researcher of the Research Institute of Digital Technologies and Law, Professor of the Department of Criminal Law and Process of the Kazan Innovation University named after V. G. Timiryasov;

E. A. Gromova, Dr. Sci. (Law), Associate Professor, Deputy Director on international activity of the Institute of Law, Professor of the Department of Civil Law and Procedure, South Ural State University (national research university);

M. V. Zaloilo, Cand. Sci. (Law), leading researcher at the Department of Theory of Law and Interdisciplinary Research of Legislation at the Institute of Legislation and Comparative Law under the Government of the Russian Federation;

I. A. Filipova, Cand. Sci. (Law), Associate Professor, Associate Professor of the Department of Labor and Environmental Law of the National Research Nizhny Novgorod State University named after N. I. Lobachevsky;

A. A. Shutova, Cand. Sci. (Law), senior researcher at the Research Institute of Digital Technologies and Law, associate professor of the department of criminal law and process of the Kazan Innovation University named after V. G. Timiryasov

Содержание

Цифровые технологии в системе правовых отношений (секция для студентов и магистрантов)

О. К. Антропцев. Квантовые технологии как инструмент обеспечения национальной безопасности.....	10
Д.П. Архипов. Практические перспективы применения цифровых технологий в расследовании преступлений	17
К. М. Бажина. Цифровое насилие: виды и классификация.....	23
Р. В. Баитов. Трансформация финансового суверенитета: вызовы правового регулирования оборота цифровых активов в России.....	27
П. С. Баишев. Проблемные аспекты правового регулирования click-wrap соглашений.....	41
Е. А. Бенчук. Алгоритмические субъекты: правовые модели ответственности и практические альтернативы	47
А. А. Богданова. Цифровые технологии в сфере долевого строительства: риски и перспективы внедрения	55
А. Д. Бочкарева. Интеллектуальная собственность без границ: перспективы и трансформация правовых институтов в метавселенной.....	68
А. С. Васильева. Развитие цифровых платформ и трудовое право	73
Н. И. Гасников. Смарт-контракты на платформе цифрового рубля	80
А. Е. Головенкина. Революционные перспективы или правовой хаос? Защита авторских прав в эпоху искусственного интеллекта	84
К. Я. Грехова. Цифровизация прокурорского надзора за исполнением антикоррупционного законодательства в государственных и муниципальных органах.....	93
Л. А. Гринюк. Авторское право в цифровую эпоху: правовые основы, вызовы и перспективы развития.....	99
К. А. Гришаева, Е. О. Якуш. Электронная подпись как инструмент цифровой трансформации права.....	104
А. Р. Дяблова. Маркировка рекламы в социальных сетях: правовая база и проблемы практики.....	112
М. А. Жижкин. Этические аспекты разработки программного обеспечения и систем искусственного интеллекта	123
С. А. Задорина. Цифровизация: новые горизонты правового регулирования криптовалюты.....	131
Е. Г. Закиев, А. А. Дашкевич. Правовые аспекты применения искусственного интеллекта в управлении бизнес-процессами	146
Л. Е. Зотова. Цифровая трансформация гражданского оборота	151

Т. В. Иванова. Автоматизация юридической экспертизы локальных нормативных актов организации	163
М. М. Карев, Д. С. Яковлева. Legaltech: от автоматизации процессов к новой модели юридической деятельности.....	167
В. Д. Квитовская, А. А. Сорокопудова. Цифровые технологии, способствующие экономическому развитию международных организаций	183
А. В. Козлов. Правовые особенности использования цифровых технологий в примирительных процедурах	190
В. В. Колупаева, С. Р. Гадельшина. Правовые проблемы дистанционной продажи товаров и пути их решения	194
Д. К. Кононенко. Юридические аспекты возникновения авторских прав на генерируемые искусственным интеллектом произведения: подход России и США	201
А. С. Кочеткова, П. А. Петухова. Использование виртуальной аутопсии в расследовании преступлений	207
С. В. Кравцова. Право на цифровое забвение после смерти: пробелы правового регулирования и пути их устранения	214
А. В. Кулагина. Автоматизированное увольнение: границы допустимости и судебная практика	221
С. В. Ларцина. «Чей туфля»? Право на сгенерированную интеллектуальную собственность в практике китайских разработчиков.....	229
S. V. Lartsina, В. С. Луценко. Правовое регулирование искусственного интеллекта в Республике Корея	233
Д. В. Маслова, А. И. Морочковская. Роль чат-ботов в системе правовой поддержки населения.....	241
А. Г. Мухатдинова. Правовые аспекты использования регуляторных «песочниц» (regulatory sandboxes)	247
А. А. Олифиренко. Общедоступные данные в регулировании обучения ИИ-моделей.....	253
К. С. Павлова. Влияние цифровизации судебной деятельности на доступность и эффективность правосудия в условиях современной правовой системы.....	257
А. О. Исакова. Криптовалюта в Российской Федерации: проблемы правового режима и перспективы регламентации	261
А. А. Подъячева. Концепция «Smart notary»: цифровая трансформация нотариальной деятельности в России	271
Д. И. Рябина, А. А. Сидорова. Блокчейн в государственных реестрах: опыт и проблемы внедрения	279
Т. Б. Сабитов. Вопросы обучения больших языковых моделей и авторского права в России и в мире	290
А. Э. Сеитова. Взаимосвязь между интернет-зависимостью и предрасположенностью к преступному поведению	296

К. А. Сергеева. Новые объекты интеллектуальной собственности: перспективы правового регулирования.....	302
К. С. Сэу. Проблемы собирания и оценки электронных доказательств в уголовном процессе	311
И. Н. Тарасов. Особенности охраны и защиты цифровых прав. Способы защиты цифровых прав	319
Д. В. Терещенко. Смарт-контракты в страховании космических запусков и миссий	324
А. А. Тесленко. Метавселенные как вызов для правового регулирования.....	333
Ю. А. Трасковская. Электронное правосудие в республике Беларусь: современное состояние и перспективы развития.....	340
В. В. Савкина, Е. В. Тужикова. Цифровой контроль и родительский надзор	348
Д. В. Усиков. Виртуальная личность как слеодообразующий объект в системе цифровой криминалистики	355
В. В. Федорова. Автор VS нейросеть: как соблюсти баланс интересов в современном авторском праве.....	365
А. А. Хазиева. Особенности использования отдельных видов электронных и цифровых доказательств в судебной практике	369
А. М. Шамсутдинова. Проблемы привлечения к административной ответственности за оскорбление в мессенджерах с помощью голосовых сообщений: вопросы квалификации и анализ практики	382
А.Е. Шмелев. Интеграция цифровых платформ online dispute resolution (ODR) в модель «суда с множеством дверей»: опыт зарубежных стран.....	386
Н. С. Яковлева. Смарт-контракты в договоре поставки: особенности правового регулирования и проблемы применения.....	391
Ю. В. Пантазий. Криптовалюта: правовое положение и перспективы распространения.....	396

Цифровые технологии в системе правовых отношений (секция для студентов и магистрантов)

УДК 342.92

О. К. Антропцев,

студент,

Московский государственный юридический университет
имени О.Е. Кутафина (МГЮА)

Квантовые технологии как инструмент обеспечения национальной безопасности

Аннотация. Квантовые технологии становятся новым вызовом для национальной безопасности государства, поскольку существующие механизмы шифрования являются неустойчивыми против квантовых алгоритмов. В условиях беспрецедентного противостояния России и стран запада вопросы национальной безопасности имеют особое значение для нашей страны. Обеспечение суверенитета государства напрямую зависит от лидерства государства в сфере разработок квантовых технологий, обеспечения технологического прорыва. Исследование показало, что квантовые технологии дают не только преимущества для обеспечения сохранности данных, в первую очередь обеспечения государственной тайны посредством использования новых технологий шифрования, более точного моделирования результатов управленческих решений, выявления рисков и проблем, но и создают угрозы. В связи с чем особого внимания со стороны государства заслуживает не только создание условий, направленных на стимулирование исследований в сфере квантовых технологий, но и установление правовых рамок, имеющих своей целью предупредить использование квантовых разработок в качестве инструмента, направленного против национальной безопасности государства, а также в преступных целях. Правового закрепления требует понятийный аппарат, а также состав принципов, которые должны быть положены в основу правомерного применения квантовых технологий.

Ключевые слова: государственное управление, квантовые технологии, квантовые коммуникации, квантовые сети, национальная безопасность, постквантовая криптография, технологический суверенитет

Quantum technologies as a tool of enforcement of national security

Abstract. Quantum technologies are becoming a new challenge for the national security of the state, since existing encryption mechanisms are unstable against quantum algorithms. In the context of an unprecedented confrontation between Russia and Western countries, national security issues are of particular importance for our country. Ensuring the sovereignty of the state directly depends on the leadership of the state in the field of quantum technology development, ensuring a technological breakthrough. The study showed that quantum technologies provide not only advantages for ensuring the safety of data, primarily ensuring state secrets through the use of new encryption technologies, more accurate modeling of the results of management decisions, identifying risks and problems, but also create threats. In this regard, special attention from the state deserves not only the creation of conditions aimed at stimulating research in the field of quantum technologies, but also the establishment of a legal framework aimed at preventing the use of quantum developments as a tool directed against the national security of the state, as well as for criminal purposes. The conceptual apparatus, as well as the composition of the principles that should form the basis for the lawful use of quantum technologies, require legal consolidation.

Keywords: public administration, quantum technologies, quantum communications, quantum network, national security, post-quantum cryptography, technological sovereignty

Введение. В 21 веке, в веке технологий, помимо развития цифровых технологий, которые совершили поистине гигантский скачок в своем развитии, включая технологии искусственного интеллекта, квантовые технологии стали тем новым флагманом, изучением и разработкой которого занимаются во всем мире. Их возможности в сфере безопасных коммуникаций являются практически безграничными, способными обеспечить технологическое лидерство любому государству, вывести обеспечение национальной безопасности на беспрецедентный уровень.

В бюджете Соединенных Штатов Америки (например, федеральные инвестиции в новый испытательный полигон квантовых технологий в 2024 году составили 140 миллионов долларов [5]), Европейского союза, Китая (расходы Китая на квантовые технологии превышают 15 миллиардов долларов [5]), Российской Федерации на поддержку развития и создания условий для исследования и разработки квантовых технологий и квантовых компьютеров выделяются значительные суммы денег, что свидетельствует об особом приоритете данного направления для каждого государства. Создаются специальные научные центры, формируются партнерства государственных структур, бизнеса и научных школ, идет беспрецедентная гонка за поиском специалистов, внедряются про-

граммы обучения для подготовки ученых, специализирующихся на квантовых технологиях, что подтверждает особое внимание и значимость новых технологий [9].

Квантовые технологии позволяют создать существенные преимущества в разных отраслях и решить множество задач, которые имеют приоритетное направление для государства, дать конкурентное преимущество субъектам хозяйственной деятельности. Однако, в противовес преимуществам есть и ряд недостатков, которыми являются дороговизна и сложность установки оборудования, а также существенные затраты на научно-исследовательские разработки. Таким образом, области применения существенно сужаются для всеобщего пользования, однако, не для применения в государственном управлении.

В рамках настоящего исследования попробуем проанализировать достоинства и недостатки внедрения квантовых технологий в государственное управление.

Основная часть. В промежутке с 2020 Российская Федерация выстраивает курс политики, при котором высокие технологии внедряются в государственное управление. В настоящее время уже активно используется искусственный интеллект для анализа огромных массивов данных, цифровые платформы для создания доступности граждан к государственным услугам, аналитике, которая становится основой для принятия управленческих решений. Большие данные, собираемые государством, приобретают особую ценность, и обеспечение их защиты является приоритетом для государства, которое выстраивается на проведении политики использования отечественного программного обеспечения, включая разработки инструментов их шифрования, передачи по защищенным каналам связи, хранения исключительно на территории России. Речь идет не только об информации, в отношении которой установлен режим государственной тайны, но и любой персональной информации граждан. В последние годы многие системы обеспечения безопасности и существующие механизмы шифрования находятся под угрозой, поскольку учеными было установлено, что создание квантового суперкомпьютера способно разрушить любые механизмы защиты, которые имеются в настоящее время, а это уже вопрос угрозы национальной безопасности. Если раньше казалось, что квантовые компьютеры – это что-то из мира фантастики, возможные разработки через десятилетия, то сегодня они становятся реальностью, хотя и не обладают еще достаточной мощностью, чтобы разрушить существующие механизмы защиты.

В Российской Федерации внимание к квантовым технологиям было обращено на государственном уровне несколько лет назад, в частности, в Указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» в качестве задачи для обеспечения информационной безопасности было указано на совершенствование средств и методов на основе квантовых вычислений [4]. 30 ноября 2021 было принято постановление Правительства РФ № 2133 «О создании инновационного научно-исследовательского центра «Квантовая» долина», которое закрепило предоставление льготного режима для компаний, занимающихся разработками в сфере квантовых технологий. Этот шаг дал основу для углубленного развития в сфере данных техноло-

гий. Второй крупный шаг был сделан в 2023 году, когда после встречи с учеными 13 июля Президент дал поручение Правительству Российской Федерации обеспечить утверждение национального проекта по формированию экономики данных до 2030 года [1], при которой технологии квантовой безопасности внедряются для обеспечения государственной безопасности.

Крупнейшим представителем таких компаний с 2020 года является РЖД, которые совместно с «Ростелекомом» разработали дорожную карту, одобренную со стороны ТК 26 и Росстандарта [2]. Эта дорожная карта включает в себя 50 направлений и участие 15 организаций, что должно дать сильный толчок в развитии квантовых коммуникаций.

Говоря о квантовых технологиях, следует разобраться, что они из себя представляют. В настоящий момент их можно разделить на 3 группы:

1 группа – гибридные инфраструктуры, алгоритмы и приложения для квантовых вычислений. Данная группа включает в себя квантовые эффекты, такие как суперпозиция и запутанность, которые используются для ускорения решения определенных классов вычислительных задач, выходящих за пределы возможностей классических систем, основанных на логических битах. Диапазон задач, которые потенциально могут быть ускорены, простирается от оптимизации или моделирования до сложных приложений машинного и глубокого обучения. Обозначенные характеристики позволяют в многомерной плоскости более эффективно осуществлять решение задач, а, соответственно, обеспечивать более точное прогнозирование, моделирование разных ситуаций [8]. С точки зрения государственного управления, такие механизмы позволяют моделировать влияние тех или иных управленческих решений, находить более эффективные и оптимальные для государства, выявлять причины кризисов и избегать их.

2 группа – технологии CERN как демонстратор квантовых платформ. Особенностью данной группы является высокая чувствительность когерентных квантовых систем, которая используется для разработки новых классов датчиков. Детекторы, начиная от приборов, измеряющих локальную наноразмерную информацию, и заканчивая устройствами, основанными на когерентности планетарного масштаба, могут значительно повысить точность и открыть возможности для новых протоколов измерения [8].

3 группа – квантовые сети и коммуникационный узел для исследований. Одиночные или запутанные фотоны и их квантовые состояния используются для реализации доказательно безопасных протоколов связи через оптоволоконные сети или квантовые запоминающие устройства, способные хранить квантовые состояния [8]. Именно эта группа представляет наибольший интерес для достижения высокого уровня национальной безопасности.

Квантовый алгоритм был открыт в 1994 году Питером Шором [5], который при наличии мощного квантового компьютера позволяет взломать любой шифр, созданный в настоящее время, причем если раньше считалось, что это под силу исключительно суперкомпьютеру, то сегодня по оценкам ученым может быть достаточным использование компьютера с меньшим объемом процессора. Например, в 2019 году Гугл (Google) представил 53-кубитный компьютер,

который решил задачу, невыполнимую для классических суперкомпьютеров, позднее IBM продемонстрировал квантовые системы со 127 и 433 кубитами [5].

Таким образом, одной из приоритетных задач является разработка технологий, которые будут устойчивы к расшифрованию квантовыми компьютерами. Речь идет о создании новых механизмов шифрования с использованием квантовых технологий, которые получили название «постквантовая криптография». Приоритетным для национальной безопасности является, с одной стороны, перевод всех данных, информации государства в зашифрованную форму на основе квантово-устойчивых алгоритмов, с другой стороны, создание квантово-устойчивых каналов обмена данными и информации между всеми органами государственного управления. В настоящее время изучается две такие технологии: квантовое распределение ключей, а долгосрочной перспективе создание квантовой сети, которая объединит квантовые компьютеры.

Зарубежные страны активно занимаются исследованиями и созданием таких технологий. Примером опыта США являются упомянутые разработки IBM, Google, оборонного ведомства США. Интересен опыт использования данных технологий у других стран. Германия имеет обширную практику по созданию и первому опытному использованию квантовых технологий. Там реализуется инициатива QuNET, которая представляет из себя проект, направленный на создания цифрового суверенитета Германии в области кибербезопасности для государственных органов [6]. Данный проект реализуется Институтом прикладной оптики и точной механики имени Фраунгофера (IOF), Института имени Генриха Герца (HHI), Институтом связи и навигации Германского аэрокосмического центра (DLR-KN) и Институтом физики света имени Макса Планка (MPL). В инициативу QuNET входят такие направления, как квантовые технологии, которое включает в себя группу по исследованию возможностей исследования квантов, квантовые вычислительные машины, которые представляют компьютеры будущего способные воспринимать и обрабатывать огромные массивы данных, при этом обеспечивая максимальную безопасность, квантовые коммуникации, что является наиболее интересным, поскольку исследует возможности использования квантовых коммуникаций с точки зрения как безопасности, так и границ их применения, квантовую визуализацию, а также квантовое зондирование, которое направлено на использование квантовых свойств материи.

Учитывая, что технологии активно развиваются, несут в себе не только преимущества для государственного управления, как было указано ранее с точки зрения моделирования управленческих процессов, обеспечения беспрецедентной защиты данных и информации, что так же способно решить проблему борьбы с мошенничеством в цифровой среде, но и создают значительные риски, включая случаи получения доступа к возможностям квантовых технологий отдельными государствами и использованием их против нашей страны, способных нанести существенный урон национальной безопасности, а также со стороны криминальных структур, которые могут использовать их против граждан, хозяйствующих субъектов и государства, то следует обратить внимание на определенную неясность правового регулирования данной сферы. Действительно, в настоящее время отсутствует четкое понимание всей совокупности

отношений, которые могут возникнуть, понимания механизмов из-за неясности самой сферы, что создает трудности в регулировании самой сферы. Тем не менее ряд стран внедряет данные технологии в различные сферы. Понимание и осознание рисков требует внимания государства к созданию необходимого правового поля, направленного в первую очередь на создание не только благоприятной среды для разработок, но и определения рамок, направленных на предупреждение причинения вреда гражданам и государству.

В этой связи следует обратить внимание на распоряжение Правительства Российской Федерации от 11.07.2023 №1856–р «Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года» [3]. Особого внимания в рамках данной концепции заслуживает определение принципов регулирования отрасли квантовых технологий, среди которых особое внимание заслуживает обеспечение прав и свобод человека и гражданина, так называемый человеко-ориентированный подход, а также приоритет безопасности государства. Тем не менее, данное распоряжение является первым шагом, но, как показывает анализ активного развития квантовых технологий в зарубежных странах, вовлечение частных субъектов в этот процесс, необходимо уже сейчас принимать нормативные правовые акты, которые определяют в первую очередь понятийный аппарат в сфере квантовых технологий, субъектный состав лиц, вовлеченных в процесс создания, апробации и внедрения таких технологий, установит принципы их использования и запрета на применение квантовых технологий в случае выявления риска причинения вреда жизни и здоровью граждан, национальной безопасности. Представляется, что данные принципы целесообразно дополнить следующими: запретом использования в противоправных целях, обеспечения сохранения традиционных ценностей, прозрачности, недопустимости недобросовестной конкуренции.

Следует также обратить внимание, что любое обеспечение соблюдения правил поведения должно обеспечиваться государственным механизмом. В связи с чем представляется целесообразным уже сейчас разрабатывать нормы, которые будут устанавливать административную и уголовную ответственность в случае разработки и применения квантовых технологий в противоправных целях.

Заключение. Обращение государства и научного сообщества к квантовым технологиям, применение мер, направленных на стимулирование их разработок и внедрения, открывает новую эру, уже не цифрового, а квантового мира. Исключать, что он станет реальностью в ближайшее десятилетие нельзя, поскольку цифровые технологии за короткий промежуток времени совершили беспрецедентный скачок в своем развитии, и искусственный интеллект уже вошел в нашу жизнь, что казалось фантастикой несколько лет назад, причем именно он становится тем механизмом, который позволяет ускорить развитие создания квантовых алгоритмов и технологий. Появляются публикации, создаются проекты по развитию квантового искусственного интеллекта, например, проект «Гигафабрика ИИ» в Европейском союзе [7].

Квантовые технологии действительно способны стать инструментом обеспечения национальной безопасности государства, повысить качество государственного управления, в том числе за счет более точного прогнозирования,

более качественной аналитики, моделирования результатов различных управленческих решений. При этом они имеют и обратную сторону, способную нанести непоправимый ущерб национальной безопасности государства, повлечь утрату суверенитета. В связи с чем государству необходимо не только создавать условия для стимулирования научных разработок, но и использовать правовые средства, направленные на обеспечение правомерного использования квантовых технологий, установить правовые рамки и принципы их применения и внедрения, что может найти свое отражение в отдельном федеральном законе, а также посредством внесения изменений в Уголовный кодекс РФ в части установления уголовной ответственности в случае применения квантовых технологий во вред гражданам и национальной безопасности государства.

Список литературы

1. Владимир Путин дал поручения по нацпроекту экономики данных и развитию квантовых технологий. URL: <https://d-russia.ru/vladimir-putin-dal-poruchenija-po-nacproektu-jekonomiki-dannyh-i-razvitiju-kvantovyh-tehnologij.html?ysclid=Imp94ghxx8411372431> (дата обращения: 02.09.2025).
2. Правовое регулирование отрасли квантовых коммуникаций: перспективы и направления. URL: <https://proquant.ru/quantums/trends/pravovoe-regulirovanie-otrasli-kvantovykh-kommunikatsiy-perspektivy-i-napravleniya?ysclid=mcytoxdbfv661786792> (дата обращения: 02.09.2025)
3. Об утверждении Концепции регулирования отрасли квантовых коммуникаций в Российской Федерации до 2030 года: Распоряжение Правительства РФ от 11.07.2023 №1856-р // СЗ РФ. 2023. №30. Ст. 5712.
4. Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 №400 // СЗ РФ. 2021. №27 (часть II). Ст. 5351.
5. Ivezic M. Quantum Technology Use Cases in Government & Defense. 30.08.2024. URL: <https://postquantum.com/quantum-computing/use-cases-government-defense/> (дата обращения: 05.09.2025).
6. Our Quantum Research Project. The Center of Excellence in Photonics in Jena, Germany. URL: <https://quantum-technology.org/en/quantum-research-projects.html#-h3-Quantum-Communication-h3> (дата обращения: 02.09.2025).
7. Proposal for a Council Regulation on amending Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/14887. 15.07.2025. URL: <https://data.consilium.europa.eu/doc/document/ST-11675-2025-INIT/en/pdf> (дата обращения: 02.09.2025).
8. Quantum Technology Initiative research. 2025. URL: <https://quantum.cern/research> (дата обращения: 02.09.2025)
9. Барчуков, В. К. Организационно-правовые основы информационного обеспечения и применения искусственного интеллекта в деятельности правоохранительных органов: диссертация ... кандидата юридических наук.

Д.П. Архипов,
студент,
Российский технологический университет МИРЭА

Практические перспективы применения цифровых технологий в расследовании преступлений

Аннотация. Статья посвящена анализу современных тенденций интеграции цифровых технологий в правоохранительную деятельность для противодействия усложняющейся преступности и обработки больших массивов данных. В ходе исследования выявлены перспективные направления развития и внедрения технологий: прогнозная аналитика, идентификация личности, установление связей и обеспечение сохранности доказательств. Также отмечается, что для успешной интеграции и получения высокой эффективности цифровых систем, необходимо обеспечить финансовую и высоко квалифицируемую кадровую потребность, а также проработка возможных правовых проблем.

Ключевые слова: искусственный интеллект, правоохранительная деятельность, цифровизация, криминалистика, большие данные, зарубежные страны, машинное обучение, прогнозирование преступности

D.P. Archipov,
Student,
Russian Technological University MIREA

Practical prospects for the application of digital technologies in the investigation of crimes

Abstract. The article is devoted to the analysis of modern trends in the integration of digital technologies in law enforcement activities to counter the growing complexity of crime and the processing of large data sets. The study identified promising areas for the development and implementation of technologies, including predictive analytics, personal identification, establishing connections, and ensuring the preservation of evidence. It also noted that in order to successfully integrate and achieve high efficiency in digital systems, it is necessary to provide financial and highly qualified personnel requirements, as well as.

Keywords: artificial intelligence, law enforcement, digitalization, forensics, big data, foreign countries, machine learning, and crime forecasting

Введение. В последнее время цифровые технологии активно проникают во все сферы общества, включая правоохранительную деятельность, становясь ключевым инструментом для повышения эффективности работы органов правопорядка. Вместе с тем усложняется деятельность преступников, в том числе и в киберпространстве, увеличивая на сотрудников нагрузку и объем данных

необходимых для сбора, анализа, хранения и обеспечения их сохранности, при этом данный аспект деятельности является одним из ключевых в раскрытии преступлений. Вместе с тем, внедрение цифровых технологий – процесс не быстрый, поскольку связан не только с техническими аспектами, но и с юридическими и этическими. Это порождает ряд препятствий для повсеместного применения новых технологий в правоохранительной деятельности.

При этом, различного рода цифровые технологии применяются в зарубежных странах. На основании вышеуказанного, хотелось бы рассмотреть опыт применения перспективных технологий в различных странах, и проанализировать возможность внедрения таковых в отечественную правоохранительную систему, что позволит повысить эффективность и результативность органов расследования.

Основная часть. Прежде чем перейти к опыту применения технологий в зарубежных странах, рассмотрим те средства, которые уже стоят на вооружении правоохранительных ведомств в Российской Федерации.

Для начала стоит рассмотреть направление, связанное с использованием алгоритмов машинного обучения для обработки и анализа больших объемов данных. Они позволяют выявить не только очевидные, но и косвенные, неочевидные связи между лицами, местами и событиями. Стоит отметить, что данные модели способны обрабатывать информацию из множества различных источников, от баз данных находящихся в распоряжении правоохранительных органов до различных аудио- и видеозаписей и трекеров геолокации, позволяя тем самым обработать достаточно объемный пласт информации, необходимый для дальнейшей деятельности, а также выявлять различные закономерности и связи между различными данными. При этом результат такого исследования будет получен значительно быстрее, чем при традиционном способе.

С учетом того, что в России достаточно активно развивается проект «умный город», внедряющий различные цифровые технологии в повседневную жизнь, в том числе различные датчики и системы видеонаблюдения, алгоритмы обучения вполне способны при необходимости идентифицировать различных людей. Например, с 2018 года в стране действует такая система идентификации, как «Лица России», которая собирает данные из различных источников, включая камеры видеонаблюдения в общественных местах, базы данных правоохранительных органов, социальные сети и посредством использования искусственного интеллекта и алгоритмов машинного обучения система распознает лица и ищет подозреваемых [5].

Отдельного упоминания стоят и другие модели ИИ, вроде «Блок», «Маньяк» и «Криминалист» [9]. Как утверждает Антон Шустиков, глава проекта в области кибербезопасности некоммерческого просветительского проекта SakesCats, про систему «Маньяк»: разрабатываемый ИИ должен отмечать сотни параметров, начиная от способа совершения преступного деяния, заканчивая виктимностью, ставя главной целью работы – объединить множество разрозненных фактов, преступлений в одну серию убийств и составить его психолого-криминологический портрет, а также попытаться спрогнозировать дальнейшие действия.

При этом стоит отметить слова Константина Негачева, сооснователя компании VRT, уже про другую разрабатываемую систему «Блок», созданную для расследования различных экономических преступлений: ее задача – это помочь установить способ совершения, схему мошенничества и составлять карту преступлений привязывая к ним различные обстоятельства.

Анализируя опыт зарубежных стран, отметим опыт Великобритании, где с сентября 2024 года в правоохранительных органах заработал ИИ-инструмент «Soze», разработанный компанией Akkodis. Данный сервис способен проанализировать множество различных источников данных: видеоматериалы, финансовые транзакции, социальные сети, электронные письма и иные источники – «выполнив 81 год работы за 30 часов». [2]

Другим важным аспектом является предиктивная аналитика. Уже сейчас Системы машинного обучения способны выявлять различные закономерности, помогая составлять crime heat map, указывая на регионы и области, в которых будет наивысший риск совершения преступления. А с учетом того, что ИИ способен быстро и эффективно измерить различные показатели, статистические и иные данные определяющие детерминанты преступности и ее последствия, это способно обеспечить их максимальную достоверность и полноту проведенного исследования. [3]

Как было сказано ранее, в отечественном арсенале на вооружении стоит система «Криминалист», которая способна искать потенциальных преступных деятелей, а также места совершения преступного деяния, основываясь на внутренних базах данных правоохранителей: почерк преступлений, данные экспертиз и другие [8].

Естественно, за рубежом имеются схожие системы, одной из которых является американская платформа Palantir Gotham. По своей сути Palantir Gotham представляет собой операционную систему для работы с данными, использующую искусственный интеллект и расширенную аналитику для решения поставленных задач и используется в различных сферах обеспечения безопасности общества и государства, объединяя разрозненную информацию из разных баз данных, находит между ними взаимосвязи и составляя подходящую визуализацию, хотя и применяется преимущественно федеральными структурами помогая им в поиске преступных структур и осуществлять антитеррористическую деятельность.

В то же время, в различных городах имеются системы, хранящие в себе разрозненные локальные базы данных, для дальнейшего анализа и структуризации информации. И одной из многих таких систем является Blue CRUSH действующая на основе анализа статистики и осуществляя прогноз о следующих местах проявления преступного инцидента и ее деятельность уже снизила уровень преступности на 30%.

Еще такой программой является система PredPol разработанная в Калифорнийском университете и основной задачей была также составление прогноза и указание предположительных мест осуществления противоправных деяний. А система Strategic Subjects List действующая в Чикаго вовсе выявляла

лиц, склонных к совершению преступлений. По словам местных правоохранителей, большая часть задержанных входила в этот список [10].

Однако стоит отметить, что данные программы сталкиваются с некоторыми проблемами связанной с логикой их работы. В случае, когда исследователи получили доступ для изучения PredPol, чтобы понять, как происходит прогноз преступности, они обнаружили, что данная система использует для своей деятельности метод «тепловой карты», основанный на данных географии, а также финансовых и имущественных показателях: когда сотрудник полиции направляется в какой-то район и производит там арест, программа считает, что в этом районе высока вероятность совершения новых преступлений. Таким образом происходит обучение на основе данных, которые получают из криминальных районов, вследствие чего образуются «порочный цикл», воспроизводя этнические предубеждения, при этом полицейские отправляются в одни и те же районы чаще чем в другие, а также увеличивая количество сотрудников, отправленных туда [3].

Проблемы имеются и у системы Strategic Subjects List. Данная система использует для своей деятельности смешанный подход: личностно-ориентировочный – анализ личности исходя из полученных документов, характеризующих личность, а также информацию из сети интернет и социальных сетей, – и ранее описанный географический, с созданием «тепловой карты». Полицейский Департамент, по их утверждению, использует систему для ранжирования лиц с судимостью в зависимости от вероятности их причастности к стрельбе или убийству в качестве жертвы или преступника. На данный момент система в рамках личностно-ориентировочного подхода оценивает следующие показатели: количество случаев, когда он становился жертвой стрельбы, возраст на момент последнего ареста, количество случаев, когда он становился жертвой побоев или нападений при отягчающих обстоятельствах, количество предыдущих арестов за насильственные преступления, количество предыдущих арестов за хранение наркотиков, динамика преступной активности в последнее время и количество предыдущих арестов за незаконное использование оружия. Используя эти факторы, алгоритм выставляет оценку от 1 до 500, где более высокие баллы соответствуют большему риску участия в будущих в перестрелках или убийствах, и, следовательно, могут стать подозреваемыми или жертвами вооруженных нападений. При этом, несмотря на то, что указывается, что все факторы между собой равны, после анализа самого списка, исследователями было выявлено, что наибольший фактор, влияющий на оценку, это возраст человека, с динамикой на то, что чем старше человек, тем ниже оценка в данной категории – это указывает, что система придерживается концепции «чем старше человек, тем ниже вероятность совершения и участия в преступной деятельности». Несмотря на заявления Полицейского Департамента, Strategic Subjects List также содержит в себе информацию о поле, расе, месте жительства и месте последнего ареста человека, при этом при расчете баллов используются данные об арестах, что так же является достаточно неэффективным решением для вычисления показателя преступной деятельности. Так же отмечается противоречие в правовой сфере: несмотря на то, что официально систему нельзя использовать

для избрания мер пресечения, в действительности существуют приказы, которые разрешают использовать Strategic Subjects List для осуществления следственных действий, в том числе отслеживание лиц, включенных в данный список, и их персональных данных, защищенные Четвертой поправкой в Конституцию США. Главным опасением является, что выставляемая оценка в рамках данного списка, может легализовать проведение различных следственных действий, без серьезного и достоверного подтверждения [4].

Так или иначе, в иной сфере параллельно с предиктивной аналитикой и созданием crime heat map, в НИИ идет активное исследование возможностей ИИ в рамках создания 3D портрета человека по имеющейся на руках цепочке ДНК. В отечественной практике об этом говорит передача ФКУ НПО «Специальная техника и связь» МВД России тендера на исследование в 2021 году ПАО «Центр генетики и репродуктивной медицины «Генетико»». Согласно тендеру, исполнитель должен был сделать соответствующую систему ИИ способную определить общефизические (расу, национальность, телосложение, пол, возраст) признаки подозреваемых, и в том числе составление фоторобота искомого лица. По состоянию на текущий момент информации о конкретных результатах исследования не обнаружено несмотря на то, что договор был исполнен. [6]

Тем временем, исследование Китайской академии наук, в рамках которого ученые смогли создать ИИ Difface, который способен реконструировать трехмерное лицо основываясь лишь только на ДНК, при этом погрешность реконструкции составляет 3,5 мм. Согласно проведенному исследованию, участники эксперимента при использовании 5 лиц для идентификации, «правильное» лицо выбиралось в 75%. Однако, когда число лиц для выбора было увеличено, то и число правильного выбора снизилось до 50% [1].

Не стоит забывать про технологию Блокчейна, которая может стать достаточно сильным средством для обеспечения различного рода взаимодействий, в частности безопасности и легализации доказательственной базы в судопроизводстве. Как отмечает в своей работе Зиновьева Н.С., технология блокчейна представляет собой одновременно и подтверждения транзакции, и часть общей истории транзакции, так как данные записываются в зашифрованную цепочку и ключ доступа к этой информации есть только у владельца – то есть блокчейн представляет собой структуру хранения данных, организованную посредством последовательных блоков, объединенных между собой алгоритмами шифрования. Эти блоки содержат хронологически упорядоченную информацию, что гарантирует целостность и неизменяемость данных. Однако с учетом того, что биржи криптовалют сохраняют информацию о транзакции и об IP-адресах пользователей, при известном номере криптовалютного кошелька, можно будет отследить все адреса транзакции [7].

Соответственно использование данной технологии внутри судебной и правоохранительной системы так же возможно, так как позволит сотрудникам обеспечивать сохранность во время хранения или исследования электронной документации и цифровых следов.

Заключение. Опыт различных стран подтверждает перспективность использования цифровых технологий в борьбе с преступностью. Британская по-

лиция применяет ИИ для ускорения расследований; американские системы ИИ помогают прогнозировать место и время будущих преступлений. Россия также движется в этом направлении, однако для успешной интеграции и работы таких систем требуется достаточно высокий уровень профессиональной подготовки и высокий уровень финансового обеспечения. В то же время дальнейшая разработка и интеграция систем на основе ИИ может поднять ряд этических и правовых вопросов по их использованию, на что понадобится дополнительное нормативно-правовое сопровождение для разрешения возможных проблем.

Список литературы

1. A New AI Tool Can Recreate Your Face Using Nothing But Your DNA. URL: <https://www.zmescience.com/science/news-science/ai-dna-3d-facial-reconstruction/>
2. AI tool that can do '81 years of detective work in 30 hours' trialled by police. URL: <https://news.sky.com/story/amp/ai-tool-that-can-do-81-years-of-detective-work-in-30-hours-trialled-by-police-13220891>
3. Biased policing is made worse by errors in pre-crime algorithms | New Scientist. URL: <https://www.newscientist.com/article/mg23631464-300-biased-policing-is-made-worse-by-errors-in-pre-crime-algorithms/>
4. Aaron Tucek Constraining Big Brother: The Legal Deficiencies Surrounding Chicago's Use of the Strategic Subject List. URL: <https://legalforum.uchicago.edu/print-archive/constraining-big-brother-legal-deficiencies-surrounding-chicagos-use-strategic>
5. Вичугова А. Как сделать город безопасным: Big Data и Machine Learning против преступности. URL: <https://bigdataschool.ru/blog/crime-mapping/>
6. Завьялов И.А. Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений. Вестник Московского университета МВД России. 2021; (3): С. 228–236. URL: <https://cyberleninka.ru/article/n/zarubezhnyy-opyt-ispolzovaniya-iskusstvennogo-intellekta-v-raskrytii-prestupleniy>
7. Зиновьева Н.С. Возможности блокчейн-технологии в раскрытии и расследовании преступлений в интернет-пространстве // Вестник Восточно-Сибирского института МВД России № 3, 2018, С.184–189. URL: <https://vestnikesiirk.ru/ru/nauka/article/59013/view>
8. Искусственный интеллект в криминалистике. URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_криминалистике
9. Цифровое око правосудия. Как роботы помогают искать преступников в России [Электронный ресурс] URL: https://incrussia.ru/understand/bolshoy_brat/
10. Шевелева К.В. Возможности использования технологий искусственного интеллекта в правоохранительной деятельности: зарубежный опыт // Право и государство: теория и практика. 2023. № 7(223). С. 448–450. http://doi.org/10.47643/1815-1337_2023_7_448.

К. М. Бажина,
студент,
Казанский инновационный университет
имени В.Г. Тимирязова

Цифровое насилие: виды и классификация

Аннотация. В статье подробно рассматриваются виды цифрового насилия в сети «Интернет», приводятся примеры и способы проявления цифрового насилия в современных реалиях. Вместе с тем автор группирует виды цифрового насилия в классификацию по выявленным признакам, в том числе гендерным, возрастным и другим. В статье автор делает акцент на трендах цифрового насилия как на главном факте развития и популяризации данной формы деструктивного поведения индивидов.

Ключевые слова: цифровое насилие, общество, гендерное насилие, деструктивное поведение, киберпреступность, цифровые технологии, цифровизация

K. M. Bazhina,
student,
Kazan Innovative University
named after V.G. Timiryasov

Digital violence: types and classification

Abstract. The article examines in detail the types of digital violence on the Internet, providing examples and manifestations of digital violence in the modern context. Furthermore, the author groups the types of digital violence into a classification based on identified characteristics, including gender, age, and others. The article emphasizes the trends of digital violence as a key factor in the development and popularization of this form of destructive individual behavior.

Keywords: digital violence, society, gender-based violence, destructive behavior, cybercrime, digital technologies, digitalization

Введение. В настоящее время человечество продвинулось в изучении новых технологий, позволяющих хранить личную информацию на различных сайтах в сети «интернет» и ознакамливаться с любой доступной информацией о других людях, имея только несколько незначительных данных. Это объясняется тем, что каждый день создаются все более новые информационные ресурсы, программы, благодаря которым у людей есть возможность познать мир, находясь в одной единственной точке. Вместе с этим возникает потребность во введении мер по обеспечению безопасности информации, которую вносят в сеть «Интернет» [1. С. 205].

Основная часть. Несмотря на то, что Интернет дает возможность быстро выполнять различные банковские операции, рассылать и копировать информацию вне зависимости от расстояния, социальные сети оказывают серьезное воздействие на мышление, а иногда это приводит к появлению негативных идей и поведения отдельных людей, которые не граничат с нормами морали и общественной нравственности. Поэтому вполне справедливо говорить о том, что термин «цифровое насилие» имеет место быть [2. С. 205].

В разных источниках данное понятие трактуется по-разному, но имеют общее значение. Например, цифровое насилие – травля с использованием цифровых технологий, повторяющееся поведение, направленное на то, чтобы запугать, разозлить или пристыдить тех, на кого направленно воздействие» или цифровое насилие – акт насилия, который совершается, усугубляется и усиливается частично или полностью с помощью ИКТ технологий или цифровых медиа в отношении лица по признаку его пола. Источники описывают цифровое насилие как преступление против личности с использованием информационных технологий, причем преступление длительного характера, так как воздействие на человека происходит в течение какого-то времени.

Понятия охватывают отдельные виды цифрового насилия: от онлайн-домогательств до «порномести» и цифрового изнасилования. Чтобы было проще ориентироваться в понятиях, нужно классифицировать цифровое насилие по нескольким критериям.

Одним из вида классификации можно считать возраст жертвы цифрового насилия:

1. Дети – до 16 лет. Часто подвергаются кибербуллингу и кибергруммингу (онлайн груминг), а также цифровой бойкот.

Кибербуллинг – целенаправленная травля в интернете, запугивание человека с использованием сети «Интернет»: социальных сетей, мессенджеров, игровых платформ. К сожалению, дети в процессе социализации имеют тенденцию выбирать слабых детей или тех, кто отличается от них самих по какому-либо признаку. Есть случаи, когда кибербуллинг сопровождается цифровым бойкотом, который характеризуется исключением ребенка из групп других детей и полное игнорирование. У такого вида цифрового насилия могут быть квалифицированы по нескольким статьям, в том числе за кибербуллинг предусмотрена уголовная ответственность по нескольким статьям в зависимости от причиненного вреда лицу.

Кибергрумминг – наиболее страшный для ребенка вид цифрового насилия. Это вид сексуального насилия против детей в интернете. Совершеннолетние лица мужского пола знакомятся с малолетними лицами младше 14 лет с целью инициирования сексуального контакта. При груминге преступники могут вступать в прямой личный контакт с малолетними через круг знакомых ребенка и осуществлять развратные действия или оказывая влияние на ребенка. Кибергрумминг происходит преимущественно в сети «Интернет». За подобные преступления лицо может получить как административное наказание в виде штрафа, так и уголовное наказание, в том числе лишение свободы.

2. Лица от 18 до 24 лет. Это категория лиц, которая подвергается большей части цифрового насилия: киберсталкинг и доксинг, сексторшен, порноместь, апскертинг, слатшейминг. К сожалению, по данным Women's Aid более чем у 50% резидентов опроса, которые лично столкнулись с цифровым насилием, оно было связано с прямыми угрозами жизни и здоровью и треть из всех угроз были выполнены.

Киберсталкинг и доксинг схожи между собой – представляет сбор данных о жертве с целью манипуляции потерпевших. Не удивительно, так как прогресс в цифровой среде неизбежно приводит к утечке личной информации лица с различных сайтов, даже тех, которые принято считать безопасными для использования. Хотя, конечно, нельзя говорить о том, что понятия идентичны. Главное различие в том, что киберсталкинг происходит как в сети, когда сталкер отправляет множество сообщений с угрозами о публикации личных данных, которые преступник смог найти, так и в реальной жизни – отправляя вещи и подарки или поджидая где-то на лице. Доксинг работает только в сети.

Сексторшен (или цифровая сексторция) – отдельная форма шантажа, при которой лицо угрожает опубликовать компрометирующую информацию о жертве в сети «Интернет». Часто, преступниками становятся знакомые или близкие жертвы, которые добровольно получили информацию. Так или иначе, подобному насилию могут подвергаться и подростки, которые более подвержены манипуляции с помощью угроз распространения фото родственникам и друзьям, но сообщить в правоохранительные органы не решаются по определенным причинам.

Порноместь – публикация интимных фото и видео материала с целью причинить страдания жертве, а равно как выложено с целью отомстить. Как и в случае с сексторшенгом, интимные материалы публикуются из мести бывшим партером или супругом или другими близкими жертвы. В отдельных случаях порноместь может быть основана на дипфейке. Данное понятие появилось с момента создания продвинутого искусственного интеллекта, так как понятие дипфейка – создание порно контента с жертвой при помощи искусственного интеллекта.

Помимо классификация цифрового насилия по возрастной категории, мы можем классифицировать виды насилия по гендерному признаку.

Изначально, цифровому насилию подвергались в основном женщины, что подтверждается исследованиями организации WNOA с 2000 по 2013 год о том, что от цифрового насилия (а тогда – онлайн-домогательства) пострадали 70% женщин против 25% мужчин. Но в зависимости от половой принадлежности люди подвергаются разным видам цифрового насилия.

1. Мужской пол – чаще подвергаются оскорблениям и унижениям. Это такие виды цифрового насилия как кибербуллинг, понятие которому было приведено ранее в рамках классификации по возрастному признаку. Мужчины чаще сталкиваются с оскорблениями, переходящие в физическую угрозу, которые таковой и остается только в сети, не переходя в реальный физический контакт.

2. Женский пол – к сожалению, женщины подвергаются более серьезным видам цифрового насилия из тех, которые существуют на сегодняшний день. Если мужчины реально сталкиваются только с оскорблениями и унижениями,

то женщины сталкиваются еще и формами сексуального цифрового насилия. По данным организации CCRI, которые напрямую занимаются вопросами онлайн-насилия, только 10% мужчин подверглись порноместе и использованием дипфейка, остальные 90% – женщины.

Заключение. Если резюмировать исследования, проведенные рядом международных организаций, то можно сделать выводы о том, что цифровое насилие в настоящее время стоит наравне с физическим насилием и причиняет столько же ущерба психике [2. С. 206].

Одним из решений данной проблемы в нашем обществе может стать понижение латентности данных преступлений, так как, по тем же исследованиям, жертвы насилия редко обращаются за помощью в уполномоченные организации и сообщают о них администраторами Интернет-площадок. В настоящее время необходимо проводить мероприятия по разъяснению и освещению видов цифрового насилия, как с ним бороться и как правильно реагировать в таких ситуациях, чтобы избежать ущерба, как физического, так и психологического.

Список литературы

1. Шутова А. А. Современные тенденции использования информационно-телекоммуникационной сети в процессе совершения преступления // Пробелы в российском законодательстве. 2015. № 4. С. 205–208. EDN UZFDRT.

2. Абделькарим Я.А. Судебная аргументация как механизм правовой защиты детей от цифрового сексуального насилия и детской порнографии // Journal of Digital Technologies and Law. 2025. Т. 3, № 2. С. 203–221. <https://doi.org/10.21202/jdtl.2025.9>. EDN: gvmhzz.

Трансформация финансового суверенитета: вызовы правового регулирования оборота цифровых активов в России

Аннотация. В статье анализируется влияние цифровых активов на концепцию финансового суверенитета государства. Выдвигается и доказывается тезис о том, что регуляторная политика Российской Федерации представляет собой двоякую концепцию, заключающийся в ограничительном регулировании частных цифровых валют (криптовалют) и в проактивном внедрении государственной цифровой валюты (цифрового рубля) как инструмента для укрепления контроля над национальной денежной системой. На основе формально-юридического и сравнительно-правового анализа рассматриваются ключевые публично-правовые механизмы, применяемые государством, и делается вывод о том, что регулирование цифровых активов является частью более широкого процесса адаптации государственного суверенитета к цифровой эпохе.

Ключевые слова: финансовый суверенитет, цифровые активы, криптовалюта, цифровой рубль, цифровая валюта центрального банка, публичное право, финансовый контроль

R. V. Baitov

Student,

Novosibirsk State University (NSU)

Transformation of financial sovereignty: legal challenges of regulating digital assets in Russia

Abstract. The article analyzes the impact of digital assets on the concept of state financial sovereignty. It proposes and substantiates the thesis that the regulatory policy of the Russian Federation constitutes a dual-track approach. This approach consists of the restrictive regulation of private digital currencies (cryptocurrencies) and the proactive implementation of a state-backed digital currency (the digital ruble) as a tool to strengthen control over the national monetary system. Based on formal legal and comparative analysis, the paper examines key public law mechanisms employed by the state and concludes that the regulation of digital assets is part of a broader process of adapting state sovereignty to the digital era.

Keywords: financial sovereignty, digital assets, cryptocurrency, digital ruble, Central Bank Digital Currency, public law, financial control

Введение. Концепция финансового суверенитета, включающая монополию государства на эмиссию денег и контроль над денежно-кредитной политикой, является одним из ключевых элементов современной государственности. В XXI веке эта концепция проходит через период значительной трансформации,

обусловленной развитием цифровых технологий. Появление и распространение частных цифровых активов, в первую очередь, криптовалют, создает новые условия для функционирования национальных финансовых систем. Их трансграничный и децентрализованный характер влияет на такие традиционные сферы государственного контроля, как валютное регулирование, налогообложение и система противодействия отмыванию доходов и финансированию терроризма (далее – ПОД/ФТ).

В ответ на эти изменения многие государства, включая Россию, приступили к разработке собственных цифровых валют центральных банков (ЦВЦБ). Этот процесс представлял собой попытку адаптировать инструменты денежно-кредитной политики к цифровой экономике и модернизировать национальную платежную инфраструктуру. Таким образом, в правовом поле на данный момент времени формируются два параллельных трека регулирования: один – для частных цифровых активов, другой – для государственной цифровой валюты.

Регуляторная политика Российской Федерации в этой сфере представляет собой сбалансированный двусторонний подход, направленный на адаптацию и укрепление финансового суверенитета в новых условиях.

Первый компонент этого подхода – это ограничительное регулирование частных цифровых активов. Его суть заключается в признании криптовалют в качестве объекта имущественных прав, что позволяет интегрировать их в правовое поле для целей налогообложения и антикоррупционного контроля, но с одновременным запретом на их использование в качестве средства платежа для защиты монополии национального рубля. Второй компонент – это проактивное развитие государственной цифровой валюты, цифрового рубля, как нового инструмента для повышения эффективности и прозрачности публичных финансов и укрепления контроля над национальной денежной системой.

Основная часть

1. Финансовый суверенитет в XXI веке: от монополии на эмиссию к контролю над цифровыми протоколами

1.1. Классическая доктрина финансового суверенитета

Финансовый суверенитет представляет собой неотъемлемую составляющую государственного суверенитета и выражается в праве государства самостоятельно определять и проводить свою денежно-кредитную, бюджетную и налоговую политику. В основе этой доктрины лежит идея о том, что эффективный контроль над финансовой системой является необходимым условием для поддержания экономической стабильности и реализации государственных функций. В российской правовой доктрине традиционно выделяют несколько ключевых элементов, формирующих содержание этого понятия.

Центральным элементом является эмиссионный суверенитет – исключительное право государства в лице его центрального банка на выпуск (эмиссию) национальной денежной единицы. Эта монополия, закреплённая на конституционном уровне, позволяет государству управлять денежной массой и является фундаментом всей национальной денежной системы [12. С. 51].

Наряду с эмиссией, финансовый суверенитет включает в себя полномочия по проведению единой денежно-кредитной политики, направленной на защиту

и обеспечение устойчивости национальной валюты. К этому же блоку относятся бюджетный и налоговый суверенитет – право самостоятельно формировать и исполнять бюджет, а также устанавливать и взимать налоги и сборы. Эти полномочия в совокупности обеспечивают макроэкономическую стабильность и способность государства выполнять свои социальные и экономические функции [12. С. 52–53]. Таким образом, классическая модель финансового суверенитета опирается на централизованные институты и четко определенные правовые механизмы контроля над денежным обращением. Важно подчеркнуть, что эта классическая модель является не просто набором экономических инструментов, но и фундаментальным элементом общественного договора. Монополия государства на эмиссию денег и право взимать налоги в национальной валюте исторически легитимировала само государство, создавая на его территории единое экономическое пространство. Таким образом, финансовый суверенитет – это экономическое отражение монополии государства на легитимное насилие. Эффективный контроль над денежной системой позволяет государству не только финансировать свои прямые функции (оборона, управление), но и проводить масштабную социальную и экономическую политику, перераспределяя ресурсы и сглаживая кризисы. Именно поэтому любые вызовы этой монополии воспринимаются государством не как технические, а как экзистенциальные.

1.2. Вызовы децентрализации

Появление и глобальное распространение частных цифровых валют (криптовалют) формирует принципиально новые вызовы для всех ключевых элементов финансового суверенитета. В отличие от предыдущих финансовых инноваций, которые действовали в рамках существующей государственной системы, криптовалюты предлагают альтернативную, децентрализованную архитектуру, функционирующую вне прямого контроля национальных регуляторов.

Во-первых, прямой вызов направлен на эмиссионную монополию государства. Эмиссия большинства криптовалют, таких как Биткойн, происходит не по решению центрального банка, а на основе заранее заданного криптографического алгоритма (протокола), который не может быть изменен по воле одного участника или государственного органа. Это фактически означает появление частной, алгоритмической формы эмиссии денег, которая напрямую конкурирует с государственной [12. С. 54].

Во-вторых, трансграничная природа и анонимность криптовалютных транзакций создают серьезные препятствия для реализации государством функций валютного контроля и ПОД/ФТ. Операции могут совершаться напрямую между пользователями из разных юрисдикций, минуя традиционных финансовых посредников (банки), которые выступают в роли «привратников» и агентов государственного контроля. Это усложняет отслеживание подозрительных операций и противодействие незаконному выводу капитала [30. С. 745].

В-третьих, указанные характеристики создают риски для налогового суверенитета. Сложность идентификации участников транзакций и определения их налогооблагаемой базы (например, дохода от прироста капитала) открывает возможности для уклонения от уплаты налогов, подрывая доходную часть государственного бюджета [12. С. 55].

Таким образом, криптовалюты следует рассматривать не просто как новый класс активов, а как системный феномен, потенциально способный сформировать параллельную финансовую инфраструктуру, менее прозрачную и подконтрольную государству [30. С. 780]. В экономической теории этот вызов ассоциируется с идеями Ф. фон Хайека о «денационализации денег», который предвосхитил появление частных, конкурирующих с государственными валют. В этой парадигме базовые криптовалюты рассматриваются как аналог «золотого стандарта», а стейблкоины – как современная форма частных денег, что подчеркивает фундаментальность их расхождения с фиатной денежной системой [4. С. 90]. Именно эта системная угроза и послужила катализатором для разработки государствами собственного ответа на данный вызов. Новизна вызова, брошенного криптовалютами, заключается не в каком-то одном из этих факторов, а в их синергетическом сочетании. История знала и частные деньги, и трансграничные системы расчетов, и инструменты для уклонения от налогов. Однако криптовалюты впервые объединили в себе децентрализованную эмиссию, глобальный охват с первого дня существования, криптографическую защиту и высокую степень псевдонимности. Именно эта комбинация создает эффект «идеального шторма» для классической модели суверенитета, поскольку она одновременно подрывает контроль на всех уровнях: эмиссионном, транзакционном и фискальном.

1.3. Цифровые валюты центральных банков (ЦВЦБ) как ответ

Глобальная тенденция по исследованию и разработке цифровых валют центральных банков стала одной из определяющих черт финансового ландшафта 2020-х годов, причем подавляющее большинство центральных банков мира активно изучают эту возможность [25. Р. 501]. Импульс к этому процессу был в значительной степени ускорен появлением частных глобальных стейблкоинов, которые были восприняты государствами как прямая угроза их монетарному суверенитету [23. Р. 77].

В ответ на системные вызовы, исходящие от децентрализованных финансовых инструментов, центральные банки по всему миру инициировали исследования и разработку собственных цифровых валют (ЦВЦБ). Данный процесс представляет собой не просто технологическую модернизацию, а стратегическую попытку государств адаптировать инструменты финансового суверенитета к новой цифровой реальности и сохранить контроль над национальной денежной системой.

ЦВЦБ представляет собой цифровую форму фиатных денег, которая, в отличие от безналичных средств на счетах в коммерческих банках, является прямым обязательством центрального банка перед конечным держателем [14. Р. 87]. Это ключевое отличие позволяет государству сохранить свою центральную роль в платежной системе, предложив населению и бизнесу безопасный и гарантированный государством цифровой платежный инструмент. Таким образом, государство не просто конкурирует с частными цифровыми валютами, но и стремится перехватить технологическую инициативу, интегрировав преимущества цифровизации в существующую финансовую архитектуру.

Согласно комплексному исследованию Международного валютного фонда, основные мотивы центральных банков включают повышение финансовой доступности для населения, увеличение эффективности платежных систем и усиление трансмиссионного механизма денежно-кредитной политики [28. р. 6]. Внедрение ЦВЦБ рассматривается как способ решения нескольких стратегических задач. Во-первых, оно может повысить эффективность и устойчивость национальной платежной системы. Кроме того, на глобальном уровне внедрение ЦВЦБ часто связывают с задачей расширения финансовой инклюзии, то есть предоставления доступа к современным финансовым услугам для населения, не охваченного банковской инфраструктурой, что особенно актуально для развивающихся стран и удаленных территорий [2. С. 70]. Во-вторых, оно предоставляет новые, более гибкие инструменты для проведения денежно-кредитной политики. В-третьих, что особенно важно в контексте суверенитета, оно создает инфраструктуру для более полного и оперативного мониторинга финансовых потоков, повышая прозрачность для целей налогообложения и ПОД/ФТ.

Тот факт, что к 2021 году ведущие экономики мира в рамках G7 выработали общие принципы для разработки розничных ЦВЦБ, подчеркивает, что их внедрение рассматривается как вопрос стратегической важности, затрагивающий основы финансовой стабильности и международного взаимодействия [15]. Таким образом, глобальный тренд на создание ЦВЦБ является прямым ответом на вызовы децентрализации и служит основой для стратегии усиления финансового суверенитета в XXI веке.

2. Стратегия сдерживания: публично-правовые рамки оборота криптовалют в России

2.1. Легализация в качестве «иного имущества»

Российский подход к регулированию криптовалют является ярким примером стратегии сдерживания. Вместо полного запрета, который мог бы привести к уходу рынка в тень, или полной легализации в качестве платежного средства, что создало бы риски для финансового суверенитета, законодатель выбрал компромиссный путь. Основой этого подхода стало принятие Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте...» (далее – Закон о ЦФА), который впервые ввел криптовалюты в правовое поле, но с существенными ограничениями.

До принятия этого закона правовая природа криптовалют была предметом острых дискуссий, что создавало правовую неопределенность [11. С. 145]. Закон о ЦФА разрешил эту неопределенность, определив цифровую валюту как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации... и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных».

Ключевым моментом является то, что, дав легальное определение, законодатель не приравнивал цифровую валюту к деньгам. Напротив, он прямо закрепил ее статус как имущества [10. С. 60]. При этом в российской правовой док-

трине подчеркивается, что такая квалификация является упрощенной. Более глубокий анализ показывает, что правовая природа криптовалюты ближе к особому обязательственному праву. В этой конструкции нет единого эмитента-должника, а обязанными лицами выступают все остальные участники информационной системы, которые в силу правил системы обязуются принимать данную криптовалюту. Ключевое различие между «цифровыми правами» (имеющими конкретного эмитента-должника) и «цифровой валютой» (где должник является распределенным) и легло в основу их разного правового режима в российском законодательстве [7. С. 161]. Такой подход имеет двойственные последствия. С одной стороны, признание криптовалюты имуществом позволяет включать ее в гражданский оборот: она может быть предметом сделок купли-продажи, залога, наследоваться, включаться в конкурсную массу при банкротстве. Это создает основу для ее интеграции в экономику в качестве инвестиционного актива [6. С. 13].

С другой стороны, ключевым элементом стратегии сдерживания стало введение Законом о ЦФА прямого запрета на использование цифровой валюты на территории РФ для оплаты товаров, работ и услуг. Этот запрет направлен непосредственно на защиту монополии рубля как единственного законного платежного средства и на предотвращение рисков для национальной денежной системы [10. С. 61]. Таким образом, правовой режим криптовалют в России был сконструирован таким образом, чтобы, с одной стороны, вывести их из "серой зоны", а с другой – юридически изолировать их от основной денежной системы, ограничив их функционал ролью спекулятивного или инвестиционного актива. По сути, российским законодателем была создана уникальная правовая конструкция «ограниченного допущения». Признав криптовалюту имуществом, государство легализовало сам факт владения ею, что позволило применять к ней нормы о наследовании, банкротстве и, что самое важное для государства, налогообложении. В то же время, запретив ее использование в качестве средства платежа, государство нейтрализовало главную угрозу для своего финансового суверенитета. Такой подход можно охарактеризовать как юридический прагматизм: вместо того чтобы пытаться запретить технологию, которую невозможно полностью контролировать, государство предпочло встроить ее в существующие правовые рамки на своих условиях, максимизируя фискальные выгоды и минимизируя монетарные риски.

2.2. Инструменты публичного контроля

Признав криптовалюту имуществом, государство получило формальные основания для распространения на операции с ней существующих механизмов публичного контроля. Однако применение этих механизмов, разработанных для централизованной финансовой системы с ее институтами (банками), к децентрализованым и анонимным транзакциям крайне затруднено, что дополнительно подчеркивает ограниченный характер "стратегии сдерживания". Основные усилия государства по установлению контроля сосредоточены в следующих сферах:

1. **Налогообложение.** Признание криптовалюты имуществом означает, что доходы физических и юридических лиц от операций с ней (например, от продажи по более высокой цене) подлежат налогообложению. Однако Закон о

ЦФА не установил специальных правил налогообложения, создав правовой вакуум. На практике этот пробел восполняется разъяснениями Министерства финансов и Федеральной налоговой службы, которые носят характер "мягкого права". Основные проблемы заключаются в сложности документального подтверждения расходов на приобретение криптовалюты (для уменьшения налоговой базы) и определения ее рыночной стоимости на момент совершения сделки, что создает правовую неопределенность для налогоплательщиков [10. С. 63].

2. Противодействие отмыванию доходов (ПОД/ФТ). Закон о ЦФА прямо указывает на то, что оборот цифровых валют должен соответствовать требованиям законодательства о ПОД/ФТ (Федеральный закон № 115-ФЗ). Однако применение норм, разработанных для централизованной финансовой системы, к децентрализованным транзакциям крайне затруднено. Это усугубляется техническими трудностями, с которыми сталкиваются правоохранительные органы при отслеживании транзакций между различными блокчейнами и установлении связи между псевдонимными адресами и реальными физическими лицами, что подробно задокументировано в аналитических обзорах [22. Р. 5]. Государственный контроль в основном сосредоточен на операторах обмена цифровых валют на фиатные деньги (криптовбиржах, обменниках), которые обязаны проводить идентификацию клиентов. Тем не менее, значительная часть оборота, включая прямые P2P-переводы, остается вне эффективного надзора, что ограничивает действенность системы ПОД/ФТ в этой сфере [10. С. 62]. Данные опасения не являются уникальными для России; международные институты, такие как МВФ, также подчеркивают значительные риски, которые нерегулируемые стейблкоины создают для финансовой стабильности и целостности глобальной финансовой системы, особенно в контексте ПОД/ФТ [12. Р. 12].

3. Антикоррупционный контроль. С 2021 года государственные служащие и иные лица, подпадающие под действие антикоррупционного законодательства, обязаны декларировать принадлежащую им цифровую валюту. Эта мера направлена на повышение прозрачности активов чиновников и является логическим следствием признания криптовалюты имуществом. Однако, как и в случае с ПОД/ФТ, практическая реализация этого требования сталкивается с проблемой верификации. Проверить достоверность и полноту сведений, предоставленных в декларации, особенно если активы хранятся на некастодиальных кошельках, для контролирующих органов представляется крайне сложной задачей [10. С. 64].

2.3. Сравнительно-правовой аспект

Специфика российской «стратегии сдерживания» становится более отчетливой при ее сравнении с основными международными подходами к регулированию криптовалют. Глобальный ландшафт в этой сфере крайне неоднороден и варьируется от всеобъемлющего регулирования до полного запрета.

На одном полюсе находится Европейский Союз, который выбрал путь создания комплексной и детализированной регуляторной среды. Принятый Регламент о рынках криптоактивов (MiCA) устанавливает единые правила для всего союза, вводя режим лицензирования для поставщиков услуг в сфере криптоактивов (CASPs), а также требования к эмитентам стейблкоинов, защите прав по-

требителей и обеспечению рыночной целостности [21]. Цель ЕС – не столько сдержать, сколько упорядочить и легализовать рынок, создав для него прозрачные и предсказуемые правила игры.

На противоположном полюсе находится Китай, который последовательно реализует политику полного запрета. В КНР запрещены не только операции по обмену криптовалют и их использование в качестве платежного средства, но и деятельность по их добыче (майнингу). Такой жесткий подход мотивирован стремлением обеспечить полную финансовую стабильность, предотвратить отток капитала из страны и устранить любую конкуренцию для государственной цифровой валюты – цифрового юаня.

Соединенные Штаты демонстрируют третий, фрагментированный подход, основанный на применении уже существующего законодательства. Регулирование осуществляется различными ведомствами, в первую очередь Комиссией по ценным бумагам и биржам (SEC) и Комиссией по торговле товарными фьючерсами (CFTC), которые рассматривают криптовалюты либо как ценные бумаги, либо как товары [29]. Это приводит к так называемому «регулированию через правоприменение» (regulation by enforcement), где правовой статус многих активов определяется в ходе судебных разбирательств, что создает высокий уровень неопределенности для участников рынка [26]. Эта регуляторная неопределенность находит отражение и в продолжающихся дебатах внутри самих США, что подчеркивается в дискуссионном документе Федеральной резервной системы, где указывается на нерешенные вопросы конфиденциальности, финансовой стабильности и надлежащей роли государства в цифровой платежной системе [17. р. 18].

Наконец, существует дозволительная модель (например, в Швейцарии), которая создает максимально благоприятные условия для инноваций при соблюдении базовых требований в сфере ПОД/ФТ. На этом фоне российская модель предстает как особый «срединный путь». Она значительно жестче, чем комплексный подход ЕС и фрагментированный подход США, из-за прямого запрета на платежи, что является ключевым элементом сдерживания. Однако она не является тотальным запретом, как в Китае, поскольку признает криптовалюты имуществом и допускает их оборот в качестве инвестиционного актива. Такое позиционирование подтверждает наш тезис о целенаправленной стратегии, направленной на изоляцию криптовалют от национальной денежной системы при сохранении частичного контроля над ними как над объектами собственности.

3. Цифровой рубль как инструмент усиления финансового суверенитета

3.1. Правовая природа и статус цифрового рубля

Если регулирование криптовалют демонстрирует стремление государства минимизировать риски путем изоляции нового феномена от национальной денежной системы, то проект цифрового рубля представляет собой противоположную стратегию – проактивную интеграцию цифровых технологий для укрепления и модернизации государственного контроля. Правовая основа для этого была заложена летом 2023 года с принятием пакета федеральных законов,

внесших изменения в Гражданский кодекс Российской Федерации, законодательство о национальной платежной системе и ряд других актов.

Ключевым нововведением стало официальное признание цифрового рубля третьей формой национальной валюты, наряду с наличными и безналичными денежными средствами. Данный законодательный шаг напрямую решает фундаментальную правовую задачу, определенную Международным валютным фондом: необходимость четкого закрепления статуса ЦВЦБ в национальном валютном законодательстве и наделения центрального банка явными полномочиями на его эмиссию [19. Р. 10]. В отличие от криптовалют, которым был присвоен статус «иного имущества», цифровой рубль с юридической точки зрения был признан именно деньгами [3. С. 11]. Эта фундаментальная разница определяет его правовой режим: он обладает статусом законного платежного средства, обязательного к приему по номинальной стоимости на всей территории Российской Федерации.

С точки зрения правовой природы, цифровой рубль представляет собой прямое обязательство Банка России перед его владельцем. Это отличает его от безналичных денег, которые являются обязательством коммерческого банка перед клиентом по его счету. Цифровые рубли учитываются на цифровых кошельках граждан и организаций, открытых на специальной платформе, оператором которой является Банк России [9. С. 50]. Этот выбор в пользу централизованной архитектуры соответствует одной из ключевых моделей, выделенных Банком международных расчетов, и противопоставляется гибридным или косвенным моделям, где коммерческие банки играют более значительную операционную роль [14. Р. 91]. Такая одноуровневая модель расчетов, где Центральный банк выступает не только эмитентом, но и оператором всей системы, обеспечивает максимальный уровень централизации и государственного контроля над денежным обращением.

Таким образом, законодатель целенаправленно сконструировал правовую модель цифрового рубля как прямого государственного обязательства, полностью интегрированного в систему объектов гражданских прав в качестве денег [3. С. 15]. Это создало правовую основу для его использования не просто как нового платежного инструмента, а как многофункционального механизма для реализации задач публичного права, что стало ядром стратегии утверждения финансового суверенитета.

3.2. Цифровой рубль как инструмент внутреннего контроля и внешнего влияния.

Централизованная архитектура платформы цифрового рубля и ее технологические особенности, такие как программируемость расчетов, открывают для государства принципиально новые возможности по осуществлению публичного контроля, которые были недоступны при использовании наличных или традиционных безналичных денег. Эти возможности можно разделить на две ключевые сферы: усиление внутреннего контроля над публичными финансами и утверждение суверенитета на международной арене.

1. Контроль за целевым расходованием средств через смарт-контракты. Платформа цифрового рубля позволяет использовать технологию смарт-

контрактов – алгоритмов, которые автоматически исполняют заданные условия сделки. Это создает уникальную возможность для так называемого «окрашивания» денег. Государство получает технический инструмент для контроля за целевым использованием бюджетных средств, субсидий, пособий и средств, выделяемых в рамках государственных контрактов. Например, социальная выплата может быть запрограммирована таким образом, что ее можно будет потратить только на определенные категории товаров (например, продукты питания или лекарства), а оплата по госконтракту будет автоматически переведена исполнителю только после подтверждения выполнения определенного этапа работ. Это радикально повышает прозрачность публичных финансов и снижает риски нецелевого расходования и коррупции [9. С. 51–52]. Помимо повышения прозрачности публичных финансов, внедрение цифрового рубля обещает и прямые экономические выгоды для бизнеса, в первую очередь за счет сокращения транзакционных издержек. Ожидается, что тарифы на операции в цифровых рублях, в частности на эквайринг, будут значительно ниже действующих, что снизит нагрузку на предприятия [5. С. 47].

2. Повышение эффективности налогового администрирования и ПОД/ФТ. Поскольку оператором единой платформы является Банк России, все транзакции в цифровых рублях являются полностью прослеживаемыми для государственных органов (в рамках их законных полномочий). Это значительно упрощает для Федеральной налоговой службы и Росфинмониторинга задачи по мониторингу финансовых потоков, выявлению схем уклонения от уплаты налогов и пресечению операций, связанных с легализацией преступных доходов. Прозрачность системы цифрового рубля создает среду, менее благоприятную для теневой экономики, по сравнению с наличными деньгами [14. С. 90]. При этом, как отмечает Банк международных расчетов, полномасштабное внедрение ЦВЦБ способно оказать существенное макроэкономическое воздействие, затронув структуру банковского сектора и инструментарий денежно-кредитной политики, что требует от регулятора тщательной калибровки [18. р. 12]. Таким образом, прозрачность системы цифрового рубля создает среду, менее благоприятную для теневой экономики. Возможность отслеживания денежных потоков и целевого расходования средств позиционируется как эффективное средство борьбы с теневой экономикой, что способствует пополнению бюджета и снижению коррупционных рисков [5. С. 46].

Наряду с внутренними задачами, в условиях глобальной финансовой нестабильности и санкционных ограничений цифровой рубль рассматривается как потенциальный инструмент для утверждения суверенитета на международной арене. Создание технологических «мостов» между платформами ЦВЦБ дружественных стран может позволить проводить трансграничные расчеты без участия традиционной, контролируемой западными странами инфраструктуры, такой как SWIFT. В этом контексте активно исследуется возможность использования цифровых валют в международных расчетах на примере объединения БРИКС. Появление государственных цифровых валют придает новый импульс созданию альтернативной платежной инфраструктуры, способной, как отмечают исследователи, смягчить санкционное давление и повысить эффективность трансграничных экономических

отношений [4. С. 103]. Опыт Китая, активно продвигающего свой цифровой юань для международных расчетов, показывает, что ЦВЦБ могут стать важным элементом в формировании альтернативных глобальных финансовых систем. Этот подход контрастирует с позицией стран G7, которые делают акцент на совместимости ЦВЦБ с существующими международными финансовыми институтами, что подчеркивает различие в стратегических целях [24].

Таким образом, цифровой рубль является не просто платежным средством, а влечет за собой создание многофункциональной платформой, которая предоставляет государству беспрецедентные инструменты для контроля, повышая его суверенные возможности как во внутренней, так и во внешней финансовой политике. Тем самым, цифровой рубль представляет собой нечто большее, чем просто третья форма денег. Это – переход от косвенного контроля над финансовой системой (через регулирование банков-посредников) к потенциально прямому администрированию денежного обращения. Это открывает новую страницу во взаимоотношениях государства, бизнеса и гражданина. С одной стороны, это сулит беспрецедентную прозрачность и эффективность в сфере публичных финансов. С другой – ставит перед обществом и правовой доктриной сложные вопросы о границах государственного вмешательства, защите финансовой приватности и риске создания «цифрового паноптикума». Поиск баланса между эффективностью контроля и защитой прав граждан станет центральной задачей публичного права в эпоху государственных цифровых валют.

Заключение. Проведенное исследование показало, что появление и развитие цифровых активов представляет собой фундаментальный вызов для классической доктрины финансового суверенитета. В ответ на этот вызов Российская Федерация формирует целенаправленную и комплексную политику, которую можно охарактеризовать как сбалансированный двусторонний подход. Данный подход направлен не на простое реагирование на технологические изменения, а на адаптацию и утверждение суверенных прав государства в новой цифровой финансовой реальности.

В рамках исследования был подтвержден центральный тезис о двусоставной природе этой стратегии. Первый ее элемент – ограничительное регулирование частных цифровых валют. Признав их имуществом, но запретив использование в качестве средства платежа, законодатель решил ключевую задачу: минимизировал угрозы для монополии национальной валюты и стабильности денежной системы, одновременно интегрировав криптовалюты в правовое поле для целей фискального и антикоррупционного контроля. Это позволило установить над ними частичный государственный надзор, не легализуя их в качестве полноценного финансового инструмента.

Второй, проактивный элемент – это развитие государственной цифровой валюты. Проект цифрового рубля является стратегическим ответом на вызовы децентрализации. Его правовая модель как третьей формы денег и прямого обязательства Банка России, а также его технологический потенциал (программируемость, прослеживаемость) создают основу для беспрецедентного усиления публичного контроля. Цифровой рубль рассматривается не только как средство модернизации платежной системы, но и как инструмент для повышения про-

зрачности бюджетных расходов, эффективности налогового администрирования и укрепления позиций России в международных расчетах.

Вместе с тем, реализация данной стратегии сопряжена с рядом нерешенных проблем. Правовое регулирование частных криптовалют остается фрагментарным, а практическое правоприменение в сферах налогообложения и ПОД/ФТ сталкивается со значительными трудностями. В свою очередь, полномасштабное внедрение цифрового рубля ставит сложные вопросы, связанные с обеспечением кибербезопасности, защитой персональных данных, а также с обеспечением высочайшего уровня кибербезопасности всей платформы. Как показывает практика взломов криптовалютных проектов, обеспечение безопасности централизованной системы государственной важности потребует значительных и постоянных инвестиций, что является одним из ключевых вызовов при внедрении цифрового рубля [1. С. 146], и необходимостью соблюдения баланса между повышением прозрачности и защитой прав граждан.

Анализ двустороннего подхода российского регулятора вскрывает центральный парадокс современной государственной политики в сфере цифровых финансов. С одной стороны, государство в лице Центрального банка активно заимствует технологическую оболочку частных цифровых активов: идеи токенизации, криптографической защиты и даже программируемых денег (смарт-контрактов), которые лежат в основе проекта цифрового рубля. С другой стороны, оно категорически отвергает их идеологическое ядро – децентрализацию, анонимность и свободу от государственного контроля.

Этот парадокс не является противоречием, а отражает суть стратегии. Проект цифрового рубля – это, по своей сути, проект ре-централизации, использующий инструменты, созданные для децентрализации. Государство целенаправленно «перехватывает» технологическую инновацию, которая угрожала его суверенитету, и пересобирает ее таким образом, чтобы она, наоборот, служила его укреплению. Это демонстрирует, как в XXI веке адаптация суверенитета происходит не через запрет новых технологий, а через их освоение и перенаправление их потенциала на службу публичным, а не частным интересам.

В конечном итоге, правовое регулирование оборота цифровых активов перестает быть узкотехнической задачей и становится одним из центральных направлений государственной политики в XXI веке. Дальнейшее развитие законодательства и практики в этой сфере будет определять контуры финансового суверенитета России на десятилетия вперед, отражая постоянный поиск баланса между императивом государственного контроля, потребностями цифровой экономики и правами участников оборота.

Список литературы

1. Алиева Н. М. Цифровая национальная валюта – новая форма расчетов // *Journal of Monetary Economics and Management*. 2025. № 1. С. 145–149.
2. Безуглая В. А. Влияние создания и внедрения цифровых валют на глобальную экономику // *Вестник Прикамского социального института*. 2025. № 1. С. 67–72.

3. Василевская Л. Ю. Цифровой рубль: взгляд цивилиста на проблему // Lex Russica. 2023. Т. 76. № 1. С. 9–19.
4. Васильев С. А. Рынок цифровых валют как фактор трансформации архитектуры денежных систем // Вопросы теоретической экономики. 2025. № 2. С. 87–109.
5. Григорьев В. В. Преимущества и недостатки цифрового рубля // Экономика. Налоги. Право. 2023. Т. 16. № 5. С. 43–50.
6. Ефимова Л. Г. Некоторые аспекты правовой природы криптовалют // Юрист. 2019. № 3. С. 12–19.
7. Зайнутдинова Е. В. Цифровые права и цифровая валюта в российском праве: вопросы правовой природы и соотношения // Legal Concept = Правовая парадигма. 2022. Т. 21. № 4. С. 159–167. DOI: <https://doi.org/10.15688/lc.jvolsu.2022.4.22>
8. Зайнутдинова Е.В. Модели правового регулирования оборота цифровых прав и цифровой валюты // Право. Журнал Высшей школы экономики. 2023. Том 16. № 4. С. 149–182. DOI:10.17323/2072–8166.2023.4.149.182
9. Рождественская Т. Э., Гузнов А. Г. Правовое регулирование цифрового рубля // Актуальные проблемы российского права. 2024. Т. 19. № 1. С. 48–55.
10. Рождественская Т. Э., Гузнов А. Г. Цифровая валюта: особенности регулирования в Российской Федерации // Правоприменение. 2021. Т. 5. № 1. С. 58–67.
11. Савельев А. И. Криптовалюты в системе объектов гражданских прав // Закон. 2017. № 8. С. 131–147.
12. Перепелица, М. А. Финансовый суверенитет государства в условиях цифровизации национальной валюты / М. А. Перепелица // Образование. Наука. Научные кадры. – 2022. – № 4. – С. 122–126. – DOI 10.56539/20733305_2022_4_122. – EDN GKGWOY.
13. Al-Amine M. Regulating the Crypto Ecosystem: The Case of Stablecoins and Arrangements // IMF FinTech Notes. 2022. No. 22/08. 28 p.
14. Auer R. The technology of retail central bank digital currency / R. Auer, R. Böhme // BIS Quarterly Review. 2020. March. pp. 85–100.
15. Auer R., Böhme R., Cornelli G., Frost J. Central bank digital currencies: motives, economic implications and the research opportunities. Basel: BIS. 2021. 46 p. (BIS Working Paper No. 976).
16. Bank for international settlements. Rise of the central bank digital currencies. Basel: BIS. 2020. 39 p. (BIS Working Paper No. 880).
17. Board of governors of the federal reserve system. Money and payments: the u.s. dollar in the age of digital transformation. Washington, DC: Federal Reserve. 2022. 40 p.
18. Borio C. Central bank digital currencies: motives, economic implications and the research opportunities // BIS Working Paper. 2021. No. 976. 28 p.
19. Bossu W., Itatani M., Margulis C., Rossi A., Weenink H., Yoshinaga A. Legal aspects of central bank digital currency: central bank and monetary law considerations. Washington, DC: International Monetary Fund. 2020. 36 p. (IMF Working Paper No. 20/254).

20. Chen H., Siklos P. Central bank digital currency: a review and some macro-financial implications. Canberra: Centre for Applied Macroeconomic Analysis. 2021. 35 p. (CAMA Working Paper No. 12/2022).
21. Council of the EU. Regulation on markets in crypto-assets (MiCA) : 2020/0265(COD) 2020. [Электронный ресурс] URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593> (дата обращения: 18.08.2025).
22. Courtois N., Gradon K., Schmeh K. Crypto currency regulation and law enforcement perspectives. London: University College London. 2021. 27 p.
23. Eichengreen B., Viswanath-Natraj G. Stablecoins and central bank digital currencies: policy and regulatory challenges // Asian Economic Policy Review. 2022. Vol. 17. № 1. pp. 70–90. – DOI: 10.1111/aep.12365.
24. G7 finance ministers and central bank governors. Public policy principles for retail central bank digital currencies. G7 Report. 2021. [Электронный ресурс] URL: <https://www.gov.uk/government/publications/g7-public-policy-principles-for-retail-central-bank-digital-currencies> (дата обращения: 18.08.2025).
25. Garzoni A., Natarajan H., et al. The rise in popularity of central bank digital currencies: a systematic review // Journal of Economic Literature Review. 2024. Vol. 62. № 3. pp. 501–528. – DOI: 10.1186/s40854-024-00569-9.
26. Guseva Y. Regulatory fragmentation: investor reaction to sec and cftc enforcement in crypto markets / Y. Guseva, I. Hutton // Boston College Law Review. 2023. Vol. 64. pp. 1555–1618.
27. International Monetary Fund. Regulating the crypto ecosystem: the case of stablecoins and arrangements. Washington, DC: IMF. 2022. 28 p. (FinTech Notes).
28. Kiff J., Alwazir J., Davidovic S., Farias A., Khan M. A survey of research on retail central bank digital currency. Washington, DC: International Monetary Fund. 2020. 42 p. (IMF Working Paper No. 20/104).
29. Moffett T. A. CFTC & SEC: the wild west of cryptocurrency regulation // University of Richmond Law Review. 2023. Vol. 57. pp. 713–743.
30. Omarova S. T. New tech v. new deal: fintech as a systemic phenomenon // Yale Journal on Regulation. 2019. Vol. 36. No. 2. pp. 735–797.

Проблемные аспекты правового регулирования click-wrap соглашений

Аннотация. В работе рассматривается правовая природа click-wrap соглашений и проводится сравнительно-правовой анализ соответствия таких договоров основным принципам договорного права. В исследовании затрагиваются основные недостатки click-wrap соглашений и проблемы, связанные с нарушением прав и законных интересов потребителей. Автором предлагаются идеи и концепции, реализация которых, посредством применения комплексного подхода к решению актуальных проблем, поспособствует развитию механизма правового регулирования click-wrap соглашений в России.

Ключевые слова: цифровые технологии, цифровизация, договорное право, сделки, законодательство, дистанционные договоры, защита прав

P. S. Baishev,

officer cadet,

Ural Law Institute of the Ministry of Internal Affairs of Russia,

Problematic aspects of the legal regulation of click-wrap agreements

Abstract. The paper examines the legal nature of click-wrap agreements and provides a comparative legal analysis of the compliance of such agreements with the basic principles of contract law. The study highlights the main disadvantages of click-wrap agreements and problems related to violations of the rights and legitimate interests of consumers. The author suggests ideas and concepts, the implementation of which, through the application of an integrated approach to solving current problems, will contribute to the development of the mechanism of legal regulation of click-wrap agreements in Russia.

Keywords: digital technologies, digitalization, contract law, transactions, legislation, distance contracts, protection of rights

Введение. Согласно статистике DataReportal, указанной по состоянию на январь 2025 года, в России количество интернет-пользователей составило 133 миллиона человек, а уровень проникновения интернета – 92,2% [8]. Данный феномен в очередной раз подчеркивает темпы цифровизации населения, что в свою очередь отражается в вовлеченности людей в цифровое пространство. Цифровизация состоит не только в масштабном распространении Интернета или же смартфонов, но и во внедрении современных цифровых технологий во

все сферы жизнедеятельности человека, начиная от промышленных комплексов и заканчивая правовой наукой.

Основная часть. Одним из плодов цифровизации выступает электронная коммерция, неотделимо связанная с появлением Интернета. Н. В. Рубцова, проводя анализ понятия «электронная коммерция», определяет ее в общих чертах как, деятельность, связанную с использованием информационных технологий и Интернета для осуществления коммерческих операций [2. С. 24]. Исходя из материалов исследования, проведенного С. Н. Косниковым, Д. А. Королевым, Е. Н. Чивви и Д. Ю. Разумовой, можно заметить, что торговля при помощи интернет-пространства зародилась в России в начале 90-х годов [1. С. 144–145]. Чуть позже, в 1998 году, в Российской Федерации будет основан один из крупнейших маркетплейсов настоящего времени – Ozon.

Именно такие торговые площадки постепенно становятся инструментом цифровизации не только всей жизни населения, но и правовой науки. Поскольку деятельность маркетплейсов и соответствует нормам права, в частности совпадая с основными положениями договорного права, однако, из-за трансформации самих соглашений из классического бумажного формата в формат цифровой, произошла и правовая эволюция. Так, лишь в 2019 году были внесены изменения в Гражданский кодекс Российской Федерации (далее по тексту – ГК РФ), которыми были закреплены положения о заключении договоров при помощи электронных или иных технических средств, тем самым произошел толчок на пути цифровизации права [4]. Одним из таких изменений стало внесение поправок в п. 1 ст. 160 ГК РФ, где теперь письменная форма сделки стала считаться соблюденной и при заключении соглашения посредством использования электронных и иных технических средств.

Затрагивая недавнее изменение законодательных актов, стоит отметить, что одной из ключевых проблем click-wrap выступало также навязывание товаров и услуг потребителю, в том числе посредством проставления продавцом автоматических отметок о согласии потребителя с условиями сделки, однако с принятием Федерального закона от 7 апреля 2025 г. № 69 «О внесении изменений в статью 16 Закона Российской Федерации «О защите прав потребителей» данная ситуация изменилась, в связи с введением запрета таковой деятельности [7]. Такое решение законодателя мотивировано необходимостью защиты прав потребителей, что в свою очередь существенно продвинуло вперед механизм защиты прав покупателей.

В настоящее время для заключения соглашения в интернете достаточно нажатия кнопки «Я согласен» или же постановки символа в чекбоксе, именно так можно определить понятие «click-wrap». Формулируя дефиницию click-wrap соглашений, следует понимать, что они представляют собой договоры, составленные в электронной форме при помощи технических средств, принцип подписания которых состоит в реакции пользователя на предложенные условия путем проставления отметки в специально установленном фрагменте интерфейса.

Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека определяет click-wrap договор как соглашение, заключенное путем щелчка мышью по клавише «Я согласен», если это сопровождается

текстом такого договора и описанием ценовых и иных условий сделки [3]. При этом информация ведомства содержит также два ключевых критерия, характеризующих добросовестность и осознанность соглашения:

- к соглашению была приложена полная и достоверная информация о предлагаемой услуге, которая без дополнительных переходов;

- в соглашении нет заранее сделанных отметок, которые лишают потребителя возможности отказаться от дополнительных услуг.

В современном обществе люди все чаще и чаще совершают сделки при помощи гаджетов и технических устройств, именно поэтому click-wrap соглашения стали одной из наиболее распространенных форм заключения договора. Данную форму соглашения можно встретить буквально в каждом месте, при оформлении подписки на онлайн-кинотеатр, продлении или оформлении пакета связи у мобильного оператора, использовании онлайн-платформ по продаже различных товаров. Ключевая особенность click-wrap – простота использования, как для продавца, так и для покупателя.

Однако, к сожалению, события объективной реальности развиваются значительно быстрее правовой системы, что часто сказывается на правовом регулировании некоторых институтов, а как следствие и на защите прав потребителей. Все дело в том, что правовая природа click-wrap соглашений вызывает противоречия в доктрине гражданского права и сложности в правоприменительной деятельности.

Исходя из конструкции соглашения, click-wrap следует относить к категории договоров присоединения, где субъектами правоотношений выступают две стороны, одна из которых предлагает условия, а вторая принимает их без возможности внесения изменений, что нормативно закреплено в ст. 428 ГК РФ. Таким образом, соглашение состоит из двух элементов акцепта и оферты, при этом настоящим кодексом состояние акцепта в данном случае не регламентировано. Так, даже клавиша «зарегистрироваться» в ряде случаев выступает в качестве согласия лица с предложенными условиями.

Хотя click-wrap соглашения и направлены на потребителей, но считать их безоговорочно публичными нельзя, достаточно вспомнить, что для приобретения некоторых видов товаров и услуг, лицо должно соответствовать определенным критериям, например, чтобы воспользоваться услугами каршеринга, субъект должен иметь документ, удостоверяющий его права на управление транспортным средством – водительские права.

Одна из проблем click-wrap – слабая защищенность механизма при эксплуатации его несовершеннолетними. Так, сложность в данном случае состоит в том, что верификация пользователя в настоящее время не осуществляется. Взяв аккаунт родителя, несовершеннолетний может запросто приобрести товар, способный причинить вред ему и окружающим, ввиду отсутствия должного понимания у лица или непригодный для использования лицами, не достигшими восемнадцатилетнего возраста.

В соответствии с пунктом «б» статьи 447 постановления Правительства Российской Федерации от 16 сентября 2020 г. № 1479 «Об утверждении Правил противопожарного режима в Российской Федерации», продажа пиротехниче-

ских изделий лицам, не достигшим 16-летнего возраста (если производителем не установлено другое возрастное ограничение) запрещена, тогда как на маркетплейсах, такой субъект может приобрести данный товар, невзирая на имеющиеся ограничения [5]. Так, приобретая продукт, он первоначально столкнется с вопросом о подтверждении его совершеннолетия, на что получит сообщение на экран своего устройства, где, нажав кнопку «Подтвердить» и, заказав посылку в постамат, минуя ограничения, введенные для обеспечения его же безопасности. В конечном итоге происходит ситуация, при которой даже не используя аккаунт взрослого, ребенок может приобрести запрещенную для него продукцию, что в дальнейшем может повлечь негативные последствия, примером которых является инцидент, произошедший в сентябре 2024 года в Северной Осетии, когда семилетний мальчик, пытаясь взорвать пиротехнические средства остался без кисти [6]. Таким образом, мы видим актуальную проблему click-wrap – отсутствие верификации субъекта (покупателя).

Среди прочих актуальных проблем таких соглашений стоит выделить именно те, которые затрагивают в большинстве своем права и законные интересы потребителей. Так, понятие акцепта в договорах click-wrap крайне обширно и не имеет определенного толкования, что делает покупателя в данном случае уязвимым к ошибочным действиям, поскольку в разных случаях нажатие на кнопку может быть и как просто констатацией факта, и как соглашением с условиями договора. Именно поэтому в данном случае стоит рассматривать введение обязательного требования к участникам правоотношений, использующим click-wrap в своих соглашениях, а именно их обязанность указывать в условиях договора перечень действий, которые следует признавать акцептом. Данная проблема имеет свое отражение не только в действиях потребителей, но и продавцов, поскольку так они смогут обезопасить свою деятельность и в случае попытки оспорить соглашения будут иметь возможность заявить об указании условий в соглашении и не понесут убытков.

В продолжение вопроса о защите прав потребителей стоит отметить также и возможность лица после подписания документа ознакомиться с материалами соглашения и иметь к ним доступ на протяжении всего сотрудничества. Суть сложности заключается в том, что после нажатия на кнопку согласия, возможность прочтения документа пропадает. В таком случае необходимым и наиболее эффективным является дублирование условий соглашения на адрес электронной почты потребителя, которую он оставляет при регистрации аккаунта. Так, в случае необходимости, лицо сможет в нужный момент открыть материалы соглашения и тем самым защитить нарушенные права. К положениям вопроса о возможности ознакомления лица с условиями договора стоит отнести также роль дизайна самой страницы ресурса, на котором формируется документ. Следует отмечать необходимость корректного оформления презентуемой страницы, в том числе обязательное наличие на ней гиперссылок для ознакомления пользователя со всеми условиями соглашения или же, наличие обязательного к прочтению скролл-файла, открывающегося при попытке дать покупателем свое согласие, что в очередной раз позволит обезопасить его от непреднамеренного нажатия на кнопку-подтверждение.

Обеспечение возможности установления личности контрагента также считает одной из актуальных проблем click-wrap соглашений, что отчетливо демонстрирует пример с приобретением несовершеннолетним товар на маркетплейсах, где программа никак не может идентифицировать пользователя. При этом к данной ситуации также стоит относить случаи заключения соглашения третьим лицом, когда согласие на сделку хотя и дано с аккаунта пользователя, однако условия договора подтверждал отнюдь не владелец страницы.

Из этого следует еще одна проблема – отсутствие механизма обязательного подтверждения волеизъявления лица, что в некоторых случаях может поставить его права и интересы под угрозу. Введение обязательной двухфакторной аутентификации позволит избежать неправомерных действий в отношении таких лиц и поспособствует исключению случаев оформления потребителями случайных соглашений.

Заключение. Таким образом, модель click-wrap в настоящее время активно развивается зачастую в сфере электронной коммерции, на долю которой приходится весомый процент затрат потребителей, что свидетельствует о высоком уровне эксплуатации таких соглашений. Стоит отметить, что сама модель не имеет полноценного механизма правового регулирования, что подвергает под угрозу права и интересы населения, использующего данный способ заключения договора. Предложенные в работе концепции внесли бы весомый вклад в данный механизм, что способствовало бы защите не только потребителей, но и продавцов, поскольку при заключении соглашений click-wrap, продавец также может понести убытки, если покупатель подаст в суд. Хотелось бы отметить, что дальнейшее развитие отмеченного института важно для дальнейшего развития цифровой экономики России, а также защите прав и интересов лиц ее населяющих.

Список литературы

1. Косников С. Н., Королев Д. А., Чивви Е. Н., Разумова Д. Ю. История электронной коммерции в России и за рубежом // ЕГИ. 2022. №6. С. 144–147.
2. Рубцова Н. В. Электронная коммерция в фокусе соответствия теории и практики ее исследования в России // Вопросы медиабизнеса. 2025. №2. С. 20–28.
3. Об особенностях click-wrap-соглашений: информация Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека от 5 ноября 2020 г. // Информационно-правовой портал Гарант. URL: <https://www.garant.ru> (дата обращения: 21.07.2025).
4. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18 марта 2019 № 34-ФЗ // Справочная правовая система Консультант Плюс. – URL: <https://www.consultant.ru> (дата обращения: 22.07.2025).
5. Об утверждении Правил противопожарного режима в Российской Федерации: Постановление Правительства РФ от 16 сентября 2020 г. № 1479 // Справочная правовая система Консультант Плюс. URL: <https://www.consultant.ru> (дата обращения: 22.07.2025).

6. Спасти кисть не удалось: игра с пиротехникой оставила семилетнего ребенка инвалидом в Северной Осетии. Комсомольская правда [Электронный ресурс]. URL: <https://www.stav.kp.ru>

7. О внесении изменений в статью 16 Закона Российской Федерации «О защите прав потребителей: Федеральный закон от 07 апреля 2025 № 69-ФЗ // Справочная правовая система Консультант Плюс. URL: <https://www.consultant.ru> (дата обращения: 18.07.2025).

8. Internet Usage Statistics 2025 [Электронный ресурс]. URL: <https://www.demandsage.com>

Е. А. Бенчук,
студент,
Санкт-Петербургский политехнический университет
Петра Великого

Алгоритмические субъекты: правовые модели ответственности и практические альтернативы

Аннотация. Статья анализирует идею признания автономных алгоритмов и искусственных интеллектуальных систем в качестве самостоятельных юридических субъектов. Рассматриваются существующие нормативные инструменты (в частности, Директивы ЕС, законы штатов в США), судебная практика (кейсы DABUS, Ooki DAO), а также предлагаются альтернативные модели – через использование корпоративных “оболочек”, усиление ответственности производителей, введение страховых обязательств, установление административного режима.

Ключевые слова: право, цифровые технологии, искусственный интеллект, алгоритмы, субъект права, ответственность, судебная практика

Е. А. Benchuk,
student,
Peter the Great St. Petersburg Polytechnic University

Algorithmic entities: legal models of liability and practical alternatives

Abstract. The article analyzes the idea of recognizing autonomous algorithms and artificial intelligence systems (AI) as independent legal entities. It examines existing regulatory instruments (in particular, EU Directives, state laws in the USA), court cases (DABUS, Ooki DAO), and proposes alternative models through corporate shells, strict manufacturer liability, insurance obligations, and administrative regimes.

Keywords: law, digital technologies, artificial intelligence, algorithms, legal entity, liability, judicial practice

Введение. Развитие технологий искусственного интеллекта в последнее десятилетие поставило перед правом вопрос о том, каким образом следует регулировать деятельность таких систем. Современные технологии – автономные алгоритмы, DAO, генеративный искусственный интеллект – все чаще действуют без постоянного человеческого вмешательства. Появляется закономерный вопрос: кто должен нести ответственность, если машина ошибается или причиняет вред? Если на ранних этапах обсуждения центральной была идея придания искусственному интеллекту статуса особого субъекта права, подобного юридическому лицу, то на сегодняшний день юридическая практика и научные исследования постепенно приходят к выводу о нецелесообразности такой концепции.

Основная часть. Правовая идея придания искусственному интеллекту статуса особого субъекта права – обычно называемого «электронная личность» – возникла как реакция на возможные проблемы распределения ответственности при действиях автономных систем. Впервые эта инициатива прозвучала в докладе Комитета по правовым вопросам Европейского парламента в 2016 году, где было предложено рассмотреть возможность предоставления наиболее совершенным автономным системам определенного правового статуса, аналогичного юридическому лицу, чтобы они могли нести ответственность за причиненный ущерб и взаимодействовать с третьими лицами независимо [11. С. 10]. Эта идея рассматривалась не как предоставление им прав человека, а скорее как инструментальное решение проблемы «черного ящика» – когда невозможно установить, что именно привело к инциденту, особенно если автономная система действовала без ясного человеческого контроля.

В ответ на это предложение более 150 экспертов из области робототехники, искусственного интеллекта, этики и права подписали открытое письмо Европейской комиссии, в котором категорически отвергли идею создания статуса «электронной личности». Они подчеркнули, что предложение основывается на поверхностном понимании непредсказуемости и способности искусственного интеллекта к самообучению, неоправданной осторожности и научно-фантастических заблуждениях и приведет к юридической и этической путанице [15. С. 1]. Это письмо стало одним из ключевых моментов, которые заставили законодателей задуматься и замедлить принятие подобных норм.

Первые научные работы на эту тему появились еще задолго до инициативы Европейского парламента. Так, Лоуренс Б. Солум в статье 1992 года заложил основу для теоретического обсуждения, став одним из первых, кто серьезно задумался о том, что значит «правовая личность» искусственного интеллекта [18. С. 1240]. В круг основоположников данного направления входят и такие исследователи как Тимоти Л. Батлер, который рассуждал, может ли машина считаться автором в контексте авторского права [4. С. 710], и Маршалл С. Уиллик, который анализировал возможность предоставления искусственному интеллекту частичной правосубъектности в конституционном контексте [22. С. 790].

Продвижение идеи «электронной личности» сопровождалось публичными слушаниями и обсуждениями в Европарламенте, где высказывалась идея обязательного страхового покрытия для роботов и создания агентства по робототехнике и искусственному интеллекту. Однако встречались и мощные контраргументы не только от группы 150 ученых, но и от Европейского экономического и социального комитета, который в своем заключении в 2017 году заявил, что любое предоставление роботу юридического статуса несет риск морального вреда, поскольку может снять ответственность с производителя [10. С. 3].

Санкционирование или признание искусственного интеллекта субъектом права так и не вышло за рамки обсуждений. Вместо этого путь дальнейшего правового регулирования искусственного интеллекта попытались заложить через создание экспертной группы при Европейской комиссии, которая призвана разрабатывать руководства по этике и стандарты для ответственной разработки, средств трассируемости и регулирования через продуктовую ответственность [9. С. 5].

В настоящее время на смену «технологическому» подходу, который предполагал придание искусственному интеллекту «личности», пришла идея распределение ответственности между производителями, пользователями и владельцами алгоритмов. Такой подход позволяет избегать искусственного расширения круга субъектов права и сохранять устойчивость правовой системы. На данный момент принят ряд нормативных актов как в международном праве, так и в национальных правовых системах разных стран, которые уже закрепляют данный подход к регулированию искусственного интеллекта.

Так, например, в Европейском союзе были приняты несколько важных инструментов. Во-первых, в 2024 году был принят Европейский акт об искусственном интеллекте, который закрепил дифференцированный подход к регулированию систем искусственного интеллекта в зависимости от уровня риска, который они представляют, и поставил в основу принцип возложения ответственности на производителя или оператора системы [3. С. 22].

Во-вторых, в 2024 году была принята обновленная Директива о продуктовой ответственности, согласно которой понятие «продукт» расширяется и охватывает программное обеспечение и системы искусственного интеллекта [7. С. 18]. Директива вводит упрощенный порядок доказывания дефекта и причинной связи для потерпевших и устанавливает ответственность за постпродажные обновления, что в значительной мере меняет баланс интересов в пользу защиты конечных пользователей.

Наконец, третьим значимым событием стало то, что проект отдельной Директивы по ответственности за искусственный интеллект, который предполагал дополнительные облегченные механизмы привлечения к ответственности при вреде, вызванном искусственным интеллектом, был отозван органами Европейского союза в 2025 году [16. С. 2]. Это было прежде всего политическое решение, которое отражает сложность и чувствительность вопроса: с одной стороны, требуется облегчить доступ пострадавших к правовой защите, с другой стороны, законодатели опасаются избыточного регулирования, которое может затормозить инновации.

Переходя от европейской плоскости к практике иных юрисдикций, можно отметить, что в США регулирование осуществляется преимущественно через секторальные механизмы – правила и решения профильных федеральных агентств и штатов. Так, штат Вайоминг ввел условия для регистрации децентрализованных автономных организаций как обществ с ограниченной ответственностью [23. С. 2–3], что служит примером того, как применить «корпоративный подход» и корпоративную обертку к технологиям нового типа.

На острове Гернси, в свою очередь, приняли акт, признающий дееспособность электронных агентов в контрактном обороте [7. С. 2], что облегчает заключение сделок алгоритмами при условии наличия юридической ответственности со стороны связанных с ними людей или организаций.

На сегодняшний день уже имеется международная судебная практика, к которой мы можем обратиться для анализа правоприменения в данной области.

Так, по делу об искусственном интеллекте DABUS, разработанном С. Таллером, судебные органы в ряде стран, в частности в Великобритании [20. С.

8], США [21. С. 3] и в Европейском патентном ведомстве [12. С. 12], отказались признать искусственный интеллект в качестве изобретателя, указав, что право на получение патента может принадлежать только физическому лицу.

Показательным является дело, связанное с децентрализованными автономными организациями (DAO). Комиссия по торговле товарными фьючерсами США подала иск против децентрализованной автономной организации Ooki DAO в 2022 году, обвинив ее в незаконном предоставлении торговых услуг с криптовалютными деривативами частным лицам без регистрации и нарушении правил по борьбе с отмыванием денег [6. С. 5]. Сложность была в том, что DAO управляется смарт-контрактами и голосами держателей токенов, соответственно, не было ни физического, ни юридического лица, которое могло бы понести ответственность за работу системы. В ответ на это Комиссия предложила рассматривать участников, которые активно голосовали за управленческие решения в Ooki DAO, как лиц, несущих ответственность за деятельность всей организации. По сути, такое децентрализованное участие было признано аналогом участия в акционерном управлении, как если бы акционер проголосовал на собрании компании. Суд поддержал этот подход, квалифицировав DAO по существующим категориям как неформированное объединение лиц (*unincorporated association*) [6. С. 7], и фактически возложил ответственность на конкретных участников и контролирующие лица, чем создал резонансный прецедент. Это демонстрирует прагматичность подхода: даже при высокой децентрализации алгоритмическое управление не освобождает людей и организации от ответственности.

В качестве еще одного поучительного кейса следует упомянуть инцидент с автономным автомобилем компании Uber в городе Темп, штат Аризона, где в 2018 году произошло смертельное дорожно-транспортное происшествие [14. С. 15]. Расследование выявило, что юридическая ответственность легла на людей и организации, участвовавшие в тестировании и эксплуатации системы, а не на саму машину, что подчеркивает доминирующую практику трактовки искусственного интеллекта как инструмента, а не субъекта права.

Анализ судебной практики показывает, что попытки «передать» права или обязанности машине не находят устойчивой поддержки судов и регуляторов, и в случае конфликтов правоприменительная практика склоняется к тому, чтобы идентифицировать реальных людей или юридические лица, с которыми можно работать в рамках процедур исполнения решений.

Таким образом, можно выделить два основных подхода к проблеме ответственности за действия автономных систем. Первый подход, технологический, предлагал рассматривать искусственный интеллект как самостоятельного участника правоотношений, но он не нашел практической поддержки, во многом в силу этических и процедурных сложностей. Второй подход, который целесообразно обозначать как «корпоративный» подход, предполагает использование искусственного интеллекта через правовые оболочки – компании, фонды, или децентрализованные автономные организации, где права и обязанности закрепляются за юридическим лицом или участниками, а не за системой напрямую. Такой подход также называют «корпоративной оберткой» для алгоритмов.

Исходя из изложенного, современная научная мысль приходит к выводу, что на практике оптимален гибридный подход: сочетание корпоративного подхода с усиленной продуктовой ответственностью, обязательным страхованием и требованиями прозрачности и трассируемости. Корпоративная обертка позволяет выделить юридическое лицо, ответственное за действия алгоритма, придать этому лицу юридический адрес и экономическое содержание. Усиление продуктовой ответственности (как это делает Директива о продуктовой ответственности Европейского союза) облегчает положение пострадавших при доказывании дефекта. Обязательное страхование создает финансовые гарантии для возмещения вреда, а требования к трассируемости (логи, версия модели, данные обучения) делают возможным восстановление причинно-следственной цепочки при расследовании правонарушений. Такое сочетание инструментов дает надежную основу для защиты пострадавших и в то же время не требует радикального введения новой категории «юридической личности» для алгоритма.

В научной литературе и правоприменительной практике ведутся оживленные дебаты о преимуществах и рисках каждого из перечисленных подходов. Некоторые исследователи, в том числе А. Ю. Калинин [1. С. 198] и В. О. Калятин [2. С. 47], полагают, что традиционная правовая модель справляется с задачами регулирования при условии ее адаптации к цифровой специфике, и нет необходимости вводить новые категории субъектности.

Саймон Честерман считает, что многие сторонники юридического признания искусственного интеллекта опираются исключительно на практические или утилитарные соображения, например, упрощение регулирования ответственности за действия алгоритмов. Однако, как подчеркивает автор, утилитарная польза сама по себе не является достаточным основанием для создания новой категории юридических лиц. Искусственный интеллект не обладает сознанием, моральной волей или способностью к саморефлексии, а любые его действия являются лишь результатом программного обеспечения и данных, которыми его снабдили люди. По мнению Честермана, правовая система требует «субъектов», способных нести обязанности и обладать правами не только формально, но и содержательно, искусственный интеллект же такими свойствами пока не обладает [5. С. 819].

Гарри Сурден, наоборот, указывает на возможную необходимость особого режима для высокоавтономных систем в будущем, но подчеркивает риски «размывания ответственности» и появления «черных ящиков», когда невозможно будет идентифицировать виновное лицо [19. С. 1310].

Говоря о «корпоративном» подходе, особое внимание привлекает предупреждение, высказанное в работах Линна Лопакки, о риске злоупотребления инструментом «юридического фасада»: создание формальных «лиц» для алгоритмов может стать способом уклонения от ответственности, если такие юридические образования не будут иметь реального экономического содержания и контактных лиц, способных исполнять решения судов. Именно поэтому корпоративная обертка должна сопровождаться обязательными требованиями к прозрачности, идентификации управляющих и наличию средств для исполнения судебных решений [13. С. 900].

Довольно интересной выглядит точка зрения Сиины Раскуллы относительно правового статуса искусственного интеллекта: в своей статье она рассуждает о том, что правосубъектность искусственного интеллекта нельзя понимать однозначно через одну классическую теорию юридической личности. Она выделяет 3 основных подхода к пониманию юридического лица:

1) реалистический, когда юридическое лицо рассматривается как самостоятельная субъект, не зависящий от воли участников,

2) агрегатный, когда юридическое лицо – это совокупность людей, действующих сообща,

3) фикционный, когда юридическое лицо является лишь правовой фикцией, придуманной государством для удобства регулирования –

и утверждает, что искусственный интеллект сочетает в себе элементы всех трех подходов: как «реальный субъект» он способен автономно функционировать и принимать решения; как «агрегированный субъект» он остается зависимым от людей, которые его обучают, им управляют или его эксплуатируют; как «фикция» его не существует в физическом смысле вне правовой оболочки, созданной законодательством. Данную совокупность трех подходов она называет гибридной корпоративной личностью [17. С. 78].

Однако, несмотря на вышесказанные доводы касательно юридического лица, автор не поддерживает идею полной и безусловной правосубъектности искусственного интеллекта. Вместо этого она предлагает ограниченный юридический статус, который позволял бы заключать сделки и участвовать в правовых отношениях от своего имени (например, через «AI-компанию» или специальную правовую оболочку); иметь ограниченную имущественную ответственность, но только в пределах выделенного фонда или капитала, аналогично тому, как отвечает общество с ограниченной ответственностью; допускать возможность предъявления к искусственному интеллекту самостоятельных исков, однако фактическое исполнение обязательств должно обеспечиваться людьми или структурами, стоящими за системой [17. С. 78].

Особенно интересны ее рассуждения об ответственности за причиненный вред. Она пишет, что нельзя «наказать» искусственный интеллект как морального субъекта, но можно юридически закрепить за ним имущественный фонд, из которого будут выплачиваться компенсации. Такой фонд мог бы формироваться за счет обязательного страхования или специальных взносов разработчиков и операторов. Таким образом, искусственный интеллект был бы «ответственным» в правовом поле, но не в антропологическом смысле [17. С. 78]. На наш взгляд, это достойный и практико-ориентированный компромисс между «технологическим» и «корпоративным» подходами.

Заключение. Обсуждение статуса искусственного интеллекта является отражением более широкого процесса адаптации права к вызовам цифровой эпохи. Несмотря на теоретическую привлекательность идеи придания алгоритмам правосубъектности, судебная практика и нормативное регулирование показывают, что правовые системы склоняются к сохранению традиционной модели, дополняемой современными инструментами ответственности [24. С. 117–119].

Список литературы

1. Калинин А. Ю. К вопросу о возможной правосубъектности искусственного интеллекта // Право в эпоху искусственного интеллекта: перспективные вызовы и современные задачи: сборник научных статей по материалам Международного научно-практического форума «VI Сибирские правовые чтения», г. Тюмень, 17–19 октября 2024 г. Тюмень: ТюмГУ-Press, 2024. С. 195–198.
2. Калятин В. О. Определение субъекта прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта // Право. Журнал Высшей школы экономики. 2022. Т. 15 № 4. С. 24–49.
3. Artificial Intelligence Act: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence. Official Journal of the European Union, L 202, 12.07.2024.
4. Butler T. L. Can a Computer be an Author? Copyright Aspects of Artificial Intelligence. Hastings Communications and Entertainment Law Journal. 1982. Vol. 4. No. 4. P. 707.
5. Chesterman S. “Artificial Intelligence and the Limits of Legal Personality.” International & Comparative Law Quarterly, 2020, Vol. 69(4), p. 819.
6. Commodity Futures Trading Commission v. Ooki DAO, Case No. 3:22-cv-05416 (N.D. Cal., 2022).
7. Directive (EU) 2024/1799 of the European Parliament and of the Council of 13 July 2024 on liability for defective products (Product Liability Directive). Official Journal of the European Union, L 213, 10.07.2024.
8. Electronic Transactions (Electronic Agents) (Guernsey) Ordinance, 2019. States of Guernsey.
9. European Commission. Ethics Guidelines for Trustworthy AI. High-Level Expert Group on AI. Brussels, 2019.
10. European Economic and Social Committee. Opinion on Artificial Intelligence: The Consequences of Artificial Intelligence on the (Digital) Single Market, Production, Consumption, Employment and Society (INT/806-EESC-2017). Brussels, 2017.
11. European Parliament. Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). Brussels, 2016.
12. European Patent Office. Decision J 8/20 and J 9/20 (DABUS case). EPO Boards of Appeal, 21 December 2021.
13. LoPucki L. M. Algorithmic Entities // Washington University Law Review. 2018. Vol. 95. P. 887–954.
14. National Transportation Safety Board (NTSB). Collision Between Vehicle Controlled by Developmental Automated Driving System and Pedestrian (Uber Technologies, Inc., Tempe, Arizona, March 18, 2018). Highway Accident Report NTSB/HAR-19/03. Washington, DC, 2019.
15. Open Letter to the European Commission Artificial Intelligence and Robotics. Signed by 156 Experts, 2017. URL: <https://www.robotics-openletter.eu> (дата обращения: 30.08.2025).

16. Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM(2022) 496 final. Brussels, 28.09.2022 (withdrawn in 2025).
17. Raskulla, S. Hybrid Theory of Corporate Legal Personhood and Its Application to Artificial Intelligence. SN Social Sciences, 2023, Vol. 3, Article 78.
18. Solum L. B. Legal Personhood for Artificial Intelligences. North Carolina Law Review. 1992. Vol. 70. P. 1231.
19. Surden H. Artificial Intelligence and Law: An Overview // Georgia State University Law Review. 2019. Vol. 35, Issue 4. P. 1305.
20. UKIPO. Thaler v Comptroller-General of Patents, Designs and Trade Marks [2021] EWCA Civ 1374.
21. United States Patent and Trademark Office (USPTO). Decision on DABUS applications. 2020.
22. Willick M. S. Constitutional Law and Artificial Intelligence: The Potential Legal Recognition of Computers as “Persons” // Proceedings of the Ninth International Joint Conference on Artificial Intelligence (IJCAI-85). Los Angeles, 1985. P. 789–791.
23. Wyoming Decentralized Autonomous Organization Supplement, Wyo. Stat. § 17–31–101 et seq. (2021).
24. Шутова А. А. Особенности квалификации преступлений, совершаемых лицами, использующими технологии искусственного интеллекта в здравоохранении // Lex Russica (Русский закон). 2023. Т. 76, № 12(205). С. 113–123. DOI 10.17803/1729–5920.2023.205.12.113–123. – EDN PQTEET.

А. А. Богданова,

студент,

Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

**Цифровые технологии в сфере долевого строительства:
риски и перспективы внедрения**

Аннотация. Цифровизация долевого строительства важный этап в становлении инновационной экономики государства. В настоящей статье рассматриваются варианты адаптации рынка недвижимости под использование технологий информационного моделирования, раскрываются преимущества и недостатки внедрения таких технологий, предлагаются варианты их использования. Непосредственно подчеркиваются перспективы использования технологий: прозрачность сделок, усиление контроля за сферой строительства, автоматизация процессов. Автор рассматривает варианты внедрения и использования цифровых технологий за рубежом.

Ключевые слова: технологии информационного моделирования, долевое строительство, цифровизация, строительная отрасль, информационная модель объекта долевого строительства, электронный документооборот, BIM-технологии, 3D –модель, цифровая трансформация

A. Bogdanova,

student,

Moscow State Law University. O.E. Kutafina (MSUA)

**Digital technologies in the field of shared-equity construction:
risks and prospects for implementation**

Abstract. Digitalization of shared-equity construction is an important stage in the development of the innovative economy of the state. This article examines the options for adapting the real estate market to the use of information modeling technologies, reveals the advantages and disadvantages of introducing such technologies, and suggests options for their use. The prospects for using technology are directly emphasized: transparency of transactions, increased control over the construction sector, and automation of processes. The author considers options for the introduction and use of digital technologies abroad.

Keywords: information modeling technologies, shared-equity construction, digitalization, construction industry, information model of shared-equity construction facility, electronic document management, BIM-technologies, 3D model, digital transformation

Введение. В современном мире процесс цифровизации стал неотъемлемой частью нашей жизни, с одной стороны, он упрощает нашу жизнь и увеличивает уровень комфорта, а с другой стороны создает трудности и преграды, с которыми мы сталкиваемся каждый день.

Как это исторически сложилось, одной из важнейших человеческих потребностей является потребность в безопасности и жилье. На современном этапе жизни найти комфортное жилье не такая уж и сложная вещь, как это кажется на первый взгляд. Рынок недвижимости содержит массу предложений, начиная от небольшой и уютной квартиры до роскошных премиальных апартаментов. Мир не стоит на месте, рынок недвижимости также развивается посредством внедрения цифровых технологий. Граждане активно покупают жилье на первичном рынке, посредством заключения договоров долевого участия. Предложений от Застройщиков множество, но даже при таком богатом выборе дольщики могут столкнуться с множеством риском: навязыванием дополнительных услуг Застройщиком, ущемляющими условиями прав потребителей в договорах долевого участия, нарушением срока передачи объектов долевого строительства и множеством другого. Имея в виду тот факт, что долевое строительство составляет огромный пласт современной экономики, то соответственно нужно уделять пристальное внимание для исключения злоупотреблений в этой сфере. Как раз именно цифровые технологии и помогут нам в этом.

Основная часть. Информатизация охватывает все направления человеческой деятельности, что стало поводом видоизменения отношений в сфере строительства

и их эволюционирования в цифровые. Все более заметным и актуальным становится совершенствование информационно-коммуникационных технологий и применение искусственного интеллекта (ИИ) на рынке строительства, в том числе объектов долевого строительства.

Перспективы и вызовы, которые возникают перед законодателем, застройщиком и другими участниками строительных отношений, в результате динамичного внедрения ИИ-нейронных сетей в строительную сферу, порождают адаптивное понимание природы цифровых-электронных отношений на рынке недвижимости.

В рамках реализации Стратегии развития строительной отрасли и жилищно-коммунального хозяйства Российской Федерации на период до 2030 года с прогнозом до 2035 года, утвержденной распоряжением Правительства Российской Федерации от 31.10.2022 № 3268-р [1], активно внедряются цифровые технологии проектирования и управления производственными и эксплуатационными процессами, такие как технологии информационного моделирования (далее – ТИМ) с целью достижения стратегических и национальных целей, посредством «формирования и развития цифровой системы управления жизненным циклом объектов капитального строительства, городского и жилищно-коммунального хозяйства, отвечающей современным отраслевым вызовам».

Первоначально разъясним «технологии информационного моделирования объектов капитального строительства – это совокупность технологий, производственных процессов и регламентов, обеспечивающих возможность совмест-

ного управления информацией об объекте капитального строительства на всех этапах его жизненного цикла» [2]. Буквальное толкование данного определения позволяет нам сделать вывод, что основное предназначение технологий моделирования является обеспечение прозрачности и оптимизации всех процессов строительства. На наш взгляд это бесспорное преимущество в строительстве для потребителей и государства, так как позволяет проследить весь процесс строительства, начиная от разработки проекта вплоть до введения в эксплуатацию и дальнейшего функционирования.

Интересный факт, что ранее был введен термин информационная модель объекта капитального строительства (далее – ИМ) – это совокупность данных «в электронной форме, представляющие собой взаимосвязанные сведения, документы и материалы на этапах выполнения инженерных изысканий, осуществления архитектурно-строительного проектирования, строительства, реконструкции, капитального ремонта, эксплуатации и (или) сноса объекта капитального строительства, осуществляемый с использованием информационных систем, обеспечивающих функции передачи данных между субъектами градостроительных отношений и их регистрации» [3].

Сравнивая два эти определения, мы, конечно же, в первую очередь обратили взор на, то, что они достаточно похожи, можно сказать в некой степени даже дублируют друг друга. Понятно, что термин ТИМ является родовым понятием к информационной модели, вопреки тому, что термин ТПИ стал использоваться несколько позже, чем ИМ. ТИМ вмещает в себя не только информационную составляющую проекта, но и его технологическую и юридическую звенья. В совокупности три звена создают нечто новый продукт работы и Застройщика с подрядчиками, и государственных органов и фондов, так как ускоряется процесс взаимодействия между всеми участниками строительных отношений, снижается уровень бумажной волокиты, увеличивается прозрачность всей деятельности, уменьшаются сроки взаимодействия между участниками. То есть на наш взгляд это сплошные преимущества при введении данной системы. Особенно актуально это будет в сфере долевого строительства, при привлечении денежных средств граждан или выполнение работы по государственному заказу.

Рассмотрим более подробно преимущества внедрения и обязательного использования ТИМ с июля 2025 года строительными компаниями:

- повышение точности проектирования. Конечно, и раньше многие Застройщики использовали автоматизированные технологии при проектировании, но ТИМ позволит выйти совершенно на иной уровень, появится возможность создания детализированной 3D модели проекта. 3D модель проекта позволит только на этапе создание модели увидеть какие-либо погрешности, неточности, снизит количество возможных ошибок и недочетов, хотя искусственный интеллект может тоже допустить ошибку, все-же алгоритмы чаще работают без сбоев, не допуская технических и фактических ошибок;

- повышение уровня эффективности взаимодействия между участниками строительных отношений. Все данные находятся в одном месте, представлены в цифровом формате, следовательно, любой участник может ознакомиться с необходимым ему пакетом документов, без лишних бумажных запросов, телефон-

ных переговоров и лишней траты времени перевода документа из одного формата в другой;

- снижение временных затрат создания проекта в целом, так и отдельных его этапов. Кроме того, это модернизирует работу отдельно взятых компонентов проектирования модели и функционирования ее в дальнейшем;

- возможность прогнозирования проблем, которые могут возникнуть при строительстве или в дальнейшем при эксплуатации возведенного объекта долевого строительства. Так, информационная модель, созданная посредством ТИМ, помогает заранее обнаружить и устранить недостатки в проекте, ведь в режиме реального времени можно посредством введения определенных данных смоделировать те или иные ситуации, при которых могла бы нарушиться целостность проекта и тем самым создать угрозу жизни и здоровья гражданам;

- одно из важнейших преимуществ, пожалуй, это повышение уровня прозрачности для дольщиков. Если ранее многие этапы строительства – от получения разрешения на строительство до реализации объекта доступны частично, сейчас возникает возможность проследить все процессы более детализировано, что позволяет получить полное представление о таких работах.

- применение ТИМ позволит контролировать не только сам процесс возведения объекта, но и последующие жизненные циклы объекта после его ввода. ТИМ может использоваться управляющими компаниями, не только теми, которые выбраны Застройщиками в каждом конкретном жилом комплексе, но и компаниями извне.

Таким образом, мы раскрыли лишь часть преимуществ использования ТИМ в сфере строительства, непосредственно долевого. Однако как у любого новшества, у цифровизации строительной сферы есть и недостатки.

Во-первых, до конца не понятно, похожа ли эта модель на BIM-технологий в строительстве, используемые за рубежом, можем ли мы однозначно поставить знак равенства между ТИМ и BIM-технологий? Вероятно, что нет, так как наши отечественные разработки не охватывают столь обширный процесс строительства, как в зарубежных странах. К примеру, в США активно используются BIM-технологии, начиная с 2000-х годов, при этом BIM-модель поддерживает такие процессы как: проектирование, инженерный документооборот, закупки и логистика, отчетность, последующая эксплуатация, планирование графика строительства и многое другое [4]. Наша модель на первых этапах не предполагает цифровизации стольких процессов, как за рубежом. Кроме того, есть зарубежные страны активно используют 3 или 4D модели, то у нас в настоящий период ТИМ скорее предполагает не информационную модель здания, а лишь цифровую систему взаимодействия между участниками строительных отношений.

Во-вторых, на уровне федерального законодательства отсутствуют легальные определения технологий информационного моделирования, а также информационная модель объекта строительства. Отсутствие легального определения вносит правовую неопределенность для участников строительных отношений, так как нет четкого понимания составляющих данной информационной модели и пределов использования ТИМ.

В-третьих, если же представить, что ТИМ в ближайшем будущем перерастет из цифрового пространства взаимодействия в 3D модель, то какое программное обеспечение будет лежать в основе функционирования данной системы? Будут ли какие-то единые требования к программному обеспечению или это будет на усмотрения участников, или же будет разработано новое ПО?

В-четвертых, в настоящий период времени существует сайт ДОМ.РФ, на котором любой желающий в открытом доступе может получить необходимую информацию о строительстве новостроек, краткую характеристику о застройщике, о жилом доме, документацию (проектные декларации, разрешительную документацию, отчетность Застройщика, проект договора участия в долевом строительстве (далее – ДДУ). Опять же вопрос как эти две информационные базы (системы) будут связаны между собой, если фактически документы будут дублировать друг друга?

В-пятых, переход к ТИМ довольно сложный, дорогостоящий процесс. Необходимо мощное программное обеспечение, для быстрого функционирования системы, требуются высококвалифицированные специалисты либо же необходимо выделять компании ресурсы как временные, человеческие, так и денежные для переквалификации, следовательно опять возрастают расходы. Ну и конечно, система требует постоянного обновления, что также может затруднять рабочий процесс.

В-шестых, в современном мире высок риск утечки данных, особенно в период цифровизации. Остро встает вопрос, как ТИМ будет обеспечивать сохранность данных, безопасную их передачу, особенно касаясь персональных данных или каких-то авторских решений? Вопрос остается открытым.

В-седьмых, все указанные недостатки в совокупности могут привести к вынужденному уходу ряда компаний со строительного рынка, что в конечном итоге приведет к формированию монополии, повышению цен на недвижимость.

Таким образом, внедрение ТИМ в строительную сферу имеет как достоинства, так и минусы. ТИМ – новый вызов для общества, который является неотъемлемой точкой роста для участников строительной сферы и повышение общественного уровня развития.

На повестку дня также необходимо поднять вопрос о защите прав потребителя при цифровизации сферы строительства. Очень часто в ДДУ имеются условия, ущемляющие права потребителей либо же дополнительные навязанные услуги, соответственно при нормальных условиях гражданского оборота дольщик-потребитель не заключил бы такой договор (о чем свидетельствует многочисленная судебная практика).

К примеру, частыми нарушениями является ограничение способов защиты прав дольщиков при передаче объектов долевого строительства. Частью 2 статьи 7 Федерального закона от 30.12.2004 № 214-ФЗ «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации» (далее – Федеральный закон о долевом участии) «в случае, если объект долевого строительства построен (создан) застройщиком с отступлениями от условий договора, то предусмотрено три способа защиты:

- 1) безвозмездного устранения недостатков в разумный срок;
- 2) соразмерного уменьшения цены договора;
- 3) возмещения своих расходов на устранение недостатков» [5].

Согласно вышеизложенному часть 2 статьи 7 Федерального закона о долевом участии закрепляет императивно-диспозитивно три варианта реализации права на защиту при нарушении условий о качестве объекта долевого строительства, при этом дольщик по своему усмотрению вправе воспользоваться любым из них.

Согласно пункту 9 статьи 4 Федерального закона о долевом участии к отношениям, вытекающим из договора, заключенного гражданином – участником долевого строительства исключительно для личных, семейных, домашних, и иных нужд, не связанных с осуществлением предпринимательской деятельности, применяется законодательство Российской Федерации о защите прав потребителей в части, не урегулированной настоящим федеральным законом.

Пунктом 1 статьи 16 Закона РФ от 07.02.1992 № 2300–1 «О защите прав потребителей» (далее устанавливает, что недопустимыми условиями договора, ущемляющими права потребителя, являются условия, которые нарушают правила, установленные международными договорами Российской Федерации, настоящим Законом, законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, регуливающими отношения в области защиты прав потребителей. Недопустимые условия договора, ущемляющие права потребителя, ничтожны [6].

Подпунктом 10 пункта 2 статьи 16 Закона РФ от 07.02.1992 № 2300–1 «О защите прав потребителей» (далее – Закон № 2300–1) к недопустимым условиям договора, ущемляющим права потребителя, в том числе относятся: условия, которые ограничивают право выбора вида требований, предусмотренных пунктом 1 статьи 18 и пунктом 1 статьи 29 настоящего Закона, которые могут быть предъявлены продавцу (изготовителю, исполнителю, уполномоченной организации или уполномоченному индивидуальному предпринимателю, импортеру) при продаже товаров (выполнении работ, оказании услуг) ненадлежащего качества.

В ДДУ прописывают, в частности, условие «при наличии у участника каких-либо замечаний к квартире, (отделке), стороны одновременно с передаточным актом подписывают протокол замечаний, с указанием всех имеющихся у Участника замечаний к квартире/отделке. Застройщик обязан в течение 20 рабочих дней рассмотреть требования участника, указанные в протоколе замечаний, и согласовать с участником разумные сроки устранения замечаний по имеющимся недостаткам квартиры/отделки».

Ущемляющим является и такое условие: «что не допускается устранение недостатков силами участника с возложением расходов на застройщика. Нарушение настоящего пункта влечет для Участника утрату права на устранение недостатков за счет Застройщика в пределах гарантийного срока». Иногда прописывают условия о том, что в случае, если квартира построена с нарушениями условий, предусмотренных договором, требований технических регламентов, проектной документации и иных обязательных требований, приведшим к ухуд-

шению ее качества, участник долевого строительства вправе потребовать от Застройщика только безвозмездного устранения недостатков в разумный срок». Данные условия прямо ограничивают свободу выбора способов устранения недостатков, что является недопустимым.

Таким образом, перечисленные условия ДДУ стесняют выбор способа защиты нарушенных прав участников.

Предусматривая право дольщика лишь на безвозмездное устранение недостатков, Застройщик ограничил для него возможность самостоятельного выбора способа реализации своих прав, что ущемляет права потребителя – участника долевого строительства.

Объективной невозможности изложения данного пункта договора в той редакции, которая информировала бы потребителя обо всех предусмотренных законом способов защиты его права при выявлении недостатков в передаваемом ему объекте долевого строительства, обеспечив тем самым ему свободу выбора, не установлено.

На основании изложенного положения части 2 статьи 7 Федерального закона о долевом участии носят диспозитивный характер и предполагают, в том числе указание иных условий, определяющих действия сторон в случае строительства застройщиком объекта с отступлением от условий договора, а также позволяют сторонам в договоре предусмотреть иной порядок исчисления гарантийного срока, что не нарушает права потребителя. В данном случае диспозитивность заключается не в установлении способов восстановления нарушенных прав в договоре участия в долевом строительстве, а в возможности альтернативного выбора у дольщика таких способов защиты.

В пункте 26 Обзора судебной практики Верховного Суда Российской Федерации № 4 от 23.12.2020 закреплено то, что диспозитивный характер положений части 2 статьи 7 ФЗ № 214, допускающий указание в договоре участия в долевом строительстве иных условий, определяющих действия сторон в упомянутых случаях, ограничен Законом № 2300-1, гарантирующий потребителям определенный объем их прав. Право на установление иных условий договора не может рассматриваться как основание к ограничению предусмотренных законом прав потребителя. Диспозитивность специальных норм, регулирующих отношения в области долевого строительства, направлена, прежде всего, на защиту более слабой стороны отношений в строительстве, в частности физического лица – участника долевого строительства, и может применяться в этих целях, устанавливая для указанных лиц больший объем прав, чем предусмотрено законодательством о защите прав потребителей, улучшая тем самым положение потребителя, а не ухудшая его [7].

Потребитель, подписывая заранее разработанную обществом форму договора, содержащего вышеуказанные условия, не может его изменить в одностороннем порядке, поэтому реализация законного права, гарантированного ему вышеуказанными нормами закона, ставится в зависимость от воли и желания общества как лица, оказывающего услуги, что является ущемлением прав потребителей.

Также часто Застройщик, прописывают в условиях ДДУ разумные сроки для устранения недостатков при передаче объекта долевого строительства. Такие условия рассматриваются как вносящее в правовое регулирование неопределенность, не позволяющую субъектам соответствующих правоотношений и правоприменительным органам осознавать и единообразно исчислять, и применять сроки для устранения дефектов, и предвидеть наступление ответственности за их нарушение.

Хотя при этом, есть отдельные нормативно-правовые акты, которые устанавливают сроки для устранения недостатков и конкретный алгоритм действий для реализации такого права дольщикам [8].

Одним из камней преткновения может стать также условие, по которому не понятно на кого возлагать расходы по регистрации прав дольщика на объект долевого строительства.

В связи с изменениями, вступившими в законную силу, связанными с возложением на Застройщика обязанности по направлению документов на регистрацию, а именно согласно части 6 статьи 16 Федерального закона о долевом строительстве после передачи застройщиком в соответствии со статьей 8 настоящего Федерального закона объекта долевого строительства участнику долевого строительства и осуществления государственного кадастрового учета такого объекта застройщик в срок не позднее тридцати рабочих дней со дня подписания передаточного акта, одностороннего акта или иного документа о передаче объекта долевого строительства с участником долевого строительства обязан направить в орган регистрации прав заявление о государственной регистрации права собственности участника долевого строительства на такой объект в электронной форме.

Согласно вышеизложенному, в договорах долевого участия следует указать и детализировать порядок направления на регистрацию объекта долевого строительства (квартиры) и определить порядок распределения расходов по осуществлению регистрации прав собственности на квартиру, а именно определить, какая из сторон будет оплачивать госпошлину за данную процедуру с целью в дальнейшем избежать злоупотребления правом с обеих сторон.

Положения статьи 16 Федерального закона о долевом строительстве данный вопрос не урегулировали, поэтому согласно одному из общих принципов гражданского права – свободы договора, сторонам следуют определить на кого будет возложена обязанность по оплате госпошлины за такую процедуру.

Учитывая изложенное, государственная пошлина может быть оплачена как застройщиком (с указанием в назначении платежа, что государственная пошлина оплачивается за государственную регистрацию права собственности участника долевого строительства), так и участником долевого строительства.

В отношении заключаемых в настоящее время договоров участия в долевом строительстве указанный вопрос может быть урегулирован застройщиком и участником долевого строительства непосредственно в договоре участия в долевом строительстве либо отдельным соглашением.

Кроме того, в ДДУ может содержаться условие, навязывающие дополнительные услуги: «согласование уступки прав требований по настоящему договору третьему лицу может производиться Застройщиком за отдельную плату».

Данное положение ДДУ является ущемляющим права дольщиков ввиду того, что это прямое навязывание дополнительных услуг для потребителя и покупателя объекта долевого строительства. Согласно статье 11 Федерального закона о долевом строительстве никаких дополнительных условий по оплате уступки прав требований не закреплено. Кроме того, обращаясь к положениям Гражданского кодекса Российской Федерации (далее – ГК РФ), регулирующим институт цессии (уступки прав требований), также не усматривается условий, позволяющих сделать однозначный вывод о том, что Застройщик вправе требовать с дольщика оплаты за содействие совершения уступки прав от цедента к цессионарию.

На наше усмотрение было бы разумно направить цифровизацию на устранение таких недостатков. Поэтому в рамках решения этой насущной проблемы одним из путей решения является внедрение системы анализа проектов договоров долевого участия на предмет содержания ущемляющих условий посредством ТИМ.

Ранее мы уже описывали функционирования ТИМ в общем порядке, то теперь хотелось бы углубиться и рассказать о дополнительном блоке, который можно было бы внедрить в данный проект. Блок-проекты ДДУ, в системе ТИМ будет содержать в себе не только варианты проектов договоров, но также и систему их анализа, для того, чтобы каждый потенциальный потребитель-покупатель могут удостовериться, что договор полностью соответствует требованиям законодательства и не содержит в себе каких-либо дополнительных услуг, которые, к слову, оказываются и так бесплатно или должны быть оказаны в силу закона.

Система анализа будет функционировать автоматически, то есть будет существовать некий алгоритм, который будет запрограммирован на выявление таких условий. Когда Застройщики будут подгружать проекты договоров, то предварительно они будут проходить два этапа анализа-сканирования: первичный и контрольный.

Суть первичного анализа будет заключаться в проверки основных условий договора, на предмет их соответствия требованиям действующего законодательства. Проверка будет осуществляться именно проектов договоров. Если система после сканирования обнаружит ущемляющие условия, то она автоматически заблокирует регистрацию проекта договора. Все дальнейшие операции по деятельности Застройщика также приостановятся. (Конечно, в этой связи сразу возникает вопрос, а разумно ли приостанавливать всю деятельность Застройщика, только из-за несоответствия проекта договора, требованиям законодательства, ведь это огромные финансовые потери для бизнеса, в чем тут целесообразность? Ответ неоднозначен: конечно, такая система будет рассматриваться для застройщика весьма обременительной, так как любое отклонение может приостановить процесс весей стройки, но в тоже время это гарантия и для Застройщика, и для потребителя, так как в дальнейшем, Застройщик может

быть с большой долей вероятности уверен, что у него не возникнет проблем по выплате штрафов и компенсаций за допущенные нарушения).

В случае прохождения успешной первичной проверки проект ДДУ будет зарегистрирован и размещен на сайте для доступа всех участников строительства, и конечно, потребителей. С этого периода может осуществляться активное заключение договоров долевого строительства с дольщиками–потребителями.

Контрольная проверка будет заключаться непосредственно в анализе конкретного договора долевого участия, заключенного с реальным дольщиком. Застройщик, заключив договор, будет обязан подгрузить его в систему для поиска на ущемляющие условия и дополнительные (навязанные услуги), если система не обнаружит ничего подозрительного, то после этой процедуры будет осуществлена регистрация договора в системе и данные будут автоматически направлены в Росреестр для внесения в базу зарегистрированных договоров. В ином случае, договор, не соответствующий требованиям законодательства, не будет допущен к регистрации в системе ТИМ, и данные не будут направлены в Росреестр. Система ТИМ будет уведомлять Застройщиков и дольщиков об успешной регистрации договоров, а также о внесении их в базу Росреестра.

Загрузка договоров с дольщиками будет осуществлять посредством специального шифрования в отдельный блок, с ограниченным доступом, для соблюдения требований Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ и избегания утечек данных [9].

Перечисленная выше контрольно–аналитическая система проверки договоров направлена на повышение прозрачности действий Застройщиков, обеспечение ускоренного взаимодействия между органами регистрации, Застройщиком и дольщиками.

В свете недавно внесенных изменений в часть 6 статьи 16 Федерального закона о долевом строительстве, связанными с возложением на Застройщика обязанности по направлению документов на регистрацию в орган регистрации прав заявление о государственной регистрации права собственности участника долевого строительства на такой объект в электронной форме в установленный законом срок, особенно актуально является внедрение ТИМ в сферу долевого строительства. Сами изменения законодательства намекают и подталкивают на внедрение и использование электронного документооборота и информационные модели объектов долевого строительства.

На наш взгляд, внедрение ТИМ в сферу строительства неизбежно, на данный момент такой проект реализуется во множестве государств. Так, к примеру, Швейцария как государство, относящееся к высокотехнологичной стране с инновационно развитой экономикой, в 2024 году принята конвенция «Digital Switzerland Strategy» [10] в рамках которой сфера строительства подлежит цифровой трансформации. Планируется создание 3-х мерной модели будущего объекта долевого строительства. Это позволит работать со всей проектной документацией в электронном формате.

Лидером по использованию BIM–технологий в строительстве является город-государство Сингапур. Singapore BIM Guide Version 2– это современная многоплатформенная система, содержащая шаблоны и проекты строительства

[11]. Посредством данной системы множество строительных фирм перешли на цифровое моделирование зданий и сооружений. Но ключевой фишкой системы стал проект – CORENET. Проект CORENET стало отправной точкой во внедрении цифровых технологий. В 1990-х годах он представлял собой полноценную модель здания, отвечающую специально установленным требованиям. Но важно отметить, чтобы проект был реализован на выполнение следующих условий: наличие доступных и эффективных BIM-решений; алгоритмизацию проектов; создание единого интерфейса; повышение уровня строительной культуры. На настоящий период данный проект активно функционирует и характеризуется высокими показателями точности и эффективности работы.

Вернемся непосредственно к Singapore BIM Guide Version 2. Данная система функционирует на отдельной платформе, которая содержит множество полезных ссылок на ресурсы для тех, кто желает продвинуться в сфере использования BIM-технологий, есть также справочники, научная литература, законодательные акты, то есть созданы все условия для перехода на цифровые модели, при этом каждый желающий в свободном доступе может ознакомиться с требованиями, предъявляемыми к моделям строительства.

Интересный факт, что система настолько адаптивна, что нет конкретных требований к программному обеспечению, то есть почти все форматы программ поддерживаются на данной платформе. Это, несомненно, является одним из преимуществ в применении такой системы для строительных компаний, так как не требуется значительных материальных, временных и человеческих ресурсов для того, чтобы привыкнуть работать с новым ПО.

Кроме того, переход на BIM-технологий активно поддерживается на государственном уровне, поэтому предоставляют денежные гранты на закупку компьютеров и обновлению ПО или установлению программ в строительных компаниях.

Согласно статистике, а также данным, предоставленным компанией Sweett Group, около 80% строительных компаний Сингапура используют BIM в своей работе. Высокий показатель использования цифровых технологий.

Китай использует BIM-технологии, начиная с 2002 года, но особо активно лишь с 2012 года. Используются 4D – BIM технологии, которые направлены на визуализацию графика строительства, анализа проблем конструктивности и оценки изменений с точки зрения их влияния на стоимость и график работ. Процесс моделирования строится в несколько этапов, начиная с модуля уровня комнаты, далее стеновые панели или водопроводную систему, заканчивая зданием в конце, с инфраструктурой вокруг него. BIM стало способом ускорения роста модульного строительства [12].

Вопреки тому, что некоторые передовые страны переходят или частично перешли к использованию BIM-технологий, их внедрению мешают определенные барьеры:

- отсутствие четко сформулированных требований к использованию таких технологий при строительстве;
- недостаток компетенции;
- на национальном уровне слабо развита информационная инфраструктура;
- отсутствует современное ПО [13].

Таким образом, BIM-технологий это не просто алгоритмизированная модель, это целая «вселенная», затрагивающая абсолютно все строительные процессы на всех этапах строительства. В совокупности таких технологий позволяют компенсировать затраты на строительства в большем соотношении, чем простые чертежи в 2D [14].

Заключение. Цифровизация активно внедряется в строительный бизнес, применении технологий информационного моделирования являются необходимостью. Перспективы и вызовы, которые возникают перед законодателем, застройщиком и другими участниками строительных отношений, в результате динамичного внедрения ИИ – нейронных сетей в строительную сферу, порождают адаптивное понимание природы цифровых–электронных отношений на рынке недвижимости.

Преимуществами внедрения и обязательного использования ТИМ являются: повышение точности проектирования; повышение уровня эффективности взаимодействия между участниками строительных отношений; снижение временных затрат создания проекта; возможность прогнозирования проблем, которые могут возникнуть при строительстве или в дальнейшем при эксплуатации возведенного объекта долевого строительства; повышение уровня прозрачности для дольщиков; использование ТИМ позволит контролировать циклы жизни объекта после введения его в эксплуатацию.

Однако как у любого новшества, у цифровизации строительной сферы есть и недостатки. На уровне федерального закона отсутствует легальное определения технологий информационного моделирования; сложности с программным обеспечением; проблемы совместного функционирования с сайт ДОМ.РФ; высокие финансовые затраты на переход ТИМ; высок риск утечки данных; возможный резкий спад количества застройщиков на рынке.

Перспективным в системе ТИМ является внедрение проекта-анализа проектов ДДУ для защиты прав дольщиков, с системой двухуровневого анализа проектов на содержание ущемляющих условий.

Зарубежный опыт по применению BIM-технологий в сфере строительства демонстрирует нам, что BIM-технологии не мыслятся в плоскости исключительного формирования 3D-модели как картинки, это не просто модель, построенная посредством набора алгоритмов, это целая «вселенная».

Несмотря на многочисленный зарубежный опыт интеграций BIM-технологий, в Российской Федерации необходимо создавать свой уникальный и неповторимый проект с использованием ТИМ-технологий.

Таким образом, внедрение ТИМ в строительную сферу имеет и достоинства, и недостатки. ТИМ – новый вызов для общества, который является неотъемлемой точкой роста для участников строительной сферы и повышение общего уровня развития.

Список литературы

1. Распоряжение Правительства РФ от 31.10.2022 № 3268-р «Об утверждении Стратегии развития строительной отрасли и жилищно-коммунального

хозяйства Российской Федерации на период до 2030 года с прогнозом до 2035 года» (дата обращения: 15.07.2025).

2. Приказ Москомэкспертизы от 11.10.2021 № МКЭ–ОД/21–77 «Об утверждении требований к информационным моделям линейных объектов капитального строительства» (дата обращения: 17.07.2025).

3. Постановление Правительства РФ от 17.05.2024 № 614 «Об утверждении Правил формирования и ведения информационной модели объекта капитального строительства, состава сведений, документов и материалов, включаемых в информационную модель объекта капитального строительства и представляемых в форме электронных документов, и требований к форматам указанных электронных документов» (дата обращения: 17.07.2025).

4. Ильинова В.В., Мицевич В.Д. Международный опыт использования BIM-технологий в строительстве // Российский внешнеэкономический вестник. 2021. №6. URL: <https://cyberleninka.ru/article/n/mezhdunarodnyy-opyt-ispolzovaniya-bim-tehnologiy-v-stroitelstve> (дата обращения: 18.07.2025).

5. Федеральный закон «Об участии в долевом строительстве многоквартирных домов и иных объектов недвижимости и о внесении изменений в некоторые законодательные акты Российской Федерации» от 30.12.2004 № 214-ФЗ (дата обращения: 19.07.2025).

6. Закон РФ от 07.02.1992 № 2300–1 «О защите прав потребителей» (дата обращения: 19.07.2025).

7. «Обзор судебной практики Верховного Суда Российской Федерации № 4 (2020)» (утв. Президиумом Верховного Суда РФ 23.12.2020) (дата обращения: 20.07.2025).

8. Постановления Правительства РФ от 29.12.2023 № 2380 «Об установлении особенностей передачи объекта долевого строительства участнику долевого строительства» (дата обращения: 20.07.2025).

9. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (дата обращения: 20.07.2025).

10. Конвенция «Digital Switzerland Strategy» 13.12.2024. URL: <https://digital.swiss/en/strategy/strategie.html> (дата обращения: 21.07.2025).

11. Singapore BIM Guide Version 2 URL: https://www.bim.cic.hk/en/resources/publications_detail/27 дата обращения: 21.07.2025).

12. Доможирова Е. А., Степанова Ю. С., Винидиктова М. Е. Преимущества BIM технологий на примере китайского опыта // ИВД. 2019. №3 (54). URL: <https://cyberleninka.ru/article/n/preimuschestva-bim-tehnologiy-na-primere-kitayskogo-opyta> (дата обращения: 21.07.2025).

13. Зотова К.А., Ланкина Ю.А., Мельникова Н.С. Внедрение методов информационного моделирования в зарубежных странах // Огарев–Online. 2022. №3 (172). URL: <https://cyberleninka.ru/article/n/vnedrenie-metodov-informatsionnogo-modelirovaniya-v-zarubezhnyh-stranah> (дата обращения: 21.07.2025).

14. Ильинова В.В., Мицевич В.Д. Международный опыт использования BIM-технологий в строительстве // Российский внешнеэкономический вестник. 2021. №6. URL: <https://cyberleninka.ru/article/n/mezhdunarodnyy-opyt-ispolzovaniya-bim-tehnologiy-v-stroitelstve> (дата обращения: 21.07.2025).

А. Д. Бочкарева,

магистрант,

Российская государственная академия
интеллектуальной собственности (РГАИС)

**Интеллектуальная собственность без границ: перспективы
и трансформация правовых институтов в метавселенной**

Аннотация. В настоящей статье рассматриваются перспективы правового регулирования вопросов интеллектуальной собственности в метавселенных, дается оценка возможности применения существующего законодательства Российской Федерации, рецепции зарубежного опыта в национальное законодательство.

Ключевые слова: диджитализация, результат интеллектуальной деятельности, метавселенная, авторское право, товарные знаки, NFT

A.D. Bochkareva,

Master's student,

Russian State Academy of Intellectual Property (RGAIS)

**Intellectual property without borders: prospects and transformation
of legal institutions in the metaverse**

Abstract. This article examines the prospects for legal regulation of intellectual property issues in metaverses, and assesses the possibility of applying the existing legislation of the Russian Federation and the reception of foreign experience into national legislation.

Keywords: intellectual property, metaverse, copyright, trademarks, NFT

Введение. Повсеместная диджитализация порождает новые формы социального взаимодействия, среди которых особое место занимают метавселенные. Эти виртуальные среды, сочетающие возможности виртуальной и дополненной реальности, становятся пространством активного экономического оборота, где создаются и используются цифровые объекты, имеющие спорную правовую природу. В связи с чем возникает вопрос: как действующее российское законодательство будет охранять права авторов и правообладателей в подобных цифровых экосистемах, которые достаточно активно проникают в нашу жизнь. Действующая нормативная база, закреплённая в части четвертой Гражданского кодекса Российской Федерации (далее – ГК РФ), пусть и ориентирована изначально на традиционные виды объектов интеллектуальной собственности, даёт правоприменителю необходимый базис, позволяющий разрешать вопросы в эпоху генеративного искусственного интеллекта и метавселенных без специ-

ального законодательства [1]. Анализ положений ГК РФ ее положений позволяет сделать вывод о том, что многие нормы обладают достаточной гибкостью и могут быть применены к объектам, интегрированным метавселенных.

Основная часть. Перечень объектов авторских прав, предусмотренный ст. 1259 ГК РФ не является исчерпывающим, в связи с чем к ним можно отнести и произведения, созданные в рамках метавселенных: 3D-модели, объекты цифровой архитектуры, дизайн виртуальных пространств и произведения цифрового искусства. Верховный Суд РФ неоднократно указывал, что размещение произведения в сети Интернет является способом использования в контексте правомочий, составляющих исключительное право правообладателя, а копирование цифрового объекта без согласия автора является нарушением исключительных прав [2]. Метавселенные по правовому режиму близятся к сети Интернет, в связи с чем имеет смысл утверждать, что публикацию цифрового объекта в метавселенной подлежит рассматривать как форму доведения произведения до всеобщего сведения (п. 11 ч. 2 ст. 1270 ГК РФ). А отсутствие в национальной правовой системе обязанности правообладателя регистрировать права на объекты авторского права для придания им правовой охраны, позволяет использовать существующие механизмы защиты на такие объекты без специального регистрационного порядка, который может претерпеть изменения в эпоху метавселенных. Существующая практика по квалификации результата интеллектуальной деятельности в качестве охраняемого объекта авторского права при наличии творческого вклада должна претерпеть изменения и в части расширения и конкретизации перечня возможных действий, выступающих доказательством внесения творческого вклада в создание объекта.

Перспективным представляется и применение положений о промышленных образцах. С учетом сформировавшейся практики, не признающей пользовательский интерфейс объектом авторских прав, в альтернативной стратегии защиты может служить оформление прав на промышленный образец [5]. Подход, отраженный в Директиве (ЕС) 2024/2823 Европейского парламента и Совета от 23 октября 2024 г. о правовой защите промышленных образцов, определяющий в качестве промышленного образца как объект, имеющий материальную форму, так и объект, материализованный в нефизической форме, является наиболее соответствующим реалиям [4]. Для реализации указанного подхода в рамках национального законодательства действующая ст. 1352 ГК РФ подлежит расширительному толкованию в части отнесения к изделию также цифрового объекта, обладающего признаками новизны и оригинальности.

Вопрос правовой охраны товарных знаков в условиях функционирования метавселенных приобретает особую актуальность, поскольку именно средства индивидуализации позволяют обеспечивать устойчивость гражданского оборота и предотвращать недобросовестное использование брендов в цифровой среде. Согласно ст. 1477 ГК РФ товарный знак является обозначением, служащим для индивидуализации товаров юридических лиц или индивидуальных предпринимателей. В традиционной доктрине речь идет о материальных товарах, однако экономическая практика последних лет демонстрирует формирование особого сегмента виртуальных объектов, обладающих стоимостью и вовлекае-

мых в гражданский оборот. Виртуальные аватары, цифровая одежда, аксессуары, элементы виртуальной недвижимости или произведения цифрового искусства – все это образует категорию «виртуальных товаров», использование товарных знаков в отношении которых должно рассматриваться как охраняемое законом. Ключевым дискуссионным вопросом в данном контексте является проблема классификации таких товаров в рамках Международной классификации товаров и услуг (МКТУ), на которую опирается российская и международная система регистрации товарных знаков. Действующая редакция МКТУ ориентирована преимущественно на физические товары, что порождает неопределенность при отнесении виртуальных объектов к определенным классам. Зарубежная практика демонстрирует тенденцию к преодолению этого пробела посредством подачи заявок, прямо указывающих на использование товарных знаков для виртуальных товаров (9, 35, 41, 42 классы). Так, корпорация Nike зарегистрировала знаки для обозначения цифровой одежды и обуви, предназначенной исключительно для использования в метавселенных. Прецедентное значение имеет и дело *Hermès International v. Rothschild* (США, 2023), в котором суд признал NFT-реплики сумок «Birkin» нарушением исключительных прав правообладателя, несмотря на отсутствие физического аналога [6]. В Европейском союзе развивается концепция, согласно которой виртуальные товары могут охраняться в рамках действующего регулирования товарных знаков, без необходимости создания отдельной правовой категории. Регламент (ЕС) № 2017/1001 «О товарных знаках Европейского союза» закрепляет универсальные критерии охраноспособности, которые применимы и в цифровой среде [3]. Это свидетельствует о признании охраны товарных знаков как универсального механизма, способного адаптироваться к изменяющимся условиям экономики, подвергающейся диджитализации. Для российского правового порядка концептуальных препятствий к применению действующих норм части четвертой ГК РФ в отношении виртуальных товаров нет, использование товарного знака в метавселенной может квалифицироваться как его использование в сети Интернет. Для обеспечения правовой определенности представляется целесообразным формирование блока мягкого права, регулирующего порядок охраны товарных знаков применительно к виртуальным товарам и NFT, на доктринальном уровне возможно обсуждение вопроса о необходимости дополнения МКТУ отдельными позициями, отражающими специфику виртуальных объектов.

Представляется, что охрана изобретений в условиях метавселенных может задать новые векторы в стратегии правовой охраны. Уже сейчас законодательство позволяет правообладателям оформлять права на разработки в области информационных технологий и искусственного интеллекта, однако вопросы с приданием правовой охраны изобретениям, сгенерированным искусственным интеллектом, который является ключевым генератором новых функциональных возможностей метавселенных, по-прежнему остаются не определенными. Разрешение данного вопроса с учетом экономических предпосылок позволит очертить правовой режим для технических решений, функционирующих исключительно в виртуальной среде.

Ноу-хау в условиях метавселенных приобретает особое содержание. Согласно ст. 1465 ГК РФ секретом производства признаются сведения, обладающие коммерческой ценностью и охраняемые в силу неизвестности их третьим лицам. Виртуальные миры расширяют рамки этого понятия: охране могут подлежать алгоритмы синхронизации пользователей, протоколы рендеринга, способы защиты цифровых объектов, модели функционирования маркетплейсов и системы монетизации. Метавселенная выступает не только носителем собственных секретов производства, но и пространством оборота ноу-хау ее пользователей, что требует разграничения между информацией, принадлежащей платформе, и сведениями, охраняемыми резидентами. Решение возможно через пользовательские соглашения, устанавливающего порядок взаимодействия обладателей информации, однако практические договорные механизмы подлежат выработке и проверке на устойчивость.

Особое значение имеет фиксация режима конфиденциальности. В цифровой среде традиционных мер (договоров, регламентов), предусмотренных законодательством о коммерческой тайне, недостаточно – необходимы смарт-контракты, криптографическая защита, токенизированный доступ, что обеспечит охрану и служат доказательствами в случае спора. Ранее рассмотренные подходы, рассматривающие использование объекта интеллектуальной собственности в метавселенных в качестве такого способа использования, как размещение в сети Интернет (доведение до всеобщего сведения) порождают ряд вопросов о применимости ноу-хау как формы правовой охраны к объектам интеллектуальной собственности, интегрированным непосредственно в метавселенные.

Таким образом, анализ институтов интеллектуальной собственности в контексте метавселенных показывает, что цифровые миры формируют новые формы проявления объектов интеллектуальной собственности, которые требуют адаптации к особенностям виртуальной экономики. Основным вызовом заключается в трансграничном характере виртуальных экосистем и высокой динамике оборота цифровых объектов, что ставит под вопрос традиционные подходы. Особое внимание заслуживает институт ноу-хау, играющий ключевую роль в обеспечении функционирования метавселенных. Технологические, организационные и экономические сведения, используемые платформами и пользователями, формируют основу конкурентного преимущества, однако правовые механизмы их охраны пока недостаточно разработаны.

Для российского права перспективным направлением является развитие разъяснений по применению существующих национальных норм к объектам метавселенных. Данная тема представляет интерес и для Евразийской системы охраны интеллектуальной собственности, ведь только комплексное исследование институтов интеллектуальной собственности через призму национального и регионального регулирования, позволит обеспечить баланс интересов участников виртуальных экосистем и создать устойчивую правовую основу для развития цифровой экономики.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 22.07.2024) // Собрание законодательства РФ. 2006. № 52 (1 ч.). Ст. 5496
2. Обзор судебной практики рассмотрения гражданских дел, связанных с нарушением авторских и смежных прав в информационно-телекоммуникационной сети Интернет (утв. Президиумом Верховного Суда РФ 29.05.2024. URL: https://www.consultant.ru/document/cons_doc_LAW_477422/ (дата обращения: 06.09.2025).
3. Регламент (ЕС) 2017/1001 Европейского Парламента и Совета от 14 июня 2017 г. о товарном знаке Европейского Союза., Европейский союз (ЕС). URL: <https://www.wipo.int/wipolex/ru/legislation/details/18298> (дата обращения: 06.09.2025).
4. Директива (ЕС) 2024/2823 Европейского парламента и Совета от 23 октября 2024 г. о правовой защите промышленных образцов. URL: <https://eur-lex.europa.eu/eli/dir/2024/2823/oj/eng> (дата обращения: 06.09.2025).
5. Apple Computer, Inc. против Microsoft Corp., 35 F.3d 1435 (9th Cir. 1994). URL: <https://law.justia.com/cases/federal/appellate-courts/F3/35/1435/605245/> (дата обращения: 06.09.2025).
6. United States District Court of the Southern District of New York [2023]: Hermes Int'l v. Rothschild, No. 22-CV-384-JSR, 2023 WL 1458126 (S.D.N.Y. Feb. 2, 2023). URL: <https://www.wipo.int/wipolex/en/judgments/details/1841> (дата обращения: 06.09.2025).

А. С. Васильева,

магистрант,

Московский государственный университет

имени М.В. Ломоносова

Развитие цифровых платформ и трудовое право

Аннотация. Данная статья посвящена актуальной в настоящее время проблеме – особенностям правового регулирования применения труда с использованием цифровых платформ. В ходе исследования был проанализирован зарубежный опыт разграничения трудовых и гражданско-правовых отношений возникающих с использованием цифровых платформ, а также исследован вступающий в силу в 2026 году Федеральный закон «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации». Сделаны выводы о целесообразности дополнения и уточнения условий для отнесения деятельности «исполнителей» на цифровых платформах к гражданско-правовым отношениям.

Ключевые слова: цифровые платформы, междисциплинарность, платформенная занятость, трудовые отношения, цифровизация, цифровые технологии, цифровая трансформация

A.S. Vasilyeva,

Master's student,

Lomonosov Moscow State University

Development of digital platforms and labor law

Annotation. This article is devoted to a currently relevant problem – the specifics of the legal regulation of the use of labor using digital platforms. The study analyzed foreign experience in distinguishing labor and civil law relations arising from the use of digital platforms, and also examined the Federal Law "On Certain Issues of Regulating the Platform Economy in the Russian Federation", which comes into force in 2026. Conclusions are drawn about the expediency of supplementing and clarifying the conditions for classifying the activities of "performers" on digital platforms as civil law relations.

Keywords: digital platforms, interdisciplinarity, platform employment, labor relations, digitalization, digital technologies, digital transformation

Введение. В настоящее время цифровая экономика является одним из ведущих факторов экономического роста, развития торговли, обеспечения притока различных ресурсов и стимулирования увеличения предпринимательской активности [12. Р. 2203]. Цифровая экономика непосредственно основывается на внедрении и популяризации использования цифровых платформ.

Основная часть. Цифровые платформы, в данном случае, рассматриваются как «инновационная форма организации рынка и экономической деятельности с посреднической функцией» [5].

В силу новизны явления цифровых платформ и представление о них как о целой экосистеме создает сложности в обеспечении их правового регулирования.

Как и любое новое явление цифровая платформа становится новым объектом правовых исследований, требующим, с одной стороны, тщательного анализа, с другой стороны, скорости реагирования на изменяющийся мир [4. С. 131].

Основные две методологические сложности, с которыми сталкиваются при исследовании правового регулирования цифровых платформ:

- жесткость их регулирования с целью обеспечения стабильности и безопасности;
- отсутствие должного регулирования [5. С. 7].

Обе методики имеют негативные и позитивные последствия. Негативное последствие жесткого регулирования состоит в стагнировании экономического роста, что перекрывает позитивные результаты использования платформенной экономики.

Отсутствие должного регулирования порождает большое количество лакун, ведущих к неодинаковому применению норм права к схожим отношениям.

Представляется, что оптимальной концепцией правового регулирования цифровых платформ будет нахождение баланса между различными методиками правового регулирования в различных видах правовых отношений для обеспечения развития экономики. Как отмечает R.E. Lofstedt, методологический ориентир для такой многоаспектной проблематики должен быть принцип предосторожности, т.к. необходимо находить такой оптимум регулирования, который обеспечит экономический рост [11].

Экономический рост прежде всего переопределяется техническим развитием, количественными характеристиками и качественным состоянием природных и трудовых ресурсов, влиянием глобализации, экономической политикой и т.д. [7. С. 30]. Для обеспечения экономического роста также требуется найти баланс и обеспечить качественное взаимодействие между ресурсами.

Одним из аспектов, который может обеспечивать экономическое развитие и рост, являются трудовые ресурсы.

Именно трудовые ресурсы являются главной производительной силой общества и позволяют приводить в действие экономику, поэтому от их правового положения зависит развитие цифровых платформ, национальная безопасность и стабильность и как результат экономический рост.

Трудовым ресурсом государства является часть населения, которая обладает физическими и умственными способностями для трудовой деятельности для трудовой деятельности.

Для повышения их мотивации к труду Трудовой Кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (далее – ТК РФ) устанавливает гарантии трудовых прав и свобод граждан, создает благоприятные условия труда, защиту прав и интересов [1].

Регулирование применения труда с использованием цифровых платформ является сложным междисциплинарным вопросом, охватывающим трудовое и гражданское права. Проблема разграничения трудовых и гражданско-правовых

отношений при организации труда на цифровых платформах не урегулирована. Во многих странах данная проблема активно находит свое отражение в судебной практике.

Так, в 2019 году Мюнхенский земельный суд Германии рассмотрел исковое заявление пользователя цифровой платформы к провайдеру об установлении трудовых отношений. В исковом заявлении утверждалось, что в возникших отношениях истец подчинялся правилам платформы (трудовому распорядку), задачи назначались императивно без возможности выбора, работал в течении 20 часов в неделю и систематически получал вознаграждение. Суд вынес решение, что у истца отсутствовала обязанность выполнять какие-либо задачи на платформе, и постановил, что труд в данном случае отсутствует, поскольку отсутствует такой его характерный критерий как личная зависимость, поэтому отношения не могут быть признаны трудовыми [9].

В 2020 году Кассационный суд Франции признал водителей Uber работниками. Суд проанализировал, что свобода водителей заключается лишь в возможности выбирать время и место работы, однако в иных аспектах водители находятся в подчинении работодателя: их контролирует работодатель через приложения, работодатель их может ограничить, заблокировать доступ к мобильному приложению, если на водителя поступают жалобы пассажиров или если водитель часто отказывается от поездок [13].

В 2020 году суд Калифорнии по иску Генерального прокурора Калифорнии признал водителей компаний Uber и Lyft работниками. Мотивировочная часть решения была схожа с мотивировочной частью решения Кассационного суда Франции.

В 2021 году компания Uber проиграла дело в Верховном суде Великобритании по вопросу о правовом статусе водителей. Судьи единогласно постановили, что водители Uber являются работниками, имеющими право на такие права, как минимальная заработная плата, отпускные и перерывы для отдыха [14].

В 2022 году во Франции вынес решение о том, что компания Deliveroo, специализирующаяся на доставке еды и продуктов, должна уплатить штраф в размере 9,7 млн. евро за неуплату социальных взносов. Данное решение было мотивировано тем, что приложение, в котором работали курьеры, позволяло определять их геолокацию в режиме онлайн, отследить маршрут, действующая рейтинг система позволяла премировать и депремировать курьеров. Суд постановил, что данные признаки указывают на трудовые отношения [15].

В наиболее известных судебных прецедентах судебная власть встает на сторону признания отношений между работником («исполнителем») и цифровой платформой трудовыми. Однако при таком регулировании отношений между работниками и работодателем имеет несколько негативных последствий:

- неопределенность вида отношений между «исполнителем» и цифровой платформой;
- отсутствие гарантий для «исполнителей», реализующих свое право на труд на цифровой платформе;
- повышенная нагрузка на судебную систему из-за споров о признании отношений трудовыми;

– потенциальная дискриминация «исполнителей» цифровых платформ в связи с неоднозначностью решения вопроса о наличии или отсутствии трудовых отношений;

– убытки компаний – цифровых платформ в связи с признанием судами отношений между «исполнителем» и цифровой платформой трудовыми.

Таким образом, скудность правового регулирования отношений на цифровых платформах и попытки выстраивания политики защиты «исполнителей» цифровых платформ с помощью судебных решений приводят к негативным последствиям, представляющим угрозу стабильному росту и развитию экономики.

Кроме того, такая недостаточность правового регулирования, но при этом развивающаяся в одном направлении судебная практика, также ограничивает цифровые платформы, т. к. для наиболее выгодной реализации предпринимательской деятельности на цифровых платформах анализируется правовая ситуация о рисках признания отношений с «исполнителями» трудовыми, и исходя из этого делается вывод о необходимости заключения между «исполнителем» и цифровой платформой трудового или гражданско-правового договора.

В настоящее время для организации регулирования цифровых платформ Федеральный закон от 31.0.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации», вступающий в силу 01.10.2026 (далее – ФЗ «О платформенной экономике») [2].

Согласно п. 1 ст. 15 ФЗ «О платформенной экономике» «исполнитель», являющийся индивидуальным предпринимателем или физическим лицом, применяющим специальный налоговый режим, лично выполняющий работы, оказывающий услуги, вправе осуществлять такую деятельность в рамках гражданско-правовых отношений с использованием посреднической цифровой платформы в случае соответствия его деятельности одновременно следующим требованиям:

1) предлагаемый «исполнителю» к исполнению заказ направлен на выполнение конкретной работы, оказание конкретной услуги и не предусматривает наличия у такого «исполнителя» режима (графика) работы и соблюдения им правил внутреннего трудового распорядка и содержащих нормы трудового права локальных нормативных актов оператора и (или) пользователя-заказчика;

2) «исполнитель» самостоятельно принимает решение о выполнении работ, об оказании услуг и вправе не принимать заказ без применения к нему мер ответственности, за исключением случаев добровольного выбора таким «исполнителем» периода времени, в течение которого он обязуется выполнять работы, оказывать услуги;

3) «исполнителю» не допускается выполнение дополнительных работ, оказание дополнительных услуг;

4) за выполненную работу или оказанную услугу с использованием посреднической цифровой платформы «исполнителю», являющемуся физическим лицом, оператором начисляется вознаграждение в рамках каждого заказа отдельно;

5) выполнение работ, оказание услуг «исполнителем», являющимся физическим лицом, не предусматривает:

а) привлечения третьих лиц;

б) предоставления «исполнителю» дополнительных социальных гарантий за счет оператора и (или) пользователя-заказчика;

в) предоставления оператором и (или) пользователем-заказчиком «исполнителю», еженедельных выходных дней и отпуска, предусмотренных трудовым законодательством Российской Федерации.

Таким образом, ФЗ «О платформенной экономике» предусматривает несколько условий, при которых оператор цифровой платформы может вести деятельность в рамках гражданско-правовых отношений.

Однако в вышеприведенных положениях ФЗ «О платформенной экономике» существует место для злоупотребления со стороны операторов цифровой платформы по отношению к исполнителям.

Во-первых, условие о наличии конкретной работы может быть подвергнуто различному истолкованию. В связи с тем, что работа на цифровых платформах осуществляется в форме фриланса или работы по требованию [6. С. 15], она всегда будет направлена на выполнение конкретного задания. При этом, чаще всего, при завершении выполнения одного задания, «исполнитель» переходит к следующему, поэтому критерий «конкретного задания» размывается.

Во-вторых, формальная возможность выполнения условий об отсутствии режима (графика) работы и обязанности по соблюдению правил внутреннего трудового распорядка зависит от цифровой платформы. Так, если понимать под режимом (графиком) работы – зафиксированные в письменной форме данные о начале и окончании рабочего дня, времени перерыва для отдыха и питания и т.п., то наличие такого документа зависит от цифровой платформы, также как и утверждение правил внутреннего трудового распорядка.

Таким образом, из формального толкования закона следует что, если данные документы цифровая платформа не согласовала и не утвердила, тогда ряд условий для заключения гражданско-правового договора выполняется. Данный подход может необоснованно ограничить права «исполнителей».

В данном случае, требуется рассматривать существует ли в действительности систематичность в выполнении «исполнителем» задач. Режим работы «исполнителя» на цифровой платформе может не требовать определенного расписания и согласования с самой цифровой платформой, при этом «исполнитель», учитывая загруженность платформы и стоимость оплаты за выполнения заданий, может систематично выходить в различные временные промежутки.

Правила внутреннего трудового распорядка как положения, содержащие порядок приема и увольнения, основные права, обязанности и ответственность сторон, режим работы, время отдыха, меры поощрения и взыскания, а также иные вопросы регулирования отношений (абз. 4 ст. 189 ТК РФ), Во-первых, может отсутствовать у цифровой платформы в связи ее нежеланием утверждать данный локальный нормативный правовой акт, Во-вторых, могут находиться у цифровой платформы в документах с различными наименованиями, при этом «исполнители» при выполнении заданий в любом случае подчиняются правилам платформы по режиму работы, времени отдыха мер поощрения, ответственности и т.д.

В-третьих, условие об отсутствии обязанности принять задания, кроме того периода, когда «исполнитель» сам обязался принимать задания также является неоднозначным, т.к. фактически:

- иллюстрирует случай, когда «исполнитель» согласовал график и принимает задачи, что в совокупности, может быть, одним из признаков трудовых отношений;

- создает иллюзию, что «исполнитель» может отказаться от закона без применения мер ответственности. Часто «исполнитель» может использовать цифровую платформу как единственный источник доходов, поэтому он не может свободно отказываться от задач в определенные промежутки времени. Также меры ответственности является неопределенным понятием.

Цифровая платформа может применять косвенные методы воздействия при отказах «исполнителя» от выполнения задания, например, снижать рейтинг исполнителя в системе, снижать уровень оплаты, ограничивать географию выполнения заданий исполнителем (в случае, если выполнение заданий на платформе связано с территорией) и т.д.

В-четвертых, условие об осуществлении деятельности в рамках гражданско-правовых отношений на цифровой платформе, если оплата осуществляется отдельно за каждый заказ, а также предоставление цифровой платформой «исполнителю» социальных гарантий, отпуска, еженедельных выходных дней, также не являются определяющими в разграничении гражданско-правовых и трудовых отношений, т.к. его исполнение зависит от воли цифровой платформы.

Таким образом, проанализированные условия закона не могут являться существенными критериями разграничения гражданско-правовых и трудовых отношений. Их целесообразно изменить:

- в подп. 4 п. 1 ст. 15 ФЗ «О платформенной экономике» включить критерий осуществления периодических выплат работнику, «которые являются для него единственным и (или) основным источником доходов» [3], следовательно изложить как: «за выполненную работу или оказанную услугу с использованием посреднической цифровой платформы «исполнителю», являющемуся физическим лицом, оператором начисляется вознаграждение в рамках каждого заказа отдельно, не являющиеся для него единственным и (или) основным источником доходов»;

- добавить подп. 5 п. 1 ст. 15 ФЗ «О платформенной экономике»: «цифровая платформа не обеспечивает «исполнителя» инструментами, материалами и механизмами работодателя».

Заключение. Таким образом, цифровые платформы являются новой формой организации рынка. Для ее функционирования и обеспечения экономического роста необходимо нахождение баланса в ее правовом регулировании. Важнейшая проблема разграничения гражданско-правовых и трудовых отношений при организации труда на цифровых платформах в настоящее время не урегулирована.

Условия для возможности регулирования деятельности «исполнителя» на цифровой платформе в рамках гражданско-правовых отношений поименованы во вступающем в силу 01.10.2026 Федеральном законе «О платформенной экономике» часто зависят от воли цифровой платформы и требуют дополнений.

Список литературы

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // СЗ РФ. 07.01.2002. № 1 (ч. 1). Ст. 3.
2. Федеральный закон от 31.07.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» // СЗ РФ. 04.08.2025. № 31. Ст. 4643.
3. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 06.02.2024 № 43-КГ23-8-К6 // Бюллетень Верховного Суда РФ. 2024. № 10.
4. Васильева А.С. искусственный интеллект и защита персональных данных работников // Цифровые технологии и право. Сборник научных трудов III Международной научно-практической конференции. В 6-ти томах. Казань, 2024. С. 77 – 81.
5. Кошель А.С., Кузьминов Я.И., Кручинская Е.В., Лесив Б.В. Поиск регуляторного оптимума деятельности цифровых платформ (сравнительный анализ) // Право. Журнал Высшей школы экономики. 2025. Т. 18. № 2. С. 4–58.
6. Линец А.А. Роль трудового права в экономической системе общества на современном этапе: дис. ... д-ра юр. наук. М., 2021. 509 с.
7. Нуртдинов Р.М. Экономический рост и его факторы: учебно-методическая разработка. Набережные Челны: Камский издательский дом. 2010. 95с.
8. Потапов А.В. Юридическое лицо как субъект трудовых и непосредственно связанных с ними отношений: дис. ... канд. юр. наук. М. 2022. 231 с.
9. Landesarbeitsgericht München, Urteil vom 4.12.2019/ Aktenzeichen: 8 Sa 146/19 URL: https://www.arbg.bayern.de/imperia/md/content/stmas/lag/muenchen/pressemitteilung_-_crowd.pdf (дата обращения: 22.08.2025)
10. pressemitteilung_-_crowd.pdf (дата обращения: 22.08.2025)
11. Lofstedt R. E. (2023) The precautionary principle: risk, regulation and politics. Process, Safety and Environmental Protection, vol. 81, no. 1, pp. 36–43.
12. Paun C., Ivascu C., Olteteanu A., Dantis D . (2024) The main drivers of e-commerce adoption: a global panel data analysis. Journal of Theoretical and Applied Electronic Commerce Research, vol. 19, issue 3, pp. 2198–2217.
13. URL: <https://www.kommersant.ru/doc/4276785>
14. Uber Loses U.K. Ruling on Drivers in Blow to Gig Economy. URL: <https://www.bloomberg.com/news/articles/2021-02-19/uber-loses-u-k-top-court-ruling-on-drivers-employment-status?srnd=markets-vp> (дата обращения: 22.08.2025).
15. AFP: суд во Франции оштрафовал компанию по доставке Deliveroo почти на €10 млн. URL: <https://tass.ru/ekonomika/15636391> (дата обращения: 06.09.2022)

Смарт-контракты на платформе цифрового рубля

Аннотация. Цель исследования состоит в выявлении гражданско-правовых проблем применения смарт-контрактов при осуществлении расчетов с цифровым рублем. Автор анализирует предложенные Банком России механизмы реализации смарт-контрактов на платформе цифрового рубля. Автор приходит к выводу, что действующее регулирование не является достаточным, поскольку не содержит норм о порядке регистрации договора с применением смарт-контракта на платформе цифрового рубля, значении регистрации договора на такой платформе, порядке исполнения смарт-контракта. Подчеркивается необходимость разработки комплекса нормативных положений, которые обеспечат стабильность и безопасность расчетов цифровыми рублями посредством смарт-контрактов.

Ключевые слова: цифровой рубль, смарт-контракты, Банк России, информационная система, заключение договора, регистрация договора, исполнение обязательств

N. I. Gasnikov,

postgraduate student,

St. Petersburg State University of Economics

Smart contracts on the digital ruble platform

Abstract. The purpose of the study is to identify the civil law problems of using smart contracts when making payments with the digital ruble. The author analyzes the mechanisms proposed by the Bank of Russia for implementing smart contracts on the digital ruble platform. The author concludes that the current regulation is not sufficient, since it does not contain rules on the procedure for registering an agreement using a smart contract on the digital ruble platform, the meaning of registering an agreement on such a platform, and the procedure for executing a smart contract. The need to develop a set of regulations that will ensure the stability and security of settlements in digital rubles through smart contracts is emphasized.

Keywords. digital ruble, smart contracts, Bank of Russia, information system, conclusion of an agreement, registration of an agreement, fulfillment of obligations

Введение. Банк России (далее – ЦБ РФ) рассматривает платформу цифрового рубля не просто как новое средство для осуществления платежей, но и как инструмент трансформации основных процессов в экономике, предоставляющий новые возможности участникам гражданского оборота [1]. Одной из них

должна стать возможность применения смарт-контрактов при расчетах цифровыми рублями. ЦБ РФ указывает, что смарт-контракты, также обозначенные как самоисполняемые сделки, обеспечат мгновенное исполнение сделок, связанных с переводом денежных средств между субъектами гражданского права при наступлении определенных сторонами условий, исключат риски их неисполнения [1]. Из этого следует, что платформа цифрового рубля будет не просто совокупностью специальных банковских счетов, между которыми будет осуществляться движение цифровых рублей, но и инструментом, позволяющим следить за исполнением субъектами принятых на себя обязательств, что обуславливает актуальность гражданско-правового осмысления возможных юридических препятствий и последствий их применения.

Основная часть. Вопрос о правовой природе смарт-контрактов является дискуссионным в отечественной цивилистике. Некоторые авторы полагают, что смарт-контракты являются самостоятельным договорным типом [2]. В других работах указывается, что необходимо различать смарт-контракт как программу и как ««цифровую надстройку» классического договора»[3], которая предназначена для решения технических вопросов исполнения обязательств. В этом отношении смарт-контракт относится к категории «особых несамостоятельных договорных конструкций, расположенных в первой части ГК РФ, которые отражают особенности заключения или специальные правовые последствия любого гражданско-правового договора, если он отвечает указанным законом признакам»[4].

Смарт-контракты получили нормативное закрепление в статье 309 ГК РФ, согласно которой, допускается включение в сделку условия об исполнении ее сторонами возникающих из нее обязательств при наступлении определенных обстоятельств без направленного на исполнение обязательства отдельно выраженного дополнительного волеизъявления его сторон путем применения информационных технологий, определенных условиями сделки. Из этой нормы следует, что специальное условие об исполнении обязательств с помощью «смарт-контракта» применимо к любым видам договоров. Таким образом, действующее законодательство подтверждает обоснованность позиции, квалифицирующей его не в качестве самостоятельного договорного типа, а способа формирования условия исполнения обязательств.

Если обратиться к описанию предполагаемого ЦБ РФ применения смарт-контракта при расчетах цифровыми рублями, изложенного в Концепции цифрового рубля и докладе об актуальном состоянии проекта [1, 5], то следует сделать вывод, что оно в полной мере соответствует формулировке ст. 309 ГК РФ. ЦБ РФ предполагает, что применение смарт-контракта будет происходить в три этапа:

- заключение договора, содержащего условие об оплате цифровыми рублями с применением смарт-контракта, за пределами платформы цифрового рубля (например, в иной информационной системе);
- регистрация договора на платформе ЦБ РФ;
- исполнение после поступления на платформу необходимой информации.

Условие о применении смарт-контракта при оплате цифровыми рублями может быть включено в договор, заключенный в любой из предусмотренных законом форм, в том числе устной, поскольку законодательный запрет отсутствует. Для этого необходимо только наличие у обеих сторон договора соответствующего счета. При этом возникает вопрос о порядке передачи информации о факте заключении договора и его условий для принятия к исполнению в рамках платформы цифрового рубля, а также способах идентификации субъектов, передающих соответствующие распоряжения. В настоящее время закон, нормативные акты ЦБ РФ и типовые формы договоров указанных положений не содержат, что следует признать недостатком правового регулирования, без устранения которого эффективное и безопасное применение смарт-контрактов не представляется возможным.

Далее возникает вопрос о значении регистрации договора на платформе цифрового рубля. Этот этап описанной в документах ЦБ РФ процедуры вызывает ассоциации с государственной регистрацией сделок, предусмотренной ст. 164 ГК РФ и необходимой для наступления правовых последствий сделки. С одной стороны очевидно, что такая регистрация на платформе ЦБ РФ не является государственной регистрацией по смыслу приведенной нормы, и в настоящее время отсутствуют законные основания для отступления от общего правила, установленного ст. 432 и 433 ГК РФ. При этом возникают обоснованные сомнения в исполнимости договора в части оплаты, когда договор, содержащий условие об оплате цифровыми рублями с применением смарт-контракта, считается заключенным до его регистрации на платформе, однако в такой регистрации в последствии будет отказано. В этом случае сторона, в пользу которой должна быть произведена оплата, будет вынуждена рассчитывать либо на заключение дополнительного соглашения об изменении порядка оплаты, либо требовать расторжения договора и взыскания убытков. Такие последствия не соответствуют цели создания надежного инструмента исполнения сделок. Это, в свою очередь, обуславливает необходимость нормативного закрепления значения такой регистрации, ее условий (например, требование о достаточности средств на счете), ее последствий (например, положение о блокировании средств на счете до определенного договором срока), а также последствий отказа в регистрации для обеспечения стабильности и предсказуемости отношений между участниками гражданского оборота.

Осуществление перевода на основании договора, содержащего условие о применении смарт-контракта, является услугой ЦБ РФ, оказываемой в рамках договора счета цифрового рубля. При этом в настоящее время нормативные акты не содержат специальных положений о порядке ее оказания, в том числе формы и способе передачи информации, являющейся основанием для перевода средства, способов верификации ее источника, что является существенным с учетом целей внедрения рассматриваемой разновидности расчетов.

Заключение. В настоящее время совокупность правовых норм, предназначенных для регулирования отношений, возникающих в связи с применением смарт-контрактов при расчетах цифровыми рублями, явно является недостаточной. Необходимы разработка и принятие комплекса норм, который сформирует

порядок заключения и исполнения подобных договоров в целях достижения предполагаемых целей внедрения технологии смарт-контрактов при расчетах. Интересны и перспективны исследования о том, что дальнейшее развитие концепта метавселенных в России будет зависеть от результатов тестирования цифрового рубля [6. С. 201].

Список литературы

1. Цифровой рубль: текущий статус проекта // Сайт Банка России. URL: https://cbr.ru/content/document/file/177415/digital_ruble_30062025.pdf (дата обращения 01.09.2025).
2. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. Т. 16. № 3. С. 32–60.
3. Рожкова М. А. Смарт-контракт в договорной практике: программный код и «цифровая надстройка» классического договора // Журнал Суда по интеллектуальным правам. 2023. № 1(39). С. 60–72.
4. Ефимова Л. Г., Сизимова Б. Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 21–28.
5. Концепция цифрового рубля // Сайт Банка России. URL: https://www.cbr.ru/content/document/file/120075/concept_08042021.pdf (дата обращения 01.09.2025).
6. Ситников М. С. Финансово-правовое развитие общественных отношений с использованием цифровых валют в метавселенных // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 200–220. <https://doi.org/10.21202/jdtl.2024.11>. EDN: yxcjno.

А. Е. Головенкина,
студент,
ФГБОУ ВО «Марийский государственный университет»

**Революционные перспективы или правовой хаос?
Защита авторских прав в эпоху искусственного интеллекта**

Аннотация: Целью данной статьи является рассмотрение спорных вопросов авторства произведений, созданных с использованием нейросетей, а также возможности предоставления правовой охраны таким произведениям. Изучение подходов к определению творчества с учетом текущего развития технологии искусственного интеллекта (ИИ) на основе актуальной судебной практики.

Ключевые слова: искусственный интеллект, автор, интеллектуальная собственность, результат интеллектуальной деятельности, творчество, автор, новые технологии, маркировка

A. E. Golovyonkina,
4th year student of the Faculty of Law, Mari State University,

**Revolutionary prospects or legal chaos?
Protection of copyright in the era of artificial intelligence**

Abstract: The purpose of this article is to address the controversial issues of authorship of works created using neural networks, as well as the possibility of granting legal protection to such works. The article examines approaches to defining creativity, considering the current development of artificial intelligence (AI) technology, based on relevant judicial practice.

Keywords: artificial intelligence, author, intellectual property, result of intellectual activity, creativity, author, new technologies, marking

Введение. Тенденция развития права интеллектуальной собственности в условиях стремительного совершенствования искусственного интеллекта в настоящее время является одной из самых актуальных и обсуждаемых тем. Сейчас новые технологии используются повсеместно, в связи с чем их правовая регламентация – важный для разрешения вопрос. Нейросеть не просто помогает человеку в умственной работе, а она способна изменить окружающий мир по своему замыслу и поменять все законы мироздания так, что мы сможем заметить это уже слишком поздно.

Основная часть. Искусственный интеллект (далее – ИИ) стал настоящим цифровым другом для всего человечества в двадцать первом веке. По правде, он стал не только оптимальным инструментом, как первоначально предполагалось,

а вовсе крупнейшем героем национальных стратегий и элементом частого, актуального обсуждения. Изучение правового регулирования новых технологий – необходимая профессиональная цель, поскольку искусственный интеллект является одним из самых успешных изобретений в истории человечества, ни одна технология до сегодняшнего дня даже отдаленно не приближалась к способностям человека. Однако его появление привело многих людей, особенно молодое поколение, к неправильному пониманию сути результатов, полученных новыми технологиями. Нередко имитацию результатов интеллектуальной деятельности ошибочно принимают за оригинальные творения, полагая, что такие подделки заслуживают правовой защиты.

Сопоставляя человеческий и компьютерный интеллект, мы увидим одинаковый результат – правильная интерпретация каких-либо внешних данных, которая производилась ранее мозгом индивида для создания и изобретения чего-то нового. Б. В. Ахлибининский отмечает, что «процесс мышления человека качественно отличается от того, что происходит в машине... В машине нет осознания происходящего в ней процесса...»¹ Но как предотвратить угрозы, которые начинает создавать изобретенная человеком машина?

К счастью или к сожалению, на данный момент репутация и характеристика искусственного интеллекта страдают. Это происходит либо из-за излишней упрощенности, которая проявляется в расплывчатости и неопределенности текста, либо из-за чрезмерной усложненности, которая обусловлена неоправданными фактами.

По этой причине разделяют слабый и сильный искусственный интеллект, подразумевая, что сильный ИИ способен мыслить и осознавать себя, а слабый искусственный интеллект так поступать не может. Термин «слабый искусственный интеллект» используется для того, чтобы подчеркнуть его ограниченность одной установленной задачей. Примеры включают виртуальных помощников, таких как Siri или Alexa, и системы, используемые для рекомендации контента в социальных сетях или для персонализации рекламы. С другой стороны, сильный ИИ относится к теоретической концепции машины с сознанием, разумом, способной к самопознанию и эмоциям, что на данный момент остается в области научной фантастики.

Однако мы не должны забывать о том, что в большинстве своем человек по-прежнему остался творцом по натуре и продолжает писать, создавать и изобретать. Развитие технологии ИИ «разрушает монополию человека на творчество, демистифицирует творчество, снижает уровень индивидуальности и отражения личности-творца в конечном результате»². Самый главный тезис, которого нужно придерживаться в данной проблеме, на мой взгляд, это то, что субъектом творческой деятельности признается именно человек, т. е. гражданин

¹ Ахлибининский Б.В. Кибернетика и тайны психики. Л., 1996. С. 138.

² Сесицкий Е.П. Проблемы правовой охраны результатов, создаваемых системами искусственного интеллекта: дис. ... канд. юрид. наук. М., 2018. С. 45.

творческим трудом которого создан результат интеллектуальной деятельности. Поскольку искусственный интеллект не является субъектом права, он не может признаваться автором произведений интеллектуальной собственности.

Законодатель, называя объект правовой охраны результатом интеллектуальной деятельности, тем самым подчеркивает, что данный объект охраняется в силу того, что он создан интеллектуальным трудом. На то, что результаты интеллектуальной деятельности суть именно результаты, созданные человеком, обращается внимание во многих документах ВОИС.

Тем не менее на уровне этой же Всемирной организации интеллектуальной собственности (ВОИС) концептуально обсуждался вопрос о возможности охраны в режиме интеллектуальной собственности результатов, полученных искусственным интеллектом.³

Что получается в итоге? Правовая неопределенность статуса искусственного интеллекта и подходы к решению вопроса авторства и охраны произведений, созданных с использованием технологий ИИ, различаются в зависимости от страны:

- в США Управление по авторским правам (USCO) подтверждает, что произведения, созданные исключительно ИИ, не могут получить защиту авторского права;
- в Великобритании авторские права могут быть закреплены за лицом, осуществляющим контроль над ИИ;
- в Китае и ЕС продолжается активное обсуждение возможных подходов к данному регулированию.

Большинство стран склоняются к мнению, что авторские права на произведения, созданные с применением искусственного интеллекта, принадлежат лицам или организациям, иницирующим процесс создания, программирующим алгоритмы либо применяющим технологии ИИ в качестве инструментов творчества.

Что же в России?

Согласно Национальной стратегии развития искусственного интеллекта на период до 2030 г., ИИ – это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека».⁴ Право в области искусственного интеллекта и авторского права действительно переживает этап интенсивного развития и адаптации к новым реалиям цифровой эпохи. Законодательство большин-

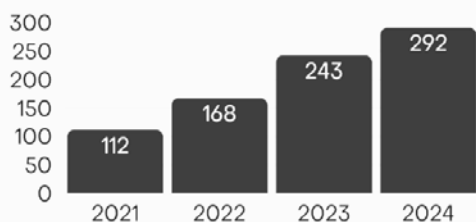
³ Проект концептуального документа по вопросам, касающимся политики в области интеллектуальной собственности и искусственного интеллекта. URL: https://www.wipo.int/meetings/ru/doc_details.jsp?doc_id=470053.

⁴ Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указом Президента РФ от 10.10.2019 N 490 (ред. от 15.02.2024 N 124) "О развитии искусственного интеллекта в Российской Федерации". URL: <http://government.ru/docs/all/124098/>

ства стран мира, включая Россию, активно обновляется и дополняется нормами, но пока о четких универсальных правилах и стандартах в этой сфере говорить рано.

За последние 4 года отмечается рост количества дел, связанных с использованием искусственного интеллекта, на 39%

Наблюдается устойчивая динамика роста количества дел: **от 112 дел в 2021 году до 292 дел в 2024 году**



Резкий рост числа дел, связанных с искусственным интеллектом, совпадает с периодом активного внедрения генеративных моделей искусственного интеллекта и нейросетей в широкий пользовательский сектор (2022-2023 гг.)

В разрезе судебных инстанций преобладают дела **первой инстанции, составляющие более двух третей от общего количества (69,7% - за 4 года)**



Диаграмма наглядно демонстрирует классический «фильтрационный эффект» судебной системы, где каждая последующая инстанция рассматривает значительно меньшее количество дел. Соотношение дел, переходящих из первой инстанции в апелляцию, составляет примерно 32% (186 из 583), а из апелляции в кассацию — около 28% (52 из 186)

Рис. 1 Анализ судебной практики в Российской Федерации по спорам, связанными с использованием искусственного интеллекта

Поэтому сегодня остро встает ряд вопросов: о создании искусственным интеллектом объектов авторских прав и стоит ли эти права вообще подвергать правовой защите. Чтобы прояснить ситуацию, необходимо разграничивать два объекта:

- объект, сгенерированный искусственным интеллектом;
- объект, созданный с помощью искусственного интеллекта.

В первом случае, очевидно, речь идет о создании объектов, которые появляются в результате самостоятельного разрешения ИИ какой-либо задачи, поставленной ему человеком, но при решении которой участие человека минимально и выражается, собственно, только в самой постановке задачи. Как известно, субъектом творческой деятельности признается исключительно человек (и этот постулат пока стабильно неопровержим в подавляющем большинстве стран). При этом в данной ситуации за действиями человека как пользователя никак не усматривается творческий характер. С учетом этого поднимать вопрос о том, что сгенерированные объекты следует относить к объектам интеллектуальной собственности (ИС), как мне кажется, нет никаких оснований. То есть в тех случаях, когда объект создается (генерируется) силами исключительно ИИ, такие объекты не могут рассматриваться в качестве авторских произведений (у них нет автора – человека) и регулироваться законодательством об ИС (эти объекты созданы не в результате творческой деятельности).

Во втором же случае речь идет о тех ситуациях, когда человек использует ИИ в качестве инструмента при решении стоящих перед ним задач и получает желаемый результат. В некоторых случаях подобный результат может вполне подпадать под легальное понятие «результат творческой деятельности» (человека) и, соответственно, под действие норм законодательства об ИС.

Сразу надо оговориться, что в США художнику было отказано в регистрации авторских прав на указанное изображение, а впоследствии (в 2023 году) Бюро авторских прав США отказало художнику и в апелляции на это решение. Бюро авторских прав США, являющееся регулятором в сфере авторского права, в своем отчете признало, что художники, писатели и другие авторы могут получить авторские права на работы, созданные с использованием ИИ, но для этого необходимо, чтобы «творческий вклад автора был ощутим». То есть вопрос о том, будет ли тот или иной объект, созданный с использованием ИИ, признаваться авторским произведением будет решаться в зависимости от значимости творческого вклада человека.

Для того чтобы ИИ создал произведение, необходимо участие человека. Однако, учитывая текущий уровень развития технологии ИИ, некорректно говорить о произведениях, созданных ИИ автономно. Предпосылкой автономности является наличие воли – продукта психики человека. Нейросеть, не имеющая собственной воли, может генерировать контент только по запросу человека. То есть отправной точкой для "творчества" ИИ является воля человека. Логично, что в таком случае именно человек, изъявивший волю на создание конкретного произведения с использованием ИИ, и должен считаться автором созданного произведения.

Деятельность творческого характера открывает широкие возможности для внедрения современных технологических решений, среди которых особое место занимают компьютерные программы и нейронные сети. Тем не менее решающим условием признания результатов такой деятельности объектами интеллектуальной собственности остается наличие значительного элемента человеческой креативности, позволяющий идентифицировать конкретного автора произведения. Этот подход соответствует тенденциям развития современной судебной практики.

Ярким примером является постановление Арбитражного суда г. Москвы, принятое в ноябре 2023 года, относительно незаконного размещения видеоролика, созданного с помощью технологии дипфейков. Технология дипфейков предполагает синтезирование визуального и звукового содержания с использованием методов глубинного машинного обучения (deep learning). Компания ООО "Рефейс Технолоджис" инициировала судебное разбирательство против ООО "Бизнес Аналитика", обвиняя последнюю в незаконном распространении ее аудиовизуальной продукции, созданной усилиями группы творческих сотрудников: режиссера сценария, оператора, специалиста по моушн-дизайну и актера.

Ответчик настаивал на том, что использование технологий искусственного интеллекта автоматически лишает результат права защиты через механизмы авторского права и допускает свободную публикацию такого продукта. Суд отверг эти аргументы, указывая, что технология дипфейков применялась исключительно для модификации существующего материала, а не для его изначально-го создания. Несмотря на активное привлечение искусственного интеллекта, процесс создания контента включал значительную долю личной творческой активности человека.

Суд постановил удовлетворить иск истца полностью, признав факт нарушения ответчиком исключительных прав на произведение. Данный прецедент подтверждает, что действующее российское законодательство охраняет результаты интеллектуальной деятельности, полученные с привлечением инструментов ИИ, подчеркивая важность вклада человеческих усилий в творческий процесс.

Кроме того, сейчас многие IP-юристы говорят о важности такого элемента как обязательная маркировка произведений, созданных с использованием искусственного интеллекта (например, обозначением "AI"), во избежание введения третьих лиц в заблуждение. Такие предложения, звучащие в доктрине⁵, заслуживают всяческой поддержки, так как их реализация отвечает принципу добросовестности и может самостоятельно обеспечить права лиц, полагающихся на создание произведений представителями творческих профессий.

В марте 2025 года Китай опубликовал Директиву о маркировке контента, произведенного с использованием искусственного интеллекта. Документ начнет действовать с сентября того же года. Согласно требованиям директивы, каждый созданный ИИ материал должен иметь специальную отметку на каждом этапе своего жизненного цикла – от момента появления до публикации и последующего распространения. Поставщикам услуг, использующим искусственный интеллект, предписано размещать заметные метки на своем контенте в установленных местах. За нарушение требований предусмотрена ответственность: организации и частные лица обязаны соблюдать положения документа и не имеют права менять, подделывать или уничтожать установленные законом маркировки.

Актуальность разработки нормативных правовых актов, регламентирующих обязательное маркирование продуктов интеллектуальной деятельности, генерируемых искусственным интеллектом, продиктована стремительным ростом случаев внедрения новейших цифровых инструментов в творческий процесс креативных групп и специализированных студий, занимающихся созданием визуальных образов и художественных концепций. Иллюстрацией указанного тренда служит проект, инициированный студией Артемия Лебедева, заключающийся в создании специализированной компьютерной системы автоматического формирования элементов корпоративного дизайна и торговой символики, обозначенной названием «Николай Иронов».

Представленная интеллектуальная система основана на принципах глубинного машинного обучения и обладает функционалом автономной генерации уникальных графических композиций и брендового оформления. «Нейродизайнер» за год работы собрал целое портфолио из проектов. Это работы для видеоблогеров, кафе, баров, приложений и других брендов. Всего, по данным студии, нейросеть выполнила более 20 коммерческих проектов.

⁵ Зыков С. В. Смежные права как режим охраны результатов, созданных искусственным интеллектом // Интеллектуальная собственность. Авторское право и смежные права. 2023. № 5. С. 35–36.

Возрастающая потребность в маркировке очевидна. Она необходима не только для изображений, но и для всех видов медиаконтента, включая аудио и видео, генерируемых искусственным интеллектом, связана с массовым распространением так называемых дипфейков (от английского deepfakes). Такие материалы представляют собой специально обработанные аудио-, видео- и другие файлы, созданные с применением алгоритмов глубокого обучения (deep learning), и содержат заведомо неверную или вымышленную информацию. Эта технология стала мощным инструментом социальной манипуляции, позволяя создавать убедительные подделки.⁶

Примечательные примеры подобного вида дезинформации включают вирусные фотографии Папы Римского и сцен взрывов вблизи Пентагона, распространившиеся в интернете весной 2023 года. Данные фейки привлекли внимание широкой международной общественности, подчеркнув опасность подобных явлений.⁷

Вопрос введения обязательной маркировки контента, созданного с применением технологий искусственного интеллекта, особенно актуальным становится именно в связи с распространением дипфейков. Так, эксперт Е.М. Корних подчеркивает важность разработки специальных методов и инструментов, позволяющих автоматически выявлять и удостоверять материалы, созданные с использованием технологий дипфейка. Это предполагает внедрение надежных алгоритмов, способных эффективно обнаруживать и контролировать распространение недостоверного контента, генерируемого такими технологиями.

В условиях, когда произведения человека неотличимы от произведений, созданных с использованием ИИ, а клиент желает получить уникальный продукт человеческого творчества, такое введение в заблуждение недопустимо.

Прогноз до 2030 года: количество дел увеличится на 310%

Общий рост дел, связанных с искусственным интеллектом, на 310% свидетельствует о значительном разрыве между скоростью технологических изменений и адаптивной способностью правовых институтов. Данный феномен описывается в рамках концепции "правового отставания" (legal lag) Уильяма Огберна.

до 50%

увеличится доля дел по интеллектуальной собственности

до 30%

увеличится процент административных правонарушений за счет расширения автоматизированных систем контроля правонарушения

до 18 %

увеличится доля уголовных дел в связи с ростом киберпреступности

Рис. 2 Прогноз от Исследовательского центра «ABL»

⁶ Рожкова М. А. Объекты, сгенерированные ИИ, и объекты, создаваемые человеком с использованием ИИ, – суть различий. // Закон.ру. 2025. 12 февраля.URL: https://zakon.ru/blog/2025/2/12/obekty_sgenerirovannnye_ii_i_obekty_sozdavaemye_c

⁷ М. В. Самарцева Правовой режим результатов работы ИИ [Текст] // Digital law Journal. 2024. № 3. С. с. 19–65.

За последнее десятилетие дискуссия вокруг интеграции цифровых технологий и системы защиты прав интеллектуальной собственности приобрела особую остроту. Несмотря на интенсивные обсуждения, единого мнения относительно того, как именно должны формироваться правовые рамки регулирования цифрового пространства, до сих пор не сложилось. Российские законодатели продолжают находиться в процессе активного поиска оптимальных правовых механизмов, способных эффективно реагировать на современные вызовы цифровой эпохи. Эта неопределенность отражает сложность адаптации традиционных норм права к новым реалиям информационного общества, требуя тщательного анализа существующих подходов и выработки новых решений, соответствующих динамике технологического прогресса.

Подводя итог представленным аргументам и обозначив ключевые проблемы современности, целесообразно сформулировать ряд выводов, отражающих необходимость адаптации существующего правового поля к новым реалиям цифровой эпохи:

1. Быстрое развитие цифрового пространства требует срочного обновления законодательства для эффективной защиты прав на интеллектуальную собственность. Современные информационно-коммуникационные системы существенно преобразуют традиционные механизмы творчества, затрудняя эффективное использование результатов интеллектуальной деятельности, защиту авторских прав и получение справедливого вознаграждения.

2. Основная проблема заключается в снижении риска ущемления творческих способностей и трудовой деятельности человека вследствие активного внедрения автоматизированных интеллектуальных систем. Автоматизированные алгоритмы обработки данных способны создавать контент, имитирующий творчество человека, что вызывает сомнения относительно уникальности творческого продукта и ставит под угрозу доходы творческих работников.

3. При создании новых объектов с помощью систем искусственного интеллекта, таких как тексты, изображения, аудио- и видеоматериалы, обязательно наличие специального обозначения, подтверждающего участие генеративного ИИ в процессе формирования результата.

Список литературы

1. Ахлиблинский, Б. В. Кибернетика и тайны психики / Б. В. Ахлиблинский. Ленинград: Лениздат., 1966. 138 с.

2. Сесицкий Е. П. Проблемы правовой охраны результатов, создаваемых системами искусственного интеллекта: диссертация. М., 2018. 45 с.

3. Проект концептуального документа по вопросам, касающимся политики в области интеллектуальной собственности и искусственного интеллекта. URL: https://www.wipo.int/meetings/ru/doc_details.jsp?doc_id=470053 (дата обращения: 30.08.2025).

4. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указом Президента РФ от 10.10.2019 N 490 (ред. от 15.02.2024

№ 124) "О развитии искусственного интеллекта в Российской Федерации"). URL: <http://government.ru/docs/all/124098/> (дата обращения: 30.08.2025).

5. Абзац 5 п. 80 Постановления Пленума Верховного Суда РФ от 23.04.2019 N 10 "О применении части четвертой Гражданского кодекса Российской Федерации" / [Электронный ресурс] // Консультант плюс: [сайт]. URL: <https://www.consultant.ru> (дата обращения: 30.08.2025).

6. Решение Арбитражного суда г. Москвы от 30.11.2023 по делу N A40-200471/23-27-1448. URL: https://kad.arbitr.ru/Document/Pdf/4d7f0305-69af-44fe-8841-a59e84aa7deb/8dedc372-21f6-4751-ab3c-8a320fe435ce/A40-200471-2023_20231130_Reshenija_i_postanovlenija.pdf?isAddStamp=True (дата обращения: 30.08.2025).

7. Зыков С. В. Смежные права как режим охраны результатов, созданных искусственным интеллектом [Текст] // Интеллектуальная собственность. Авторское право и смежные права. 2023. № 5. С. 335–36.

8. М. В. Самарцева Правовой режим результатов работы ИИ [Текст] // Digital law Journal. 2024. № 3. С. 19–65.

9. Intellectual Property Office. (2021, March). Artificial intelligence and intellectual property: call for views. Consultationoutcome. Summary of questions. UK Government. <https://www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views/summary-of-questions>

10. Рожкова М. А. Объекты, сгенерированные ИИ, и объекты, создаваемые человеком с использованием ИИ, – суть различий // Закон.ру. 2025. 12февраля. URL: https://zakon.ru/blog/2025/2/12/obekty_sgenerirovannye_ii_i_obekty_sozdavaemye_c

**Цифровизация прокурорского надзора за исполнением
антикоррупционного законодательства в государственных
и муниципальных органах**

Аннотация. В данной статье исследуется проблема низкой эффективности традиционных методов прокурорского надзора за исполнением антикоррупционного законодательства, основанных на выборочных проверках. Автор обосновывает необходимость цифровой трансформации надзорной деятельности для перехода от контроля последствий к упреждающему контролю. В работе выделены ключевые проблемы цифровизации: фрагментированность данных между ведомствами, недостаточная цифровая грамотность сотрудников, риски кибератак. Предлагаются пути их решения, включая создание единой межведомственной платформы, обучение персонала и усиление защиты информации. Делается вывод о том, что комплексная цифровизация является необходимым условием для повышения эффективности противодействия коррупции.

Ключевые слова: прокуратура, прокурорский надзор, коррупция, антикоррупционное законодательство, противодействие коррупции, государственные и муниципальные органы, цифровизация

K. J. Grekhova,

student,

Far Eastern Federal University

**Digitalization of prosecutorial supervision of the implementation
of anti-corruption legislation in state and municipal authorities**

Abstract. This article examines the problem of low efficiency of traditional methods of prosecutorial supervision over the implementation of anti-corruption legislation based on random inspections. The author substantiates the need for digital transformation of supervisory activities to move from control of consequences to proactive control. The work highlights the key problems of digitalization: fragmentation of data between departments, insufficient digital literacy of employees, risks of cyberattacks. Ways to solve them are proposed, including the creation of a single interdepartmental platform, personnel training and strengthening of information security. It is concluded that comprehensive digitalization is a prerequisite for increasing the effectiveness of combating corruption.

Keywords: prosecutor's office, prosecutorial supervision, corruption, anti-corruption legislation, combating corruption, state and municipal authorities, digitalization

Введение. На сегодняшний день коррупция остается одной из системных угроз национальной безопасности России, подрывающей доверие граждан к государственным институтам, искажающей принципы законности и справедливости. В науке рассматривается множество определений понятия «коррупция», однако существует легальное определение, которое приведено в ст. 1 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции» [21]. Обобщая, коррупцией считается незаконное использование должностным лицом своих полномочий ради личной выгоды или выгоды третьих лиц, а также дача или получение взятки, что наносит значительный ущерб обществу или государству.

Основная часть. По данным Генеральной прокуратуры России в 2024 г. выявлено свыше 70 тыс. нарушений антикоррупционного законодательства в государственных и муниципальных органах [24]. При этом указанные нарушения допускаются и должностными лицами высокого ранга (главами муниципальных образований, высшими должностными лицами субъектов РФ и др.), многие из которых непосредственно задействованы в процессе выработки антикоррупционных мероприятий.

В сложившихся условиях эффективность прокурорского надзора за исполнением антикоррупционного законодательства приобретает особую значимость. Прокуратура, как универсальный орган надзора, обеспечивает соблюдение правовых норм в деятельности государственных и муниципальных органов, предотвращая злоупотребления и формируя превентивную антикоррупционную среду. Но на сегодняшний день традиционные методы прокурорского надзора, основанные на выборочных и плановых проверках, зачастую носят запоздалый характер и не позволяют эффективно выявлять сложные коррупционные схемы. Развитие цифровизации в сфере государственного управления открывает возможности для принципиального изменения парадигмы надзорной работы. Таким образом, цифровизация прокурорского надзора за исполнением антикоррупционного законодательства способна перевести его из “контроля за последствиями” в “упреждающий контроль”, повысив эффективность работы надзорных органов.

Характеризуя коррупцию как главный барьер на пути развития нашего общества, в своих ежегодных Посланиях Федеральному Собранию Российской Федерации, а также в обращениях на расширенных заседаниях коллегий органов МВД России, ФСБ России, Генеральной прокуратуры Российской Федерации Президент Российской Федерации неоднократно подчеркивал необходимость более активной борьбы правоохранительной и судебной систем с коррупционными преступлениями, повышения их раскрываемости, совершенствования антикоррупционного законодательства и его неукоснительного соблюдения представителями власти, а также воспитания в гражданах нетерпимости к любым, в том числе бытовым проявлениям коррупции.

Цифровизация в современности – общемировой тренд развития экономики и общества, который основан на преобразовании информации в цифровую форму, что приводит к оптимизации экономических процессов и улучшению общего благосостояния населения [22. С. 47].

Сфера прокурорско-надзорной деятельности, являясь неотъемлемой частью системы государственного контроля и управления, подвергается активному внедрению новейших информационных и коммуникационных технологий [1. С. 10].

В органах прокуратуры уже созданы и функционируют некоторые компоненты цифровой среды, включая автоматизированные информационные комплексы «НАДЗОР» и «КАДРЫ-ОП», систему «Архивное дело ОП» и систему информационного обеспечения финансово-хозяйственной деятельности, автоматизированное рабочее место «Статистика».

Тем не менее, комплексное обследование информационных ресурсов прокуратуры, проведенное Генеральной прокуратурой России совместно с Министерством связи и массовых коммуникаций РФ, позволило выявить наличие ряда серьезных недостатков: отсутствие единообразных стандартов создания и использования информационных систем, ненадежность системы защиты информационных ресурсов и отслеживания их состояния, низкая степень автоматизации контрольно-надзорной деятельности, неразвитость механизмов взаимодействия с ведомственными и государственными информационными системами, а также слабая оснащенность компьютерной техникой в сочетании со значительной степенью ее изношенности [2. С. 36]. Указанные недостатки носят системный характер и затрагивают все без исключения направления работы органов прокуратуры.

В связи с этим можно выделить ряд проблем, возникающих на пути к цифровизации прокурорского надзора за исполнением антикоррупционного законодательства в государственных и муниципальных органах на сегодняшний день.

Во-первых, существует проблема фрагментированности данных и отсутствия единого межведомственного информационного пространства. Данные, необходимые для эффективного анализа коррупционных рисков (сведений о доходах служащих, недвижимости, государственных и муниципальных закупках), рассредоточены по информационным системам различных органов исполнительной власти (ФНС России, Росреестр, ФССП и т.д.). Эти системы часто технически и технологически несовместимы, прокурорские работники не всегда могут оперативно получить полную картину для анализа, а ручной сбор и свод данных занимают колоссальное время. Фрагментированность данных и отсутствие единого межведомственного информационного пространства можно устранить благодаря:

1. Созданию Единой национальной платформы данных по противодействию коррупции, что будет предполагать не просто техническое соединение систем, а разработку единых стандартов форматов данных и правил обмена информацией;

2. Внедрению модели “единого окна” для прокурорского запроса, что позволит прокуратуре в рамках надзорных мероприятий получать прямой санкционированный доступ к необходимым массивам данных в режиме реального времени, минуя длительную процедуру официальных запросов в каждый властный субъект, что позволит не только выявлять, но и предотвращать коррупционные преступления в органах публичной власти.

Во-вторых, проблемы коренятся внутри самих органов прокуратуры. Внедрение цифровых инструментов наталкивается на недостаточную цифровую грамотность части прокурорских работников. Сотрудники привыкли работать с бумажными носителями, а к данным из автоматизированных систем уровень доверия гораздо ниже. Во избежание этого необходимо проводить системное обучение новым компетенциям: будущих прокурорских работников обучать работе в цифровой среде еще во время получения высшего образования, вводя в учебные планы дисциплины, ориентированные на работу в цифровой среде, а для действующих сотрудников внедрять обязательные программы повышения цифровой квалификации. Кроме того, система поощрения использования цифровых инструментов в повседневной работе будет стимулировать служащих применять новые технологии гораздо активнее.

В-третьих, активное внедрение цифровых технологий ставит вопрос возникновения новых рисков. Централизация огромных массивов конфиденциальной информации (персональные данные, декларации, материалы проверок) в единых цифровых системах органов прокуратуры создаст реальную угрозу кибератак со стороны иностранных государств или возможных коррупционных групп, заинтересованных в сокрытии своей деятельности. Антикоррупционное направление прокурорской деятельности привлекает к себе много внимания, более того, в данном случае речь идет о работе с органами государственной и муниципальной власти. И так, подобная утечка данных может привести к катастрофическим последствиям. Поэтому необходимо внедрить сквозные технологии шифрования на всех этапах сбора, передачи и хранения данных, регулярно тестировать все цифровые системы на возможность проникновения и контролировать утечки данных, привлекая ведущих отечественных специалистов в сфере кибербезопасности, создать такую систему, в которой будет жесткое регламентирование доступа к информации для выявления угроз извне, а также использовать собственное программное обеспечение с целью снижения зависимости от зарубежных систем.

Указанные проблемы создают некие препятствия на пути цифровизации данного направления в работе органов прокуратуры. Однако цифровизация неизбежна с целью повышения результативности противодействия коррупции в государственных и муниципальных органах со стороны органов прокуратуры. Следовательно, внедрение цифровых технологий требует принятия оперативных решений со стороны законодателя, просчета всевозможных рисков и введения ряда дополнительных законодательных изменений, которые обеспечат надежную защиту и эффективность. В статье выделено несколько проблем, с которыми сталкивается в настоящее время и еще может столкнуться наше государство на пути к цифровизации, приведены варианты их разрешения. Полагаю обоснованным суждение о том, что реализация на практике указанных предложений позволит повысить эффективность и объективность прокурорского надзора за исполнением антикоррупционного законодательства в государственных и муниципальных органах, сократить временные затраты на проведение проверок, перейти от тотального контроля и надзора к риск-ориентированному, а, рассматривая глобально, приведет к росту уровня прозрачности деятельности

прокуратуры и положительно скажется на борьбе с коррупцией в российском государстве в целом.

Заключение. Роль прокуратуры в противодействии коррупции в государственных и муниципальных органах сложно переоценить, поскольку, как отмечается в литературе, прокуратура занимает ведущее место в системе субъектов противодействия коррупции, осуществляет функции координации, а также самостоятельно реализует предоставленные ей полномочия по осуществлению прокурорского надзора за исполнением законодательства о противодействии коррупции [18. С. 67]. Цифровизация прокурорского надзора за исполнением антикоррупционного законодательства представляет собой не просто техническую модернизацию, а кардинальную трансформацию самой парадигмы надзорной деятельности. Она знаменует переход от традиционного подхода, основанного на выборочных проверках и работе по факту выявленных нарушений, к модели, упреждающей нарушения до их выявления, прогнозирования правонарушений.

Список литературы

1. Бессарабов В.Г. Прокуратура в системе государственного контроля Российской Федерации: автореферат дис. ... д-ра юрид. наук. Москва, 2001, 46 с.
2. Иванов А.В. Прокурорский надзор за исполнением антикоррупционного законодательства в органах местного самоуправления. М.: РГУП, 2020.
3. Инсаров О.А., Андреев Б.В. Цифровая трансформация органов прокуратуры Российской Федерации // Вестник Университета прокуратуры РФ. 2018. № 5. С. 35–41.
4. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
5. Коробейников Б.В. Нерешенные вопросы противодействия органов прокуратуры коррупции // Публичное и частное право. 2014. № 3. С. 106–112.
6. Послание Президента Российской Федерации Федеральному Собранию от 29.02.2024 г. б/н. URL: <http://www.kremlin.ru/acts/bank/50431> (дата обращения: 25.08.2025).
7. Письмо Министерства труда и социальной защиты РФ от 15 апреля 2022 г. N 28–6/10/П–2479 Об актуализации Обзора практики привлечения к ответственности государственных (муниципальных) служащих за несоблюдение ограничений и запретов, неисполнение обязанностей, установленных в целях противодействия коррупции.
8. Постановление Правительства РФ от 26.02.2010 № 96 (ред. от 20.04.2024) "Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов" (вместе с "Правилами проведения антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов", "Методикой проведения антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов").
9. Приказ Генпрокуратуры России от 14.09.2017 № 627 (ред. от 27.05.2024) "Об утверждении Концепции цифровой трансформации органов и

организаций прокуратуры до 2025 года" (вместе с "Концепцией цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года").

10. Приказ Генпрокуратуры России от 10.10.2022 № 581 (ред. от 16.10.2024) "Об осуществлении прокурорского надзора и реализации прокурорами иных полномочий в сфере противодействия коррупции".

11. Расширенное заседание коллегии Генеральной прокуратуры от 19.03.2025 г. URL: <http://www.kremlin.ru/events/president/news/76484> (дата обращения: 04.08.2025).

12. Расширенное заседание коллегии МВД от 02.04.2024 г. URL: <http://kremlin.ru/events/president/news/73770> (дата обращения: 16.08.2025).

13. Расширенное заседание коллегии ФСБ от 28.02.2023 г. URL: <http://kremlin.ru/events/president/news/70597> (дата обращения: 16.08.2025).

14. Роль прокуратуры в осуществлении надзора за исполнением законодательства о противодействии коррупции. Р.Р. Хасанов, помощник прокурора Туринского района, юрист 3 класса. URL: <https://turinskgo.ru/news/show/id/1516> (дата обращения: 04.08.2025).

15. Рябова В.С., Улизко К.А. Прокурорский надзор в области противодействия коррупции на муниципальной службе // Современная юриспруденция: актуальные вопросы, достижения и инновации: Материалы XII Международной научно-практической конференции (г. Пенза, 25 сентября 2018 г.). Пенза, 2018. С. 154–157.

16. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы".

17. Указ Президента РФ от 16.08.2021 № 478 (ред. от 26.06.2023) "О Национальном плане противодействия коррупции на 2021 – 2024 годы".

18. Усманова Р.М., Бойко Н.Н. Противодействие коррупции в системе местного самоуправления: проблемы теории и практики: монография. Sterlitamak: Sterlitamakский филиал БашГУ, 2018. 103 с.

19. Федеральный закон "Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов" от 17.07.2009 N 172-ФЗ (последняя редакция).

20. Федеральный закон "О прокуратуре Российской Федерации" от 17.01.1992 N 2202-1 (последняя редакция)

21. Федеральный закон от 25.12.2008 № 273-ФЗ (ред. от 08.08.2024) "О противодействии коррупции".

22. Халин В.Г., Чернова Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. 2018. № 10. С. 46–63.

23. Шмелев М.М. Проблемы прокурорского надзора за исполнением законов о противодействии коррупции // Крымские юридические чтения: материалы научно-практической конференции (г. Симферополь, 16 октября 2015 г.). Симферополь, 2016. С. 280–284.

24. Официальный Интернет-портал Генеральной прокуратуры Российской Федерации. URL: <https://epp.genproc.gov.ru/web/gprf/activity/statistics/of-fice/result> (дата обращения: 20.08.2025)

Л. А. Гринюк,
студент,
Российский государственный университет
имени А. Н. Косыгина

**Авторское право в цифровую эпоху:
правовые основы, вызовы и перспективы развития**

Аннотация. Авторское право в условиях цифровой экономики становится не только инструментом охраны индивидуальных интересов создателей, но и важным элементом регулирования потоков знаний, инноваций и культурного обмена. Статья анализирует правовые и экономические аспекты трансформации системы авторских прав в эпоху цифровизации. Рассматриваются изменения продолжительности и объема правовой охраны, влияние технологий на механизмы распространения произведений, новые модели лицензирования и бизнес-практики. Особое внимание уделяется вопросам соблюдения авторских прав в Интернете, включая проблемы цифрового пиратства, алгоритмического лицензирования и использования искусственного интеллекта в создании и распространении контента. На основе анализа существующей литературы и эмпирических данных определяются ключевые пробелы исследований, а также направления для развития правового регулирования, обеспечивающего баланс интересов авторов, потребителей и посредников.

Ключевые слова: авторское право, интеллектуальная собственность, цифровизация, правовое регулирование, интернет, искусственный интеллект, лицензирование, бизнес-модели, пиратство, цифровая экономика, технологии, правоприменение, данные, программное обеспечение, алгоритмическое лицензирование

L.A. Grinyuk,
bachelor's student,
A.N. Kosygin Russian State University

**Copyright in the digital age: legal foundations, challenges, and prospects
for development**

Abstract. The article analyzes copyright in the digital economy, which is becoming not only a tool for protecting the individual interests of creators, but also an important element in regulating the flow of knowledge, innovation, and cultural exchange. The author analyzes the legal and economic aspects of the transformation of the copyright system in the era of digitalization. It examines changes in the duration and scope of legal protection, the impact of technology on the mechanisms of distribution of works, new licensing models, and business practices. Particular attention is paid to issues of copyright compliance on the Internet, including the problems of

digital piracy, algorithmic licensing, and the use of artificial intelligence in the creation and distribution of content. Based on an analysis of existing literature and empirical data, key research gaps are identified, as well as directions for the development of legal regulation that ensures a balance of interests between authors, consumers, and intermediaries.

Keywords: copyright, intellectual property, digitization, legal regulation, internet, artificial intelligence, licensing, business models, piracy, digital economy, technology, law enforcement, data, software, algorithmic licensing

Введение. Авторское право, как фундаментальная категория права интеллектуальной собственности, представляет собой систему норм, обеспечивающих охрану творческих произведений и интересов их создателей. Оно призвано стимулировать развитие культуры и науки, поддерживать инновационные процессы и формировать благоприятные условия для распространения знаний. С переходом к цифровой экономике вопросы функционирования авторского права приобрели особую актуальность: цифровые технологии меняют характер создания и использования произведений, трансформируют модели бизнеса в культурных и креативных индустриях, а также ставят перед правоприменителями и исследователями новые вызовы [2].

Основная часть. Современная дискуссия об авторском праве охватывает не только правовые, но и экономические аспекты. С одной стороны, чрезмерная охрана может препятствовать свободному обмену знаниями и замедлять инновации. С другой – недостаточная защита ведет к пиратству и снижению стимулов к творчеству. Именно поэтому актуально исследовать баланс интересов авторов, пользователей и посредников в цифровую эпоху [7].

Исторически развитие авторского права шло от защиты печатных изданий к регулированию широкого круга объектов – от литературных и музыкальных произведений до программного обеспечения, баз данных и аудиовизуального контента. Ключевым трендом XX–XXI веков стало постепенное расширение сроков охраны и сферы действия авторского права. Если ранее основной задачей было обеспечить автора доходом на протяжении жизни, то сегодня защита распространяется и на наследников, зачастую на срок более 70 лет после смерти создателя.

В эпоху цифровизации это вызывает дискуссии: насколько оправдано столь длительное ограничение общественного доступа к произведениям? Сторонники расширенной защиты указывают на необходимость сохранения стимулов к созданию и инвестированию в контент. Критики же отмечают, что чрезмерное продление сроков препятствует культурному обмену и развитию новых форм творчества, основанных на переработке существующих произведений.

Кроме того, современное законодательство усиливает акцент на трансграничный характер авторских прав. Международные соглашения, такие как Бернская конвенция и Договор ВОИС по авторскому праву, закрепляют универсальные стандарты охраны [1]. Однако именно цифровые технологии демонстрируют, что даже единые нормы сталкиваются с трудностями практического приме-

нения: Интернет не признает государственных границ, а механизмы правоприменения в разных юрисдикциях сильно различаются.

Цифровая революция изменила способ создания, хранения и распространения произведений. Сегодня любой пользователь может не только мгновенно получить доступ к произведениям искусства, литературы или науки, но и сам стать их создателем и распространителем. Цифровизация породила новые вызовы: доступность контента, реплики и обход блокировки, нелегальные копии распространяются через VPN и зеркала сайтов. Интернет активно используется для пиратства, что требует адаптации законодательства. Все это приводит к ряду новых вызовов:

Рост цифрового пиратства. Копирование и передача файлов обходят традиционные барьеры, а борьба с незаконным распространением часто наталкивается на ограничения юрисдикции [3].

Массовое вовлечение пользователей в творчество. Социальные сети и платформы позволяют каждому производить и делиться контентом, создавая огромное количество произведений, которые формально охраняются авторским правом.

Изменение моделей потребления. Вместо покупки физических носителей акцент смещается на подписки, стриминговые сервисы и доступ «по требованию».

Законодательство стремится адаптироваться к этим процессам. Принятие европейской Директивы о цифровом едином рынке 2019 года, введение мер по блокировке пиратских сайтов в ряде стран, появление концепции «notice-and-takedown» – все это примеры попыток приспособить охрану авторских прав к цифровой среде.

С развитием технологий меняется не только способ распространения произведений, но и сами объекты авторского права. На первый план выходят:

Программное обеспечение и базы данных. Их правовой статус требует уточнения: программные коды признаются литературными произведениями, но их использование подчиняется особым лицензионным схемам.

Мультимедийные продукты. Синтез текста, музыки, видео и интерактивности создает гибридные объекты, защита которых не всегда укладывается в традиционные рамки.

Произведения, созданные с помощью искусственного интеллекта. Вопрос об авторстве и охране таких произведений остается дискуссионным: может ли машина считаться автором, или право принадлежит разработчику алгоритма, владельцу данных или пользователю системы?

Технологии также открывают новые возможности для защиты прав. Развитие блокчейн-технологий позволяет создавать децентрализованные реестры авторских прав, обеспечивать прозрачность лицензионных сделок и контроль за использованием произведений. Алгоритмы машинного обучения применяются для автоматического выявления нарушений, например, на платформах видеохостинга.

Биржевые стримеры и платформы меняют структуру доходов индустрии – от подписки до распределенных лицензий. В России наблюдается опыт Ян-

декс.Музыки и прямых договоров с исполнителями, а также концепции smart-контрактов и блокчейн-реестры [3].

Одна из центральных проблем цифровой эпохи – это соотношение прав авторов и прав пользователей. Системы жесткого контроля доступа часто воспринимаются обществом как чрезмерные, ограничивающие свободу информации. Одновременно правообладатели указывают на необходимость защиты инвестиций [8. Р. 274–276].

Эмпирические исследования показывают, что борьба с пиратством путем репрессивных мер не всегда эффективна: блокировки обходятся, а судебные разбирательства занимают годы. Более успешным подходом считается развитие легальных сервисов, которые обеспечивают удобство и доступность контента при разумной стоимости. Примером может служить рост популярности стриминговых платформ, позволивших значительно снизить уровень нелегального скачивания музыки и фильмов [7. Р. 18–19].

Однако в сфере научных публикаций проблема остается острой: открытые базы и «теневые библиотеки» конкурируют с дорогостоящими издательскими подписками, что вновь ставит вопрос о балансе интересов [6. Р. 24–26].

Современные исследования демонстрируют неоднозначное влияние цифровизации на авторское право:

- расширение доступа к произведениям стимулирует инновации и кросс-культурные обмены;
- ужесточение охраны может приводить к росту транзакционных издержек и снижению числа производных произведений;
- легальные цифровые сервисы оказываются более результативными в борьбе с пиратством, чем строгие санкции;
- алгоритмическое лицензирование и автоматизированные платформы снижают издержки заключения сделок, но вызывают вопросы о прозрачности и справедливости распределения доходов.

Таким образом, дальнейшее развитие системы требует учета не только правовых норм, но и социально-экономических последствий.

Особого внимания заслуживает взаимодействие авторского права и технологий искусственного интеллекта. С одной стороны, ИИ используется для охраны прав – например, для распознавания плагиата или мониторинга нелегального распространения контента. С другой – он сам становится инструментом творчества. Музыка, тексты, изображения, созданные нейросетями, бросают вызов классическим концепциям авторства и оригинальности [5. Р. 1–2].

По российскому законодательству ИИ не может считаться автором – авторство связано исключительно с человеком. Однако ИИ-гены часто вызывают коллизию: результаты могут быть близки к оригиналу, но правового режима нет [4].

Современное законодательство пока не дает исчерпывающих ответов. Большинство юрисдикций признают автором только человека. Но по мере роста значимости машинного творчества эта позиция будет требовать пересмотра или выработки гибридных моделей, учитывающих вклад как человека, так и алгоритма.

Авторское право в цифровую эпоху находится на переломном этапе. Оно должно выполнять двойную функцию: стимулировать творчество и инновации, одновременно обеспечивая справедливый доступ общества к культурным и научным благам.

Основные вызовы связаны с быстрыми изменениями технологий, появлением новых объектов охраны, трансграничным характером нарушений и необходимостью поддерживать баланс интересов различных участников. Решения видятся в сочетании правовых реформ, развития технологических инструментов охраны и создании устойчивых экономических моделей, основанных на справедливом распределении доходов.

Заключение. Для науки остаются открытыми вопросы о влиянии алгоритмического лицензирования, регулировании прав на произведения, созданные ИИ, а также о формировании оптимальной политики в области доступа к данным и научным публикациям. Их изучение позволит обеспечить дальнейшее развитие системы авторского права в условиях цифровой экономики.

Список литературы

1. Договор ВОИС по авторскому праву // World Organization of Intellectual Property (WIPO). URL: <https://www.wipo.int/treaties/ru/ip/wct/> (дата обращения: 25.02.2025)
2. Жапарова А. Б. Актуальные проблемы защиты авторских и смежных прав в условиях цифровой экономики // Актуальные исследования. 2024. №40 (222). Ч.II. С. 33–35. URL: <https://apni.ru/article/10177-aktualnye-problemy-zashity-avtorskih-i-smezhnyh-prav-v-usloviyah-cifrovoj-ekonomiki> (дата обращения: 16.04.2025).
3. Канаев, И. А. Системные нарушения авторских прав в российском цифровом пространстве / И. А. Канаев. Текст : непосредственный // Молодой ученый. 2025. № 18 (569). С. 287–289. URL: <https://moluch.ru/archive/569/124871/>. (дата обращения: 16.04.2025).
4. Шеленговский П.Г., Грачева Д.А. Искусственный интеллект и авторское право в современных условиях. ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2023;8(3):79–85. URL: <https://doi.org/10.21686/2411-118X-2023-3-79-85>. (дата обращения: 16.04.2025).
5. Gillespie, Tarleton. Content moderation, AI, and the question of scale // Big Data and Society 7 (2):2053951720943234. 2020. P. 1–2.
6. Kaiser, F., Cuntz, A., and Peukert, C. Batman Forever? The Role of Trademarks for Reuse in the US Comics Industry // Research Policy, 2023. P. 24–26.
7. Lu, Shijie & Rajavi, Koushyar & Dinner, Isaac. The Effect of Over-the-Top Media Services on Piracy Search: Evidence from a Natural Experiment // Marketing Science. 40. 2021. P. 18–19.
8. Patnuskar Aditi Ganesh, Sanjay Jathar Padmabhushan, Singh Devendra, Suresh Mallik Laxmi. The Impact of Digital Piracy on Intellectual Property Rights (IPR) Enforcement // International Journal of Emerging Technologies and Innovative Research (IJETIR). 2023. ISSN 2583–0554. P. 274–276.

К. А. Гришаева,

студент,

Белорусский государственный университет транспорта,

Е. О. Якуш,

студент,

Белорусский государственный университет транспорта

Электронная подпись как инструмент цифровой трансформации права

Аннотация. В современных условиях цифровизации общества электронная и цифровая подписи приобретают особую значимость как инструменты подтверждения воли и заключения договоров в дистанционной среде. Статья посвящена анализу принципов функционирования электронной подписи, ее правового регулирования и криптографических механизмов защиты. Особое внимание уделено вопросам аутентификации подписанта, обеспечению целостности документа и предотвращению несанкционированного вмешательства, включая угрозы со стороны вредоносного программного обеспечения, атак с «инкрементальным обновлением» и методов обертывания подписи. Рассмотрены современные методы идентификации пользователя: пароли, физические носители, биометрические данные, а также комбинации этих методов, и их влияние на надежность цифровой подписи. Анализируются механизмы работы PKI-систем и роль удостоверяющих центров, применение хэш-функций для проверки подлинности и сохранности документов. Приведен обзор правового регулирования в Республике Беларусь, включая признание юридической силы электронных документов, подписанных цифровой подписью, и меры защиты от подделок и несанкционированных изменений.

Ключевые слова: электронная подпись, цифровая подпись, криптография, хэш-функцию, аутентификация, биометрические данные, физические носители, дистанционный документооборот, подлинность документа, информационная безопасность, электронный документ

K. A. Hryshayeva,

student,

Belarusian State University of Transport,

Y. O. Yakush,

student,

Belarusian State University of Transport

Electronic signature as a tool of digital transformation of law

Abstract. In the current context of societal digitalization, electronic and digital signatures have gained significant importance as instruments for confirming consent and executing contracts in remote environments. This article analyzes the principles

of electronic signature operation, its legal regulation, and cryptographic protection mechanisms. Special attention is given to issues of signer authentication, document integrity, and prevention of unauthorized interference, including threats from malicious software, incremental update attacks, and signature wrapping methods. Modern user identification methods are examined, including passwords, physical tokens, biometric data, and combinations of these methods, and their impact on the reliability of digital signatures is assessed. The article also analyzes the functioning of PKI systems and the role of certification authorities, as well as the use of hash functions to verify document authenticity and integrity. An overview of legal regulation in the Republic of Belarus is provided, including recognition of the legal force of electronic documents signed with a digital signature and measures to protect against forgery and unauthorized alterations.

Keywords: electronic signature, digital signature, cryptography, hash functions, authentication, biometric data, physical tokens, remote document flow, document authenticity, information security, electronic document

Введение. Технология электронной подписи на практике показала высокую эффективность и востребованность во множестве сфер. Сегодня нет необходимости присутствовать лично, чтобы заключить договор, даже если он связан с крупными финансовыми обязательствами. Государственные органы также активно используют эту технологию, предоставляя гражданам возможность дистанционной подачи документов в налоговые, страховые, образовательные и иные учреждения [5. С. 45]. Примеры можно продолжать долго, однако при всей очевидной пользе возникает один важный и до сих пор нерешенный вопрос: каким образом удостовериться, что именно то лицо, которое указано в качестве подписанта, действительно подтвердило свою волю и «наложило подпись» на электронный документ [10. С. 12]?

Основная часть. Для того, чтобы разобраться в сложностях, связанных с цифровой подписью, необходимо вернуться к истокам самой идеи использования подписи как средства подтверждения воли и заключения договоров. Подпись изначально выполняла несколько функций, и одна из ключевых состояла в том, чтобы доказать факт достижения согласия между сторонами. До ее широкого применения, когда уровень грамотности был низким, основным способом выражения воли служили устные заявления. Но очевидно, что этот метод имел значительные недостатки: если обещание нарушалось, доказать его наличие было крайне сложно. В качестве решения использовались свидетели, которые подтверждали обязательства сторон. Однако отсутствие свидетелей либо их заинтересованность в исходе дела приводили к существенным трудностям в защите прав. Именно поэтому общество стало искать более надежные способы закрепления волеизъявления, включая обряды и клятвы, особенно распространенные в республиканский период Древнего Рима [7. С. 88].

Со временем рукописная подпись утвердилась как наиболее удобный и юридически значимый инструмент выражения воли. Устные договоренности продолжали существовать, но их значение в сделках, связанных с крупными ценностями, заметно уменьшилось. Причина заключалась в том, что подпись

обладала особым качеством – возможностью убедительно доказывать согласие лица с определенными обязательствами [9. С. 103].

Сегодня развитие информационно-коммуникационных технологий радикально изменило экономику и вновь поставило под сомнение традиционные подходы к заключению договоров. Возникла объективная потребность в замене рукописной подписи ее цифровым аналогом. Причем дело было не столько в ненадежности старых методов, сколько в их ограниченности в электронной среде. Так, бумажный страховой договор с подписями сторон и печатью компании полностью удовлетворяет юридические требования, но становится крайне неудобным, если клиент хочет дистанционно оформить полис, выбирая оптимальный вариант на сайте страховщика. В таких условиях электронная подпись стала логичным и необходимым решением [1].

Цифровая подпись представляет собой особый вид электронной подписи, обладающий дополнительными характеристиками, которые направлены на обеспечение более высокого уровня доверия к источнику информации и сохранению целостности электронного документа [3]. Кроме того, цифровая подпись позволяет защитить содержание сообщения от несанкционированного вмешательства третьих лиц. Ключевое отличие цифровой подписи от обычной электронной заключается в применении криптографических методов защиты [8]. Как и в случае с простой электронной подписью, существует множество разновидностей цифровых подписей, обусловленных разнообразием подходов к использованию криптографии.

Несмотря на предпринимаемые меры, невозможно достичь абсолютной и неразрывной связи между человеком и техническим устройством. РКИ-система способна подтвердить лишь то, что конкретное сообщение было создано с использованием определенного закрытого ключа. Однако это еще не означает, что сам владелец ключа непосредственно участвовал в процессе подписания. Существуют различные виды закрытых ключей, использование которых может сопровождаться дополнительными механизмами защиты:

1. Ввод сведений, доступных только владельцу (например, пароля). В этом случае злоумышленнику для подделки подписи необходимо предварительно завладеть данной информацией. Получить ее можно с помощью интернет-атак – таких как фишинг, внедрение вредоносного программного обеспечения, либо традиционными методами, включая скрытое наблюдение. Дополнительный риск возникает, если пользователь настроил автоматическое сохранение пароля на своем устройстве: любой, кто получит к нему доступ, сможет подписать документ.

2. Использование физического носителя, принадлежащего владельцу (например, USB-накопителя). Такой подход значительно снижает вероятность несанкционированного цифрового вмешательства, однако полностью исключить угрозы нельзя: устройство можно потерять, оставить без присмотра в общем доступе или оно может быть похищено.

3. Применение биометрических характеристик (радужка глаза, голос, манера речи, отпечатки пальцев и др.). Несмотря на уникальность этих параметров, гарантировать абсолютную защиту они не способны. Например, отпечаток

пальца – наиболее распространенный способ биометрической аутентификации – может быть скомпрометирован: от создания искусственного клона до использования пальца третьего лица с похожими признаками, а также из-за ошибок самой системы считывания.

4. Комбинирование нескольких методов одновременно. Применение хотя бы двух различных способов аутентификации существенно повышает уровень защищенности, но не исключает рисков полностью. Так, злоумышленник может сначала узнать пароль, затем похитить носитель с закрытым ключом и в дальнейшем самостоятельно использовать его для подписания документа.

Суть криптографической защиты состоит в преобразовании данных в такой вид, который исключает возможность их прочтения или изменения посторонними лицами. Для этого применяются специальные алгоритмы, превращающие сообщение и подпись в зашифрованную комбинацию символов, не имеющую смысла без последующей дешифровки. Доступ к содержанию документа может быть получен только тем субъектом, который обладает соответствующими средствами расшифровки. Такой подход обеспечивает не только конфиденциальность, но и подтверждает подлинность, целостность и неизменность данных.

Феномен подделки подписей известен человечеству уже многие столетия. Несмотря на это, в большинстве случаев даже искусно выполненную подделку рукописной подписи удастся выявить. Это связано с тем, что рукописная подпись всегда состоит из символов, оставленных рукой человека, а способы ее подделки ограничиваются, как правило, имитацией или копированием с использованием вспомогательных материалов вроде копировальной бумаги. Методы проверки подлинности в данном случае также достаточно ограничены – это графологический анализ почерка либо изучение физических и химических характеристик бумаги.

В цифровой среде ситуация выглядит сложнее: разновидностей электронных подписей гораздо больше, как и возможных способов их фальсификации. Аналогами графологической экспертизы и анализа бумаги здесь выступают многочисленные методы технической проверки, позволяющие установить факт вмешательства. Одним из ключевых подходов считается выявление устройства, с которого была выполнена подпись. Для этого могут использоваться такие параметры, как IP-адрес, MAC-адрес или уникальный отпечаток устройства. Их точность и степень информативности зависят от способа передачи данных.

При работе через специализированные онлайн-сервисы, предназначенные для электронной подписи, все операции фиксируются в журналах системы, однако доступ к этой информации, как правило, возможен только по решению суда. Если же подпись ставилась при обмене электронными письмами, то определить IP-адрес отправителя можно без специальных средств, просто открыв заголовки письма. Кроме того, сам электронный документ способен содержать дополнительные данные об устройстве, использованном при подписании. Эти сведения известны как метаданные документа.

Наиболее распространенным инструментом считается определение геолокации по IP-адресу. Данный метод позволяет установить, из какой сети факти-

чески было отправлено сообщение. Если выясняется, что оно было отправлено из места, где подписант заведомо не находился, это может служить весомым аргументом в пользу версии о подделке. Однако стопроцентным доказательством такой метод считаться не может. Причина в том, что современные средства обхода, такие как VPN-сервисы и прокси-серверы, позволяют пользователю искусственно изменить свое виртуальное местоположение. Таким образом, даже при наличии IP-адреса всегда сохраняется вероятность того, что фактическое место нахождения подписавшего скрыто.

Современные методы криптографической защиты базируются на применении ключей. Под ключом понимается уникальное значение, используемое в алгоритме для преобразования исходного текста в зашифрованный или, напротив, для восстановления первоначального содержания. Существуют два основных типа систем: симметричные и асимметричные. В симметричных схемах один и тот же ключ применяется как для шифрования, так и для дешифрования. В асимметричных системах используются два взаимосвязанных ключа – открытый и закрытый. Закрытый ключ остается в распоряжении владельца подписи и применяется для создания цифровой подписи, тогда как открытый может использоваться любым получателем для проверки ее подлинности.

Для обеспечения надлежащего уровня доверия в асимметричных системах часто применяется институт удостоверяющих центров. Такие организации публикуют и поддерживают базы данных открытых ключей, связывая их с конкретными физическими или юридическими лицами посредством выдачи цифровых сертификатов. Подобная инфраструктура получила название PKI (Public Key Infrastructure) и является ключевым элементом доверенной среды электронного взаимодействия.

Особое значение в функционировании цифровых подписей играет использование хэш-функций. При формировании подписанного сообщения к нему прикрепляется хэш – своеобразный «отпечаток» исходного текста. Хэш представляет собой уникальную последовательность символов, которая создается на основе содержания документа, но не позволяет восстановить исходный текст. Если при передаче изменяется хотя бы один символ сообщения, результат хэширования будет совершенно иным. Для проверки подлинности получатель самостоятельно вычисляет хэш от принятого текста и сравнивает его с расшифрованным хэшем, прикрепленным к сообщению. Если значения совпадают, значит документ подлинный, не изменен и действительно подписан заявленным субъектом.

В Республике Беларусь правовой режим цифровых подписей закреплен в Законе от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи» [2]. В соответствии с данным актом, электронная цифровая подпись рассматривается как реквизит электронного документа, предназначенный для защиты его от подделки и подтверждения принадлежности подписи конкретному субъекту. Закон устанавливает, что электронный документ, подписанный ЭЦП, обладает такой же юридической силой, как и документ на бумажном носителе, заверенный собственноручной подписью. Кроме того, нормативный акт определяет требования к удостоверяющим центрам, порядок

выдачи и применения ключей, а также меры безопасности, обеспечивающие доверие к электронному документообороту.

Независимо от того, в какой форме реализуется подпись – будь то традиционная собственноручная подпись на бумажном документе или ее электронный аналог, используемый в цифровой среде, – вопрос ее подлинности является принципиальным для установления юридической значимости самого документа. Подлинность подписи всегда предполагает, что лицо, указанное в качестве подписавшего, действительно осуществило акт подписания. В противном случае подпись теряет свою правовую ценность, а документ не может рассматриваться как надлежащее выражение воли соответствующего субъекта. В правоприменительной практике встречаются ситуации, когда полномочия на подписание документа предоставлены представителям, действующим от имени других лиц. В таких случаях юридическая сила документа сохраняется только при условии, что представитель использует собственную подпись, дополнив ее указанием на свой представительский статус. Это необходимо для того, чтобы не возникало сомнений относительно того, кто именно выразил волю и в чьих интересах действовал при подписании документа. Особого внимания заслуживает ситуация, когда документ действительно был подписан обозначенным лицом, но впоследствии подвергся изменениям без согласия подписавшего. В подобных случаях юридическая квалификация становится более сложной: формально подпись остается подлинной, однако сам документ уже не отражает первоначального содержания, согласованного сторонами. Следовательно, такой документ утрачивает доказательственную силу и рассматривается как ненадлежащий, что по своим последствиям сопоставимо с использованием поддельной подписи. Более того, подобные случаи могут привести к существенным правовым рискам, включая оспаривание сделки или признание документа недействительным. Следует подчеркнуть, что уязвимость документа к подобным рискам во многом зависит от характера применяемой электронной подписи. Наиболее простые формы электронной подписи, не относящиеся к категории цифровых, в значительной степени ограничены с точки зрения защиты информации и механизмов аутентификации. В ряде случаев такие подписи могут сводиться лишь к элементарному действию – например, указанию имени или инициалов в конце электронного сообщения либо текста документа. Однако подобные способы идентификации, несмотря на их формальное соответствие базовым критериям подписи, практически не способны гарантировать достоверность авторства. Они не обеспечивают достаточного уровня уверенности в том, что именно указанное лицо является инициатором подписания, а также не защищают документ от несанкционированных изменений.

В ряде случаев возможно возникновение ситуации, когда к документу прикрепляется подлинная подпись, однако сам документ был заранее изменен преступником, в том числе при проведении вредоносной компьютерной атаки [6]. Причем подобное вмешательство может происходить практически одновременно с процессом подписания. Один из наиболее распространенных примеров связан с применением вредоносного программного обеспечения: пользователю на экране демонстрируется корректная версия документа, в то время как факти-

чески электронная подпись прикрепляется к иному содержимому. В результате у подписанта формируется уверенность в том, что он подписывает именно тот текст, который видит, тогда как на деле юридическую силу получает другой документ.

Кроме того, в цифровой среде существуют и более изощренные способы манипуляции с уже подписанными файлами. К их числу относят так называемые атаки с «инкрементальным обновлением». Суть подобных атак заключается в том, что в ряде форматов, в частности PDF, предусмотрена возможность поэтапного внесения изменений, которые воспринимаются как легитимное дополнение. Таким образом, документ действительно может быть подписан автором в первоначальной редакции, но затем в него встраивается новый фрагмент информации. Программные средства, предназначенные для чтения PDF-файлов, зачастую определяют лишь сам факт наличия подписи и корректность ее проверки, однако не способны зафиксировать факт последующего добавления текста или иных элементов, так как такие изменения «маскируются» под правомерное обновление документа самим автором.

Помимо этого, существуют и иные сценарии изменения содержания подписанных документов. Например, особую угрозу представляют так называемые «атаки с обертыванием подписи». Их цель заключается не в полном уничтожении подписи или ее подмене, а в модификации внутренней структуры документа таким образом, чтобы средства защиты не смогли распознать несоответствие. Подобные действия позволяют злоумышленникам внедрить новые элементы в документ, не нарушив его формальной валидности и не вызвав сообщений о повреждении подписи.

Именно такие примеры наглядно демонстрируют, что даже наличие электронной подписи не всегда гарантирует абсолютную защиту документа от несанкционированных изменений.

Заключение. Таким образом, развитие электронных и цифровых подписей стало неизбежным этапом эволюции правовых и технических инструментов подтверждения воли сторон [4]. С одной стороны, они позволяют существенно упростить и ускорить документооборот, обеспечивая возможность заключения сделок и подачи заявлений дистанционно, без необходимости физического присутствия. С другой стороны, практика применения показывает наличие серьезных рисков, связанных с подлинностью подписи и сохранностью содержимого документа. Решение этих проблем требует комплексного подхода, включающего совершенствование правового регулирования, внедрение надежных криптографических алгоритмов и повышение уровня цифровой грамотности пользователей. Только в условиях сочетания технических и правовых гарантий электронная подпись сможет выполнять свою ключевую функцию – служить достоверным подтверждением воли лица и надежным инструментом защиты его прав и интересов в цифровом пространстве [5; 10]. Именно поэтому достаточно ценны исследования, посвященные электронной подписи и в целом доверия к технологии, а также различным аспектам ее безопасности [11. С. 373].

Список литературы

1. Аналитический обзор: Рынок электронной подписи в России и СНГ 2022–2023. М.: CRPT, 2023. 54 с.
2. Об электронном документе и электронной цифровой подписи: Закон Респ. Беларусь от 28 дек. 2009 г. № 113–З // Нац. реестр правовых актов Респ. Беларусь. 2010. № 4. 2/1624.
3. Алферов, А. П. Криптография: основы современной защиты информации / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин. 3-е изд. СПб.: БХВ–Петербург, 2021. 576 с.
4. Иванов М. А. Правовые риски использования электронной подписи: монография. М.: Юстицинформ, 2022. 198 с.
5. Касперский Е. И. Тренды цифровой безопасности 2023: угрозы для бизнеса и государства // Лаборатория Касперского. 2023. 20 февр. URL: <https://www.kaspersky.ru/blog/top-cyberthreats-2023-business/48845/> (дата обращения: 03.09.2024).
6. Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3(34). С. 218–221. EDN REWTKJ.
7. Римское частное право: учебник / под ред. И. Б. Новицкого, И. С. Перетерского. М.: Юрайт, 2021. 608 с.
8. Тубанова Ю. Б. Риски при использовании электронной подписи и меры по их минимизации / Ю. Б. Тубанова, К. М. Тимохин // Налоговая политика и практика. 2019. № 6 (198). С. 68–73. EDN YICECZ.
9. Сергеев А. П. Гражданское право: в 3 т. Т. 1: Общая часть / А. П. Сергеев, Ю. К. Толстой. 10-е изд., перераб. и доп. М.: Проспект, 2022. 1024 с.
10. Соколова О. В. Электронный документооборот и электронная подпись: практическое руководство. 5-е изд., перераб. и доп. М.: Инфра–М, 2023. 285 с.
11. Харуна И. О., Айдоноджи П. А., Бейда О. Дж. Проблемы и перспективы нормативного регулирования системы электронных платежей в Нигерии // Journal of Digital Technologies and Law. 2024. Т. 2, № 2. С. 372–393. <https://doi.org/10.21202/jdtl.2024.19>

А. Р. Дяблова,

студент,

Российская академия народного хозяйства
и государственной службы
при Президенте Российской Федерации

**Маркировка рекламы в социальных сетях:
правовая база и проблемы практики**

Аннотация. В статье исследуются правовая база и практические аспекты маркировки рекламы в социальных сетях. Цель работы – проанализировать действующее законодательство и выявить ключевые проблемы реализации норм о маркировке рекламы, а также разработать практические рекомендации по их преодолению. Особое внимание уделено анализу судебной практики, разъяснений контролирующих органов и алгоритмам взаимодействия с операторами рекламных данных. В работе представлены сравнительные характеристики трех ведущих операторов рекламных данных, описан подробный алгоритм регистрации и маркировки рекламы, включая практический пример из телеграм-канала автора. Результаты исследования могут быть использованы юристами, маркетологами и блогерами для обеспечения соответствия рекламных материалов требованиям законодательства и избежания ответственности.

Ключевые слова: право, цифровые технологии, маркировка рекламы, социальные сети, реклама, законодательство, цифровая юриспруденция, практические проблемы

A. R. Dyablova,

student,

Institute of Law and National Security
of the RANEPa under the President
of the Russian Federation

**Marking of advertising in social networks:
Legal basis and practical problems**

Abstract. This article examines the legal framework and practical aspects of advertising labeling in social networks. The purpose of the study is to analyze the current legislation, identify key challenges in implementing advertising labeling requirements, and develop practical recommendations for overcoming these issues. Special attention is given to the analysis of judicial practice, clarifications from regulatory bodies, and algorithms for interacting with advertising data operators. The paper presents comparative characteristics of three leading advertising data operators and describes a detailed algorithm for advertising registration and labeling, including a practical example from the author's Telegram channel. The research findings can be

used by lawyers, marketers, and bloggers to ensure compliance of advertising materials with legal requirements and to avoid liability.

Keywords: law, digital technologies, advertising labeling, social networks, legal framework, advertising, legislation, informational law, practical issues, digital jurisprudence

Введение. Маркировку рекламы регулирует Федеральный закон от 02.07.2021 № 347-ФЗ «О внесении изменений в Федеральный закон «О рекламе» (далее – ФЗ № 347-ФЗ).

С 2022 года в силу вступил закон о маркировке рекламы в интернете, а с 2023 за ее отсутствие была введена ответственность в виде штрафов. Это усложнило работу маркетологов и рекламодателей, так как возникли сложности с пониманием того, какой контент нужно маркировать, какие посты можно считать рекламными, как происходит процесс маркировки и куда передавать данные о рекламе. Поскольку четкого закона о маркировке рекламы в социальных сетях в российском законодательстве долгое время не было, возникло множество сложностей с публикацией рекламных постов.

В 2025 году маркировка рекламы стала регламентироваться законом более детально. В соответствии с законом, маркировка рекламы – это добавление к каждому рекламному объявлению сообщения о том, что оно является рекламой, а также данных рекламодателя и уникального номера, который называется токеном. Эту информацию размещают в конце текстового объявления, на рекламных креативах в виде картинок, а в видеороликах в моменты демонстрации прямой рекламы. На разных площадках средств массовой информации и (или) маркетплейсов маркировка может появляться в виде всплывающих окон.

Из закона следует, что рекламодатели, рекламораспространители, операторы рекламных систем обязаны предоставлять информацию о рекламе в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации (оператор рекламных данных). Ответственность за маркировку лежит на распространителе рекламы – например, блогере, у которого заказали интеграцию, или владельце сообщества, который разместил рекламный пост. Однако в договоре об оказании рекламных услуг может быть прописана ответственность рекламодателя, поэтому ему желательно контролировать маркировку рекламы, которую он размещает на сторонних площадках.

Что касается юридической ответственности, то с 1 сентября 2023 года за отсутствие маркировки на рекламе вводится ответственность в виде штрафов. Размер штрафа зависит от того, кто признается нарушителем. Для граждан, в том числе самозанятых, штраф составляет от 2 000 до 2 500 рублей, для должностных лиц – от 4 до 20 тысяч рублей, для юридических лиц – от 100 до 500 тысяч рублей. Штрафы могут выписать как Роскомнадзор, так и Федеральная Антимонопольная Служба (далее – ФАС). Роскомнадзор отвечает за вынесение штрафов, полученных за отсутствие в рекламном посте токена или переданных в Единый Реестр Интернет Рекламы (далее – ЕРИР) данных. ФАС выносит

штрафы за отсутствие нужной в рекламной интеграции информации, даже если она зарегистрировано в ЕРИР.

Комиссия Роскомнадзора провела конкурс по отбору операторов рекламных данных, по результатам которого такой статус получили семь организаций. Три наиболее известные из них можно сравнить по следующим критериям: тариф; скорость и качество поддержки; функционал; помощь с маркировкой.

Общество с ограниченной ответственностью «Яндекс оператор рекламных данных» предоставляет возможность бесплатного использования своего сервиса. На платформе доступны поддержка Яндекс Рекламы и форма обратной связи. Кабинета, позволяющего заранее изучить оператора рекламных данных, нет. На сайте также доступен большой блок с обучающими материалами про маркировку.

Сначала Оператор рекламных данных был предназначен преимущественно для тех, кто использует инструменты Яндекса. В этом случае токен создается автоматически, а необходимая информация сразу отправляется в ЕРИР. Для корректной передачи информации в ЕРИР рекламодатель должен заполнить только несколько полей. В марте 2024 года заработал полноценный кабинет оператора рекламных данных, в котором все участники рекламного рынка могут бесплатно зарегистрировать креативы, получить токены и отчитаться по любым форматам рекламы.

Общество с ограниченной ответственностью «ВК рекламные технологии» также, как и «Яндекс оператор рекламных данных, предоставляет возможность бесплатного использования своего сервиса. В случае, если нужна помощь, можно обратиться в работающую круглосуточно поддержку. Из преимуществ можно отметить наличие демо-кабинета. Кроме этого, на сайте есть раздел «Помощь» с инструкциями по маркировке рекламы. Оператор рекламных данных VK в первую очередь создан для сбора и передачи данных о рекламе, запущенной на собственных площадках VK, но работает с разными рекламными системами.

Общество с ограниченной ответственностью «ОРД-А», в отличие от описанных выше конкурентов взимает плату за посредничество. Если в отчетном периоде данные не передавались, то ничего оплачивать не надо. Если данные были переданы, то сумма будет складываться из минимального платежа в размере 5000 руб.; стоимости передачи актов со статистикой, которые разделены по креативам согласно тарифной зоне; передачи креативов саморекламы – 15 руб. за 1 Мб.

На тарифную зону влияет сумма рекламы по загруженным актам. Если сумма актов по креативам была до 500 000 руб., то к оплате начислится только минимальный платеж. Если сумма была более 500 000 до 3 млн руб., то сумма к оплате будет 20 000 руб. Больше сумма – выше стоимость тарифа. Техническая поддержка работает слабо: ответ может задерживаться до 7 дней. На сайте демо-кабинета нет – заранее изучить кабинет не получится. Несмотря на это, оператор предоставляет объемные бесплатные гайды и видеоуроки по использованию кабинета.

Суть закона о маркировке рекламы в интернете заключается в том, что определенные рекламные сообщения, направленные на российскую аудиторию, должны регистрироваться в ЕРИР. Маркировку нужно размещать на каждом объявлении, она должна быть легко читаемой и заметной.

Согласно ФЗ № 347-ФЗ маркировке подлежат баннеры, таргетированная реклама, онлайн-трансляции, видеоролики и аудиозаписи, нативная реклама, PR-публикации и пресс-релизы, упоминание бренда в роликах и подкастах, самореклама.

Нативная реклама также подлежит маркировке, однако четкого определения для нее в законе нет. Федеральная антимонопольная служба рассматривает каждый случай отдельно и изучает контекст сообщения. Если он, скорее, информационный, чем коммерческий, то маркировать его не нужно. Желательно помещать всю информацию о рекламодателе и токены даже на посты с нативной рекламой: за их отсутствие тоже можно получить штрафы.

Если реклама размещается из зарубежных стран, но при этом направлена на отечественную аудиторию, маркировка все равно нужна. Если реклама размещена за рубежом и при этом не направлена на российскую аудиторию, то тогда рекламу маркировать не нужно. Важно иметь в виду то, что реклама не должна быть направлена на соотечественников, иначе, несмотря на местоположение, реклама будет считаться рекламой именно по российскому законодательству. Иными словами, будучи резидентом РФ, прорекламировать русскоязычному населению тайскую косметику, живя в ОАЭ, не получив за отсутствие маркировки штраф, не получится.

Маркировке не подлежат реклама, не размещаемая в интернете; социальная реклама; реклама, направленная на зарубежную аудиторию; реклама в собственных email и SMS-рассылках; информация, которая не выделяет один или несколько товаров из ассортимента или не подчеркивает конкурентные преимущества бренда, справочные и информационные материалы, информация о себе в своем аккаунте и ссылка на другие свои ресурсы, личные рекомендации в виде органичного упоминания товара и (или) услуги, обзоры, отзывы, партнеры и спонсоры (без признаков рекламы)

Кроме этого, не считаются рекламными посты и обзоры у блогеров, если информация интегрирована органично; без акцента на товаре; не нарушает сюжет; не выражает положительное отношение блогера к товару определенной фирмы.

Информация о собственных продуктах или о собственных ресурсах на других площадках, размещаемая на сайте рекламодателя или в его же социальной сети рекламой не является. Но если из множества товаров выделяется один конкретный, то ФАС может признать это рекламой. На такой креатив будут действовать все законодательные требования, которые связаны с рекламой, в том числе и о маркировке.

Вернемся к ФЗ № 347-ФЗ, в соответствии со статьей 1 которого «реклама должна содержать пометку «реклама», а также указание на рекламодателя такой рекламы и (или) сайт, страницу сайта в информационно-телекоммуникационной сети «Интернет», содержащие информацию о рекламодателе такой рекламы».

В семнадцатом пункте этой же статьи указано, что «распространение рекламы в информационно-телекоммуникационной сети «Интернет» допускается при условии присвоения оператором рекламных данных соответствующей рекламе идентификатора рекламы, который представляет собой уникальное цифровое обозначение, предназначенное для обеспечения прослеживаемости распространенной в информационно-телекоммуникационной сети «Интернет» рекламы и учета информации о такой рекламе».

Здесь под уникальным цифровым обозначением подразумевается токен – «уникальное цифровое обозначение» которое предоставляется оператором рекламных данных по итогам регистрации организации, договора, площадки размещения и креатива.

Следовательно, в рекламной интеграции должны содержаться следующие пункты: слово «Реклама»; информация о рекламодателе, включая форму организации, название для юридических лиц или ФИО для физических лиц; ИНН рекламодателя; рекламный токен.

По итогам тестирования трех самых известных операторов рекламных данных было выявлено, что «ВК рекламные технологии» является наиболее удобным и понятным для маркировки рекламы сервисом, поэтому алгоритм маркировки рекламы будет описан с опорой именно на этого оператора.

Сначала необходимо открыть сайт «ВК рекламные технологии», перейти в кабинет и пройти регистрацию. В кабинете, появившемся после регистрации, во вкладке «контрагенты» необходимо выбрать «добавить контрагента» и в открывшемся поле ввести собственные ФИО, ИНН, номер телефона, тип (физическое или юридическое лицо). Далее следует поле «роли». Их четыре: рекламодатель, агентство, рекламная система и издатель. Если с рекламодателем все понятно, то с остальными ролями стоит разобраться. Рекламная система – один из видов рекламораспространителей. Она участвует в цепочке передачи данных о рекламе в ЕРИР, маркирует все запущенные через нее креативы токеном, который ей предоставляет оператор рекламных данных проще говоря, рекламная система – посредник между оператором рекламных данных и заказчиком. Издатель – блогер, публикующий рекламу. Агентство – посредник между рекламодателем, распространителем и контролирующими органами/

Блогеру, планирующему публиковать рекламу, необходимо выбрать роль «издатель».

После выбора роли необходимо перейти к категории «площадки», где нужно «добавить площадку» и ввести данные о площадке (телеграм, вк и (или) пр.). Такие площадки подходят под категорию «сайт». Напротив окна «контрагент является владельцем данной площадки» галочку не ставить. В течение нескольких часов площадка автоматически подтвердится и перейдет из категории «в обработке» в категорию «площадка подтверждена в ЕРИР».

Таким же образом необходимо зарегистрировать рекламодателя во вкладке «Контрагенты». Важно поменять роль с «издатель» на «реklamодатель».

Далее следует создать договор во вкладке «договор» как «оказание услуг». Предметом договора является «распространение рекламы». Сумма до-

говора – сумма по чеку самозанятого. Рекомендуется включать в прайс трех-процентный налог.

Последний шаг – выбрать площадку размещения рекламы и сформировать креатив во вкладке «креатив». Тип креатива – текст, тип рекламной кампании – «показ».

Получившийся уникальный цифровой код (токен) скопировать и вставить в текст рекламной интеграции (рис.1).

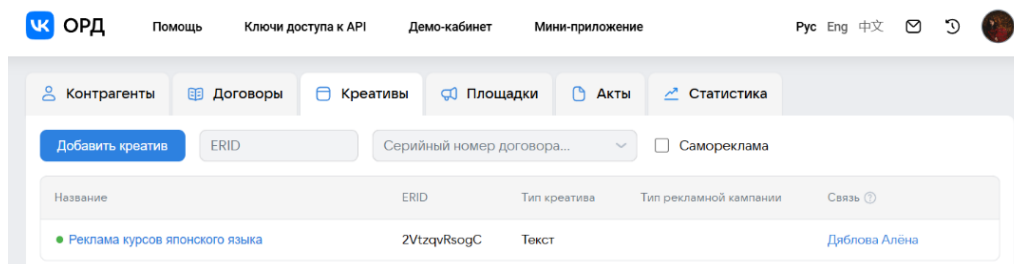


Рис. 1 Вкладка «Креативы» в Операторе рекламных данных ВК

Отчитывается по итогам рекламной кампании тот, кто получал токен, то есть тот, кто регистрировал креатив (маркировал рекламу)

Участники рынка должны предоставлять статистику по креативам каждый месяц на протяжении всего периода размещения рекламных материалов.

Статистика предоставляется не позднее конца отчетного месяца. Например, если статистика передается за апрель 2025, то передача должна осуществиться до 30 мая 2025. По окончании рекламной кампании креатив необходимо зарегистрировать по следующему образцу (рис.2).

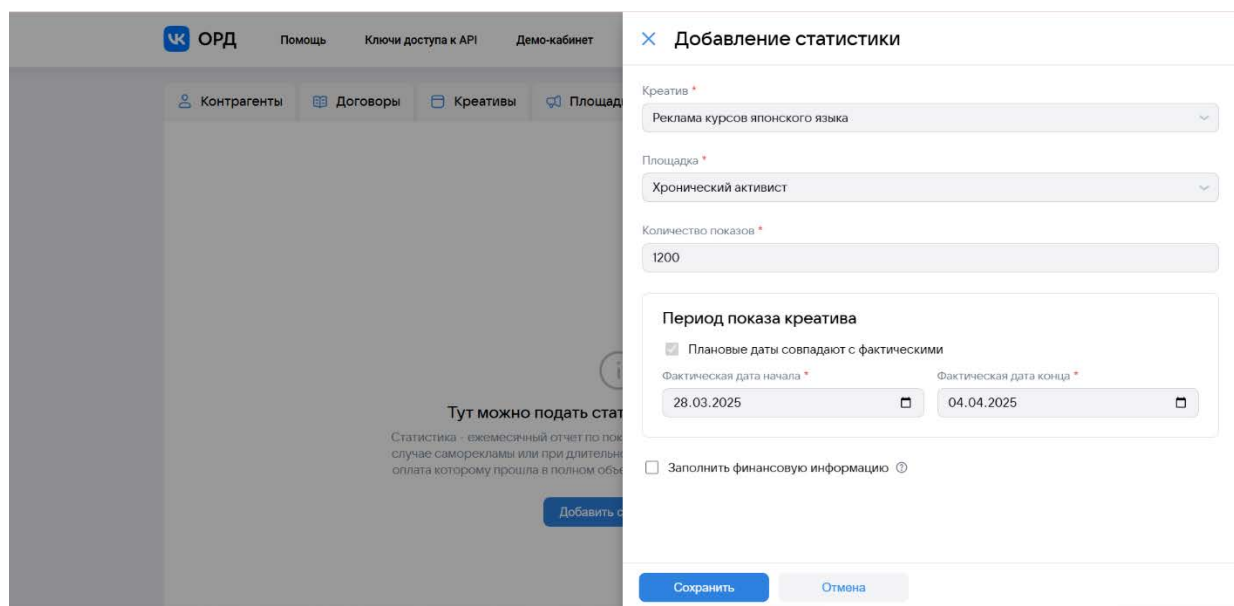


Рис. 2. Отчетность по статистике в операторе рекламных данных "VK ORD"

Если рекламный пост не является саморекламой, то по нему также нужно подать акт. При подаче отчетности обязательно необходимо следить за тем, чтобы даты из договора совпадали с датами из акта, иначе можно получить штраф за ошибки при маркировке.

Акт подается до конца следующего за отчетным месяцем месяца. То есть, если кампания закончилась 30 мая, акт подается до 30 июня, но обычно блогеры и агентства подают акты со статистикой в течение недели после окончания кампании.

В актах есть пункт «разаллокация». Рекламный сбор считается именно от него. В нем указывается сумма за размещение рекламно-информационных материалов по договору о распространении рекламы или сумма гонорара агента за организацию распространения рекламы. А в основном пункте «сумма» указывается весь рекламный бюджет. Например, рассмотрим цепь «рекламораспространитель–рекламодатель» с рекламным бюджетом 35.000 рублей. Здесь в разаллокации и сумме мы укажем одну и ту же сумму. А вот в цепи «рекламодатель–рекламное агентство–рекламораспространитель» мы создадим два акта: первый акт между рекламодателем и рекламным агентством и второй – между рекламным агентством и рекламораспространителем. Условно, рекламный бюджет – 40.000 рублей: из них – 35.000 рублей – цена размещения рекламно-информационных материалов, 5.000 рублей – гонорар агентства. Тогда первый акт (рекламодатель – рекламное агентство) пройдет следующую разаллокацию: общая сумма – 40.000 рублей, разаллокация – 35.000 рублей. Второй акт (рекламное агентство – рекламораспространитель): общая сумма – 40.000 рублей, разаллокация – 5.000 рублей. Проще говоря, рекламодатель платит агентству за РИМ, а блогер агентству – за маркировку рекламы.

Статистику по креативу можно или подавать отдельно, или прикреплять к акту.

Обратимся к телеграм-каналу «Хронический активист», владельцем которого является автор исследовательской работы. На основе описанного алгоритма была промаркирована реклама в одном из постов цепи «рекламодатель – рекламораспространитель».

Сперва была пройдена регистрация в качестве контрагента, затем поданы данные о телеграм канале в ЕРИР, получено одобрение, креатив зарегистрирован и вставлен в пост.

Наглядно все действия выглядят следующим образом (рис.3, 4).

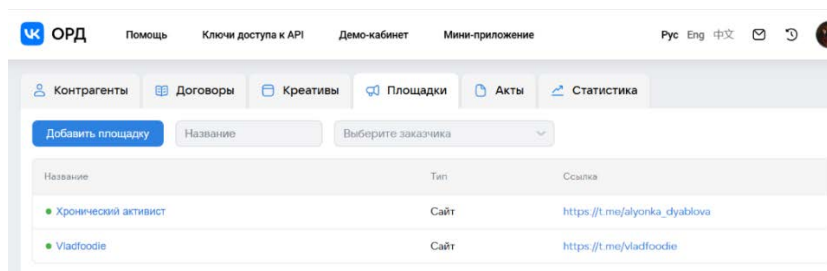


Рис. 3 Зеленый кружок слева от названия площадки означает, что канал прошел проверку в ЕРИР и признан площадкой распространения рекламы

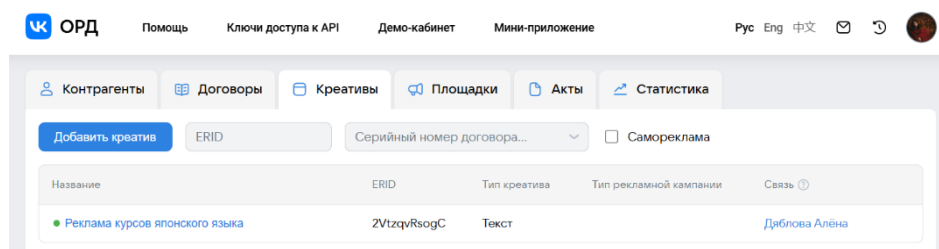


Рис. 4 Зарегистрированный в операторе рекламных данных рекламный пост

Токен для рекламного поста появляется сразу, а данные о рекламе переходят в ЕРИР с небольшой задержкой. (3–4 дня).

Последний этап – подача отчетности по итогам рекламной кампании, которая подается в течение месяца с момента окончания рекламной кампании. Пост по окончании стоит удалить, иначе придется подавать так называемую «вечную отчетность» и платить налог за показы ежемесячно. Итоговый результат выглядит следующим образом (рис.4).

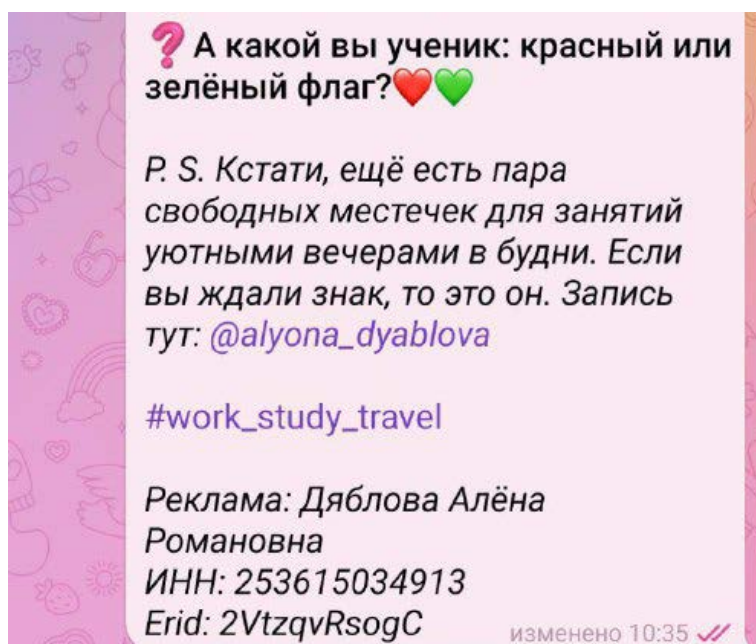


Рис. 4 Правильно промаркированная реклама

В случае, если имеет место цепь «рекламодатель – рекламное агентство – рекламораспространитель», алгоритм будет тот же, за исключением того, что договоров и актов будет два: первый договор между рекламодателем и рекламным агентством, второй – между агентством и рекламораспространителем. Акты обязательно нужно прикреплять к изначальному договору. Изначальным договором считается договор между рекламодателем и рекламным агентством.

Помимо работы с ОРД важно не забыть и про ЕРИР. В августе 2025 года на сайте появилась вкладка «мои отчисления», где теперь по итогам каждого квартала необходимо подписывать декларации и оплачивать рекламный сбор в

размере 3%. Проще всего это сделать через портал «Госуслуги». Сбор оплачивается путем таких же операций, которые применяются при оплате любого другого налога или штрафа. Оплачивает рекламный сбор либо каждый участник цепочки самостоятельно, либо тот участник, на которого возложена такая задача: чаще всего это рекламное агентство. В случае, если агентство оплачивает налог за всех участников цепочки, на этапе получения креатива нужно поставить галочку в окне «сбор оплачивает посредник», остальным участникам в случае такой договоренности ничего платить не нужно. Сумма налога отсчитывается по актам. Для договоров с типом «Договор оказания услуг» базой расчета является общая сумма (без учета НДС), указанная в детализации акта. Если в акте отсутствует детализация, то базой расчета будет являться общая сумма (без учета НДС) акта. Для договоров с типом «Посреднический договор» базой расчета является сумма (без учета НДС) посреднического вознаграждения.

С сентября 2023 года начали действовать штрафы за отсутствие маркировки рекламы в интернете и нарушение требований к ней. Следовательно, появились и судебные прецеденты по делам о нарушении маркировки рекламы.

В 2024 году некоммерческая организация в лице телеграм-канала «Змеиногогорский вестник» разместила рекламу магазина «Домострой», в которой отсутствует пометка «реклама» и сведения о рекламодателе. Идентификатор рекламы в посте присутствовал, но пометки «реклама» и информации о рекламодателе не было, что оказалось достаточным для признания рекламы ненадлежащей. Организация объяснила нарушение техническим сбоем, из-за которого блок с маркировкой отобразился не полностью, но такие доводы не принесли результата.

В соответствии с еще одним прецедентом, в сообществе в социальной сети «ВКонтакте» было опубликовано объявление о предоставлении срочных микрозаймов. Пост был размещен без токена. Антимонопольное ведомство пришло к выводу, что пост является рекламой и на него распространяются требования ст. 18.1 Закона о рекламе. Компанию привлекли к административной и назначили штраф в размере 200 тыс. руб.

Дело коснулось не только отечественных социальных сетей. На YouTube-канале и на платформе Дзен блогер опубликовал два видео, в которых присутствовала реклама чистящего средства и посуды. В одном ролике маркировки не было, а в другом в качестве рекламодателя был указан ИП с неверным ИНН, а сам токен, согласно ЕРИР, использовался для рекламы текстиля. Нарушителю был назначен штраф в размере 30 тыс. руб. но что интересно, предприниматель обратился в суд для обжалования решения и добился положительного результата. Суд ограничился устным замечанием и освободил ИП от административной ответственности в связи с малозначительностью правонарушения.

Важно не только правильно маркировать рекламу, но и проверять ее на отсутствие правонарушений.

Часто при написании рекламы рекламораспространители допускают ошибки, нарушающие Федеральный закон № 347-ФЗ. Во-первых, законом запрещено использование слов «лучший», «первый», «номер один» без указания конкретного критерия, который имеет объективное подтверждение. Во-вторых,

выпускать рекламу с отсутствием дисклеймеров о наличии противопоказаний и необходимости ознакомления с инструкцией или получения консультации специалистов.

В ходе проведения исследования на тему «Маркировка рекламы в социальных сетях: правовая база и проблемы практики» было выявлено, что эффективная маркировка рекламы является важным аспектом, обеспечивающим прозрачность и честность в коммуникации между брендами и потребителями. Правовая база, регулирующая этот процесс, продолжает развиваться, адаптируясь к быстро меняющемуся цифровому ландшафту и новым форматам рекламы.

Несмотря на наличие законодательных норм, в практике маркировки рекламы остается ряд проблем, к которым можно отнести недостаточную осведомленность пользователей о правилах маркировки, неоднозначность некоторых законодательных формулировок и сложности в их применении на практике.

Важным шагом к улучшению ситуации является необходимость повышения уровня информированности как рекламодателей, так и пользователей о правилах маркировки.

Заключение. Таким образом, для достижения эффективной маркировки рекламы требуется комплексный подход, включающий как правовые, так и практические меры. Важно продолжать исследование данной темы, чтобы разрабатывать рекомендации, способствующие улучшению практики маркировки рекламы в социальных сетях. Это позволит не только защитить интересы потребителей, но и защитить рекламодателей от штрафов, что в итоге будет выгодно всем участникам рынка.

Список литературы

1. О внесении изменений в Федеральный закон "О рекламе": Федер. закон Рос. Федерации от 2 июля 2021 г. № 347-ФЗ (ред. от 24.07.2023) Рос. газ. 2023. 25 июля
2. Кодекс Российской Федерации об административных правонарушениях [Текст]: от 30.12.2001 № 195-ФЗ (ред. от 24.04.2020) // Собрание законодательства РФ. 07.01.2002.
3. Решение Алтайского краевого управления Федеральной антимонопольной службы России от 02.08.2024 по делу № 022/05/18.1-816/2024. URL: <https://br.fas.gov.ru/> (дата обращения: 28.04.2025).
4. Решение Арбитражного суда Челябинской области от 09.08.2024 по делу № А76-18744/2024 URL: <https://br.fas.gov.ru/> (дата обращения: 28.04.2025).
5. Решение Арбитражного суда Свердловской области от 24.06.2024 по делу № А60-14604/2024. URL: <https://br.fas.gov.ru/> (дата обращения: 28.04.2025).
6. Инструкция по работе с оператором рекламных данных VK [Электронный ресурс] // Expert VK. URL: <https://expert.vk.com/articles/instruktsiya-porabote-s-ord-vk/> (дата обращения: 19.03.2025).
7. МедиаНетологии. Как маркировать рекламу в 2024 году // Netology. URL: <https://netology.ru/blog/01-2024-ad-labeling#how> (дата обращения: 19.03.2025).

8. Национальный Рекламный Форум. Маркировка рекламы в интернете в 2024 году // Advertisingforum.ru. URL: <https://advertisingforum.ru/blog/markirovka-reklamy-v-internete-v-2024-godu/#block-1> (дата обращения: 18.03.2025).
9. Онлайн-курс. Маркировка рекламы // Stepik. URL: <https://stepik.org/course/210486/promo?search=6631124056> (дата обращения: 18.03.2025).
10. Оператор рекламных данных ВК. URL: <https://sandbox.ord.vk.com/?reason> (дата обращения: 17.03.2025).
11. Оператор рекламных данных Яндекс. URL: <https://ord.yandex.ru/> (дата обращения: 17.03.2025).
12. Оператор рекламных данных «ОРД-А». URL: <https://ord-a.ru/> (дата обращения: 17.03.2025).
13. Эриашвили Н. Д. Правовое регулирование рекламной деятельности. М.: ЮНИТИ-ДАНА: Закон и право, 2018. 240 с.
14. Яндекс.Дзен. Инструкция по маркировке рекламы в Телеграм. Где брать и как правильно вставлять ЕРИД // VC.ru. URL: <https://vc.ru/marketing/1074264-instrukciya-po-markirovke-reklamy-v-telegram-gde-brat-i-kak-pravilno-vstavlyat-erid> (дата обращения: 21.03.2025).
15. Telegram-канал «Хронический активист». URL: https://t.me/alyonka_dyablova (дата обращения: 27.04.2025).

М. А. Жижкин,

студент,

Московский государственный технический
университет имени Н. Э. Баумана

Этические аспекты разработки программного обеспечения и систем искусственного интеллекта

Аннотация. В работе рассматриваются ключевые этические вызовы, связанные с разработкой программного обеспечения и использованием систем искусственного интеллекта. Основное внимание уделено вопросам защиты персональных данных, обеспечению прозрачности и объяснимости алгоритмов, а также проблеме алгоритмических предвзятостей и дискриминации. В исследовании проанализированы принципы ответственного ИИ, включая прозрачность, контроль и подотчетность, рассмотрены примеры автономных решений и их последствия для пользователей. Отдельный раздел посвящен законодательным инициативам Российской Федерации в сфере регулирования технологий искусственного интеллекта. На основе выявленных проблем предложены выводы о необходимости комплексного подхода – от улучшения качества обучающих данных до внедрения этических норм на уровне компаний и государства – для обеспечения справедливого и безопасного развития цифровых технологий.

Ключевые слова: этические аспекты, разработка, программное обеспечение, искусственный интеллект, цифровые технологии, цифровизация

Ethical aspects of software and artificial intelligence systems development

M. A. Zhyzhkin,

Student,

Moscow state technical university named after N. E. Bauman

Abstract. The paper examines the key ethical challenges associated with software development and the use of artificial intelligence systems. The main focus is on issues of personal data protection, ensuring transparency and explainability of algorithms, as well as the problem of algorithmic bias and discrimination. The study analyzes the principles of responsible AI, including transparency, control, and accountability, and examines examples of autonomous solutions and their implications for users. A separate section is devoted to legislative initiatives of the Russian Federation in the field of regulation of AI technologies. Based on the identified problems, conclusions are drawn about the need for an integrated approach – from improving the quality of training data to implementing ethical standards at the company and government levels – to ensure the fair and safe development of digital technologies.

Keywords: ethical aspects, development, software, artificial intelligence, digital technologies, digitalization

Введение. Сегодня уже сложно представить жизнь без программного обеспечения и систем искусственного интеллекта, они окружают нас повсюду – от мобильных приложений до медицинских диагностических платформ и аналитики в бизнесе. Разработка технологий идет стремительными темпами, как мы знаем, стартапы выпускают продукты буквально за считанные месяцы, нейросети обучаются на огромных массивах данных, а пользователи все чаще готовы делиться личной информацией ради удобства и скорости сервисов. Но вместе с этим появляются и новые риски. Грань между «полезной автоматизацией» и «угрозой безопасности» оказывается очень тонкой. Именно поэтому на первый план выходит вопрос этики в программной инженерии и искусственном интеллекте. Сегодня важно не только создавать рабочие и надежные системы, но и делать это ответственно, честно и с учетом интересов общества.

Основная часть

1. Ответственный искусственный интеллект

1.1. Принципы ответственного ИИ: прозрачность, объяснимость, контроль

Искусственный интеллект (ИИ) становится необходимой составляющей нынешнего общества, воздействуя на разнообразные области бытия – от медицины и финансов вплоть до автотранспорта и образования. Но вместе с ростом способностей ИИ появляются и основательные этические вызовы. Ответственный искусственный интеллект – это аспект, который подразумевает исследование и применение ИИ с учетом моральных основ, подобных как прозрачность, честность, подотчетность и безопасность. Тема ответственного искусственного интеллекта очень многогранная. Тут речь идет не только о том, как строятся алгоритмы, но и о том, как они вплетаются в жизнь общества. Получается, что это и про инженерию, и про этику, и про законы одновременно. Обычно говорят про несколько принципов. Самый очевидный – прозрачность. Алгоритм должен быть понятен. Не полностью, конечно, потому что детали программирования мало кто разберет, но хотя бы в общих чертах, а именно откуда берутся данные, что с ними происходит и на основе чего выдается результат. Пример легко найти в медицине. Допустим, система ставит диагноз. Врач не может просто «поверить на слово» – ему нужно знать, какие факторы программа учла. Иначе доверия к технологии не будет. В праве похожая история, т.е. если суд использует ИИ модели, важно понимать, на чем они основаны. Дальше идет вопрос контроля. Как ни крути, последнее слово должно оставаться за человеком. Без этого все превращается в риск. Беспилотные автомобили – классический пример, они умеют ехать сами, но, если случается нештатная ситуация, водитель обязан иметь возможность перехватить управление. Есть еще одна серьезная проблема – предвзятость данных. ИИ учится на том, что ему дали. Если в этих данных есть перекосы, дискриминация или ошибки, то он их только закрепит. В финансах, например, это может означать, что система несправедливо отказывает людям в кредите. В образовании – что алгоритм «недооценивает» учеников из определенных групп. И вот здесь, на мой взгляд, и проявляется настоящая суть «ответственного ИИ». Это не про то, чтобы запретить технологии или, наобо-

рот, бесконтрольно внедрять их. Про баланс, как сделать так, чтобы они помогали, но при этом оставались под контролем человека и общества.

Некоторые вызовы этике ИИ очень похожи на проблемы, связанные с проектированием различных предметов и устройств. Разработка робота, собирающего трубы на буровой установке, не более сложна с моральной точки зрения, чем разработка офисной мебели. Однако, когда алгоритмы ИИ берут на себя когнитивную работу с социальными аспектами – когнитивные задачи, ранее выполнявшиеся людьми, – возникает острая необходимость соблюдать социальные требования [1. С. 119].

Системы ИИ должны быть защищены от злоупотреблений и кибератак, которые могут привести к утечке данных или неправильным решениям.

1.2. Проблема автономных решений и их влияние на пользователей

Автономные системы, способные принимать решения без вмешательства человека, представляют собой одну из самых сложных этических проблем в области ИИ. Например, если автономная система совершает ошибку, кто несет за это ответственность? В частности, в случае аварии с участием автономного автомобиля виноват производитель, разработчик алгоритма или владелец транспортного средства?

Например, можно вспомнить случай с машиной Uber, которая в 2018 году сбила пешехода. Это событие стало громким не только из-за самой трагедии, но и потому, что сразу поднялся спор: кто виноват? Компания? Водитель, который вроде бы сидел за рулем, но не управлял? Или сама система, которую, по сути, никто напрямую «не контролировал»? По данным Verge, американский регулятор в сфере безопасности транспорта начал разбирать, как именно работает автопилот Tesla. Эксперты из Национального управления по безопасности дорожного движения США (NHTSA) выяснили любопытную деталь: почти во всех зарегистрированных авариях система отключалась буквально за несколько секунд до столкновения. Разработчики построили это так, чтобы компанию нельзя было привлечь к суду по обвинению в «умышленном ущербе» из-за работы автопилота [9]. Тут появляется и еще один пласт обсуждения. Автономные системы иногда оказываются в положении, где все варианты плохие. Это тот самый пример с «проблемой вагонетки», только уже применительно к машинам. Большинство моделей ИИ стремятся к выбору, который уменьшает число человеческих жертв. Но если ситуация сложнее, то вопрос становится куда острее: кого защищать – пассажира или пешеходов? И есть еще психологический момент. Люди могут чувствовать, что у них отбирают контроль. Машина сама принимает решение, а человек в этот момент остается в стороне. Из-за этого уровень доверия к таким технологиям снижается, даже если статистика говорит, что они в среднем безопаснее.

Если мы говорим про те же автомобили, не приведет ли частое использования автопилота, ИИ систем к деградации человеческих навыков, как это произошло в гражданской авиации, где человек выполняет только взлет и посадку, а выдерживает машину на эшелоне автопилот, также современные компьютерные системы даже при пилотировании человеком обычно защищают самолет от сваливания, больших углов атаки и т.п. Стефано Фурланис (Stefano Furlanis),

капитан Ethiopian Airlines считает, что не автоматика сама по себе является проблемой, а чрезмерная зависимость от нее [11]. Это высказывание можно отнести к любой сфере, в которой что-то зависит от искусственного интеллекта или автоматики.

1.3. Законодательные инициативы в области ИИ в Российской Федерации.

В России вопросы регулирования искусственного интеллекта становятся все более актуальными с учетом роста внедрения технологий ИИ во всех сферах жизни общества, от здравоохранения до промышленности и государственного управления. В рамках этих процессов государство разрабатывает нормативно-правовые акты, направленные на установление этических стандартов, защиту прав пользователей и обеспечение безопасности при использовании технологий ИИ.

Российское законодательство в сфере ИИ находится на стадии формирования, но уже обозначены ключевые направления – этические принципы, защита данных, безопасность и надежность, транспарентность решений (создание специального механизма для объяснения прочны принятия такого решения).

На данный момент в России рассматриваются несколько законопроектов и подготовлены различные стратегические документы, касающиеся регулирования ИИ:

Стратегия развития искусственного интеллекта до 2030 года утверждена Правительством Российской Федерации. Она определяет основные цели и задачи развития ИИ, и тут важно понимать, что вместе с технологиями нужны еще и правовые, и этические рамки, чтобы использование ИИ было безопасным и социально ответственным.

Можно сказать, что отдельное внимание в законе уделяется автономным транспортным средствам. Законопроект о беспилотниках вводит правила их эксплуатации, включая безопасность, ответственность за происшествия и соблюдение правил дорожного движения [6]. Это одна из самых обсуждаемых сфер применения ИИ. Нужно отметить поправки к ФЗ-152 «О персональных данных». Поскольку ИИ активно анализирует большие объемы данных, закон усиливает требования к сбору, хранению и обработке информации. При этом разработчики должны обеспечивать прозрачность алгоритмов, которые принимают решения на основе этих данных. Еще один момент – проект закона «Об искусственном интеллекте», который находится на стадии обсуждения. Он направлен на комплексное регулирование всех аспектов работы ИИ. Замглавы Минцифры Александр Шойтов пояснил: «Нужно регулировать эту сферу, и мы этим занимаемся. Одно из направлений – обезличивание данных». Он добавил, что при пилотных проектах, наращивая технологии, важно переходить к общему регулированию, расширяя и масштабируя правильные решения. На уточняющий вопрос он отметил, что закона, который это обеспечивал бы, пока нет, но его разрабатывают.

Российские регуляторные инициативы отличаются следующими особенностями:

- Государственная инициатива (большинство мер разрабатываются под эгидой государственных органов, что обеспечивает централизованное управление процессом).

- Межведомственное взаимодействие (при создании нормативных актов участвуют различные ведомства, включая Министерство цифрового развития, Министерство экономического развития и другие профильные организации).

- Социальная ориентация (законодательство стремится учитывать интересы граждан, защищая их права и гарантируя безопасность при использовании технологий ИИ).

В будущем ожидается дальнейшее успешное совершенствование законодательства в сфере ИИ.

Алгоритмы машинного обучения (МО) становятся неотъемлемой частью нашей повседневной жизни, влияя на решения, которые касаются каждого из нас. Однако, несмотря на их кажущуюся объективность, эти системы могут проявлять предвзятость, отражая исторические и социальные предрассудки.

2. Борьба с алгоритмическими предвзятостями

2.1. Причины появления предвзятостей в алгоритмах машинного обучения

Модели МО (машинного обучения) обучаются на данных, собранных из реального мира. В случае, если в предшествующем конкретные категории людей сталкивались с дискриминацией либо ограничениями, алгоритмы имеют все шансы воспринимать эти паттерны. К примеру, если в определенных профессиях преимущественно были заняты представители сильного пола, алгоритм способен воспринимать девушек в данных ролях в виде исключения, что приводит к понижению их шансов на трудоустройство в определенном месте. При разработке алгоритмов важно учитывать баланс и разнообразие данных. Если модель обучается на несбалансированных данных, она может неправильно интерпретировать закономерности. К примеру, метод, предназначенный с целью моделирования преступности, способен ошибочно рассматривать конкретные группы населения наиболее предрасположенными к преступлениям (например, предвзятое отношение правоохранительных органов к определенным этническим группам, как в США). Разработчики алгоритмов часто представляют собой однородную группу с похожими взглядами и опытом. Это может привести к созданию систем, которые не учитывают разнообразие и потребности различных групп населения. Например, системы распознавания лиц, обученные преимущественно на изображениях определенных этнических групп, могут плохо работать с лицами представителей других групп. «Предвзятость алгоритмов ИИ может быть частично ограничена стандартами и этическими принципами, закрепленными в программных документах. Но одно лишь нормативное правовое регулирование неспособно устранить эту проблему. Во-первых, разнообразие принципов, рамок, руководств и стандартов создает возможность лавировать между ними, чтобы оправдать существующие алгоритмы «как есть», не внося в них изменения, а также создает проблему несопоставимости многих стандартов. Во-вторых, как было отмечено выше, предвзятость алгоритмов может в значительной степени порождаться предвзятыми решениями в реальной жизни,

которые алгоритм «усваивает» во время обучения на реальных данных. Разработка механизмов выявления и корректировки этого «усвоения», таким образом, становится ключевым элементом в преодолении проблем неэтичности алгоритмов ИИ» [2].

Предвзятость в алгоритмах – это не просто техническая проблема, а серьезный социальный вызов. Для ее решения необходимо:

1. Гарантировать, чтобы данные, в которых учатся алгоритмы, отображали многообразие реального общества.

2. Создатели обязаны являться открытыми в отношении методов и информации, применяемых с целью изучения моделей, для того чтобы общество имело возможность дать оценку и равным образом опровергнуть выводы, принимаемые алгоритмами.

3. Введение профессионалов из различных областей, в том числе социологов, специалистов по психологии и правозащитников, в процесс разработки и оценки алгоритмов.

Восприятие и предотвращение предвзятости в алгоритмах – это этап к формированию наиболее объективного сообщества, где технологические процессы предназначаются на благо всех без исключения, а не только отдельных групп. Следовательно, основная причина – это предвзятые обучающие данные.

2.2. Примеры дискриминации в ИИ.

Правовое положение о дискриминации отражено в статье 26 Международного пакта о гражданских и политических правах: «Все люди равны перед законом и имеют право на равную защиту закона без любых проявлений дискриминации. Справедливый закон запрещает любую дискриминацию и обеспечивает гарантию равноправия для всех, также закон должен обеспечивать эффективную защиту от дискриминации по любому основанию, таким как раса, цвет кожи, пол, язык, религия, политические или иные взгляды, национальное или социальное происхождение, имущество, рождение или другой статус». Кажется бы, что все вопросы, связанные с дискриминацией, изучены и обрели правовой статус. Однако на сегодняшний момент возникает новое проявление предвзятости, которое весьма трудно предугадать и предусмотреть. Эта новая волна дискриминации связана с распространением и проникновением во все сферы жизни ИИ. ИИ действительно начинает технологическую революцию, и, хотя ему еще предстоит «захватить» мир, есть более насущная проблема, с которой мы уже столкнулись, – предвзятость ИИ. «Предвзятость ИИ – это основное предубеждение в данных, которые используются для создания алгоритмов ИИ, что в итоге может привести к дискриминации и другим последствиям» [3. С. 179].

Как мы уже знаем, основная причина – это предвзятые обучающие данные. Если данные, на которых обучает модель, уже имеет признаки перекоса к определенным группам лиц (например, определенная группа чаще получала отказы в выдаче кредита в прошлом), то ИИ просто «научится» повторять эту несправедливость. Вторая причина – выбор признаков, который может быть косвенно связан с сентиментальными характеристикам, даже если напрямую они никак не учитываются при скрытой дискриминации. Самое опасное – это

скрытая дискриминация т.е. когда чувствительный признак не отображается в данных, на которых модель обучалась, но алгоритм угадывает его путем определенных логических размышлений в ходе обучения. Чисто технически, определенный уровень дохода, место проживания, тип занятости и т.п. может косвенно отразить расу или пол человека. Из-за этого хочется поднять такой вопрос: «ИИ точно может быть справедливым?».

Заключение. Проведенный анализ показал, что главные этические вызовы в сфере разработки ПО и систем ИИ связаны с защитой персональных данных, прозрачностью алгоритмов, преодолением предвзятости и ответственностью за использование технологий. Принципы минимизации сбора информации и получения осознанного согласия пользователей требуют не только законов, но и формирования зрелой корпоративной культуры. Концепция «ответственного ИИ», включающая прозрачность и объяснимость решений, уже находит отражение в международной практике, но в российском контексте еще нуждается в развитии и механизмах контроля. Анализ причин алгоритмических предвзятостей и примеров дискриминации показал: наибольший эффект дает комплексный подход – от внимательной подготовки обучающих данных до корректировки моделей после их внедрения. В итоге можно сказать, что только совместные усилия разработчиков, юристов и государства способны обеспечить безопасное, справедливое и доверительное развитие цифровых технологий.

Список литературы

1. Харитонов Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. 2021. Вып. 53. С. 488–515. DOI: 10.17072/1995-4190-2021-53-488-515.
2. Смирнова А. И. Предвзятость как проблема алгоритмов ИИ: этические аспекты // Философия и общество. 2023. № 3. С. 118–126. DOI: 10.30884/jfio/2023.03.07.
3. Каштанова Е. В., Лобачева А. С. Проблемы предвзятости и дискриминации человеческого капитала в системах искусственного интеллекта // Государственный университет управления. Москва, Россия. 2023. № 3. С. 176–185.
4. Российская Федерация. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 10.07.2023) "О персональных данных" // Официальный интернет-портал правовой информации. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 25.04.2025).
5. Гражданский кодекс Российской Федерации (часть четвертая): Статья 1286.1. Открытая лицензия на использование произведения науки, литературы или искусства // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_64629/e0c0d28fc67b7998751c3a7f98f6be9dfb789911/ (дата обращения: 25.04.2025).
6. Бегишев И.Р. Правовое регулирование беспилотных транспортных средств // Транспортное право. 2021. № 3. С. 7-10. EDN BFFKKJ.

7. Регулятор в США занялся инженерным анализом работы автопилота Tesla – система отключается за секунды до аварии // Habr. URL: <https://habr.com/ru/news/671020/> (дата обращения: 25.03.2025).

8. В РАН заявили, что работа с ИИ требует правовых изменений для защиты человеческой сущности // ТАСС. URL: <https://nauka.tass.ru/nauka/20005585> (дата обращения: 23.03.2025).

9. Деградация базовых навыков пилотов. URL: <https://aviasafety.ru/19514/> (дата обращения: 25.03.2025).

10. Правительство разработает закон об искусственном интеллекте // РБК. URL: <https://www.rbc.ru/rbcfreenews/649b950c9a794732a27a407b> (дата обращения: 03.04.2025).

11. Защита персональных данных: что меняется в 2024 году // Гарант. URL: <https://www.garant.ru/article/1555428/> (дата обращения: 28.04.2025).

12. Как приложения в смартфонах "видят" наши действия. И чем мы рискуем в этом случае // ТАСС. URL: <https://tass.ru/obschestvo/6132879> (дата обращения: 23.04.2025).

Цифровизация: новые горизонты правового регулирования криптовалюты

Аннотация. Статья посвящена актуальной проблеме развития и правового регулирования цифровых прав – новой категории прав, возникающей в условиях цифровизации общества. Автор анализирует природу цифровых прав, подчеркивая их уникальные характеристики: существование исключительно в электронной форме, специализированные механизмы реализации, а также сочетание имущественных и неимущественных аспектов. Особое внимание уделяется международному опыту правового регулирования цифровой сферы. В статье поднимается вопрос о необходимости совершенствования национальных законодательных механизмов для эффективной защиты цифровых прав в условиях стремительного технологического прогресса. В статье рассматривается эволюция правового статуса криптовалют в России, в частности изменения в законодательстве 2021 года, признавшие цифровые валюты имуществом для целей исполнительного производства. Проанализирована судебная практика, включая прецедентные решения. Особое внимание уделяется криминологическим аспектам обращения криптовалют. В работе исследуются основные риски, связанные с использованием цифровых активов в противоправной деятельности: от финансовых махинаций до финансирования терроризма.

Ключевые слова: цифровые права, цифровизация, криптовалюта, цифровые активы, статус криптовалюты, система налогообложения, финансовые преступления, террористическое финансирование, судебная практика

S. A. Zadorina,

Student,

National Research University Higher School of Economics

Digitalization: new horizons for legal regulation of cryptocurrency

Annotation. The article addresses the current challenges in the development and legal regulation of digital rights—a new category of rights emerging in the context of societal digitalization. The author examines the nature of digital rights, emphasizing their unique characteristics: their exclusive existence in electronic form, specialized implementation mechanisms, and the combination of both proprietary and non-proprietary aspects. Attention is given to international experience in the legal regulation of the digital sphere. The article raises the question of the need to improve national legislative mechanisms to ensure the effective protection of digital rights amid rapid technological progress. The study also explores the evolution of the legal status of cryptocurrencies in Russia, particularly the 2021 legislative amendments that recognized digital currencies

as property for enforcement proceedings. Precedential judicial decisions are analyzed, including landmark rulings. Special focus is placed on criminological aspects of cryptocurrency circulation, examining key risks associated with the use of digital assets in illicit activities—ranging from financial fraud to terrorist financing.

Keywords: digital rights, digitalization, cryptocurrency, digital assets, legal status of cryptocurrency, taxation system, financial crimes, terrorist financing, judicial practice.

Введение. За последние десятилетия мир подвергся значительным изменениям, в большинстве своем это связано с развитием глобальной сети Интернет и широким внедрением различных цифровых инструментов в нашу жизнь. В связи с этим, развитие получила новая категория прав – «цифровые права». Цифровые права, это права существующие исключительно в электронной форме, они могут быть использованы для владения, управления и распоряжения цифровыми активами, касаются как имущественных, так и личных неимущественных прав. Реализация таких прав возможна только через специализированные цифровые системы, что и отличает их от традиционного понятия прав.

Вопрос о необходимости совершенствования правового регулирования в цифровой сфере неоднократно вставал перед мировой общественностью, так, например Хартия глобального информационного общества (Окинава, 22 июля 2000 г.), принятая представителями восьми ведущих мировых держав, включая Россию, провозглашает необходимость укрепления соответствующей политики и нормативной базы, содействующих сотрудничеству по оптимизации глобальных сетей, борьбе со злоупотреблениями, которые подрывают целостность сети, по сокращению разрыва в цифровых технологиях, инвестированию в людей и обеспечению глобального доступа и участия в этом процессе.

В качестве основополагающих правил Хартия предусматривает:

- развитие эффективного механизма защиты частной жизни потребителя, а также защиты частной жизни при обработке личных данных, обеспечивая при этом свободный поток информации;
- дальнейшее развитие и эффективное функционирование электронной идентификации, электронной подписи, криптографии и других средств обеспечения безопасности и достоверности операций.

В Хартии также подтверждена обязанность государств согласовывать свои действия по созданию безопасного киберпространства, безопасности информационных систем, защищенных от преступности, в том числе от транснациональной организованной преступности.

Тот же вопрос был освещен и в рамках заседаний Генеральной Ассамблеи ООН. В Резолюции Генеральной Ассамблеи ООН от 18 декабря 2013 г. № 68/167 «Право на неприкосновенность личной жизни в цифровой век» отмечается, что быстрые темпы технологического развития позволяют людям во всех регионах мира пользоваться новыми информационными и коммуникационными технологиями и в то же время повышают способность правительств, компаний и физических лиц отслеживать, перехватывать и собирать информацию, что может нарушать или ущемлять права человека (особенно право на

неприкосновенность личной жизни). При этом подчеркивается, что необходимость обеспечения общественной безопасности может оправдывать сбор и защиту некоторой конфиденциальной информации, но государства должны гарантировать соблюдение в полном объеме своих международно-правовых обязательств в сфере прав человека. В Резолюции содержится призыв ко всем государствам: а) уважать и защищать право на неприкосновенность личной жизни, в том числе в контексте цифровой коммуникации; б) положить конец нарушениям этих прав и создавать условия для предотвращения таких нарушений, в том числе путем обеспечения соответствия национального законодательства их международным обязательствам; в) провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех международных обязательств; г) учредить новые или продолжать использовать уже имеющиеся независимые, эффективные внутренние надзорные механизмы, способные обеспечивать транспарентность в соответствующих случаях и под-отчетность в отношении слежения государств за сообщениями, их перехвата и сбора личных данных.

В России цифровые права получили свое признание в 2019 году с внесением изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации. Согласно статье 141.1 ГК РФ, цифровые права в гражданском кодексе являются полноценными объектами имущественных прав. Благодаря признанию цифровых прав объектами гражданских прав мы можем свободно осуществлять сделки, дарения, наследование, где объектом является цифровое право.

Однако, несмотря на значительное внимание государства, обращенное на регулирование цифровой среды, действующее законодательство не отвечает, в полной мере, вызовам современности и нуждается в детальной проработки, устранении противоречий и приведению понятийного аппарата в стройную и понятную структуру.

Основная часть

Цифровизация: мировые тенденции развития. В современном мире происходят глобальные трансформации различных сфер жизни, в основном такие процессы связаны с развитием глобальной сети «Интернет». «Интернет образует самостоятельное юридически значимое пространство, которое может быть рассмотрено наряду с территорией земли, водным и воздушным пространством, определяющими суверенные границы государства. Киберпространство – новая юридическая фикция, связанная с информацией» [14. С. 13]. Благодаря широкому распространению технологий мы живем в эпоху цифровизации, она пронизывает все сферы жизни современного общества. Поскольку, данный процесс неизбежно охватил значительный круг общественных отношений, существует необходимость осветить вопрос взаимовлияния цифровизации и правовой сферы. Процесс активного развития и внедрения новых технологий на сегодняшний день выступает ключевым катализатором модернизации правовых институтов, существующих инструментов и механизмов правового регулирования, расширяет круг об-

щественных отношений, требующих нормативного регулирования. Цифровизация» оказывает заметное воздействие прежде всего на сферу правового регулирования, являясь важным фактором, обуславливающим ее динамику. В нее вовлекаются новые общественные отношения, которые прежде либо не существовали, либо не требовали правового регулирования или объективно не могли быть урегулированы правом [15]. Глобализация, которая происходит в том числе в сфере правоприменения, имеет позитивные черты. Позитивные черты, безусловно, это обмен опытом, взаимопроникновение традиций, подходов, культуры, в том числе юридических культур и традиций. Есть при этом и совершенно негативные проявления глобализации, например, когда имеют место попытки экстерриториального применения права в обход тех международных норм. По сути, это даже уже не применение права, а применение права силы.

В то время, когда право стояло на пороге грядущих изменений, цифровое право, в свою очередь, боролось за свое существование и признание, стремительное развитие информационных компьютерных технологий поставило мировое сообщество перед необходимостью не просто признания, а адаптации структуры и системы права. Причем если в частном праве ИКТ лишь формально преобразуют многие институты и нормы, то для публичного права существует тенденция к нейтральности и экстерриториальности, что неизбежно ведет к потере государственного суверенитета.

Многие страны, в том числе Россия, предприняли ряд мер для адаптации и урегулирования нормативной базы, в связи с вызовами информационной среды, например, в 2016 году завершилась работа над проектом Е-Кодекс – европейской транснациональной системы документооборота, в настоящее время, продолжает действовать и «Цифровая повестка» стран-членов ЕАЭС рассчитана до 2025 года. В России, в свою очередь, с 2019 года был запущен масштабный Национальный проект «Цифровая экономика», который завершился в конце 2024 года и охватил значительные сферы для активного внедрения цифровых технологий. На смену уже принят новый национальный проект «Экономика данных и цифровая трансформация государства», нацеленный на дальнейшее расширения сферы информационных технологий, в том числе, на цифровую модернизацию государственного и муниципального управления и ключевых отраслей экономики. На сегодняшний день активно продолжается работа над внедрением концепции цифрового рубля. Цифровой рубль – это третья легальная валюта, выпуском которой занимается Центральный Банк РФ. По своей сути, это цифровой аналог обычного рубля, обеспечиваемый Центральным Банком. Концепция предполагает несколько особенностей:

1. Хранение цифрового рубля осуществляется через цифровой кошелек, открытый напрямую в Центральном Банке, нет необходимости в открытии обычного банковского счета.

2. Полный контроль над эмиссией, обращением и всеми транзакциями, не является децентрализованным активом.

3. Центральный Банк выступает единственным и ключевым оператором системы.

Использование цифрового рубля в качестве платежного средства носит добровольный характер, никаких обязательных требований по открытию цифровых кошельков не предусмотрено. Планомерное внедрение цифрового рубля планируется в несколько этапов, начиная с сентября 2026 года. Первым этапом, намеченным на осень, станет использования цифрового рубля крупнейшими банками и торговыми сетями, далее планируется подключение банков с универсальными лицензиями, а уже к 2028 году малый бизнес войдет в сферу использования цифрового рубля.

Цифровизация приводит к изменению характера социальности: в него постепенно входят на правах субъектов и новых нетипичных объектов явления, по старой юридической классификации имеющие неживой, не субъектный и не объектный характер, – инженерия генома, биотехнологии, Интернет, искусственный интеллект, новые финансовые инструменты, в том числе криптовалюта.

«Фактически эти технологии представляют собой гибриды, объединяющие человека с нечеловеческими сущностями, причем последние, будучи созданными, получают известную автономность от человека. Старое разделение, на котором основывалось право физических вещей как независимых объектов, с одной стороны, и общества, культуры, состоящих из автономных субъектов, – с другой, начинает переживать кризис. Право в традиционном разделии не дает надежной юридической защиты отношениям человека в мире новых технологий и уже сейчас замещается неправовыми регуляторами» [12. С. 17]. В связи с чем, классическое и привычное отраслевое деление Российского права, не отвечает той гибкости и динамике, которая требуется для таких многомерных объектов и соответственно, не может предоставить исчерпывающие инструменты регулирования.

Понятие криптовалюты и ее статус. Активное развитие Интернета и расширение интеграционного пространства в сфере финансового регулирования приводят к появлению новых финансовых продуктов и инструментов, основным предназначением которых является удовлетворение возросших потребностей хозяйствующих субъектов в эффективном, безопасном и оперативном денежном обмене. Одним из таких инструментов является криптовалюта – децентрализованная электронная валюта, созданная Сатоси Накамото в 2009 г.

Криптовалюта, как уже отмечено выше, это децентрализованная цифровая валюта или виртуальные деньги, которые защищены специальным цифровым кодом и работают на базе блокчейна. Что примечательно, легального определения в законодательстве не содержится, однако нормативная база Российской Федерации дает нам понять, что криптовалюта это одна из разновидностей цифровой валюты.

Чем же вызвана такая популярность криптовалюты? Именно международная доступность и отсутствие привязки к банковским системам сделала сделки с участием криптовалюты такими популярными. Действительно, существуют как серьезные преимущества, так и значительные недостатки данного вида валют, рассмотрим некоторые из них, к положительным сторонам стоит отнести:

1. Широкие возможности диверсификации инвестиционного портфеля, поскольку существует огромное многообразие криптовалют

2. Высокий уровень безопасности, доступ к валюте имеет только лицо, обладающее специальным ключом доступа

3. Удобство и универсальность, для того чтобы начать пользоваться криптовалютой достаточно иметь доступ в интернет.

4. Децентрализованный характер валюты, все операции регулируются только участниками блокчейн-сети без привязки к банку и являются полностью анонимными.

Несмотря на удобство использования такого средства платежа, существует и ряд отрицательных аспектов:

1. Крайне высокий уровень волатильности. Криптовалюта может терять огромные проценты за минимальный период времени.

2. Тенденция к принятию регуляторных мер. Существует ряд стран, где любые операции с криптовалютой запрещены, также, отсутствие возможности влиять на эмиссию и операции с криптовалютой заставляет страны вводить определенные ограничения.

3. Одна из самых низких скоростей транзакций. Связана с техническими особенностями технологий блокчейна.

4. Зависимость от общего настроения участников финансового рынка. Это связано с отсутствием реальной ценности криптовалюты, отсюда риск манипулирования рынком.

Финансовые Активы и цифровая валюта, действительно вызывали оживленную дискуссию, а суды начали сталкиваться с делами, в которых фигурировала криптовалюта, биткойны и т.д. и что с ними делать было непонятно. В 2018 году Государственная дума приняла Федеральный закон № 259-ФЗ, который ввел легальное понятие цифровой валюты, тем самым, совершив первую попытку по урегулированию вновь возникшего объекта права. На основании ч. 11 ст. 1 можно сделать вывод, что цифровые финансовые активы и цифровые валюты имеют особую правовую природу и не являются безналичными или электронными денежными средствами, а также не относятся к бездокументарным ценным бумагам [13].

Для определения правового режима криптовалюты ключевое значение имеет то, куда мы ее относим, к цифровым активам или цифровой валюте

Цифровые финансовые активы (ЦФА) – цифровые права, включающие денежные требования и права по ценным бумагам, выпускаемые конкретными эмитентами через специализированные информационные системы

Цифровая валюта – совокупность электронных данных, которые могут использоваться как средство платежа или инвестиций, при отсутствии обязанного лица перед обладателем таких данных.

На данный момент, криптовалюта признана цифровой валютой, с особыми изъятиями, например, запрет на использование криптовалюты как средства платежа внутри страны.

Статус криптовалюты для целей уголовного права. Несмотря на то, что достаточно долгое время статус криптовалюты был неоднозначным, в вышеупомянутый Федеральный закон были внесены изменения 1 января 2021 го-

да, которые определили криптовалюту как имущество для целей исполнительного производства

Цифровую валюту впервые признали имуществом в спорах о банкротстве. В деле № А40–124668/2017 Девятый арбитражный апелляционный суд 15 мая 2018 года обязал должника предоставить финансовому управляющему доступ к криптокошельку. При этом суд указал, что любое имущество должника, которое имеет экономическую ценность для кредиторов, не может произвольно исключаться из конкурсной массы. Криптовалюту фактически признал имуществом и Верховный суд в определении по делу № 44–КГ20–17–К7 в начале 2021 года, данное решение стало отражением введенных изменений Федерального закона №259-ФЗ.

Принципиально значение признания криптовалюты имуществом имело в области уголовного права, в том числе, исполнительного производства. На протяжении многих лет непонятно было, а как квалифицировать, если предметом спора являлась криптовалюта. Помимо этого, до 2025 года не существовало возможности для конфискации цифровой валюты, поскольку Уголовный кодекс и Уголовно-процессуальный кодекс не содержал легального понятия цифровой валюты, а также, не было предусмотрено соответствующего механизма изъятия, из-за таких особенностей как, анонимность, отсутствия физических свойств такого вида валюты и сложностей получения ключей доступа к материальным носителям и крипто кошелькам. Первым шагом в разрешении этого вопроса стало решение районного суд в Санкт-Петербурге, который впервые разрешил следователю наложить арест на украденную цифровую валюту, хранящуюся на криптокошельках обвиняемого по уголовному делу уже в 2022 году. В 2025 году Государственная Дума РФ в первом чтении приняла законопроект №902782–8, который признает цифровую валюту имуществом для целей Уголовного и Уголовно-процессуального кодексов, а также регламентирует действия следователя по ее изъятию и признанию вещественным доказательством.

Данный законопроект породил дискуссии в рамках Петербургского Юридического Форума, обсуждались различные способы регламентации процедуры изъятия, получение удаленного доступа, помимо воли владельца криптокошелька и сложности, с которыми придется столкнуться следственным органам, в том числе, проблемы с получением кода доступа. Также возникает вопрос, как будет производиться оценка таких криптоактивов в целом и в случае, если объект, подлежащий конфискации будет утрачен. Законопроект предполагает привлечения особого рода специалиста для проведения процедуры конфискации, однако, кто будет обучать таких специалистов, какие требования к ним будут предъявлены, пока непонятно, возможно, этот вопрос будет освещен в соответствующем Постановлении Правительства, о котором идет речь в пояснительной записке к проекту.

Налогообложение криптовалюты. Ситуация с налогами в отношении криптовалюты за последние годы претерпела значительные изменения, в пользу ужесточения контроля доходов, полученных в результате сделок с криптовалютой, этот тезис находит свое подтверждение в высказываниях *Александра Вайса*, члена комиссии по ЦФА ТПП РФ и РСПП РФ:

«ФНС и Росфинмониторинг активно усиливают надзор. С 2021 года биржи обязаны передавать данные о клиентах по запросу. Введен блокчейн-анализ для отслеживания крупных транзакций. Проводятся проверки при подозрении в уклонении от налогов, особенно при выведении средств через зарубежные платформы.

Дополнительно, с 2022 года действует налоговое регулирование: доходы от операций с криптовалютой подлежат декларированию и обложению НДФЛ [1].

Для начала необходимо осветить ситуацию, которая сложилась до принятия глобальных изменений, а именно, до принятия Федерального закона от 31.07.2020 №259-ФЗ «О цифровых финансовых активах» и Федерального закона от 29.11.2024 № 418-ФЗ. До 2021 года никакого специального регулирования налогового вопроса в отношении криптовалюты не устанавливалось, поскольку статус криптовалюты не был понятен, как было замечено ранее именно Федеральный закон от 31.07.2020 №259-ФЗ «О цифровых финансовых активах» определил криптовалюту как имущество, что и дало соответствующий толчок для дальнейшей модернизации налогового вопроса. Ранее, налогообложение строилось на базовых концепциях, предусмотренных, Налоговым Кодексом РФ. На операции с криптовалютой распространялся налог НДФЛ, то есть, необходимо было уплатить соответствующую сумму, после того как владелец криптовалюты конвертировал ее в фиатные средства, именно с момента конвертации криптовалюта считалась доходом.

Федеральным законом от 29.11.2024 № 418-ФЗ были установлены конкретные правила налогообложения всех операций с криптовалютой, включающие куплю-продажу и майнинг, для физических и юридических лиц. Некоторые важные положения данного акта: для целей налогообложения, криптовалюта признается имуществом, также проведена дифференциация налога для физических лиц: майнинг – доходы облагаются по ставке 13–22% в зависимости от размера дохода; купля-продажа – прибыль от операций облагается по ставке 13–15%; в свою очередь для юридических лиц: налог на прибыль – 25% с доходов от майнинга и торговли; НДС – 20% с операций реализации (за исключением майнинга).

Помимо этого, закон установил порядок определения стоимости цифровой валюты в целях исчисления налога на доходы физических лиц и налога на прибыль организаций, а также теперь оператор майнинговой компании должен сообщать все сведения, которые касаются процесса майнинга в налоговый орган, для внесения в специализированный реестр, а также нести ответственность за неисполнение данной обязанности. Действительно, майнинг в России не запрещен, однако Правительство установило определенные ограничения по потреблению электроэнергии в процессе майнинга. Также стоит заметить, что майнинг на некоторых территориях запрещен, это территории Северного Кавказа (Дагестан, Ингушетия, Северная Осетия, Карачаево-Черкесия, Чечня, Кабардино-Балкария), в некоторых регионах Сибири (Иркутская область, Забайкальский край, Бурятия), а также (Донецкая народная республика, Луганская народная республика, Запорожская область, Херсонская область.) это связано, с дефицитом мощности сетей электроэнергии. Различное регулирование ставок

налогообложения также предусмотрено для таких групп как налоговые резиденты РФ и нерезиденты:

Налоговые резиденты имеют возможность понижения ставки, в случае если документально будут подтверждены понесенные расходы на процесс майнинга, нерезиденты не имеют такой возможности

Для нерезидентов установлена фиксированная ставки налогообложения 30%.

Актуальный вопрос, связан и с тем, как определяется стоимость криптоактива для целей налогообложения. Поскольку технически это действительно может вызывать затруднения из-за высокой волатильности валюты, в России предусмотрели механизм такой оценки:

1. В случае, получения доходов путем майнинга стоимость криптовалюты зависит от даты получения цифровой валюты и получения права свободно ей распоряжаться

2. Если доход получен путем осуществления сделки купли-продажи, курс определяется по дате реализации.

Рыночная котировка соответствует цене, установленной на момент закрытия торгов на криптобирже. Налоговые резиденты могут выбрать котировку любой криптобиржи, при условии ее соответствия следующим критериям:

- объем торгов равен более 100 млрд руб. за сутки;
- предоставлены истории изменения котировок сроком более 3 лет.

Если происходит такая ситуация, при которой сделки с одной и той же цифровой валютой совершались через разные биржи, например, две и более биржи, то в таком случае, налогоплательщик вправе самостоятельно выбрать рыночную котировку, соответствующую одной из бирж, на которой производились торги.

Риски, связанные с появлением криптовалюты. В связи с возникновением и активным распространением новых финансовых инструментов перед мировой общественностью встали и новые вопросы, связанные с рисками применения таких объектов в нелегальной деятельности. Криптовалюты действительно является привлекательным инструментом для разного рода мошенников, хотя бы из-за анонимности транзакций и отсутствия полноценного регулирования со стороны государства.

Растущий интерес к криптовалюте вызвал и пропорциональный рост преступной деятельности, помимо финансовых преступлений активизировались также террористические организации, активно использующие цифровые валюты для финансирования своей деятельности. Говоря о рисках, связанных с распространением криптовалюты стоит отметить, как некоторые частные:

1. Высокие риски инвестором из-за отсутствия стабильности курса

2. Манипуляции отдельных лиц, так называемые схемы Pump and Dump, с англ. – «накачать и сбросить», когда закупается множество неизвестных видов валюты и искусственно повышается ее реальная стоимость, а затем следует сильный обвал курса.

3. Потеря доступа к денежным средствам, если владелец потеряет числовой код доступа или просто его забудет, восстановить доступ не предоставляется возможным.

4. Технические риски, помимо сложностей, которые вызывает обычное замедление сети, существует понятие «развилки» сети или Форка блокчейна (от англ. fork – «разветвление»). Это происходит, поскольку все взаимодействия внутри сети строятся на правиле консенсуса, когда одна часть сообщества не принимает изменения, которых хочет другая, происходят так называемые развилки. Опасность заключается в том, что во время развилки сети, образуется два независимых блокчейна вместо одного, это приводит к уязвимости для хакерских атак, а также к потере доверия к проекту, поскольку такое разветвление способно изменить даже подход к транзакциям. Ярким примером форка является случай, произошедший с биткоином в Bitcoin Cash, сообщество не пришло к консенсусу в вопросе масштабируемости и размера блоков, в связи с этим, появился новый блокчейн с другим подходом к транзакциям.

Помимо частных, существуют и общегосударственные риски, некоторые из них выделял и Центральный Банк РФ в отчете за 2022 год [5], помимо частных (угроза благосостоянию граждан)

1. Риски для финансовой стабильности

Активное использование криптовалюты может приводить к образованию теневого сектора экономики и снижению финансирования реального.

Также вследствие перетока капитала из традиционной финансовой системы на криптовалютный рынок существует риск снижения объемов финансирования реального сектора экономики. Отток средств из традиционных ценных бумаг (акций, облигаций) в криптовалюты приведет к падению капитализации российского фондового рынка и ограничит возможности эмитентов по привлечению инвестиций.[5].

2. Риски, связанные с нелегальной деятельностью. Риски этой категории, как и было сказано выше, связаны с такой особенностью криптовалюты как анонимность, именно из-за анонимности транзакций криптовалюта привлекательна для отмыwania средств и нелегальных покупок в теневом интернете. Мою точку зрения поддерживает и вышеупомянутый отчет ЦБ РФ, в последние годы криптовалюты (в частности, Bitcoin) используются на всех стадиях преступной деятельности. Использование криптовалют наиболее характерно для преступлений, связанных с незаконным оборотом наркотиков и выплатой вознаграждений за их реализацию.

Поскольку механизм использования криптовалюты в террористических организациях достаточно неоднозначный, разумнее будет раскрыть этот аспект более подробно.

Рост интереса к криптовалютам со стороны террористических организаций вызван ее особенностями по обеспечению относительной анонимности, трансграничности переводов, большой стоимостью, доступностью и широким распространением в DarkNet (основной площадке теневого рынка оружия, наркотиков и запрещенной литературы) [3]. Все это усложняет контроль со стороны правоохранительных органов. Террористические организации по всему миру прибегают к использованию такого финансирования для того, чтобы остаться незамеченными и получить средства для осуществления своих преступных действий. Финансирование терроризма предполагает прохождения нескольких этапов:

1. Ввод средств. На этом этапе, злоумышленники самостоятельно либо через третье лицо осуществляют ввод денежных средств на криптокошелек и осуществляют покупку на крипто бирже

2. Этап лееринга (от англ. *layering* – «наслаивание»). Это основной этап, поскольку на нем осуществляется «дробление суммы», множество транзакций осуществляется на разные адреса счетов, чтобы скрыть подозрительный перевод. Для этого используют специализированные сервисы, так называемые миксеры или тумблеры, которые смешивают криптовалюту и создают сложную сеть транзакционных цепочек.

3. Этап интеграции. После успешного сокрытия источника платежа, криптовалюта вводится в легальное денежное пространство и на эти денежные средства, с помощью которых можно осуществлять любую финансовую операцию.

Мировой общественности известно несколько громких дел, где предметом финансирования вступала именно криптовалюта:

- компания военного крыла ХАМАС, бригад аль-Кассама, проводившаяся в период с 2019 по 2020 год. Потенциальным жертвам предлагалось перевести биткоин на статический адрес, который публиковался в социальных сетях. А затем для каждой жертвы генерировался новый уникальный адрес, что затрудняло отслеживание средств;

- план «Аль-Каиды» и террористических организаций Сирии. Группы создали систему отмывания денег, используя мессенджер Telegram и другие популярные социальные сети для призыва к пожертвованиям криптовалюты.

- теракт в Крокус Сити Холле [9].

Адрес кошелька был размещен в Telegram-канале, связанном с "Голосом Хорасана" (*"Виляят Хорасан" входит в "Исламское государство", обе организации признаны террористическими и запрещены в РФ*). Кошелек впервые появился в Сети 12 марта. Данный кошелек был активен, а ссылка ежедневно обновлялась. Он был размещен в Telegram-канале экстремистской направленности, приходившие в кошелек суммы практически сразу из него уходили. После дня теракта переводы с этого криптокошелька и на него больше не осуществлялись.

Международный опыт. Однозначного ответа на вопрос по поводу статуса криптовалюты нет и на международной арене, поскольку даже на теоретическом уровне, все еще не существует единообразного подхода для классификации такого вида цифровой валюты. На данный момент существует три модели регулирования криптовалюты.

1. Полное признание криптовалюты. Страны, которые придерживаются данного подхода полностью признают криптовалюты как товара и инвестиционного инструмента.

2. Частичная легализация. Страны такого подхода ограничивают применение криптовалюты в финансовых операциях, например, не признают законным платежным средством, но операции все равно подлежат налогообложению.

3. Полный запрет. Страны данного подхода запрещают использование цифровой валюты, под угрозой применения соответствующих санкций.

Концепции полного признания придерживается США, страна рассматривает криптовалюту как имущество, а не цифровую валюту. Также, с доходов от прода-

жи криптовалюты существует необходимость уплачивать налог на прибыль. В июле 2025 года США приняли ряд законов, регулирующих рынок криптовалют. Во время проведения «Криптонедели» Конгресс принял три ключевых закона, наиболее важный из них GENIUS Act, впервые на федеральном уровне утвердил порядок регулирования стейблкоинов – криптовалюты, привязанной к доллару. Закон установил правила эмиссии и требования к резервам компаний-эмитентов.

По пути частичной легализации движется Российская Федерация. Россия не признает криптовалюту платежным средством, однако криптовалюта выступает в качестве частного актива, нельзя оплатить товары или услуги, однако можно покупать и продавать через иностранные биржи, использовать как инструмент для инвестиций. Таким образом, на данный момент, криптовалюта в нашей стране находится в серой зоне.

Полного запрета данного финансового инструмента придерживается Китай. Власти страны ввели запрет не только на торговые операции связанные с криптовалютой, но и частное владение такой валютой. Такой запрет власти Китая объясняют стремлением строго контролировать движения капитала в стране, а также развитием инициативы цифровой национальной валюты – юаня.

На мой взгляд, полный запрет криптовалюты ведет к негативным последствиям, поскольку это увеличивает риск создания незаконного цифрового рынка, а как следствие, возникновение теневого сектора экономики.

Возможные решения проблем. В связи со значительным расширением круга объектов и субъектов правового регулирования, ранее неизвестные Российскому праву, возникает ряд проблем, требующих решения. Одна из них, это трудности с регулированием новых финансовых инструментов. Нормативные правила и нормы установить, конечно, можно, однако сложности возникают с контролем соблюдения таких норм, а также отсутствие механизмов для осуществления такого контроля и надзора.

Очевидно, что потребность в обеспечении правового регулирования необходимым высокотехнологическим инструментарием, прежде всего позволяющим осуществлять контроль за деятельностью субъектов права, существует [15].

Путь регулирования стремительно развивающегося мира действительно сложная задача, поскольку создание и разработка норм – это достаточно длительный процесс и право просто не успевает за таким массивом изменений. Все цифровые права, в том числе, связанные с криптовалютой, на данный момент носят фрагментарный характер, это разрозненные, отрывочные нормы с отсутствием даже минимальной систематизации.

Поэтому одной из ключевых задач на данный момент является создание систематизированной базы законодательства, например, цифрового кодекса, идея которого, была разработана специалистами Института государства и права РАН, а также, необходимость создания такого кодекса подчеркивал и действующий председатель Конституционного Суда РФ Валерий Зорькин на просторах Петербургского Юридического Форума «Одним из вариантов такой систематизации могло бы стать принятие Информационного кодекса Российской Федерации. Эта идея получила свою реализацию подготовленной Институтом государства и права РАН в 2014 г. Концепции проекта Информационного кодекса Российской Фе-

дерации. В основу концепции положено право граждан на информацию и формы его реализации. В советское время информационное право рассматривалось в качестве элемента административного права, основным методом которого является метод императивных предписаний со стороны государственных органов. В контексте ныне действующей Конституции РФ необходима разработка конституционно-правовой концепции информационного права, основу которого должно составлять конституционное право граждан на информацию.

Информационный кодекс призван конкретизировать конституционное право человека и гражданина на информацию, урегулировать общие вопросы оборота информации в Российской Федерации, закрепить ряд правовых понятий, связанных с оборотом информации, а также установить общие требования к государственным информационным системам, которые будут разрабатываться, вестись и поддерживаться соответствующими органами государственной власти, государственными органами. Законодателю предстоит определить основные формы оборота информации, установив права и обязанности его участников, непротиворечивым образом определить правовой режим информации в публично-правовой и частноправовой сферах, а также основания, формы и пределы применения информационных технологий в деятельности соответствующих субъектов права» [7]. Концепция кодекса активно обсуждалась с 2014 года и добилась признания в 2024 году, однако дальше обсуждений это пока не двинулось, несмотря на серьезную потребность в систематизации.

Кодекс решил бы следующие проблемы:

1. Четкое определение природы и правового статуса новых цифровых объектов права в информационном пространстве
2. Систематизация отрывочных норм, содержащихся в федеральных законах и локальных нормативно-правовых актах, тем самым провести анализ на противоречие норм друг-другу и устранение существующих пробелов
3. Выработка единых подходов к регулированию для цифровых объектов, которое позволит образовать единообразный подход в правоприменительной практике судов, а не единичные решения
4. Правовую базу, для возможности реализации гражданами право на использование и распространение информации, гарантированное Конституцией РФ.

Наличие сильной и упорядоченной правовой базы в области цифровых прав – это ключ не только к пониманию их сущности, но и к правовой определенности и возможным ограничениям со стороны государства. На данный момент, существует сложность в определении грани что является легальным и дозволенным, а что собой представляет выход за рамки и представляет угрозу.

Также важно избегать чрезмерного регулирования, особенно когда это касается таких объектов как цифровые валюты, поскольку даже на данный момент не хватает технической оснащенности для регулирования данного вида объектов права. В случае, если государство прибегнет к реализации стратегии чрезмерного регулирования, то все операции с цифровыми валютами уйдут в теневой сектор экономики, это приведет не только к технической сложности отслеживания таких операций, но и к еще большим проблемам правового регулирования такого явления, а также размытию уже существующих ограничений.

Помимо этого, решения проблем, возникающих в области регулирования криптовалюты невозможно осуществлять только в рамках одного государства, необходимо использовать комплексный подход для разработки международных стандартов регулирования, поскольку криптовалюта носит трансграничный характер. Сейчас никаких общепринятых стандартов нет, более того, не существует стандартов не только в области сделок с криптовалютой, но и в определении ее статуса, поскольку где-то она является имуществом, где-то валютой и т.д. Решением может стать разработка международных правовых норм, содержащих правила лицензирования криптоактивов, поскольку это поможет выводить финансовые операции такого характера из серой зоны и предотвратит использование этих средств в целях финансирования терроризма, а также поспособствует противодействию отмывания средств.

Заключение. Сегодня мы являемся наблюдателями и участниками глобальных процессов, происходящих во всем мире и один из наиболее важных процессов это цифровизация. Это одна из ступеней развития, за которой нам, а в особенности правовой системе нужно успевать и идти с ней в ногу, полный отказ от проникновения данного процесса в сферу жизни человека невозможен практика наименее информационно развитых государств показала всему миру, что противодействие такому процессу не только невозможно и губительно поскольку:

- снижение экономических показателей, поскольку большинство стран осуществляют экономическое сотрудничество посредством цифровых ресурсов, у стран с отсутствием налаженных цифровых процессов в области экономики снижается уровень конкурентоспособности на мировом рынке;

- рост рисков для безопасности. Страны, которые игнорируют процессы цифровизации не смогут победить киберпреступность и защитить себя от таких преступлений;

- снижения уровня жизни населения. Отказ от цифровизации усложняет не только привычные нам процессы, но и в разы уменьшает эффективность производства, что напрямую влияет на благосостояние граждан таких стран.

В данном контексте более эффективен путь наименьшего сопротивления, а в идеале, мы должны придерживаться пути своевременного развития и линейной модернизации этих процессов. Что касается новых объектов права, необходимо начинать с определения их правовой природы для дальнейшего регулирования всех связанных процессов. Фрагментарное регулирование нормами и локальными актами не является эффективным инструментом. Право должно своевременно реагировать на возникновение новых феноменов для создания системы, в которой каждый участник, тех или иных отношений, получает гарантию правовой определенности, гарантию соблюдения его прав и равные возможности для их реализации, аналогичную мысль выразил и Вадим Виноградов декан факультета права НИУ ВШЭ, руководитель рабочей группы по законодательству в сфере интернет-технологий и цифровизации ОП РФ: «Право, как всегда, отстаёт от реальности и технического прогресса, а технологии заставляют нас торопиться с поиском ответа на эти вопросы выработкой новых правовых решений, чтобы предусмотреть все правовые риски. Важно, чтобы в таком правовом регулировании были заложены возможные механизмы защиты интересов человека» [2].

Список литературы

1. Киселева, А. А. Учет и налогообложение операций с криптовалютой в 2024 году // Audit-it.ru. 2023. 15 ноября. URL: <https://www.audit-it.ru/articles/account/assets/a1032583/1115206.html> (дата обращения: 01.09.2025).
2. Ляпунов, С. И. ЦБУ: что это такое и как работает новый инструмент валютного контроля / С. И. Ляпунов // ГАРАНТ.РУ: информационно-правовой портал. URL: <https://www.garant.ru/article/1554367/> (дата обращения: 01.09.2025).
3. Миронов А. О. Роль криптовалют в совершении преступлений террористической и экстремистской направленности в современных условиях // Baikal Research Journal. 2023. № 4. С. 1693–1694.
4. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федеральный закон от 31.07.2020 № 25ФЗ (ред. от 02.07.2024) // Собрание законодательства РФ. 2020. № 31 (ч. I). Ст. 5018.
5. Отчет Банка России об использовании цифровых финансовых активов за 2022 год. URL: <https://cbr.ru/press/event/?id=12623> (дата обращения: 01.09.2025).
6. Поветкина, Н. А. «Финтех» и «регтех»: границы правового регулирования / Н. А. Поветкина, Ю. В. Леднева // Право. Журнал Высшей школы экономики. 2018. № 1. С. 46–67.
7. Право в цифровом мире // Российская газета. 2018. № 115 (7579). С. 8.
8. Росфинмониторинг раскрыл, как финансировался теракт в «Крокусе»: [статья от 25.04.2024] // Российская газета [сайт].
9. URL: <https://rg.ru/2024/04/25/rosfinmonitoring-raskryl-kak-finansirovalsia-terakt-v-krokuse.html> (дата обращения: 01.09.2025).
10. Сидоренко Э. Л. Криминологические риски оборота криптовалют // Экономика. Налоги. Право. 2017. № 6. С. 152–154.
11. Сидоренко Э. Л. Криптовалюта как новый юридический феномен // Общество и право. 2016. № 3 (57). С. 193–196.
12. Синюков В. Н. Фундаментальные проблемы юридической науки. М., 2019. 17 с.
13. Ситник А. А. Цифровые валюты: проблемы правового регулирования // Актуальные проблемы российского права. 2020. Т. 15, № 11. С. 103–113. DOI: 10.17803/1994-1471.2020.120.11.103-113.
14. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5–17.
15. Хабриева Т. Я. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85–101.

Е. Г. Закиев,
студент,
Белорусский государственный университет транспорта,
А. А. Дашкевич,
студент,
Белорусский государственный университет транспорта

**Правовые аспекты применения искусственного интеллекта
в управлении бизнес-процессами**

Аннотация. В статье рассматриваются правовые аспекты применения искусственного интеллекта в управлении бизнес-процессами. Отмечается, что использование AI позволяет автоматизировать документооборот, прогнозировать спрос, оптимизировать управление персоналом и внедрять смарт-контракты. Вместе с тем возникают правовые проблемы, связанные с защитой персональных данных, распределением ответственности за решения AI и определением прав на результаты интеллектуальной деятельности, созданные с его участием. Цель исследования – выявить основные правовые риски и предложить пути совершенствования нормативной базы. Новизна работы заключается в комплексном анализе национальных и международных подходов к регулированию AI и формулировании предложений для гармонизации законодательства в условиях цифровой экономики.

Ключевые слова: искусственный интеллект, бизнес-процессы, цифровая трансформация, правовое регулирование, персональные данные, ответственность, интеллектуальная собственность, смарт-контракты, международное право

E. G. Zakiev,
student,
Belarusian State University of Transport,
S. S. Sidorov,
Candidate of Law, Senior Lecturer,
Belarusian State University of Transport

**Legal aspects of applying artificial intelligence
in business process management**

Abstract. The article examines the legal aspects of applying artificial intelligence in business process management. It is noted that AI enables automation of document workflow, demand forecasting, personnel management optimization, and the implementation of smart contracts. At the same time, legal challenges arise, including personal data protection, allocation of liability for AI-driven decisions, and the determination of rights to intellectual property created with the participation of AI. The purpose of the study is to identify key legal risks and propose ways to improve the

regulatory framework. The novelty of the work lies in a comprehensive analysis of national and international approaches to AI regulation and in formulating recommendations for the harmonization of legislation in the digital economy.

Keywords: artificial intelligence, business processes, digital transformation, legal regulation, personal data, liability, intellectual property, smart contracts, international law

Введение. Современная цифровая экономика характеризуется стремительным внедрением инновационных технологий, среди которых особое место занимает искусственный интеллект. Его применение в управлении бизнес-процессами становится ключевым фактором повышения эффективности компаний, позволяя автоматизировать рутинные операции, улучшать прогнозирование и анализ, а также формировать новые модели взаимодействия с клиентами и партнерами. Согласно международным прогнозам, к 2030 году вклад AI в мировую экономику может превысить 15 трлн долларов США, что подчеркивает его стратегическое значение для бизнеса.

Однако столь интенсивное развитие технологий сопровождается возникновением сложных правовых вопросов. На практике остро встают проблемы распределения ответственности за решения, принятые с использованием AI, защиты персональных данных, обеспечения прозрачности алгоритмов, а также определения правового статуса результатов интеллектуальной деятельности, созданных с помощью машинного обучения. При этом национальные и международные правовые системы пока не выработали единых подходов к регулированию данных вопросов, что создает риски как для бизнеса, так и для общества.

Актуальность исследования обусловлена необходимостью анализа существующих правовых механизмов регулирования применения AI в управлении бизнес-процессами, выявления их недостатков и разработки предложений по совершенствованию законодательства. Целью работы является исследование правовых аспектов использования искусственного интеллекта в бизнесе и формулирование рекомендаций, направленных на гармонизацию национального регулирования с международными тенденциями.

Основная часть. Правовое регулирование применения искусственного интеллекта на международной арене развивается неравномерно. Наиболее значимым шагом в этой области стало принятие Регламента Европейского Союза о применении искусственного интеллекта (AI Act, 2024), который впервые установил комплексные требования к разработке и внедрению интеллектуальных систем [1]. Документ вводит классификацию рисков и выделяет категории AI-продуктов, от которых зависит степень юридического контроля. В первую очередь внимание уделяется прозрачности алгоритмов, обеспечению защиты персональных данных и закреплению ответственности разработчиков. В Соединенных Штатах отсутствует единый федеральный закон об искусственном интеллекте, однако действуют рекомендации Национального института стандартов и технологий (NIST), а также активно развиваются корпоративные этические кодексы, что демонстрирует приоритет саморегулирования [2].

Во многих странах СНГ, отдельного закона, посвященного искусственному интеллекту, пока не существует. Вместе с тем правовое регулирование осуществляется посредством применения норм действующего законодательства. Например, Закона Республики Беларусь «О защите персональных данных» (2021) [3], а также норм гражданского, трудового и информационного права. На уровне Евразийского экономического союза ведутся дискуссии о необходимости унификации подходов к регулированию цифровых технологий, однако до сих пор эти инициативы носят фрагментарный характер. В научной литературе отмечается, что именно разрозненность нормативных подходов и отсутствие согласованной правовой доктрины создают наибольшие трудности при внедрении AI в сферу бизнеса [6].

Искусственный интеллект активно используется в различных сферах управления бизнесом, что объясняется его способностью обрабатывать большие массивы данных и выявлять закономерности, недоступные традиционным методам анализа [5, 10]. Наиболее заметные результаты достигаются в области документооборота, где AI-системы способны автоматически анализировать тексты договоров, выявлять ошибки и предлагать оптимизацию [4, 6]. В логистике и маркетинге технологии машинного обучения применяются для прогнозирования спроса и оптимизации цепей поставок, что позволяет компаниям снижать издержки и повышать конкурентоспособность [10]. Все большую популярность приобретают интеллектуальные CRM-системы, ориентированные на персонализацию клиентского опыта и предсказание потребительских предпочтений [5]. В кадровом управлении алгоритмы используются для оценки резюме и отбора персонала, а в финансовой сфере – для анализа операций и выявления признаков мошенничества [5]. Наконец, важным направлением становятся смарт-контракты на основе технологии блокчейн, которые позволяют автоматизировать исполнение договорных обязательств без участия посредников [1, 10].

Эти примеры свидетельствуют о том, что AI становится системообразующим элементом в управлении современным бизнесом. Однако повсеместное внедрение интеллектуальных технологий неизбежно сопровождается возникновением сложных правовых проблем, требующих своевременного научного осмысления и законодательного регулирования [4, 6, 7].

Главным вызовом при использовании искусственного интеллекта в бизнесе является проблема ответственности. Если интеллектуальная система принимает решение, повлекшее причинение ущерба, неясно, кто должен нести юридическую ответственность: разработчик, владелец системы или конечный пользователь [4, 8]. Отсутствие четко закрепленных норм в этой сфере создает ситуацию неопределенности и потенциальных конфликтов.

Не менее важным остается вопрос защиты персональных данных. Поскольку алгоритмы машинного обучения требуют значительных объемов информации, компании вынуждены обрабатывать данные работников и клиентов, что повышает риск нарушения их прав и свобод [3, 7]. В условиях недостаточно развитого регулирования возрастает вероятность неправомерного использования информации и ее утечек.

Проблема интеллектуальной собственности также вызывает оживленные дискуссии. Результаты, созданные при помощи AI – будь то тексты, изображения, программы или аналитические отчеты – не всегда могут быть однозначно отнесены к объектам авторского права [9]. Международная практика пока не выработала согласованного подхода к определению их статуса, что создает правовые коллизии и осложняет оборот результатов интеллектуальной деятельности.

Отдельного внимания заслуживают этические вопросы. Использование AI может вести к дискриминации работников или соискателей при автоматизированном отборе, а также к социальным последствиям в виде массового сокращения рабочих мест. Недобросовестные практики применения технологий усиливают необходимость разработки механизмов правового контроля, которые бы сочетали инновационное развитие с защитой общественных интересов [6, 8].

Для минимизации правовых рисков и повышения эффективности применения искусственного интеллекта в бизнес-практике необходим комплексный подход. Прежде всего следует разработать национальную стратегию регулирования AI, которая учитывала бы международный опыт [1–3]. Важным направлением должно стать закрепление требований к прозрачности алгоритмов, включая их объяснимость и возможность проверки решений [7, 8].

Кроме того, требуется разработка правовых норм, определяющих распределение ответственности между участниками оборота AI-систем. Это позволит устранить существующую неопределенность и повысить доверие к технологиям [4, 6]. Усиление правовой защиты персональных данных в условиях автоматизированной обработки и создание механизмов независимого контроля также должны стать приоритетами. Особого внимания заслуживает формирование правового статуса результатов деятельности, созданных с помощью AI, что позволит компаниям более эффективно использовать интеллектуальные продукты [3, 9].

Наконец, для предотвращения недобросовестных практик необходимо внедрение этических кодексов и корпоративных стандартов. Гармонизация национального законодательства с международными нормами будет способствовать интеграции государства в глобальную цифровую экономику и снижению барьеров для трансграничного сотрудничества [1, 10].

Заключение. Применение искусственного интеллекта в управлении бизнес-процессами открывает новые возможности для повышения эффективности, оптимизации операций и развития инновационных моделей ведения бизнеса. В то же время активное внедрение AI сопровождается сложными правовыми и этическими вопросами, связанными с распределением ответственности, защитой персональных данных и определением прав на результаты интеллектуальной деятельности, созданные с помощью алгоритмов машинного обучения.

Проведенный анализ показал, что существующие национальные и международные нормативные базы находятся на разных стадиях развития и в ряде случаев не обеспечивают достаточной правовой определенности для участников цифрового рынка. Для минимизации рисков и эффективного использования AI в бизнесе необходимо разрабатывать комплексные стратегии регулирования,

устанавливать прозрачные правила работы алгоритмов, закреплять ответственность участников и усиливать защиту персональных данных.

Научная новизна работы заключается в комплексном рассмотрении проблем правового регулирования искусственного интеллекта в бизнесе и формулировании практических рекомендаций по гармонизации национального законодательства с международными тенденциями. Реализация предложенных мер позволит обеспечить баланс между инновационным развитием технологий и защитой прав граждан, создавая основу для устойчивого цифрового бизнеса в условиях глобальной экономики.

Список литературы

1. Artificial Intelligence Act: Regulation of the European Parliament and of the Council on Artificial Intelligence, 2024 // EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0690> (дата обращения: 01.09.2025).
2. OECD Principles on Artificial Intelligence, 2019 // OECD. URL: <https://www.oecd.org/going-digital/ai/principles/> (дата обращения: 06.09.2025).
3. Закон Республики Беларусь «О защите персональных данных» от 7 мая 2021 г. № 80-З // Национальный правовой интернет-портал РБ. URL: <http://pravo.by/document/?guid=12551&p0=H12100080> (дата обращения: 01.09.2025).
4. Calo R. Artificial Intelligence Policy: A Primer and Roadmap // U.C. Davis Law Review. 2017. Vol. 51. P. 399–435.
5. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th Edition. Pearson, 2020. 1152 p.
6. Бегишев И. Р. Технология искусственного интеллекта: мировой опыт развития // Baikal Research Journal. 2020. Т. 11, № 3. С. 1. EDN RWRXO.
7. Wachter S., Mittelstadt B., Floridi L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation // International Data Privacy Law. 2017. Vol. 7, No. 2. P. 76–99.
8. Brkan M. Artificial Intelligence and the Law: European Approaches to Regulation and Liability // ERA Forum. 2021. Vol. 22. P. 1–19.
9. Хатсон, Д. Эволюция роли авторского права в эпоху произведений, созданных искусственным интеллектом // Journal of Digital Technologies and Law. 2024. Т. 2, № 4. С. 886–914. EDN SHDUEF.
10. Brynjolfsson E., McAfee A. The Business of Artificial Intelligence: What It Can – and Cannot – Do for Your Organization // Harvard Business Review. 2017. July–August. URL: <https://hbr.org/2017/07/the-business-of-artificial-intelligenc> (дата обращения: 01.09.2025).

Л. Е. Зотова,
студент,
Московский государственный университет
имени М. В. Ломоносова

Цифровая трансформация гражданского оборота

Аннотация. В последнее время большое влияние на упрощение операций и большую доступность количества действий, совершаемых субъектами гражданского права в целях свободного отчуждения или перехода материальных благ от одних лиц к другим в порядке, установленном законом, оказывает трансформация гражданского оборота в условиях технического прогресса в области цифровых технологий. Следствием этого стали фундаментальные изменения принципов работы органов власти, компаний, взаимодействия с клиентами, выходящими за рамки оцифровки существующих процессов, принятие цифрового мышления и использование возможностей технологий для внедрения инноваций, повышения эффективности и роста. В настоящей работе проводится анализ от теории гражданского оборота до его эволюции с помощью цифровизации, исследуются инструменты повышения эффективности и возможности обработки данных, методов работы юристов. Решение этих задач с меньшими затратами стало возможным благодаря цифровым технологиям, таким как большие данные, облачные вычисления, искусственный интеллект и блокчейн, расширившие возможности обработки и анализа данных, способствующие автоматизации, интеллектуальности и эффективности бизнес-процессов, комплексному преобразованию и модернизации традиционных бизнес-моделей, процессов обслуживания и систем управления.

Ключевые слова: цифровое мышление, право, цифровые технологии, облачные вычисления, искусственный интеллект, блокчейн, технический прогресс

L. E. Zotova,
student,
Moscow State University

Digital transformation of civil turnover

Abstract. Recently, the transformation of civil circulation in the context of technical progress in the field of digital technologies has had a significant impact on simplifying operations and making it easier for individuals to freely transfer or exchange material assets in accordance with the law. This has led to fundamental changes in the way governments, companies, and customers interact, going beyond the digitization of existing processes and embracing digital thinking and leveraging technology to drive innovation, efficiency, and growth. This work analyzes the theory

of civil circulation and its evolution through digitalization, exploring tools for improving efficiency and data processing capabilities, as well as legal practices.

Keywords: digital technologies, such as big data, have made it possible to solve these challenges at a lower cost

Введение. В результате глубоких социальных и технических изменений управление в эпоху цифровых технологий, как утверждается, станет доминирующей парадигмой государственного управления в XXI веке и будет опираться на фундаментальную цифровую трансформацию государственного управления. Цифровая трансформация описывает социотехнические изменения, связанные с применением цифровых технологий, и влечет за собой фундаментальные социально-экономические преобразования в отдельных людях, организациях и учреждениях государственного сектора, а также оказывает влияние на общество в целом. Цифровизация открывает огромные возможности для улучшения важнейших аспектов предоставления государственных услуг и работы административных органов всех размеров и на всех уровнях власти. Это позволяет внедрять инновационные технические решения во взаимодействие граждан и государства и повышает эффективность организации и удовлетворенность граждан. Цифровые решения повышают доступность и качество государственных услуг независимо от временных или пространственных ограничений, снижают административную нагрузку и повышают самостоятельность граждан.

Несмотря на эти многочисленные преимущества, процесс цифровой трансформации сопряжен с различными трудностями, такими как необходимость преобразования организационных структур и институциональной логики, значительные инвестиции в техническую инфраструктуру и обучение персонала для формирования новых компетенций. Следовательно, цифровая трансформация требует фундаментальных изменений во всей организационной экосистеме государственного управления и выходит за рамки технических вопросов, которые могут быть решены с помощью передачи ресурсов, таких как аутсорсинг информационно-технологических процессов и внедрение взаимодополняющих технических систем. Скорее, проблемы заключаются в наращивании организационного потенциала для облегчения адаптации цифровых технологий и в формировании цифрового мышления, чтобы использовать богатый потенциал на благо широкой общественности. Хотя считается, что эпоха жесткой экономики служит дополнительным стимулом для реформ, преодоление этих препятствий представляет собой особую проблему для небольших государственных учреждений на местном уровне (т.е., муниципалитеты). Им часто не хватает необходимых человеческих и финансовых ресурсов для освоения цифровой трансформации. Это определило актуальность данной работы.

Объектом настоящей работы являются общественные отношения, связанные с регулированием изменений гражданского оборота посредством внедрения цифровых технологий.

Предметом исследования выступают положения законодательства, регулирующие применение цифровых технологий в гражданском обороте между его участниками.

Изучая цифровую трансформацию в настоящей работе, мы будем выполнять цель, разрешим задачи, следуя нижеприведенному плану:

- рассмотреть понятие и характерные черты гражданского оборота;
- проанализировать сущность цифровой трансформации;
- раскрыть роль цифровизации в гражданских отношениях на современном этапе;
- проанализировать современные информационные (цифровые) технологии в области гражданского оборота, а также вопросы правового регулирования;
- выявить проблемы внедрения новых технологий в гражданско-правовой сфере.

При выполнении настоящего исследования мы будем применять формально-юридический метод, сравнительно-правой метод, а также анализ и обобщение.

Работа структурирована и состоит из введения, основного текста, заключения и списка использованных источников и литературы.

Основная часть. «Гражданский оборот» – это понятие традиционно широко используется не только в доктрине гражданского права, но и участниками при реализации прав и обязанностей в правоприменительной практике с использованием гражданского законодательства. Несмотря на различные подходы, попытки введения новых гипотез, привнести что-то нового в теорию проблематично по причине всесторонне изученного вопроса. Однако научные умы не сдаются и проводят исследования под новыми углами точки зрения и попытки осмыслить научную проблему. «При этом в условиях отсутствия законодательной дефиниции диапазон позиций ученых по поводу определения и содержания рассматриваемой категории весьма разнообразен» указывает Н.М. Сурнина [11. С. 157].

Российским научным сообществом на протяжении XIX–XXI веков приняты несколько основных подходов. С.Н. Братусь и Г.Ф. Шершеневич настаивают на первом подходе, доказывая видение гражданского оборота как «совокупность юридических фактов» [1. С. 70–71]. Сторонники же второго подхода (А.В. Дозорцев, О.А. Красавчиков и др.) предлагали понимать под гражданским оборотом «Совокупность отношений» [3. С. 55] – это второй взгляд на гражданский оборот, применяемый в общественных отношениях и теории права. Дальнейшее развитие доктринальной концепции позволило оформить те задачи, решение по которым преследуют в научной среде. Отсутствие единого мнения, как раз и есть тот катализатор, который и позволяет привносит новые взгляды и подходы к изучению данного вопроса, не позволяет возникнуть застою в научной среде.

Вследствие такого положения вещей среди ученых есть и третий подход, который также заслуживает не только внимания, но и подробного и всестороннего изучения, осмысления и создания инструментов для его претворения в практическую плоскость.

Интересен в этом подход Е.А. Суханова в определении понятия: «Гражданско-правовая наука разрабатывает и такие понятия и категории, которые не находят прямого законодательного воплощения, но приобретают важное теоретико-

познавательное и вместе с тем практическое значение. Примером этого является понятие гражданского или имущественного оборота – совокупности сделок всех его участников и возникающих на этой основе их обязательственных отношений, юридически оформляющих экономические отношения товарообмена» [7. С. 1208].

Возникший и бесконечно продолжающийся цивилистический оборот есть не что иное, как «оборот обязательственных прав и оборот вещей» [9. С. 60], по утверждению К.И. Скловского. Л.А. Чеговадзе дополняет это такими понятиями, как «...движение вещей, требований и прав» [13. С. 542]. «...Процесс перехода объекта гражданских прав, вследствие которого происходит постоянная или временная смена правообладателей» [4. С. 208] это и есть никогда не прекращающийся, как горный поток, процесс отношений в обществе, включает И.В. Евстафьева

Однако нельзя не заметить, что имеется и четвертый подход к данному вопросу, суть которого заключается в том, что учеными создано искусственное разделение, которое только претит полному и всестороннему изучению вопроса, уводит фокус внимания ученых мужей от разрешения действительных задач. О.А. Красавчиков отмечал, что в своих суждениях ученые «отправляются по существу от одного и того же положения, а именно – от оборотоспособности вещей, от участия тех или иных объектов в обороте» [5. С. 3]. С этим возможно согласиться, тем более что три подхода фактически дополняют друг друга и не содержат кардинальных отличий.

Есть и другой подход к данной проблематике, заключающийся в том, что необходимо поделить весь объем отношений и действий, включаемых в гражданский оборот на представление об изучаемом явлении как о некой совокупности (совокупность сделок, актов распоряжения, гражданских обязательственных и имущественных правоотношений, общественных отношений, юридических фактов, норм, случаев смены правообладателя, юридических фактов и правоотношений) и на процессе перехода (движении) субъективных прав, объектов гражданских прав, объектов гражданских прав и субъективных прав). Об этом в своих исследованиях отмечает Ю.В. Виниченко [14. С. 195]. Но все эти теории настолько неопределенны, что и не заслуживают дальнейшего исследования и внимания.

«Гражданский оборот – совокупность всех действий, совершаемых субъектами гражданского права в целях свободного отчуждения или перехода материальных благ от одних лиц к другим в порядке, установленном законом» – именно так советские ученые и юристы на практике понимали и применяли данное понятие.

В настоящей российской действительности «гражданский оборот» определяется в пункте 1 статьи 2 ГК РФ «участники гражданского оборота», в пункте 2 статьи 15 – «обычные условия гражданского оборота», в статьях 1272, 1275, 1302 – «введение (объектов) в гражданский оборот», но мы не сможем найти нормы, содержащей нахождение квинтэссенции.

Необходимо отметить то обстоятельство, что между участниками экономического оборота, использующих нормы гражданского права с целью получе-

ния доступа к товарно–денежным отношениям, услугам, информации реализуются имущественные права.

В научном сообществе под гражданским оборотом принимается оборот в экономической деятельности, как части общества и общественных отношений для насыщения всего объема имущественных потребностей ее членов распределения между ними объектов таких отношений, соотнося потребительской стоимости.

Система гражданского оборота включает в себя не только субъекты, для удовлетворения имеющихся нужд согласно абзацу 2 п. 1 ст. 2 ГК РФ, но и объекты, за их счет восполняются потребности субъектов.

Участникам же данного отношения необходимо назвать граждан, юридических лиц, публично–правовые образования: Российская Федерация, субъекты РФ, муниципальные образования.

Объектами гражданского оборота являются объекты гражданских прав, обладающие следующими свойствами формальной определенностью, которая предполагает вовлечение в оборот только тех благ, виды которых прямо обозначены в законе, возможностью отчуждения, присутствием потребительской ценности. Об этом указывает статья 128 ГК РФ. Объекты, не поименованные законом как объекты гражданских прав, таковыми не являются.

На современном этапе развития экономики более невозможно существование традиционного предприятия, не затронутого цифровизацией. «Оцифровка» бизнеса является необходимым условием сохранения его конкурентоспособности и выживания на рынке. При этом цифровизации обычно подвергаются самые разные аспекты бизнеса, начиная от конкретных продуктов и заканчивая бизнес-моделью в целом.

Цифровая трансформация, на наш взгляд, является больше практическим термином, обозначившим сложившееся на практике явление, нежели теоретическим ориентиром, под который необходимо подстраивать практику.

Анализируя подходы крупнейших игроков на различных рынках к определению сущности цифровой трансформации можно выделить ряд ключевых факторов, выделяемых ими в качестве ключевых аспектов цифровой трансформации:

- цифровые технологии как базовые элементы;
- результаты проведения цифровой трансформации;
- сферы преобразований (бизнес-модель, операционная деятельность и др.) [8. С. 568–579].

Авторы дают следующее определение цифровой трансформации: процесс преобразования существующей или формирование новой бизнес-модели организации посредством применения цифровых технологий, где центральная роль отведена эффективному управлению данными, сопровождающееся изменениями бизнес-процессов и ростом конкурентоспособности и эффективности организации [8. С. 568–579].

Иные авторы предлагают определять цифровую трансформацию как процесс кардинального изменения бизнес-модели предприятия и ее элементов, включая процесс создания и доставки ценности клиенту посредством реализа-

ции проектов с использованием цифровых технологий, в основе которых лежит эффективное управление информацией [12. С. 222–229].

На мой взгляд, более верным и точным кажется определение, данное группой авторов, потому что цифровая трансформация обязательно должна сопровождаться ростом конкурентоспособности организации, иначе смысл цифровой трансформации будет утерян, так как в целом проведение цифровизации бизнеса нацелено именно на повышение эффективности и инвестиционной привлекательности ее бизнес-модели.

Однако считаю необходимым уточнить, что еще одним обязательным элементом цифровой трансформации является сокращение издержек предприятия, например, путем сокращения персонала, чьи функции можно автоматизировать, внедрения более быстрых инструментов обработки данных, использования облачных серверов и т.д. Сокращение издержек находится в обратной зависимости с увеличением прибыли предприятия. Именно указанный фактор является ключевым при определении успешности проведения цифровой трансформации.

Начиная со второй половины XIX века взаимоотношения между членами общества претерпевают постоянные изменения, основанными на гражданских правоотношениях. Развитие науки, техники на основе новых технологий ускорили переход гражданских правоотношений к новым цифровым технологиям, к модернизации прав.

Права, изначально оговоренные и исполнявшиеся как обычаи, с развитием общественных связей были оформлены в законодательные нормы, упорядочили гражданские правоотношения, переходящие на новую стадию цифровой модели развития общества.

После того, как мы разобрали в предыдущем разделе работы сущность цифровой трансформации, перейдем к цифровизации, а также рассмотрим ряд отличий от цифровой трансформации.

Цифровизация права своей целью ставит внедрение и развитие новых цифровых технологий в построение деловых отношений, направлена на автоматизацию и упрощение деятельности участников гражданского оборота. В данном случае происходит создание специальных компьютерных программ и программных комплексов, использующих не только цифровые коды, но искусственный интеллект.

Цифровая трансформация же является более глубоким процессом модернизации, основанным не только на создании и введении в использование новых механизмов и технологий, но проводит большую модернизацию процесса ведения дел, принятия решений, создания новых принципов взаимодействия между участниками правоотношений, привносит новые требования к культуре взаимоотношений для получения новых инновационных решений ведения дел.

Цифровые права в современном российском обществе также начали занимать одну из преобладающих ролей в стремительно изменяющемся и развивающемся конкурентном рынке оказания правовых услуг в информационную эпоху.

В научной среде сложилось устойчивое мнение о том, что именно переход к установлению правовых отношений посредством использования цифровых записей в качестве подтверждающего источника права, пришло на смену подчиненности юридическим фактам, что и является по своей сущности цифровизацией. С данным утверждением можно согласиться по причине того, что в результате оцифровки и внесения в специальные программы и базы данных ранее возникшие права на основании заключенных сделок, решений судов или актов уполномоченных органов власти, стали храниться в виде цифровых записей, а подтверждением права стала являться выписка из соответствующего реестра данных. Из этого следует, что их необходимо соотносить в качестве самостоятельных объектов в гражданских правах.

В то же время вещные права возникают и фиксируются в цифровом формате посредством внесения их в специализированные цифровые реестры, где они могут храниться не только в виде цифровых записей, но и подкрепляться оцифрованными документами о совершении сделок, на основании которых они и возникли. Личные неимущественные права находятся вне оборота и не могут быть цифровыми, что прямо запрещено законом, потому что цифровизация прав создана для ускорения и облегчения их оборота.

Рассматривая в настоящей работе, деятельность юридических фирм хочется отметить, что они, как участники гражданских правоотношений в полной мере приносят в свою деятельность результаты технического прогресса, в том числе, и плоды цифровизации. Тем самым они привлекают в свою деятельность юристов, которые не только обладают познаниями в области юриспруденции, но обладающих познаниями в области пользования компьютерными технологиями и имеющих опыт работы со специализированными цифровыми комплексами. Это придает толчок в усилении конкурентоспособности на рынке оказания юридических услуг по причине того, что юридическую помощь клиенты желают получить в кратчайшие сжатые сроки, с минимальными материальными и эмоциональными затратами.

Чтобы следовать требованиям клиентов приходится полностью перестраивать свою работу, а расширение цифровых возможностей – эффективный способ достижения этой цели. Этот прогресс в цифровом развитии включает в себя цифровое архивирование данных в делах юристов, цифровую проверку поступающих документов, их систематизацию, анализ, хранение в цифровом пространстве, организацию своей работы, графика занятости и в делах, встречах с клиентами, что позволяет управлять этими процессами и сокращая при этом время на администрирование. Использование интеллектуальных функций в данной работе у юридических фирм, как следствием этого происходит и снижение материальных затрат и человеко-часов на юридическую работу в целом.

Огромным подспорьем в юридической работе являются инструменты, с помощью которых происходит управление делами, платформами, проектами. Объединенная команда юристов может слаженно работать, при этом распределение поручений и функций между членами команды, корректировка, прогнозирование результата происходит в автоматизированном порядке. В случае необходимости члены команды могут осуществлять работу удаленно (дистан-

ционно), могут привлекать в случае необходимости новых членов или специалистов в кратчайшие сроки. Все это направлено только на достижение скорейшего результата по разрешению кейса.

На это же нацелены и созданные цифровые технологии, с помощью которых клиенты получают онлайн-консультации. Консультирующим специалистом в режиме «24/7» со стороны юридической фирмы может выступать искусственный интеллект. Не во всех возникающих ситуациях он может справиться без участия человека-юриста, и поэтому в работе таких цифровых платформ предусматривается возможность перевода клиента на непосредственное участие живого юриста, которого она выбирает на основании анализа данных, полученных в процессе общения с клиентом.

Одним из результатов таких онлайн-консультаций юридические фирмы предлагают клиентам заключать смарт-контракты для разрешения дальнейшей работы над делом. Клиенту в автоматическом и защищенном цифровом пространстве (безопасном от вторжения злоумышленников) посредством одобрения заключаемой сделки подписать смарт-контракт нажатием на устройстве кнопки согласен. После чего он исполняется автоматически на протяжении всего периода его действия до полного исполнения сторонами.

Смарт-контракты находят свое применение, с одобрения Центрального Банка РФ, не только в юридической сфере, но и в иных сферах гражданских правоотношений. Одним из примеров можно рассмотреть договоры страхования, заключаемые с таким инструментом. Это дает получателю страховой выплаты получить ее, даже без посещения офиса страховой компании, реализуя алгоритмы данного цифрового инструмента.

В настоящее время, в контексте продолжающегося глубокого влияния Интернета на все аспекты человеческого общества и жизни, продолжает набирать обороты новая волна технологий, таких как большие данные, облачные вычисления, искусственный интеллект, блокчейн и Интернет вещей, которые, как ожидается, изменят наше общество и экономику. Все это, несомненно, предоставляет беспрецедентные возможности для инноваций и эволюции права и юридической индустрии.

Федеральный закон от 18.03.2019 №34-ФЗ «О внесении изменений в части 1, 2 и статью 1124 части 3 ГК РФ» зафиксировал под цифровым правом «заключение и исполнение письменной формы сделки с применением технических и/иных информационных программ (комплексов) – информационно-коммуникационных комплексов (далее – ИКТ) при наступлении обстоятельств без дополнительного извещения, привлечения, подтверждения волеизъявления к совершению и исполнению такой сделки» [1]. В связи с особенностями такой сделки она относится к сделкам об оказании услуг по предоставлению информации. Вследствие этого повсеместно принято понимание того, что информационно-коммуникационные комплексы при использовании их операторами необходимо считать создателями права по причине того, что они регулируют взаимодействие между участниками.

Федеральный закон от 02.08.2019 №259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные

законодательные акты РФ» [18] конкретизирует условия, участников, механизмы взаимодействия, порядок инвестирования при использовании инвестиционных платформ, регулирует их условия возникновения, обращение между участниками.

Непубличные акционерные общества при создании капитала используют электронные активы и права требования, условия и порядок выпуска, учета, обращения которых изложен положениями Федерального закона от 31.07.2020 №259-ФЗ «О цифровых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [18]. В нем законодателем прописан механизм и порядок взаимодействия сторон при обороте цифровых валют в нашем государстве. Федеральный закон от 31.07.2020 №258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [19] принят законодателем в целях выделения некоторых участников и отдельных видов экономической деятельности, направлен на вовлечение большего числа участников, чем развивается конкуренция, качество и ассортимент услуг и товаров.

Новые законодательные акты дополнили пробелы и недостатки Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг» [20]. Президент Российской Федерации, издав Указ Президента Российской Федерации от 10.10.2019 № 4907 [21], создал векторы и задачи, изложенные в Национальной стратегии развития искусственного интеллекта на период до 2030 г. в РФ.

Полагаю, что последствиями принятия и повсеместного использования цифровых технологий не будут появление гражданских взаимоотношений. Поэтому нельзя утверждать, что будут создаваться личности на основе оцифровки данных, использования виртуальных технологий. Все это проистекает из норм закона о цифровом авторском праве, устанавливающим возникновение их частичных элементов, реализуемых электронными техническими средствами. Признается техническая возможность воссоздания и воспроизведения их на специальном физическом цифровом носителе, в том числе цифровые финансовые активы могут быть созданы и сохранены посредством создания цифровых записей. Все эти новые цифровые инструменты нужно воспринимать только лишь, как часть сферы оказания информационных услуг в качестве товара.

Рассмотрим проблемы и трудности, с которыми сталкиваются представители гражданско-правовой сферы в области технологических исследований и разработок, и внедрения достижений. Например, отсутствие исследований приводит к слепому внедрению технологий, при внедрении технологий трудно получить базовую технологию, освоение капиталовложений низкое, услуги технологических посредников слабые, а механизм подготовки талантов несовершенен.

В процессе внедрения технологий организации часто быстро внедряют техническое оборудование в производство без проведения достаточных исследований, что приводит к повторному внедрению и пустой трате ресурсов. Кроме того, внедрение технологий в основном основано на зрелых или стандартизированных технологиях, в которых отсутствуют базовые технологии и инновационные технологии.

Усвоение внедренной технологии и вторичные инновации являются важными условиями успешного внедрения технологии.

Технологические посредники играют важную роль во внедрении технологий, но в России существуют проблемы с услугами технологических посредников, такие как отсутствие стандартизированной правовой системы, недостаточное понимание организаций, внедряющих технологии, и слабая поддержка со стороны финансовых учреждений.

Несовершенный механизм подготовки кадров и недостаточный уровень образования повлияли на конкурентоспособность учреждений и организаций в области внедрения технологий, исследований и разработок.

Отсюда проистекает и главная проблема – отсутствие единого цифрового подхода к формированию нормотворчества в цифре.

В РФ проводятся социальные и технические изменения управления, что связано со скачком в развитии цифровых технологий. Началась трансформация с национального проекта «Цифровая экономика», проводившегося с октября 2018 г. по декабрь 2024 г. Его продолжением стал национальный проект «Экономика данных и цифровая трансформация государства» на период с 2024–2030 гг., в том числе начатые проекты и направления в рамках "Цифровой экономики", продолжили развитие и продолжение. Это затронуло и когнитивные технологии, такие, как ИИ и Big Data.

По данным Министерства цифрового развития, связи и массовых коммуникаций (Минцифры) на февраль 2024 г. 86,4% домовладений подключены к интернету, 93,3% населенных пунктов с населением более 2000 жителей покрыты сетями LTE, благодаря построенным 4733 базовых станций, 5G-технологий. Доля социально значимых объектов, имеющих широкополосный доступ в интернет в 2022 г., составила 100% (118 тыс.).

Примером цифровой трансформации в 2024 г. более 70% крупных российских предприятий уже используют цифровые решения технологии Индустрии 4.0, интернет вещей (IoT), искусственный интеллект (AI) и автоматизированные системы управления помогают снизить издержки, улучшить качество продукции, повысит эффективность производства.

Заключение. Влияние цифровизации на юридическую отрасль в основном заключается в повышении эффективности, продвижении инноваций в юридических услугах, улучшении сбора юридических данных и изменении методов работы юристов. Повышение эффективности работы является особенно важным аспектом. Применяемые в юридической работе цифровые технологии юристам, как участникам гражданских правоотношений, предоставили быстрый и упрощенный доступ к делам и документам, хранящимся в облачных данных. Это позволяет к тому же производить их обработку посредством встроенных поисковых систем и на сторонних юридических ресурсах. Аналогично происходит работа с клиентами и коллегами с помощью различных инструментов онлайн-связи, чем существенно сокращая время работы по каждому из проектов.

Распространение цифровизации не только во всей экономике Российской Федерации, но отдельно в юридической открыло не только много возможно-

стей, но позволило вскрыть отдельные проблемы, разрешение которых происходит в процессе непосредственной работы. Благодаря цифровизации для клиентов произошло не только расширение спектра юридических услуг, но и создало добросовестную конкуренцию по причине открытости участников, предлагающих услуги. Следствием этого юридические фирмы в своей деятельности повышают уровень своих стандартов и качество услуг, проводят обучение и повышение профессиональной квалификации своих сотрудников, чтобы они имели практические навыки использования новых цифровых технологий. Привлечение в совместную работу над делами и проектами привело к интеграции юридической отрасли с другими участниками экономической деятельности в иных отраслях рынка.

Проблемами цифровизации стали возможные нарушения конфиденциальности данных и кибербезопасность. Юристы должны знать об этих проблемах и принимать меры для защиты данных и безопасности в сети.

С развитием Интернета и новых технологий, таких как искусственный интеллект и блокчейн, взаимоотношения между правом и технологиями претерпели серьезные изменения. Юристы и судьи, а также политики и сотрудники правоохранительных органов все чаще полагаются на цифровую информацию и программное обеспечение (интеллектуальное или иное) в своей повседневной работе.

Список литературы

1. Братусь С.Н. О понятии гражданского оборота в советском гражданском праве: докл. На заседании Сектора гражд. права Всесоюз. ин-та юрид. наук // Советское государство и право. 1949. №11. – С. 70–71.
2. Гражданский оборот. Большая российская энциклопедия. URL: bigenc.ru/c/grazhdanskii-оборот-846429?ysclid=maqc9qt4p9875760979 (дата обращения: 15.08.2025).
3. Дозорцев А.В. Объекты права государственной социалистической собственности и их классификация // Советское государство и право. 1949. №1. С. 55.
4. Евстафьева И.В. Правовое регулирование международного оборота имущественных авторских прав: дис. канд. Юрид. Наук. Саратов, 2012. С. 208
5. Красавчиков О.А. Советский гражданский оборот (понятие и основные звенья) // Вопросы гражданского, трудового права и гражданского процесса: ученые записки. СЮИ. 1957. Т. 5. С. 3
6. М. Сазонова. Право в цифре: какие разработки есть уже сейчас? URL: <https://www.garant.ru/article/1554367/#sdfootnote1anc> (дата обращения: 15.08.2025)
7. Российское гражданское право: в 2 т. / В.В. Витрянский, В.С. Ем, Н.В., Козлова и др.; отв. Ред. Е.А. Суханов, 2-е изд., стереотип. М.: Статут, 2011. Т. 2: Обязательственное право. С. 1208.
8. Силакова Л.В., Андроник А, Киселев А.Д. Сущность цифровой трансформации: понятие и процесс // Baikal Research Journal. 2024. №2. С. 568–579.

9. Скловский К.И. Механизм перехода права и последствия цессии // Хозяйство и право. 202. № 2. С. 60.
10. Судьба в руках машины: на пути к роботу-судье. URL: <https://legalacademy.ru/sphere/post/sudba-v-rukah-mashiny-na-puti-k-robotu-sude>
11. Сурнина Н.М. Информационное общество и проблемы прикладной информатики: / Н.М. Сурнина; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. Екатеринбург: Изд-во УрГЭУ. 2020. С. 157.
12. Темников А.О. Современные подходы к определению термина "цифровая трансформация" // Гуманитарные, социально-экономические и общественные науки. 2023. №3. С. 222 – 229.
13. Чеговадзе Л.А. Структура и состояние гражданского правоотношения. М.: Статут, 2004. С. 542.
14. Виниченко Ю.В. «Гражданский оборот»: подходы к пониманию и их трактовка в российской цивилистике // Бизнес. Образование. Право. Вестник Волгоградского института бизнеса. 2016. № 1(34). С. 195.
15. Морхат П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: автореф. дис. д-ра юрид. наук. М., 2018. С. 45.
16. ЦСР принял участие в работе сессии по цифровой трансформации регионов. URL: <https://www.csr.ru/ru/news/tssr-prinyal-uchastie-v-rabote-sessii-po-tsifrovoy-transformatsii-regionov-rossii/>. (Дата обращения: 15.08.2025).
17. Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации». Собрание законодательства РФ. 2019. № 31. Ст. 4418.
18. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Собрание законодательства РФ. 2020. № 31 (ч. I), Ст. 5018
19. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых в Российской Федерации». Собрание законодательства РФ. 2020. № 31 (ч. I). Ст. 5017.
20. Федеральный закон от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг». Собрание законодательства РФ. 1996. № 17. Ст. 1918.
21. Указ Президента Российской Федерации от 10.10.2019 № 4907. Собрание законодательства РФ. 2019. № 41. Ст. 5700.

Т. В. Иванова,

магистрант,

Московский государственный университет

имени М. В. Ломоносова

**Автоматизация юридической экспертизы
локальных нормативных актов организации**

Аннотация. Цель исследования – разработка теоретических основ и практических подходов к созданию системы автоматизированной экспертизы локальных нормативных актов организации. В статье обосновывается актуальность автоматизации данной процедуры для минимизации рисков и повышения эффективности нормотворчества. На основе методологии проектирования юридических систем предлагаются этапы внедрения решения: формализация требований, унификация документов и разработка программного комплекса. Определены ключевые функции системы, включая проверку на соответствие шаблону, внутренним справочникам и законодательству. Делается вывод, что система выступает инструментом поддержки эксперта, а не его заменой, и обладает значительным потенциалом для тиражирования.

Ключевые слова: автоматизация, локальные нормативные акты, юридическая экспертиза, правовые технологии, цифровые технологии, цифровизация

T. V. Ivanova,

Master's student,

Lomonosov Moscow State University

Automation of legal expertise of local regulatory acts of the organization

Abstract. The purpose of the study is to develop theoretical foundations and practical approaches to creating an automated system for reviewing local regulations of an organization. The article substantiates the relevance of automating this procedure in order to minimize risks and increase the efficiency of rule-making. Based on the methodology of designing legal systems, the article proposes the following stages for implementing the solution: formalization of requirements, unification of documents, and development of a software package. The key functions of the system are identified, including verification for compliance with the template, internal reference books, and legislation. It is concluded that the system acts as a support tool for an expert, rather than a substitute for it, and has significant potential for replication.

Keywords: automation, local regulations, legal expertise, legal technologies, digital technologies, digitalization

Основная часть. Обработка юридических текстов – одно из самых актуальных направлений внедрения технологий автоматизации работы в юридиче-

скую деятельность. В данной работе предлагается рассмотреть один из возможных аспектов автоматизации юридической деятельности – автоматизацию проведения экспертизы локальных нормативных актов организации, сформировать предложение по разработке данной системы, функциональные требования к ней.

Юридическая экспертиза проводится в рамках согласования локальных нормативных актов перед утверждением в большинстве существующих организаций. Данная экспертиза позволяет внести изменения в проект документа, устранить возможные риски, например несоответствия законодательству в процессах организации. Экспертиза проводится специалистом на соответствие определенным требованиям. Данные требования могут быть преобразованы в правила для информационной системы, которая, в свою очередь, может стать инструментом в поддержке принятия решений при осуществлении специалистом данной экспертизы.

Основная часть. В рамках данной статьи предлагаем руководствоваться следующим определением локального нормативного акта (далее – ЛНА) – официальный документ, принятый (изданный) в установленном порядке компетентным органом управления или должностным лицом, устанавливающий обязательные правила поведения в органе (организации) [1].

Функции ЛНА:

- Функция правового регулирования.
- Конкретизирующая.
- Повышение установленных государственных гарантий.
- Восполнение пробелов.
- Управленческая.
- Организационная.
- Производственная.
- Образовательная.
- Иные [2].

Таким образом, ЛНА занимают значительную роль в регулировании деятельности организаций, качество их подготовки влияет на эффективность процессов организации.

Согласно мнению М.Ю. Осипова, процесс проектирования автоматизированных систем управления для юридической деятельности включает в себя несколько этапов:

- осуществление реинжиниринга юридической деятельности с целью выделения в ней ключевых моментов;
- определение того, какие ключевые моменты юридической деятельности подлежат автоматизации;
- определение платформы для осуществления автоматизации юридической деятельности;
- создание автоматизированных систем управления юридической деятельностью [3].

Применительно к созданию автоматизированной системы, осуществляющей экспертизу локальных нормативных актов, нами предлагаются следующие этапы работ:

Определение требований, подлежащих проверке. Формирование технического задания к разрабатываемой системе: в рамках данного этапа должны быть определены правила, по которым осуществляется проверка, интерфейс, платформа.

При необходимости – корректировка существующих правил составления ЛНА, унификация шаблонов, формулировок, создание справочников.

Создание автоматизированной системы: разработка, согласование с заказчиком, тестирование, введение в эксплуатацию.

Примеры возможных проверок:

- Соответствие шаблону – заполнение обязательных полей, соответствие оформлению (шрифт, стиль и иные аспекты оформления).
- Соответствие справочникам (наименования организаций, структурных подразделений, процессов и т.д.).
- Наличие противоречий и дублирований внутри текста, с иными ЛНА и правовыми актами.

Актуальность упоминаемых по тексту документа правовых актов.

Для внедрения данной системы юридические тексты должны быть унифицированы, содержать шаблонные поля для заполнения. Унификация документов также влияет на их понятность и доступность для читателей, что также оказывает положительное влияние на деятельность организации. Система должна обладать удобным и понятным интерфейсом, также должны быть понятны способы передачи разработчикам обратной связи от пользования системой с целью ее улучшения.

Возможные проблемы и риски в рамках работы с системой:

Сложности в анализе неструктурированных данных;

Защита внутренней информации организации при использовании облачных сервисов.

Необходимо отметить, что предлагаемый инструмент не заменяет специалиста, но является инструментом, содействующим в подготовке ЛНА, соответствующего установленным законом и организацией требованиям. Потенциальные пользователи данного инструмента: лица, осуществляющие подготовку проекта ЛНА, а также лица, осуществляющие экспертизу ЛНА. Потенциальные прогнозируемые эффекты: сокращение трудозатрат на подготовку ЛНА, его экспертизу, повышение качество ЛНА, сокращение времени выпуска ЛНА. Косвенным эффектом от внедрения данной технологии, на наш взгляд, может также являться повышение удовлетворенности и вовлеченности работников данной организации.

Также стоит отметить, что на рынке информационных сервисов для юристов на данный момент отсутствует система, функционал которой позволяет автоматизировать юридическую экспертизу при согласовании ЛНА, в связи с чем мы предлагаем организациям, осуществляющим разработку данных информационных сервисов обратить внимание на данное актуальное направление развития юридических сервисов и предложить потребителям рынка описываемый продукт.

Предлагаемая система имеет потенциал для тиражирования, в том числе для использования в рамках подготовки государственных и муниципальных правовых актов.

Заключение. Таким образом, технологии автоматизации работы с юридическими документами позволяют оптимизировать работу специалистов, сократить их трудозатраты, повысить их производительность труда, сократить количество возможных ошибок, возникших в силу человеческого фактора.

Список литературы

1. Методические рекомендации по определению нормативности правовых актов субъектов Российской Федерации и муниципальных правовых актов в целях ведения федерального регистра нормативных правовых актов субъектов Российской Федерации, Федерального регистра муниципальных нормативных правовых актов и регистров муниципальных нормативных правовых актов субъектов Российской Федерации (утв. Минюстом России) // СПС Консультант Плюс.
2. Шайхутдинова Н.П. Функции локальных нормативных актов трудового права // Вестник удмуртского университета. 2014. №3. С. 209–212.
3. Осипов М. Ю. К вопросу об особенностях проектирования автоматизированных систем управления для юридической деятельности // Цифровые технологии и право. Сборник научных трудов III Международной научно-практической конференции. Казань: 2024. С. 200–206.

М. М. Карев,

студент,

Финансовый университет при Правительстве Российской Федерации,

Д. С. Яковлева,

студент,

Финансовый университет при Правительстве Российской Федерации

**Legaltech: от автоматизации процессов к новой модели
юридической деятельности**

Аннотация. В статье рассматривается феномен LegalTech как ключевое направление цифровой трансформации юридической сферы. Цель исследования – проанализировать особенности развития LegalTech в России и за рубежом, выявить его преимущества, проблемы и перспективы внедрения в правоприменительную и образовательную практику. Отмечается, что LegalTech способствует автоматизации процессов, внедрению искусственного интеллекта, развитию онлайн-разрешения споров, смарт-контрактов и аналитических технологий, что повышает эффективность юридических услуг и доступ к правосудию. Особое внимание уделено вопросам нормативно-правового регулирования, информационной безопасности, взаимодействия государственных и частных структур, а также роли LegalTech в юридическом образовании. Сделан вывод, что успешное развитие отрасли возможно при комплексном подходе, включающем совершенствование законодательства, инвестиции в отечественные технологии и подготовку специалистов, способных работать в условиях цифровой экономики.

Ключевые слова: цифровые технологии, цифровая экономика, LegalTech, искусственный интеллект, автоматизация, смарт-контракт, предиктивная аналитика, информационная безопасность

M. M. Karev,

Student,

Financial University under the Government of the Russian Federation,

D. S. Yakovleva,

Student,

Financial University under the Government of the Russian Federation

Legaltech: from process automation to a new model of legal practice

Abstract. The article examines the phenomenon of LegalTech as a key direction in the digital transformation of the legal sector. The aim of the study is to analyze the features of LegalTech development in Russia and abroad, to identify its advantages, challenges, and prospects for implementation in law enforcement and educational prac-

tice. It is noted that LegalTech contributes to the automation of routine processes, the integration of artificial intelligence, the development of online dispute resolution, smart contracts, and analytical technologies, which enhance the efficiency of legal services and access to justice. Special attention is paid to issues of regulatory legal framework, information security, interaction between public and private entities, as well as the role of LegalTech in legal education. The conclusion is drawn that successful industry development is possible only through a comprehensive approach, including the improvement of legislation, investments in domestic technologies, and the training of specialists capable of operating in the conditions of the digital economy.

Keywords: digital technologies, digital economy, LegalTech, artificial intelligence, automation, smart contract, predictive analytics, information security

Введение. Развитие LegalTech представляет собой ключевой элемент цифровой трансформации юридической деятельности в России, направленной на повышение эффективности и доступности правовых услуг. В соответствии с Указом Президента РФ от 7 мая 2024 г. № 309 национальные цели до 2030 и 2036 годов предусматривают достижение технологического лидерства и цифровой зрелости в управлении, экономике и социальной сфере, что требует перехода от автоматизации отдельных процессов к формированию новой модели юридической практики, основанной на инновационных цифровых технологиях и обеспечивающей устойчивое развитие и безопасность государства. Эта трансформация LegalTech отвечает стратегическим задачам устойчивого экономического и социального развития страны.

Основная часть. Трансформация современного общества и информатизация процессов взаимодействия людей влияют на все сферы жизнедеятельности. Информация и цифровой мир становятся неотъемлемой частью реальности, которая под их воздействием стремительно трансформируется. Границы между физическим и виртуальным стираются, формируя пространство, где люди взаимодействуют, работают и развлекаются. Этот процесс обусловлен развитием технологий, таких как искусственный интеллект (далее – ИИ), блокчейн и интернет.

Процессы информатизации социальных процессов оказывают значительное влияние и на юридическую сферу, которая играет ключевую роль в регулировании общественных отношений. Современные технологии позволяют ускорить обработку правовой информации и автоматизировать многие процессы, что способствует более эффективному функционированию правовой системы, улучшению взаимодействия между гражданами, государственными органами. Цифровая трансформация в юридической отрасли успешно изменила и модернизировала традиционную юридическую практику. Важную роль в развитии данного явления сыграли юридические технологии, или так называемые Legal technologies, LegalTech, которые применяются современными юристами и адвокатами в профессиональной деятельности.

Современные представления о LegalTech в России сегодня находятся на стадии активного обсуждения в профессиональном юридическом сообществе, в юридической науке и в системе юридического образования. Рынок Legal

technologies, или LegalTech–решений для юриспруденции за сравнительно небольшой период времени стал одним из ключевых перспективных направлений. Заинтересованы в его развитии как юридическое сообщество, так и бизнес, ориентированный на оптимизацию всех бизнес-процессов и повышение эффективности их юридического сопровождения.

В юридическом сообществе не сформировано единого понятия о LegalTech. Анализ существующей литературы позволяет говорить о нескольких возможных подходах к пониманию данного явления.

По мнению доцента информационного права и цифровой информатики Московского государственного юридического университета (далее – МГЮА) Н.В. Пальяновой, «LegalTech – это отрасль бизнеса, специализирующаяся на информационно-технологическом обслуживании профессиональной юридической деятельности, а с конца 2000-х гг. – на предоставлении потребителям юридических услуг с использованием информационных технологий» [6].

Традиционно сферу LegalTech рассматривают в широком и узком смыслах. В широком значении LegalTech понимается как система информационных, в том числе цифровых технологий по разработке, внедрению и использованию, в процессе оказания юридических услуг, а также в процессе реализации юридического образования. То есть «LegalTech – элемент цифровой экономики, способствующий реализации национальных стратегических целей и задач, программ развития» [14]. В узком смысле данная отрасль представляется как сфера информационно-технологического обслуживания профессиональной юридической деятельности. Как отмечают М.А. Рожкова и О.В. Исаева, «LegalTech – сервисы на базе информационных систем, платформы, программы, продукты и инструменты, специально созданные для юристов с целью повышения эффективности оказания юридических услуг или юридического сопровождения бизнеса» [16]. Данный подход близок к зарубежному пониманию LegalTech: технологии, улучшающие предоставление юридических услуг всем участникам правоприменительного процесса [20]. В международной практике под этим также понимают цифровое сопровождение юридической деятельности – от онлайн-платформ для связи с юристами до программных решений, позволяющих клиентам обходиться без их помощи.

В современной юридической литературе LegalTech также рассматривается как способ, метод решения юридических задач, основанный на интеграции цифровых технологий в юридическую практику. Этот подход трансформирует традиционные процессы, делая их более эффективными, доступными и экономически выгодными. Как отмечает профессор Оксфордского интернет-института Ричард Сасскинд в своей работе «Tomorrow's Lawyers», LegalTech представляет собой системный метод автоматизации, стандартизации и цифровизации юридической деятельности [21].

В процессе цифровизации общества огромную роль играет ИИ, с помощью которого представление некоторых явлений уже невозможно. Юридическая сфера также попала под влияние ИИ-технологий. Основными целями внедрения ИИ являются ускорение сложных процессов качественного анализа информации и автоматизация рутинных задач. Можно выделить подход пони-

мания LegalTech как способ интеграции права с ИИ-технологиями с целью повышения продуктивности современного юриста или адвоката.

LegalTech также является ключевым компонентом современного юридического образования. Внедрение цифровых технологий в обучение позволяет готовить юристов, способных эффективно работать в условиях цифровой трансформации правовой сферы. Ярким примером использования LegalTech в образовательной деятельности является Юридический факультет Оксфордского университета. Университет одним из первых разработал специализированный курс, направленный на формирование у будущих юристов компетенций в сфере LegalTech [25]. Но необходимо отметить некоторые проблемы, с которыми встречается современное юридическое преподавание. Фрэнсин Райан в своей работе «Rage against the machine? Incorporating legal tech into legal education» считает, что LegalTech – это не просто инструмент, на основе которого будет трансформироваться и изменяться правовая сфера, а это новый подход в изучении юриспруденции, требующий переосмысления учебных программ и решения вопросов этики и философии [24].

Анализируя существующие подходы к определению сферы LegalTech, можно выявить ее характерные признаки. Как отмечает А.В. Минбалеев, к ключевым отличительным чертам LegalTech относятся:

1. Специальная сфера применения технологий – правовая. Ее уникальность заключается в способности адаптировать цифровые инновации для решения конкретных задач юридического характера, создавая симбиоз технологических возможностей и правовых знаний.

2. Оптимизация юридических процессов. Современные технологические решения кардинально изменяют характер и специфику юридической работы: компьютеризация стандартных задач, что позволяет специалистам сосредоточиться на более сложных; создание нового формата взаимодействия между юристами и клиентами.

3. Особые объекты правоотношений. С развитием LegalTech появляются новые категории правоотношений, связанные с использованием алгоритмов ИИ в правоприменительной практике, обработкой больших массивов юридически значимых данных, применением смарт-контрактов и блокчейн-технологий.

4. Особая роль в юридической деятельности. В данном случае LegalTech рассматривается как инструментарий с использованием различных информационных технологий, продуктов, применяемый для решения юридических задач.

5. Особые средства реализации. Данный признак заключается в реализации технологий в юридической сфере. Так, на основе LegalTech реализованы программные продукты для автоматизированного анализа правовой информации, платформы для оказания дистанционных юридических услуг и системы поиска нормативно-правовых актов [6].

Четкая нормативно-правовая регламентация использования LegalTech-решений в российском законодательстве не установлена. Но в юридической науке принято понимать разрабатываемые юридические технологии и сервисы в качестве информационных систем. В соответствии со статьей 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологи-

ях и о защите информации» (далее – Закон об информации) информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. Как указывает доктор юридических наук Института законодательства и сравнительного правоведения при Правительстве Российской Федерации М.А. Рожкова, «в соответствии с указанной нормой в качестве информационных систем могут быть квалифицированы любые системы, информация в которых структурирована в базах данных и обеспечена обработкой информационных технологий и технических средств» [15]. Также М.А. Рожковой была затронута тема взаимоотношений частных LegalTech-решений с государственными, регулирование их применения. Так, статья 13 Закона об информации не предусматривает использование частных информационных систем в зависимости от усмотрения и воли их владельца, нет законодательной регламентации отношений подобного рода. Таким образом, у государственных органов есть возможность применения LegalTech-инструментов, созданных частными лицами, а также наоборот, государственные юридические технологии могут применяться на практике юридическими и физическими лицами. Однако установление правового порядка в общественных отношениях в сфере LegalTech с помощью данных норм затруднительно и не представляет особого смысла. Правовая база фрагментарна и требует дальнейшей детализации. Перспективным направлением является разработка отдельного правового режима для LegalTech, учитывающего специфику и обеспечивающего безопасность цифрового правоприменения.

Определив, что такое LegalTech, и какие признаки присущи ему, можно сформулировать следующий вывод. LegalTech представляет собой динамично развивающееся явление, которое трансформирует традиционную юриспруденцию, повышает эффективность правовой системы и открывает новые перспективы для юридического образования. Дальнейшее развитие этого направления будет зависеть от гармоничного сочетания технологических инноваций, правового регулирования и подготовки квалифицированных кадров, способных работать в условиях цифровой экономики.

Трансформация юридической практики в России и в мире в связи с современными тенденциями развития LegalTech привело к появлению различных направлений развития данной сферы. Каждое из них основывается на различных аспектах цифровизации правового поля.

Для всего мира характерна автоматизация рутинных действий с помощью современных технологий. Согласно исследованию профессоров Оксфордского университета, экспертов в сфере футурологии и будущих профессий Ричарда и Дэниэля Сасскиндов «The Future of the Professions», автоматизация составляет основу современного LegalTech, позволяя обрабатывать большинство юридических операций [17]. Например, системы ИИ ROSS Intelligence помогают в процессе подготовки юридических документов и при анализе судебных актов (разработка стратегии судебных разбирательств, поиск судебной практики, анализ договоров и т. д.). Данные технологии позволяют сократить время обработки документов, что приводит к повышению эффективности работы юридических фирм и департаментов. Как отмечает интернет-издание Право.ру, электронные

сервисы позволяют юристам тратить на 95% меньше времени на заполнение карточек дел и на 85% – на подготовку документов [26].

Как уже было отмечено ранее, развитие современного общества невозможно представить без искусственного интеллекта. Данное положение привело к появлению нового направления применения технологий в праве. ИИ-решения получили масштабное применение в системе государственных органов. Так, с помощью биометрической системы распознавания лиц на городском транспорте города Москвы «Сфера» и аппаратно-программного комплекса «Безопасный город» правоохранительные органы идентифицируют разыскиваемых лиц с высокой точностью. То есть, ИИ становится не просто инструментом оптимизации, а новым элементом правовой системы, выступающим регулятором общественного порядка и национальной безопасности государства.

Также LegalTech-решения активно внедряются в сферу регулирования споров, или так называемую сферу online dispute resolution (далее – ODR). Системы ODR чаще всего применяются при разрешении мелких гражданских дел, с помощью которых значительно сокращаются сроки их рассмотрения. В европейских странах огромную роль играет система онлайн-правосудия e-Justice [19]. В отчете «EU Justice Scoreboard 2023» были приведены данные о качестве проведения цифровизации и технологизации судебной системы стран Европейского союза, стран-участниц системы e-Justice. Средний срок рассмотрения споров сократился с шести месяцев до трех недель, а полный переход к цифровым процессуальным правилам произошел в восьми странах. В данном направлении Россия не отстает от европейских государств и США. Система «Мой Арбитр» используется в арбитражных судах для подачи исков и отслеживания статуса дел в электронном формате, снижая временные затраты на бумажный документооборот [2]. В системе уже реализована возможность проведения судебных заседаний в формате веб-конференции. Кроме того, запланирована интеграция «Единого портала государственных и муниципальных услуг» (далее – Госуслуги) с новым суперсервисом «Правосудие онлайн». Как отмечает член Президиума Верховного Суда Российской Федерации В.В. Момотов: «До 2030 года планируется реализовать переход на так называемое электронное правосудие, в котором онлайн взаимодействие будет возможно от этапа подачи иска и до самого судебного заседания». Можно сделать вывод, что внедрение ODR-систем заметно ускоряет рассмотрение судебных дел и упрощает доступ к правосудию уже сейчас, и развитие данного направления является наиболее важной составляющей цифровизации общественного строя.

Все больше в юридической практике применяются технологии предиктивной аналитики и анализа больших данных. По мнению профессора школы права Северо-Западного университета города Чикаго Д.О. Макгинниса, прогнозирование исхода дела в зависимости от собранных доказательств постепенно будет изменять существующую практику, беря на себя многие функции человека [5]. Прогнозирование исходов судебных дел с помощью предиктивной аналитики на основе больших данных и ИИ становится ключевым трендом в юридической практике. Верховным судом США при вынесении заключительного судебного акта используется модель принятия решений, основанная на про-

шлых решениях, которая точнее предсказывает исходы исков, чем команда экспертов суда [23]. В России применение юридической аналитики в судебной системе затрудняется в виду слабого развития отечественных технологий на основе ИИ. Кроме того, правовое регулирование общественных отношений, связанных с аналитической деятельностью, в России остается фрагментарным. Отсутствует комплексный законодательный подход к определению правового статуса больших данных, их оборота, защиты прав субъектов данных и ответственности операторов [1].

Смарт-контракты стали ключевым инструментом LegalTech, трансформируя подход к заключению и исполнению договоров. Смарт-контракты в LegalTech рассматриваются как программный код, который автоматически исполняет или контролирует исполнение договорных обязательств, что значительно упрощает и автоматизирует юридические процессы. Смарт-контракты позволяют сократить количество спорных сделок, механизировать исполнение некоторых обязательств и проверить полномочия подписанта. Несмотря на активное применение блокчейн-технологий в юридической сфере, правовое регулирование данного института довольно условно. Согласно гражданскому законодательству, смарт-контракт рассматривается как программа для электронных вычислительных машин, охраняемая как объект интеллектуальной собственности [3]. Специального правового регулирования общественных отношений, связанных со смарт-контрактами в Российской Федерации пока не предусмотрено. Однако некоторые аспекты нашли свое отражение в дополнениях к статье 309 Гражданского кодекса Российской Федерации, введенных в действие Федеральным законом от 18 марта 2019 г. № 34-ФЗ [9]. В Швейцарии регулятор Financial Market Supervisory Authority наиболее точно отражает сущность смарт-контракта, определяя его как метод исполнения и фиксации обязательств. При этом стоит отметить, что это не договор, а технологии, с помощью которых возможно совершение различного рода сделок.

Кроме технологий, применяемых исключительно практикующими юристами или государственными служащими, в современных реалиях появились новые, так называемые LawTech-решения. В статье М.А. Рожковой дается общее определение и объясняется правовая природа LawTech. «LawTech – это различного рода онлайн-приложения и сервисы, дающие возможность заменить традиционные способы получения юридических услуг новыми и (или) облегчающие пользователям доступ к правовой информации. Основное отличие их от LegalTech состоит в том, что эти технологические решения предназначены не для юристов, а для конечных потребителей юридических услуг, которые без непосредственного обращения к профессиональному юристу получают необходимую правовую консультацию или иную юридическую услугу (прежде всего, речь идет о гражданах и малом бизнесе)» [15]. Цель LawTech – сделать юридические услуги более доступными и удобными для широкой аудитории, снижая зависимость от традиционных юридических консультаций и уменьшая затраты на получение правовой помощи. Большой объем бесплатной информации в сети Интернет привело к появлению приложений для самостоятельного получения юридической информации, которые юристы относят к LawTech-решениям.

Согласно подходу понимания LegalTech как компонента юридического образования возможно выделение особого направления применения технологий в процессе получения высшего или дополнительного профессионального образования. Юридическое образование должно стать более гибким, доступным и практичным, чтобы соответствовать реалиям современного рынка. Как отмечают эксперты Гарвардской школы права, помимо традиционного подхода получения юридического образования студенты получают компетенции в соответствии с изменением роли юриста в будущем. Выпускники юридических факультетов приобретают навыки применения технологий, создания стартапов, а также управления проектами. В современных реалиях трансформация юридического образования только начинает свой путь. Так, в России создаются магистерские программы обучения по направлениям «Право в сфере информационных технологий (IT-право)» и «LegalTech». Кроме того, для студентов бакалавриата уже с первого курса есть возможность участия в юридических хакатонах. Таким образом, LegalTech – не просто вспомогательный инструмент, а новая парадигма юридического образования, которая формирует юристов будущего: технологически грамотных, адаптивных и способных работать в цифровой среде.

Кроме вышеперечисленных направлений развития и внедрения LegalTech возможно привести большее количество. LegalTech охватывает множество технологий, основное внимание ученых и законодателей приковано к тем направлениям, которые уже сейчас оказывают наибольшее влияние на правовую систему – автоматизация, ИИ, ODR, предиктивная аналитика, смарт-контракты и LawTech. Остальные сферы либо развиваются медленнее, либо требуют дополнительных исследований и регуляторных решений.

Каждое из этих направлений развивается неравномерно. Россия в данном контексте следует глобальным трендам. Например, планы по цифровизации правосудия демонстрируют, что страна движется в том же направлении, что и ведущие юрисдикции. При сравнении российского и международного опыта развития LegalTech становится очевидным, что в России наибольшие инвестиции приходятся на автоматизацию и онлайн-услуги. Таким образом, для гармоничного развития LegalTech-экосистемы необходимо синхронное развитие всех направлений при активном участии государства, бизнеса и образовательных учреждений.

Обеспечение информационной безопасности LegalTech-решений становится важнейшим элементом их внедрения в правовую систему государства. Современные технологии в юридической деятельности находятся на недостаточном уровне защиты данных. Кроме того, правовое регулирование информационной безопасности требует доработки и конкретизации норм. В России этот вопрос осложняется необходимостью балансировать между технологической независимостью и рецепцией международного опыта.

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) сервисы LegalTech являются информационными системами [16]. Согласно Закону об информации «информационная система –

совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [7]. Таким образом, LegalTech-решения представляют собой особый вид информационной системы, предназначенной для обработки юридически значимых данных.

Вопросы защиты данных в сфере LegalTech регулируются Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) [10]. В соответствии со статьей 19 Закона о персональных данных оператор обязан принимать меры защиты персональных данных, включая шифрование и ограничение доступа. Контроль и надзор защиты персональных данных в России осуществляют Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор, РКН) и Федеральная служба по техническому и экспортному контролю (ФСТЭК). Использование LegalTech в России требует строгого соблюдения Закона о персональных данных. Данные нормы необходимы для обеспечения безопасности данных при автоматизации юридических процессов.

Для корректного функционирования информационных систем требуется обеспечение информационной безопасности и защита персональных данных лиц, которые пользуются данными системами. В Российской Федерации обеспечение информационной безопасности является одним из ключевых стратегических национальных приоритетов [11]. Кроме того, согласно пункту «м» статьи 71 Конституции Российской Федерации обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных находится в исключительном ведении Федерации [4]. То есть данная норма подчеркивает централизованный подход к регулированию цифровой среды, включая защиту данных в сфере LegalTech.

Закрепление данных положений было отражено в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента от 5 декабря 2016 г. № 646 (далее – Доктрина)[8]. Доктрина является стратегическим нормативным правовым актом, развивающим положения Стратегии национальной безопасности Российской Федерации. Доктрина отражает современные вызовы и угрозы, связанные с развитием цифровых технологий, и определяет стратегические приоритеты государства в обеспечении безопасности личности, общества и государства в условиях информационного общества.

В рамках работы с юридическими инновациями вышеперечисленные нормативные правовые акты закрепляют следующие положения обеспечения информационной безопасности в данной сфере.

1. Защита от кибератак и обеспечение устойчивости информационных систем.

Согласно Доктрине, одной из ключевых угроз является использование информационных технологий иностранными государствами для вмешательства во внутреннюю политику России. Среди юридических технологий наиболее популярным решением автоматизации и упорядочения рутинных процессов документооборота является внедрение облачных хранилищ (от англ. cloud storage). С возникновением напряженных отношений между Россией и ряда западных стран появился особый вид кибершпионажа данных из облачных хранилищ –

CloudSorcerer. Так, в мае 2024 года эксперты Глобального центра исследований и анализа угроз «Лаборатории Касперского» (далее – GReAT) выявили кампанию данного кибершпионажа, нацеленную на российские государственные организации. Отчет GReAT указал на использование организациями зарубежных облачных хранилищ Microsoft Graph, Dropbox. Для создания условий для устойчивого развития LegalTech и защиты их от кибератак подобного рода необходима интеграция технологий кибербезопасности с современными информационными системами, так как надлежащая защита персональных и государственных данных может предотвратить их утечку, минимизировать угрозу для национальной безопасности России.

2. Развитие отечественных юридических технологий и снижение зависимости от зарубежных LegalTech-решений.

Разработка и внедрение отечественных LegalTech-решений становятся не только технологическим, но и стратегическим приоритетом, способствуя снижению зависимости от зарубежных продуктов и формируя новые стандарты в правовой практике. Кроме того, российские технологии в сфере юриспруденции, по мнению экспертов, зачастую превосходят зарубежные аналоги благодаря быстрой адаптации сервисов под специфику российского законодательства и судебной практики, а также более продуманным пользовательским интерфейсом. После введения реестра отечественного программного обеспечения крупные компании и государственные структуры все чаще отдают предпочтение российским разработчикам, что стимулирует рост внутреннего рынка LegalTech. Установление технологического суверенитета России в связи с санкционными ограничениями и геополитической нестабильностью является одной из важнейших задач на современном этапе развития цифрового общества.

Но, несмотря на рост, рынок LegalTech пока не покрывает полностью юридические потребности, и существующее программное обеспечение работает не идеально. Разработка и внедрение отечественных LegalTech-решений открывают новые возможности для трансформации правовой системы, повышения эффективности и доступности юридических услуг, а также укрепления технологического суверенитета страны.

3. Цифровизация государственных услуг.

Цифровизация государственных услуг и активное внедрение отечественных LegalTech-решений не только оптимизируют юридическую деятельность, но и оказывают значительное влияние на общество, повышая доступность, прозрачность и эффективность государственных и правовых институтов.

В России цифровая трансформация затронула практически все сферы управления и оказания государственных услуг. Наиболее яркими примерами LegalTech-решений в госсекторе стали сервисы автоматизированного мониторинга правонарушений и системы электронного документооборота. Эти инструменты позволяют гражданам и бизнесу дистанционно получать справки, подавать заявления и взаимодействовать с государственными органами без необходимости личного присутствия.

Важным шагом стало внедрение машиночитаемого права, что позволяет автоматизировать процессы нормотворчества, контроля, отчетности и судопро-

изводства. Примером таких технологий является государственная информационная система «Национальная единая среда взаимодействия участников нормотворческого процесса» (ГИС «Нормотворчество»), которая уже применяется в государственных органах исполнительной власти.

Государство активно поддерживает развитие национальных платформ, внедряет стандарты машиночитаемого права и стимулирует рост LegalTech-компаний. Согласно исследованию Сингапурского университета менеджмента «The state of legal innovation in Asia-Pacific 2020» [27] основным потребителем LegalTech являются государственные структуры, в особенности судебные органы. Тем самым, государственные органы являются основными драйверами юридических инноваций, активно формирующие цифровую среду и задающие вектор развития LegalTech-рынка. Бизнес подхватывает инициативу, но именно органы власти определяют темп и масштаб изменений, а также обеспечивают инфраструктурную и нормативную базу для развития отрасли. Подобные меры способствуют росту доверия к правовой системе и повышению эффективности государственного управления в Российской Федерации.

Проблемы обеспечения информационной безопасности LegalTech в России обусловлены как технологическими, так и правовыми аспектами. Ключевые вызовы включают недостаточный уровень защиты данных в юридических информационных системах, а также угрозы кибератак, в том числе с использованием зарубежных облачных. Особую актуальность приобретает задача технологического суверенитета и снижение зависимости от иностранных технологий.

Можно представить некоторые пути решения данных проблем.

1. При возникновении случаев кибератак на LegalTech-системы целесообразно создание и использование закрытых отечественных облачных хранилищ, интегрированных с популярными антивирусными программами (например, «Лаборатория Касперского»). Но программирование таких систем представляет сложный и долгий процесс. В связи с этим, в зарубежных странах широко применяются LegalTech-платформы по защите данных (Data Loss Protection) и конфиденциальности. Например, платформа от OneTrust нашла широкое применение среди юридических фирм США и стран Европы. Правовой основой принципов работы OneTrust являются Общий регламент по защите данных (GDPR) и Калифорнийский закон о защите прав потребителей (CCPA). Отечественные аналоги подобных платформ не создаются. Скорее всего, это связано с узкой специализацией данных программ и малым распространением LegalTech в России. С развитием информационной сферы и постепенным процессом цифровизации применение таких инструментов будет неотъемлемой частью работы с данными.

2. Популяризация применения LegalTech в России зависит от количества специалистов, которые занимаются их разработкой и внедрением. В 2023 году Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации оценило дефицит кадров примерно в 500–700 тысяч человек. Кроме того, аналитики исследовательского центра «Зарплаты.ру» выяснили, что IT-сфера нуждается в специалистах по кибербезопасности, необходимость которых особенно выявляется при работе с юридическими документами и госу-

дарственными данными (дефицит составляет 35 %). Решение данной проблемы заключается в сотрудничестве IT-компаний с образовательными организациями, чтобы компетенции выпускников соответствовали тем требованиям, которые предъявляют организации и государственные органы при трудоустройстве.

Таким образом, обеспечение информационной безопасности LegalTech в России требует комплекс некоторых мер: соответствие нормативным правовым актам, инвестиции в отечественные IT-технологии и подготовка кадров. Только при условии системного подхода, объединяющего правовые, технологические и кадровые меры, можно обеспечить высокий уровень информационной безопасности и устойчивое развитие цифровой правовой среды.

Развитие LegalTech в Российской Федерации характеризуется динамичным ростом технологических решений на фоне системных вызовов, обусловленных спецификой правовой системы и рыночной структуры. Анализ текущего состояния рынка LegalTech позволяет выделить ключевые векторы развития и институциональные ограничения.

В настоящее время выделяют следующие перспективные направления LegalTech в России:

- 1) автоматизация стандартных юридических операций, системы на основе ИИ и больших языковых моделей;
- 2) машиночитаемое право;
- 3) государственно-частное партнерство в LegalTech;
- 4) онлайн-решение споров (ODR).

Автоматизация рутинных юридических задач остается внедрение low-tech решений: онлайн-платформ для генерации документов и маркетплейсов юридических услуг (Pravoved.ru, OnlinePatent.ru, Fedor.ai – первый роботизированный юрист в России) [22]. Эти инструменты обеспечивают сокращение временных затрат на 40–60 % для малого бизнеса и физических лиц. В корпоративном секторе наблюдается рост спроса на системы управления контрактами с элементами ИИ. Так, ПАО «МТС» является лидером использования ИИ для решения корпоративных задач.

Для решения проблем больших трудозатрат и несвоевременности обнаружения нарушения сроков исполнения обязательств компания разработала систему по распознаванию текста, отслеживанию сроков и формированию претензионных документов на основе ИИ, что привело к росту производительности в 1,5 раза, а за счет улучшения дисциплины платежей контрагентов удалось сэкономить до 4 % от суммы контрактов [18].

Как уж было сказано ранее, Российской Федерацией активно поддерживается развитие проектов в области машиночитаемого права. Россия отличается от зарубежного рынка наличием общедоступных и бесплатных баз данных, содержащих законодательство и материалы судебной практики. Большинство документов в таких системах представлены в машиночитаемом формате.

Следующим перспективным направлением эксперты отмечают сотрудничество компаний с государственными структурами. В 2022 году Государственная Дума Российской Федерации внесла изменения в Федеральный закон от 21 июля 2005 года № 115-ФЗ «О концессионных соглашениях» по регулирова-

нию вопроса развития ИИ и информационных технологий (в том числе и LegalTech) посредством заключения концессионных соглашений и соглашений о государственно-частных и муниципально-частных партнерствах. Данный нормативный правовой акт должен стимулировать частные компании (например, Skolkovo LegalTech) заключать договоры с государственными органами для реализации развития юридических инноваций в России.

Работа по созданию ODR-систем в России в настоящее время приостановлена и имеет некоторый заторможенный характер. Необходимо отметить, что в 2021 году в Госдуму был внесен законопроект о создании альтернативных онлайн-механизмов урегулирования споров. Согласно проекту системы ОУС предназначены для упрощения коммуникации между покупателем и ответственными лицами в рамках процесса предъявления, рассмотрения и удовлетворения претензий потребителей через сервис информационной системы «Госуслуги».

Перспективные направления развития юридических технологий в России не ограничиваются данным перечнем. Например, эксперты считают, что в ближайшее время применение смарт-контрактов и блокчейн в юридической деятельности станет обыденностью, более половины коммерческих контрактов будут заключаться и исполняться в такой форме.

В России развитие юридических инноваций определяется как наличием определенных стимулов, так и рядом препятствий, связанных с особенностями рынка юридических услуг. Директор центра юридических технологий Фонда Сколково Антон Пронин отмечает, что преобладание небольших юридических фирм сдерживает внедрение технологий [19]. Вместе с тем, растущий спрос на доступные и эффективные решения способен стимулировать развитие LegalTech, поскольку юридические компании стремятся к снижению затрат и повышению эффективности, что подталкивает их к использованию инновационных инструментов.

Наиболее значимым барьером развития LegalTech в России является экономический фактор. Российский рынок информационных технологий характеризуется низким интересом инвесторов к инновационным решениям в сфере права. По данным Фонда Сколково, стартапы в сфере LegalTech в России обычно не привлекают более 150 000 долларов США [19]. Это ограничение существенно сдерживает масштабирование и развитие проектов, так как недостаток финансирования препятствует созданию комплексных и конкурентоспособных продуктов, способных удовлетворить потребности рынка.

Помимо экономических трудностей, существенным препятствием является психологический фактор. Профессиональные юристы и адвокаты, обладающие живым и аналитическим мышлением, часто предпочитают традиционные методы работы, полагаясь на собственный опыт и нестандартные решения для типовых задач.

Для успешного развития LegalTech в России необходимо преодолеть экономические ограничения и изменить менталитет профессионального сообщества, повысив доверие к инновационным технологиям и их роли в правовой

практике. Только комплексный подход позволит раскрыть потенциал LegalTech и интегрировать его в повседневную работу юридических компаний.

Развитие LegalTech в России имеет большой потенциал благодаря внедрению современных технологий и сотрудничеству с государством. Однако рост отрасли сдерживается экономическими ограничениями и низким уровнем доверия к таким решениям. Для успешного развития необходимо увеличить финансирование инновационных проектов и интегрировать технологий в практику.

Заключение. Подводя итоги данной статьи, хочется выделить большой потенциал в развитии LegalTech в России и в зарубежных странах. Благодаря технологиям, система правовых отношений изменится сразу в нескольких аспектах: начиная с оптимизации процессов, сокращения времени на выполнение задач, заканчивая четким следованием актуальности информации, учитывая действующие поправки, внесенные в нормативно правовые акты и другие источники права.

Опыт внедрения LegalTech показал не только положительные результаты, но и свои слабые стороны, которые важно проработать для дальнейшей эффективности. Среди них одними из наиболее важных оказались информационная безопасность и экономический фактор, выражающийся в низком проценте инвестиций в инновационные решения. Только комплексный подход устранения недостатков позволит раскрыть потенциал LegalTech и интегрировать его в повседневную работу юридических компаний и государственных органов.

LegalTech предоставляет обширные перспективы для обновления юридической сферы, улучшения качества и доступности правовых услуг, а также создания новой цифровой культуры в практике применения права. Продолжение развития этого направления будет способствовать усилению правовой системы России и ее включению в цифровую среду.

Список литературы

1. Алферов О. Л. Большие данные в юридической деятельности // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4. Государство и право: Реферативный журнал. 2023. № 3.
2. Арбитражный суд Российской Федерации. URL: <https://my.arbitr.ru/#index> (дата обращения: 12.05.2025).
3. Гражданский кодекс Российской Федерации (часть четвертая): Федеральный закон от 18.12.2006 № 230-ФЗ (ред. от 22.07.2024) // Собрание законодательства Российской Федерации. 2006. № 52 (ч. 1). Ст. 5496.
4. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 // Официальный интернет-портал правовой информации, 2020. Текст электронный. URL: <http://www.pravo.gov.ru> (дата обращения: 10.05.2025).
5. Макгиннис Джон О., Пирс Рассел Дж. Великий подрыв: как искусственный интеллект меняет роль юристов в оказании юридических услуг // Russian Journal of Economics and Law. 2019. № 2.
6. Минбалеев А. В. Понятие и признаки LegalTech: The Concept and Attributes of LegalTech // Юридический мир. 2022. № 5. С. 36–40. ISSN 1811–1475.

7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3448.
8. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50 (ч. II). Ст. 7074.
9. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18.03.2019 № 34-ФЗ // Собрание законодательства Российской Федерации. 2019. № 12. Ст. 1224.
10. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 08.08.2024) // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.
11. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 02.07.2021 № 400 // Собрание законодательства Российской Федерации. 2021. № 27 (ч. II). Ст. 5351.
12. Пальянова Н. В. Использование искусственного интеллекта в сфере Legal Tech: современные возможности и перспективы // Социально-экономическое развитие и качество правовой среды: Труды VIII Моск. юрид. форума, XIX Междунар. науч.-прак. конф. Ч. 2 (8–10 апреля 2021 г.) / МГЮА. Москва: МГЮА, 2021. С. 260–267.
13. Рожкова М. А. О правовых аспектах использования технологий LegalTech и LawTech // Право цифровой экономики. 2020. № 3. С. 1–9.
14. Рожкова М. А., Исаева О. В. и др. Legaltech, Fintech, Regtech etc.: правовые аспекты использования цифровых технологий в коммерческой деятельности. Москва: Статут, 2021. 310 с.
15. Савенко Н. Е. Legaltech в цифровой экономике и правовом регулировании экономической деятельности граждан // Право. Журнал Высшей школы экономики. 2023. № 1.
16. Стародубов О. О., Макаров В. В., Блатова Т. А., Годун А. Д. Инновационные решения ПАО «МТС» по внедрению современных услуг и технологий искусственного интеллекта // Экономика и бизнес: теория и практика. 2020. № 9–2. С. 73–77. DOI: 10.24411/2411-0450-2020-10732.
17. Цифровые решения: как повысить эффективность работы юристов // Интернет-портал «Право.ру». URL: <https://pravo.ru/lf/story/231716/> (дата обращения: 11.05.2025).
18. European e-Justice Portal. URL: https://e-justice.europa.eu/home_en (дата обращения: 09.05.2025).
19. Legal Technology Vision: Towards the digital transformation of the legal sector. Singapore: Legal Technology Cluster Committee Singapore Academy of Law, 2017. P. 4. URL: <https://www.sal.org.sg/Resources-Tools/Legal-Technology> (дата обращения: 08.05.2025).
20. OLTEP. URL: <https://www.oltep.ox.ac.uk/> (дата обращения: 14.05.2025).
21. Pronin A. Legal Innovation in Russia. New Era of Legal Innovation in Russia. LR, 2019. P. 155–159.

22. Ruger T. W. et al. The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking // Columbia Law Review. 2004. Vol. 104. P. 1150.
23. Ryan F. Rage against the machine? Incorporating legal tech into legal education // The Law Teacher. 2021. Vol. 55, № 3. Pp. 392–404.
24. Susskind R. Tomorrow's Lawyers: An Introduction to Your Future. 2nd ed. Oxford: Oxford University Press, 2017. 224 p.
25. Susskind R., Susskind D. The Future of the Professions: How Technology Will Transform Professional Services and Expertise. Bookey, 2015. Chapter 2, p. 11.
26. The state of legal innovation in Asia-Pacific 2020 // SMU Libraries. URL: https://ink.library.smu.edu.sg/sol_research/3368/ (дата обращения: 05.05.2025).

В. Д. Квитовская,
студент,
Финансовый университет
при Правительстве Российской Федерации,
А. А. Сорокопудова,
студент,
Финансовый университет
при Правительстве Российской Федерации

**Цифровые технологии, способствующие экономическому развитию
международных организаций**

Аннотация. В данной статье рассматривается влияние цифровых технологий на экономическое развитие международных организаций. Анализируются различные способы, которыми цифровые технологии способствуют повышению эффективности, прозрачности и инклюзивности деятельности международных организаций, а также их роль в стимулировании экономического роста и сотрудничества между странами. Особое внимание уделяется анализу вызовов и рисков, связанных с использованием цифровых технологий в контексте деятельности международных организаций, и предлагаются рекомендации по их преодолению. Рассмотрены примеры работы Международного союза электросвязи ООН, Всемирной организации интеллектуальной собственности, Всемирной торговой организации в области цифровизации.

Ключевые слова: цифровые технологии, международные организации, экономическое развитие, глобализация, инновации, цифровизация, устойчивое развитие

V. D. Kvitovskaya,
student,
Financial University under the Government
of the Russian Federation,
A. A. Sorokopudova,
student,
Financial University under the Government
of the Russian Federation

**Digital technologies that contribute to the economic development
of international organizations**

Abstract. This article examines the impact of digital technologies on the economic development of international organizations. It analyzes the various ways in which digital technologies contribute to improving the efficiency, transparency, and inclusivity of IOs, as well as their role in promoting economic growth and coopera-

tion between countries. The article focuses on analyzing the challenges and risks associated with the use of digital technologies in the context of international organizations and provides recommendations for overcoming these challenges. The article also explores examples of the work of the International Telecommunication Union, the World Intellectual Property Organization, and the World Trade Organization in the field of digitalization.

Keywords: digital technologies, international organizations, economic development, globalization, innovation, digitalization, sustainable development, ITU, WIPO, WTO

Введение. В эпоху стремительного развития цифровых технологий международные организации сталкиваются с необходимостью адаптации к новым реалиям и использования потенциала цифровизации для достижения своих целей в области экономического развития. Цифровые технологии, такие как искусственный интеллект (далее – ИИ), блокчейн, большие данные и интернет вещей, предоставляют международным организациям уникальные возможности для повышения эффективности своей деятельности, расширения охвата программ и проектов, а также стимулирования экономического роста и сотрудничества между странами. Институт статистических исследований и экономики знаний НИУ ВШЭ определил с помощью инструментов анализа больших данных ключевые направления развития технологий, которые формируют глобальную и национальную повестки цифрового развития экономики и общественной жизни[6]. Согласно изученным данным, искусственный интеллект становится ключевым элементом в повестке дня как на мировом, так и на российском уровне. Применение комплексного подхода к созданию ИИ-решений позволяет ускорить разработку алгоритмов и адаптировать передовые технологии для решения практических задач в различных отраслях.

В частности для российских реалий наиболее актуальными и значимыми на глобальном уровне цифровых технологий являются искусственный интеллект, киберфизические технологии, цифровая инфраструктура, цифровые финансы и индустрия аддитивных технологий (например, 3Д-печать), а также виртуального проектирования и симуляции.

Необходимо также выделить отдельно использование искусственного интеллекта в рамках цифровизации международных отношений: при взаимодействии как между государствами, так и международными организациями. Как выделяет Т. А. Гришанина в рамках своего исследования, с появлением искусственного интеллекта в международном взаимодействии, появились новые ответвления дипломатии: цифровая дипломатия и дипломатия данных [4. С. 16]. ИИ в данных сферах используется как инструмент прогнозирования мнения пользователей через социальные сети на основе анализа мнений и предпочтений. Как резюмирует автор, ИИ в дипломатии в основном в данный момент используется как тема для переговоров, дипломатический инструмент, а также как фактор изменения переговорного контекста. В целом, ИИ также используется и отдельными странами в рамках различных сфер деятельности. Так, в Российской Федерации утверждена Национальная стратегия развития искусственного

интеллекта до 2030 года. Основными целями данной стратегии в таком случае выступают достижение устойчивой конкурентоспособности российской экономики, в том числе лидирующих позиций в мире в области ИИ, обеспечение безопасности государства и повышение уровня жизни граждан.

Основная часть. Однако успешное экономическое развитие невозможно без деятельности международных организаций, в том числе с использованием технологий, отвечающих актуальным тенденциям мирового развития. Удачным примером использования современных цифровых технологий служит деятельность Международного союза электросвязи ООН, отвечающего за информационные и коммуникационные технологии. Она включает в себя разработку международных стандартов для ИКТ, которые обеспечивают совместимость и успешное функционирование различных технологий и сетей. Например, стратегический план МСЭ на 2024–2027 гг. (ITU Strategic Plan 2024–2027) [12] закреплённый в резолюции 71 четко обозначает приоритеты МСЭ в области цифрового развития, включая основные цели, направленные на расширение доступа к ИКТ, заключающейся в создании универсально доступной, безопасной и высококачественной инфраструктуры услуг и приложений в области электросвязи, а также в содействии цифровой трансформации для построения справедливого и инклюзивного использования таких технологий. Более того, Союз Электросвязи реализует множество программ, направленных на реализацию стратегических целей, обозначенных выше, например программа "Connecting the Unconnected" направленная на расширение доступа к интернету в отдалённых и сельских районах, где инфраструктура развита слабо, предоставляет техническую помощь, финансирование и экспертизу для развития широкополосной связи. Также МСЭ организует различные форумы и конференции, посвященные цифровой экономике, такие как "AI for Good Global Summit", где обсуждаются вопросы использования искусственного интеллекта для решения глобальных проблем. Помимо этого, МСЭ активно работает над укреплением кибербезопасности в различных странах мира. Global Cybersecurity Index (GCI) – это глобальный индекс кибербезопасности, который оценивает уровень кибербезопасности в различных странах мира. МСЭ использует GCI для определения приоритетов в области кибербезопасности и для мониторинга прогресса в этой области [10].

Рассматривая использование цифровых технологий нам не представляется возможным обойти стороной деятельность еще одного специализированного учреждения ООН, а конкретно деятельность Всемирной Организации Интеллектуальной Собственности. Эта организация отвечает за защиту интеллектуальной собственности и играет важную роль в стимулировании инноваций и экономического роста путем защиты прав интеллектуальной собственности. Например, ВОИС запустила онлайн-платформу для подачи заявок на международную регистрацию товарных знаков (Мадридская система) и патентов, деятельность которой дополняется Договором о патентной кооперации (РСТ), таким образом, патентная заявка может быть подана гражданином любого Договаривающегося государства РСТ или лицом, проживающим в таком государстве. Обычно она может быть подана в национальное патентное ведомство До-

говаривающегося государства, гражданином которого является заявитель или в котором он проживает, либо, по выбору заявителя, в Международное бюро ВОИС в Женеве. ВОИС разработала несколько онлайн-систем для поддержки инноваций, например eTISC – социальная платформа для обмена знаниями и идеями между Центром поддержки технологии и инноваций и пользователями интеллектуальной собственности. Включает форумы, дискуссионные группы и календари событий; WIPO INSPIRE – площадка, содержащая компиляцию отчетов о патентных базах данных, помогающая выбрать подходящие инструменты для изобретателей, желающих запатентовать свое детище и др. Стоит упомянуть, что Россия активно участвует в программе ЦПТИ, развивая национальную сеть (174 центра в 70 регионах, которые в 2023 году предоставили доступ к патентным базам данных для 25,5 тыс. человек и помогли подать 3,6 тыс. заявок на патенты)[8].

С развитием цифровых технологий в международной среде все больше и больше возрастает роль социальных сетей. С самого их появления пользователи начали объединяться по политическим, культурным, национальным и другими признакам, создавая принципиально новые общественные формирования, имеющие большее влияние, чем любые другие формы гражданских объединений. Обратив внимание на это, международные организации всерьез занялись мониторингом за деятельностью пользователей. Например, деятельность ООН по поддержанию мира включает в себя взаимодействие с компаниями – учредителями социальных сетей и выпуск обзоров и рекомендаций, анализирующих политическую обстановку для медиаторов, способствующих обсуждению проблем и возможностей взаимодействия с компаниями в посреднических и мирных процессах. Применяя ряд рекомендаций, изложенных в документах, публикуемых ООН, специалисты по медиации могут лучше понять, когда и как напрямую взаимодействовать с компаниями, работающими в социальных сетях, в вопросах анализа, стратегической коммуникации, привлечения сторон в конфликте и борьбы с вредным контентом и поведением [13].

Также касаясь исследований социальных сетей следует привести пример Международной торговой палаты (ICC). В рамках данной международной организации учрежден ESOMAR, международный представитель сообщества исследователей и специалистов по сбору и анализу данных и инсайтов, который занимается поиском информации в социальных сетях в соответствии с Международным Кодексом ICC/ESOMAR [5. С. 3–4]. Согласно положениям этого документа, целью исследования и поиска инсайтов является выход к управлению и синтезу данных, получаемых из различных источников, в том числе из социальных сетей. Деятельность ESOMAR заключается в маркетинговых и социальных исследованиях для принятия информационных решений в области потребностей потребителей. В данном случае социальные сети являются одним из наиболее доступных и разветвленных источников.

Говоря же о других цифровых инструментах, используемых международными организациями, следует упомянуть Всемирную торговую организацию (далее – ВТО). В вопросах систематизации внешней торговли эта организация является одной из основополагающих в первую очередь для стран-участниц, а

именно 164 государств. Стоит отметить, что ВТО хоть и является основной международной организацией в области мировой торговли, так и не достигла относительно цифровой иммерсии глобальной торговли, а нормы и правила так и не были приняты [9. С. 160]. Именно поэтому страны организуют торговлю друг с другом через региональные и двусторонние соглашения.

Однако, в рамках ВТО используются современные цифровые технологии, которые в разы упрощают работу с данными о странах и их продажах. Так, в 2023 году был использован новый интерактивный инструмент, World Trade Statistics, который заменил ежегодную публикацию обзора на статистику по мировой торговле. Он представляет основные данные и анализ по продаже товаров и услуг на мировом рынке, а также выявил ключевых поставщиков за прошедший год. Так, через сайт ВТО пользователи теперь могут загружать от 60 таблиц в Excel, а также через фильтры найти данные по экономике, региону или выбранным группам. Этот инструмент заметно повысил прозрачность деятельности организации и упростил работу со статистикой и аналитикой.

Международная организация, в этом случае даже уместнее “международный альянс”, которая активно пользуется благами цифровизации, является Евразийский экономический союз (далее – ЕАЭС). ЕАЭС активно вводит новые технологии в режим своей деятельности. Организация уже устанавливала стратегический план по цифровым преобразованиям в рамках развития интеграции стран-участниц. Одним из последних нововведений является интегрированная информационная система для оптимизации взаимодействия государств-участников и бизнеса. Также уже 26 сентября 2024 года Совет Евразийской экономической комиссии утвердил включение операторов электронной торговли в единый реестр для подготовки к включению главы 43.1 в Таможенный Кодекс ЕАЭС. Также, помимо этого, многие другие сферы стран-участниц уже активно взаимодействуют в цифровой среде.

Однако, в случае ЕАЭС важно учитывать и особенности этой международной организации. Так, согласно статье 1 договора о Евразийском экономическом союзе, ЕАЭС является международной организацией региональной экономической интеграции. Поэтому, именно из-за того, что организация региональная, некоторые ее инициативы было бы трудно интегрировать в другие организации с более обширной сферой действия. Несмотря на это, ЕАЭС показывает активное развитие в условиях цифровизации и международной интеграции, какие оптимизировали бы работу и других экономических союзов регионального типа.

Заключение. Резюмируя все сказанное ранее, приведенные цифровые инструменты, такие как онлайн-платформа для подачи заявок на международную организацию товарных знаков, интерактивные инструменты, заменяющие длинные тексты отчетов, внедрение искусственного интеллекта в работу с отчетностью организации и многое другое, могут значительно оптимизировать и систематизировать работу международных организаций и их отчетность в первую очередь. Данная работа изначально была направлена на то, чтобы показать внедрение цифровых технологий в деятельность организаций в экономической интеграции и то, какие результаты она приносит. Как можно увидеть, во

всех субъектах это работает по-разному: где-то находится только на начальных этапах, а где-то уже представлено в развитой системе. Однако, что в одном, что в другом случае заметна оптимизация и следование современным реалиям в рамках деятельности организаций, что важно. Поэтому, как показывают результаты исследования, международным организациям стоит активно применять новые технологии для оптимизации и наглядности их же деятельности.

Хотим предложить следующую инициативу: создание отдела по исследованию социальных сетей в рамках департамента информационных технологий ЕЭК при ЕАЭС. Социальные сети предоставляют огромный объем данных о поведении и предпочтениях потребителей. ЕАЭС же может использовать эти данные для сегментации рынка, прогнозирования спроса, а также развития межстрановой торговли. Также исследование социальных сетей может способствовать развитию системы надзора за рисками в сфере экономики: к примеру, внешние риски в инвестиционной сфере. В рамках исследования социальных сетей, этот отдел ЕЭК будет способствовать развитию предпринимательства путем создания общей краудфандинг платформы, где бизнес-сообщества и стартапы могут использовать соцсети для сбора идей и обратной связи от потребителей. Более того, через таргетированную рекламу и виральный маркетинг малые и средние предприятия могут выходить на рынки других стран-членов ЕАЭС, используя общее цифровое пространство. Данные нововведения приведут к развитию экономик и экономической интеграции стран-участниц.

Список литературы

1. Белоусов А. Л. Правовые аспекты развития финансового сектора в условиях цифровизация // Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции. 2023. С. 15–19.
2. Договор о Евразийском экономическом союзе от 29.05.2014 (ред. от 25.05.2023). URL: https://www.consultant.ru/document/cons_doc_LAW_163855/ (дата обращения: 06.09.2025).
3. Доклад о цифровой экономике. Формирование экологически устойчивого и инклюзивного цифрового будущего. ОБЗОР. URL: https://unctad.org/system/files/official-document/der2024_overview_ru.pdf (дата обращения: 06.09.2025).
4. Гришанина Т. А. Искусственный интеллект в международных отношениях: роль и направления исследования // Вестник РГГУ. Серия: Политология. История. Международные отношения. 2021. С. 10–18.
5. Международный Кодекс ICC/ESOMAR по практике проведения маркетинговых и социальных исследований, изучения общественного мнения и анализа данных. URL: <https://esomar.org/uploads/attachments/ckqtgf5ux0119kjtrrv6ovzlx-iccesomar-code-russian.pdf> (дата обращения: 06.09.2025).
6. Пиекалнитс А.С., Приворотская С.Г., Серова Т.А. Топ-10 цифровых технологий в России и мире. Институт статистических исследований и экономики знаний. URL: <https://issek.hse.ru/news/1000447295.html> (дата обращения: 05.09.2025).

7. Рыбакова М. В., Паламарчук А. В. Евразийская интеграция: контент-анализ электронных ресурсов // Научный результат. Социология и управление. 2020. Т. 6. № 2. С. 132–144.
8. Сотрудничество со Всемирной организацией интеллектуальной собственности (ВОИС). URL: <https://rospatent.gov.ru/ru/activities/inter/coop/wipo> (дата обращения: 06.09.2025)
9. Хабыева А. М. ВТО и вопросы цифровой иммерсии международной торговли // Международная торговля и торговая политика. 2022. Т. 8. № 4 (32). С. 156–164.
10. Global Cybersecurity Index 2024. URL: <https://www.itu.int/epublications/publication/global-cybersecurity-index-2024> (дата обращения: 06.09.2025).
11. ITU Connection 2030 Agenda. URL: <https://www.itu.int/highlights-report-activities/connect2030-agenda/> (дата обращения: 06.09.2025).
12. Strategic plan for the Union for 2024–2027. The Plenipotentiary Conference of the International Telecommunication Union (Bucharest, 2022). URL: <https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-E.pdf> (дата обращения: 06.09.2025).
13. United Nations Department of Political and Peacebuilding Affairs, Centre for Humanitarian Dialogue and Build Up. Monitoring of Social Media Provisions in Peace Agreements. 2024. URL: dppasocial-media-peace-mediation-framework-engagement-companies-october-2023.pdf (дата обращения: 04.09.2025).

А. В. Козлов,
студент,
Российский университет дружбы народов
имени Патриса Лумумбы

Правовые особенности использования цифровых технологий в примирительных процедурах

Аннотация. В условиях цифровизации общества все большее значение приобретают новые информационные технологии, в том числе и в правовой сфере, активное развитие получают альтернативные способы разрешения споров, включая примирительные процедуры, такие как медиация и переговоры. В Российской Федерации наблюдается активное внедрение цифровых технологий в процессы урегулирования конфликтов, что требует анализа нормативно-правовой базы, регулирующей их применение. Настоящие тезисы посвящены исследованию правовых особенностей использования цифровых платформ, видеосвязи, электронной подписи и других технологий в примирительных процедурах. Анализируются положения Федерального закона от 27.07.2010 № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)». Особое внимание уделено вопросам конфиденциальности, легитимности электронных соглашений и обеспечения процессуальных гарантий. В статье делается вывод о необходимости совершенствования законодательства для обеспечения эффективности и правовой защищенности участников цифровых примирительных процедур.

Ключевые слова: цифровые технологии, медиация, примирительные процедуры, электронная медиация, правовое регулирование

A. V. Kozlov,
Law Institute student,
Peoples' Friendship University of Russia
named after Patrice Lumumba

Legal features of the use of digital technologies in conciliation procedures

Abstract. In the context of the digitalization of society, new information technologies are becoming increasingly important, including in the legal field, and alternative dispute resolution methods, including conciliation procedures such as mediation and negotiations, are actively developing. In the Russian Federation, there is an active introduction of digital technologies into conflict resolution processes, which requires an analysis of the regulatory framework governing their use. This article is devoted to the study of the legal features of the use of digital platforms, video communications, electronic signatures and other technologies in conciliation procedures. The provisions of the Federal Law "On Alternative Dispute Settlement Procedure

with the participation of an Intermediary (Mediation Procedure)" No. 193-FZ dated 27.07.2010 are analyzed. Particular attention is paid to the issues of confidentiality, the legitimacy of electronic agreements and the provision of procedural guarantees. The article concludes that it is necessary to improve legislation to ensure the effectiveness and legal protection of participants in digital conciliation procedures.

Keywords: digital technologies, mediation, conciliation procedures, electronic mediation, legal regulation

Введение. Современные вызовы, стоящие перед обществом включая пандемию, перегруженность судебных систем и растущую потребность в оперативном разрешении споров, способствуют активному развитию альтернативных способов урегулирования конфликтов. В этом контексте особую актуальность приобретает использование цифровых технологий в примирительных процедурах – медиации, переговорах, арбитража и иных механизмов, прописанных в законе.

Основная часть. В Российской Федерации, несмотря на достаточно развитую правовую базу в сфере медиации, нормативное регулирование цифровых форм примирения остается фрагментарным и требует системного анализа. Цель работы – выявить правовые особенности применения цифровых технологий в примирительных процедурах в России, проанализировать действующее законодательство и предложить направления его совершенствования. Примирительные процедуры в Российской Федерации в основном регулируются Федеральным законом от 27.07.2010 №193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» (далее – Закон о медиации) [1]. Данный закон закрепляет правовую природу медиации как добровольного процесса, основывающегося на принципах конфиденциальности, добровольности и равноправия сторон [1]. Однако в тексте закона отсутствуют прямые нормы, регулирующие использование цифровых платформ, видеоконференцсвязи или электронного документооборота. Тем не менее, возможность дистанционного проведения медиации косвенно признается через положения о свободе выбора формы взаимодействия сторон и посредника [1]. Это позволяет толковать закон в духе современных технологических реалий, однако требует дополнительной правовой определенности. Развитие цифровых технологий в правовой сфере нашло отражение в таких актах, как Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» [2] и Федеральный закон от 07.07.2003 №126-ФЗ «О связи» [3]. Эти нормативные акты создают правовую основу для использования электронных документов и дистанционного взаимодействия. Так, согласно ст. 6 закона об электронной подписи, усиленная квалифицированная электронная подпись (УКЭП) приравнивается к собственноручной подписи на бумажном документе [2]. Однако это до сих пор не позволяет сторонам заключать медиативные соглашения в электронной форме, которое будет обладать юридической силой. Во многом все это свидетельствует о наличии достаточно серьезной проблемы относительно фактического признания цифровых форм примирения, подчеркивающее отсутствие специального законодательного закрепления и несмотря на вышеприведенные нормы, возмож-

но лишь частичное применение данной формы на определенных этапах, но не на итоговом подписании медиативного соглашения. Более того, использование цифровых технологий в примирительных процедурах сопряжено с рядом правовых рисков, частности один из основополагающих плюсов данной процедуры – это конфиденциальность [1]. Однако при использовании сторонних платформ (например, MTS Link, Яндекс Телемост) возникает риск утечки данных, особенно если сервера находятся за пределами России. В этом контексте актуален Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» [4], требующий соблюдения условий обработки и хранения информации, в котором предусмотрено, что обеспечение сохранения данных в цифровой среде является обязательным компонентом их обработки. Отдельным проблемным компонентом станет то, что не все участники процесса обладают равным доступом к цифровым технологиям. Это может нарушать принцип равноправия, закрепленный в ст. 4 Закона о медиации [1], даже в том случае, когда часть процедур прямо не запрещена к проведению законом. Отсутствие реальных технических возможностей и правового закрепления применения подобных технологий для лиц с ограниченными возможностями по доступу к информационным технологиям снижает инклюзивность цифровых процедур и ставит процесс цифровизации этих отношений перед угрозой дискриминации участников. Отдельно отметим, что медиативные соглашения могут быть признаны в суде, однако их исполнение может быть затруднено из-за недобросовестности сторон или проблем, связанных с правовым статусом соглашения, которое будет приравнено к гражданско-правовой сделке. В отличие от судебных решений, медиативное соглашение не обладает принудительной силой, если оно не удостоверено судом или нотариусом [1]. При этом для эффективного внедрения цифровых технологий в примирительные процедуры необходимо: во-первых, внести в Федеральный закон от 27.07.2010 №193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» положения о расширении возможностей для дистанционной медиации, включая требования к платформам, защите данных и возможностей на предварительных стадиях использованию электронной подписи: во-вторых, разработать стандарты цифровых медиативных платформ, соответствующие требованиям законодательства о персональных данных и кибербезопасности; в-третьих, рассмотреть возможность пробных тестирований нотариального или судебного удостоверения электронных медиативных соглашений для обеспечения их исполнимости; в-четвертых, рассмотреть возможность государственной поддержке цифровой грамотности граждан в контексте альтернативных способов разрешения споров. Примеры таких нормативных подходов уже реализуются в Европейском союзе в рамках Директива 2008/52/ЕС Европейского Парламента и Совета Европейского Союза от 21 мая 2008 года «О некоторых аспектах посредничества (медиации) в гражданских и коммерческих делах» [5]. Возможность их осмысления, переработка и последующее внедрение подобных норм в российской правовой системе могла бы способствовать развитию цифровой медиации.

Заключение. Подводя общее умозаключение, отметим, что использование цифровых технологий в примирительных процедурах в Российской Феде-

рации является перспективным этапом развития правовой системы. Однако действующее законодательство не в полной мере отвечает вызовам цифровой среды. Отсутствие четких правил по дистанционной медиации, защите данных и признанию электронных соглашений создает правовую неопределенность и невозможность применения цифровых технологий на практике. Для обеспечения эффективности, конфиденциальности и доступности примирительных процедур необходимо комплексное правовое регулирование, учитывающее как технологические, так и процессуальные аспекты. Только в этом случае цифровая медиация сможет стать полноценной альтернативой традиционным формам урегулирования споров.

Список литературы

1. Федеральный закон от 27.07.2010 №193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» // СПС КонсультантПлюс.
2. Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи» // СПС КонсультантПлюс.
3. Федеральный закон от 07.07.2003 №126-ФЗ «О связи» // СПС КонсультантПлюс.
4. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» // СПС КонсультантПлюс.
5. Директива 2008/52/ЕС Европейского Парламента и Совета Европейского Союза от 21 мая 2008 года «О некоторых аспектах посредничества (медиации) в гражданских и коммерческих делах» // НПП ГАРАНТ-СЕРВИС.

В. В. Колупаева,

студент,

Томский государственный университет
систем управления и радиоэлектроники,

С. Р. Гадельшина,

магистрант,

Томский государственный университет
систем управления и радиоэлектроники

Правовые проблемы дистанционной продажи товаров и пути их решения

Аннотация. В статье исследуется актуальная проблема правового регулирования дистанционной купли-продажи, обусловленная динамичным развитием цифровизации экономики. Анализируются ключевые различия между традиционной и дистанционной моделями купли-продажи, а также выделяются их общие системные признаки. В рамках исследования рассматривается феномен потребительского экстремизма, проводится анализ правовых и практических проблем, возникающих на различных этапах совершения дистанционной сделки. В заключение формулируются пути решений выявленных коллизий.

Ключевые слова: гражданское право, цифровые технологии, потребительский экстремизм, дистанционная продажа, розничная купля-продажа, защита прав потребителей, правовые риски, проблема практики

V. V. Kolupaeva,

student,

Tomsk State University
of Control Systems and Radioelectronics,

S. R. Gadelshina,

master's student,

Tomsk State University
of Control Systems and Radioelectronics

Legal issues of distance selling of goods and ways to resolve them

Abstract. The article examines the topical issue of legal regulation of distance selling, caused by the dynamic development of the digital economy. It analyzes the key differences between traditional and distance models of sale and purchase, as well as highlighting their common systemic features. The study examines the phenomenon of consumer extremism and analyzes the legal and practical problems that arise at various stages of a distance transaction. In conclusion, it formulates ways to resolve the identified conflicts.

Keywords: civil law, digital technologies, consumer extremism, distance selling, retail sales, consumer protection, legal risks, practical issues

Введение. В наше время отношение к покупкам сильно изменилось, не обязательно приходить в конкретный магазин, достаточно открыть приложение (а можно и не одно) и искать нужный товар, покупая в один клик. Это очень удобно т.к. любую необходимую вещь можно найти в любом месте и в любое время, что стало широко применяться и использоваться. В связи с этим возникает необходимость внедрять новые нормы права для защиты прав потребителей, как экономически слабой стороны, обеспечить безопасность сделок, а также обеспечить надлежащее качество передаваемых товаров.

Дистанционная продажа товаров регулируется Гражданским кодексом Российской Федерации и Законом Российской Федерации от 7 февраля 1992 г. № 2300–1 «О защите прав потребителей» (далее – ЗОЗПП), постановлением Правительства РФ от 31 декабря 2020 г. № 2463 «Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации» (постановление Правительства РФ № 2463).

Дистанционный договор купли-продажи заключается в момент акцепта оферты на платформах маркетплейсов, т.е. покупатель изучает дистанционно характеристику и фотографии товара. Здесь возникают риски недобросовестного поведения сторон: продавец может предоставить неполную или неверную информацию о товаре (например, фотографии товара быть обработаны или характеристика написана мелким шрифтом). Однако есть вероятность недобросовестного поведения и со стороны покупателей – вернуть продавцу не подлинный товар или вернуть товар с дефектом, который был нанесен по вине покупателя или возврат не всей комплектации товара.

Возможность заказа товаров онлайн, в любое удобное время и без посещения магазинов, способствуют эмоциональным покупкам, от которых потребители в дальнейшем отказываются т.к. понимают ненужность данной вещи. В современном обществе распространена культура потребления, чем обусловлены довольно частые заказы, которые объективно потребителю не требуются.

Одной из особенностей дистанционной купли-продажи является сложность в доказывании: трудно фиксировать и доказывать обстоятельства сделки, например состояние товара при передаче, факт получения, возврат оригинальной вещи или нет.

Из-за того, что покупатель приобретает товар удаленно, существует вероятность повреждения товара при транспортировке. Потребитель отказывается принять поврежденный товар, у продавца появляются издержки в связи с необходимостью обратно доставить товар из-за вины курьера, например. При этом проблема приобретать вещи «не на месте» в том, что у покупателя нет возможно-

сти сравнить товары, поэтому чаще заказывает несколько вещей и выбирается только одно из-за чего у продавца снова возникают расходы с транспортировкой.

Выделим ряд отличий обычной розничной купли-продажи от дистанционной:

1. Электронная форма. При обычной покупке форма купли-продажи должна быть письменной, чек же является подтверждением оплаты товара. При дистанционной покупке подтверждением заказа служит номер заказа или иной способ идентификации заказа. Это позволяет покупателю получить необходимую информацию об условиях купли-продажи.

2. Ознакомление с товаром. Когда потребитель приходит заключать договор купли-продажи очно, то у него есть возможность увидеть лично вещь, рассмотреть ее, увидеть в жизни цвет и размер. При этом продавец обязан проверить качество, свойства товара или продемонстрировать использование товара, если покупатель потребует произвести эти действия.

При дистанционной купле-продаже продавец также, как в первом случае обязан предоставить потребителю полную и достоверную информацию на сайте, в буклете или в других информационных материалах, ознакомление с товаром непосредственно будет производиться только после приезда товара, т. е. после оформления заказа/покупки, а не до как при очной купле-продаже.

3. Сроки возврата. Потребитель имеет право вернуть недовольственный товар надлежащего качества в течение 14 дней, не считая дня покупки. Для дистанционной купли-продажи такой срок устанавливается в течение 7 дней, при этом продавец имеет право устанавливать и другой больший срок. Например, на таком маркетплейсе как Wildberries некоторые продавцы одежды устанавливают срок возврата 28 дней. В связи с обязанностью продавца принять возврат товара надлежащего качества возникает злоупотребление некоторых потребителей, и такое злоупотребление получило название «потребительский экстремизм».

Под потребительским экстремизмом следует понимать попытку «недобросовестного клиента, манипулируя юридическими нормами в корыстных целях, не защитить свои права, а получить определенную выгоду и доход». Потребительский экстремизм означает, что недобросовестные граждане, злоупотребляют своими правами потребителя. К организациям (юридическим лицам) данное определение, как и сам ЗОЗПП, не относится [1]. Например, необходимо потребителю приобрести платье дочке на выпускной в детский сад и делает это на платформе маркетплейсах, потребитель выкупает вещь, мероприятие проходит и если товар не потерял свои свойства, то возвращают снова в пункт выдачи под предлогом, что платье не подошло.

Сравним общие характеристики обычной розничной купли-продажи с дистанционной:

1. Являются публичным договором. При дистанционном способе продажи товара продавец обязан заключить договор розничной купли-продажи с любым лицом, выразившим намерение приобрести товар на условиях оферты в соответствии со постановлением Правительства РФ № 2463 [6].

Предложение товаров в рекламе каталогов или на маркетплейсах обращенных к неопределенному кругу лиц признается публичной офертой, если оно содержит все существенные условия (условия о предмете: наименование и количество, цена).

2. В обоих случаях есть ограничения. При осуществлении розничной торговли в месте нахождения потребителя вне торговых объектов путем непосредственного ознакомления потребителя с товаром не допускается продажа продовольственных товаров без потребительской упаковки, а также лекарственных препаратов, медицинских изделий, ювелирных и других изделий из драгоценных металлов и (или) драгоценных камней.

В дистанционной тоже есть ограничения, например, в дистанционной купле-продаже запрещена дистанционная продажа: алкогольной продукции [2], табачной продукции [5], лекарственных препаратов, которые отпускаются по рецепту [4] при этом только аптечные организации могут продавать лекарства.

В двух способах продажи, есть товары надлежащего качества, которые не подлежат возврату, например, предметы личной гигиены, ювелирные изделия, товары бытовой химии, парфюмерно-косметические товары и другие.

3. Обязанность продавца предоставить покупателю полную и достоверную информацию о товаре, об эксплуатации товара и информацию о самом продавце.

Недобросовестность покупателей при дистанционной купле-продаже заключается в игнорировании привезенного заказа по каким-либо причинам: отключил уведомление и забыл, намеренно не идет забирать из-за ненужности или приехал заказ на большую сумму, а у потребителя этих денег уже не оказалось. Рассмотрим варианты решения проблем на самом маркетплейсе, которые при этом не окажут эффективного воздействия на лицо, которое хочет злоупотребить правом, но может помочь в определенных ситуациях:

1. Сделать обязательное условие включенных уведомлений о привозе товаров с возможностью внутри приложения отключать категории оповещения о скидках и иные – данный вариант не сможет решить проблему со злоупотреблением права, если покупатель намеренно не собирается забирать, а поможет только забывчивым покупателем.

2. Обязательное пополнение определенной суммы банка маркетплейса. Девушка заказала одежды и аксессуаров на 15.000 рублей, на тот момент у нее была такая сумма, но потом снова совершала спонтанные покупки и к приезду товаров денег не осталось, поэтому она решила проигнорировать приезд товаров. В связи с этим при заказе стоит иметь счет, на который переводится либо вся сумма, либо какой-то процент от суммы всего заказа. Так как часть денежных средств будет уплачена, то потребитель точно не проигнорирует приезд заказа, при этом если товары не были покупателем выкуплены, то сумма возвращается последнему. В полной мере проблема также не решится.

3. Использовать специальные сервисы, где будет информация о проценте выкупа потребителя товаров.

Один из сервисов, который поможет продавцам бороться с недобросовестностью покупателей это Федеральная База Неблагонадежных Покупателей.

Данная база должна быть государственной, а не частной, чтобы обеспечить регулирование и контроль над системой. «Федеральная База является хорошим вариантом сдерживания недобросовестных покупателей, поскольку если организация узнает, что к ним пришел клиент, внесенный в нее, она может оказать в получении услуги. Конечно, покупатель, которому отказали, может оставить плохой отзыв или обратиться к руководству, но в таком случае организация может аргументировать свой отказ тем, что гражданин находится в «черном списке» и покупатель может обратиться с жалобой в суд» [7. С. 348].

Если потребитель злоупотребляет своим правом, то вводить определенные ограничения, например, ограничение в сумме (посмотреть по статистике на какую сумму человек забирает заказы, а на какую игнорирует) на определенный период или ограничение единиц товаров на конкретный период (за 2 недели возможно заказать 2 товара, например) или смешанный вариант первых двух. Минус данной идеи в том, что в данном случае у экономически слабой стороны не будет гарантии его прав, а также возможно злоупотребление уже со стороны продавца и вероятность отказывать покупателю в заключении договора без объективных обстоятельств, что является незаконным для публичного договора.

Решать проблему необходимо на законодательном уровне и нужно внести дополнение о злоупотреблении правом со стороны покупателя. Во-первых, внедрить в закон «О защите прав потребителей» определение «злоупотребление правом со стороны потребителя».

Признаки, характеризующие явление злоупотребление правом:

1. Наличия права, которым злоупотребляют.

Такое право должно быть у лица, чтобы он мог выйти за его пределы. Если такого права нет, то это будет являться незаконным требованием.

2. Недобросовестность при осуществлении права.

Оценивая действия сторон как добросовестные или недобросовестные, следует исходить из поведения, ожидаемого от любого участника гражданского оборота, учитывающего права и законные интересы другой стороны, содействующего ей, в том числе в получении необходимой информации. По общему правилу пункта 5 статьи 10 ГК РФ добросовестность участников гражданских правоотношений и разумность их действий предполагаются, пока не доказано иное [3].

3. Негативные последствия.

Злоупотребление правом нарушает чьи-то права или законные интересы, причиняет вред или создает условия для этого [8].

4. Наличие умысла.

Из п. 1 ст. 10 ГК РФ следует, что злоупотребление правом – заведомо недобросовестное осуществление гражданских прав. Исходя из этого можно предположить, что для злоупотребления правом необходим умысел.

Предлагаемый вариант термина:

Злоупотребление правом со стороны потребителя – это намеренное осуществление потребителем права, данного ему законом или договором, с намерением извлечь выгоду, не исполняя или исполняя в меньшем объеме обязатель-

ство со своей стороны или причинить убытки или иные негативные последствия контрагенту.

В случае если обнаружено злоупотребление, например, покупают новогодние елочные игрушки, украшают елку, а после праздника возвращают товар (говорим про ситуации, когда товар качественный).

Чтобы выявить злоупотребление правом необходимо сопоставить следующие факты:

1. Праздники. Если тематический товар (костюмы новогодние, например, или атрибуты праздника Хэллоуина) возвращают после самих праздников, то вероятнее товар использовался уже по назначению.

2. Количество. При заказе большого количества единиц однотипных товаров в большинстве случаев часть из них оформляется на возврат.

3. Типы вещей. В интернете имеются случаи, когда пользователи заказывают на маркетплейсах навоз и не забирают его. Такой тип товара создают сотрудникам и посетителям неудобства, поэтому для такого рода вещей стоит либо ограничить срок хранения (сутки, например), включить платное ожидание после того, как вещь не забрали или ограничить продажу для подобных вещей на маркетплейсах.

Чтобы проверить использовал ли потребитель товар (вещь, например) можно с помощью экспертизы, если будет доказано, что вещь ношенная, то потребитель обязан компенсировать ее стоимость.

Далее после доказывания, что товар был уже использован потребитель обязан выплатить не только сумму экспертизы, но и убытки на перевозку.

Заключение. Государство стремится защитить экономически слабую сторону – потребителя, но даже такая сторона злоупотребляет своими правами и в таком случае, необходимо ввести меры для защиты и продавца.

Список литературы

1. Верховный суд обобщил практику по защите прав потребителей. URL: <https://www.consultant.ru/legalnews/26748/> (дата обращения 14.08.2025).

2. О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции: Федеральный закон от 22.11.1995 № 171-ФЗ (ред. от 31.07.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_8368/ (дата обращения 19.08.2025).

3. О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации: Постановление Пленума Верховного Суда РФ от 23.06.2015 № 25. URL: https://www.consultant.ru/document/cons_doc_LAW_181602/ (дата обращения 10.08.2025).

4. Об обращении лекарственных средств: Федеральный закон от 12.04.2010 № 61-ФЗ (ред. от 23.07.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_99350/ (дата обращения 10.08.2025).

5. Об охране здоровья граждан от воздействия окружающего табачного дыма, последствий потребления табака или потребления никотинсодержащей

продукции: Федеральный закон от 23.02.2013 № 15-ФЗ (ред. от 28.12.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_142515/ (дата обращения 19.08.2025).

6. Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства РФ от 31.12.2020 № 2463 (ред. от 17.05.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_373622/ (дата обращения 16.08.2025).

7. Сторожева А. Н., Дадаян Е. В., Горелова А. С. Потребительский экстремизм // Право и государство: теория и практика. 2025. № 4.

8. Что такое злоупотребление правом и какие последствия оно влечет: URL: <https://clck.ru/3Nхра6> (дата обращения: 21.08.2025).

Д. К. Кононенко,
студент,
Нижегородский государственный университет
имени Н.И. Лобачевского

Юридические аспекты возникновения авторских прав на генерируемые искусственным интеллектом произведения: подход России и США

Аннотация. Статья посвящена вопросу возникновения авторских прав на произведения, при создании которых участие человека ограничилось вводом текстового запроса искусственному интеллекту. Цель исследования – сравнить подходы к регулированию данной проблемы в Российской Федерации и США, опираясь на известные прецеденты и позиции государственных органов. В работе обосновывается вывод об отсутствии в настоящее время однозначного правового режима результатов деятельности ИИ и рассматриваются возможные пути разрешения этой неопределенности, включая введение особого правового режима или отнесение таких результатов к общественному достоянию.

Ключевые слова: искусственный интеллект, творческий вклад, авторское право, исключительное право, пользовательское соглашение, правообладатель, особый правовой режим

D. K. Kononenko,
student,
National Research Lobachevsky State University
of Nizhny Novgorod,

Legal aspects of the emergence of copyrights to works generated by artificial intelligence: the approach of Russia and the USA

Abstract. The article is devoted to the issue of the emergence of copyrights to works in the creation of which human participation was limited to entering a text query to artificial intelligence. The purpose of the study is to compare approaches to regulating this problem in the Russian Federation and the United States, based on well-known precedents and positions of government agencies. The paper substantiates the conclusion that there is currently no unambiguous legal regime for the results of AI activities and considers possible ways to resolve this uncertainty, including the introduction of a special legal regime or the attribution of such results to the public domain.

Keywords: artificial intelligence, creative contribution, copyright, exclusive right, license agreement, terms of service, special legal regime

Введение. Технологии искусственного интеллекта развиваются с огромной скоростью, как в России, так и во всем мире. Например, к 2025 году разработки крупнейших российских компаний – «Kandinsky», «GigaChat» – от ПАО

«Сбербанк», «Шедеврум» и «YandexGPT» – от ООО «Яндекс», уже активно функционируют и используются для генерации изображений и текстов, демонстрируя реальные достижения отечественного бизнеса в сфере искусственного интеллекта и глубокую заинтересованность в развитии технологий искусственного интеллекта. Кроме того, на данный момент уже функционируют такие нейронные сети, как Chat GPT 5, MidJourney, Adobe Photoshop Firefly и другие, которые могут сгенерировать научную работу, литературное произведение, код, нарисовать картину, сделать приложение или сайт и т. д.

На сегодняшний день в большинстве случаев, когда произведение генерируется искусственным интеллектом человек принимает формальное участие в его создании. Пользователь лишь формулирует идею или концепцию посредством ввода соответствующих команд технологии и не может предсказать конечный результат, так как ИИ на основе заложенных в него данных самостоятельно без творческого участия человека генерирует произведение, в связи с чем возникает вопрос об охраноспособности таких результатов и возможности их коммерциализации.

Основная часть

Практика США. Подход США к вопросу возникновения авторских прав на генерируемые искусственным интеллектом произведения сформировался через решения и акты государственных органов, а именно Бюро по авторским правам США (далее по тексту – Бюро).

Например, в 2023 году Бюро не признало право авторства на работу Мэтью Аллена «Пространственный театр с искусственным интеллектом», сгенерированную нейронной сетью Midjourney, несмотря на то, что она заняла первое место на артистической ярмарке штата Колорадо, объясняя это тем, что работа является скорее машинной, чем человеческой, и «действия г-на Аллена не делают его автором изображения Midjourney, поскольку его единственным вкладом в создание изображения Midjourney был ввод текстовой подсказки, которая его создала» [10]. Также ведомство указало, что ключом к защите авторских прав является участие человека в рассматриваемом произведении и окончательный творческий контроль над ним. Бюро сделало вывод, что этапы процесса создания работы в конечном счете зависели от того, как система Midjourney обрабатывала запросы мистера Аллена, а также отметило, что подсказки влияют на то, что генерирует Midjourney, но их интерпретация и конечный результат зависят от данных обучения системы.

Кроме того, в марте 2023 года Бюро авторских США выпустило руководство по регистрации произведений, созданных с помощью генеративного ИИ, а 29 января 2025 опубликовала 2 часть Отчета об искусственном интеллекте. В руководстве объясняется, что при рассмотрении заявки на регистрацию ведомство будет спрашивать – «является ли работа в основном результатом творчества человека, а компьютер (или другое устройство) лишь вспомогательным инструментом, или же традиционные элементы авторства в работе (литературное, художественное или музыкальное выражение, или элементы отбора, аранжировки и т. д.) на самом деле были задуманы и выполнены не человеком, а машиной» [7]. Отмечается, что при анализе материалов, созданных искусствен-

ным интеллектом, ведомство должно определить, когда пользователь–человек может считаться «создателем» результатов, полученных с помощью ИИ.

Во второй части Отчета об искусственном интеллекте Бюро авторских прав США разъяснило, что произведения искусства, созданные с помощью ИИ, могут быть защищены авторским правом – но только если в них присутствует достаточный уровень человеческого творчества. Ведомство отмечает, что простого ввода текстового запроса недостаточно, но, если человек модифицирует, структурирует или творчески интегрирует ИИ-контент, он может претендовать на защиту авторских прав. При этом Бюро отказалось распространять авторские права на полностью ИИ-сгенерированный контент, подчеркнув, что «авторское право не распространяется на материалы, созданные исключительно с помощью ИИ, или материалы с недостаточным контролем человека над выразительными элементами» [8]. Также стоит отметить, что еще в 2014 году Бюро регистрации авторских прав США выпустило Сборник практики регистрации авторских прав США, в частности, указав, что «ведомство не будет регистрировать произведения, созданные с помощью машины или простого механического процесса, который работает случайным образом или автоматически без какого-либо творческого участия или вмешательства человека–автора» [9].

Искусственный интеллект и произведения в России. На сегодняшний день политику государства в отношении искусственного интеллекта определяет Указ Президента Российской Федерации от 10.10.2019 N 490 (ред. от 15.02.2024) "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года"). Также до 2024 года действовало распоряжение Правительства РФ от 19.08.2020 2129–р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» (далее – Концепция развития искусственного интеллекта).

В сущности, данные нормативные акты определяют принципы, цели, задачи, направления, проблемы развития и использования технологий искусственного интеллекта. Несмотря на то, что Концепция развития искусственного интеллекта действовала до 2024 года – установленные ей задачи и проблемы до сих пор не решены. Одной из таких проблем является совершенствование порядка охраны прав на результаты интеллектуальной деятельности, созданные при помощи искусственного интеллекта [3].

Согласно действующим нормам, автором результата интеллектуальной деятельности может быть только гражданин, творческим трудом которого создан такой результат, а использование технологий искусственного интеллекта при создании результата интеллектуальной деятельности может быть расценено как несоответствие критерию творческого вклада в широком смысле. Кроме того, согласно позиции Верховного Суда Российской Федерации, выраженной в п. 80 постановления Пленума ВС РФ от 23 апреля 2019 года № 10 «О применении части четвертой Гражданского Кодекса Российской Федерации» результаты, созданные с помощью технических средств в отсутствие творческого характера деятельности человека, объектами авторского права не являются.

Законодательство России не устанавливает понятие и ключевые признаки творческого вклада и творческого труда. Однако, как минимум, Гражданский кодекс Российской Федерации закрепляет, что авторские права не распространяются на идеи, концепции и т. д. И как уже было ранее отмечено, в большинстве случаев, когда произведении генерируется искусственным интеллектом человек принимает формальное участие в его создании, формулируя идею и концепцию произведения. В данном случае, основываясь на действующих нормах и на классическом понимании творческого вклада, ввод команд пользователем технологии искусственного интеллекта не является творческим трудом.

На данный момент отношения между правообладателем искусственного интеллекта и его пользователем по поводу возникновения и принадлежности прав на сгенерированные произведения регулируются пользовательскими соглашениями об использовании соответствующего сервиса искусственного интеллекта (далее по тексту – Пользовательские соглашения). Такие соглашения содержат условия о принадлежности или отчуждении всех исключительных прав в пользу правообладателя сервиса искусственного интеллекта или его пользователя, а также лицензионные условия использования результатов деятельности искусственного интеллекта.

Например, согласно пункту 6.2. Соглашения об использовании сервиса GigaChat для физических лиц – Клиент, загружающий (передающий) Запрос в Сервис, является обладателем исключительного права на Сгенерированный Контент, созданный на основании такого Запроса [4].

В соответствии с пунктом 5.7. и 5.2. Пользовательского соглашения об использовании Сервиса Kandinsky – Исключительное право на Сгенерированный Контент, являющийся результатами интеллектуальной деятельности/средствами индивидуализации, принадлежит Пользователю. При этом Пользователь с момента создания Сгенерированного Контента с Использованием Сервиса предоставляет Банку простую (неисключительную) безотзывную, безвозмездную лицензию на использование Сгенерированного Контента в течение всего срока действия исключительного права на территории всего мира [5].

Таким образом, указанные положения пользовательских соглашений устанавливают, что ПАО «Сбербанк» (правообладатель Сервиса Kandinsky и GigaChat) признает принадлежность Пользователю исключительных прав на все сгенерированные по его запросу произведения.

Другим примером является Соглашение об условиях использования сервиса «Шедеврум», правообладателем которого является ООО «Яндекс». Однако после анализа Соглашения об условиях использования сервиса «Шедеврум» автор настоящей работы пришел к выводу, что в нем не содержится четкого пункта по вопросу возникновения и принадлежности исключительных прав на сгенерированные Сервисом «Шедеврум» произведения.

Думается, что по соглашению именно ООО «Яндекс» является обладателем исключительных прав на сгенерированные их Сервисом произведения. Этот вывод следует из пункта 3.3 пользовательского соглашения, в соответствии с которым ООО «Яндекс» предоставляет Пользователю право использование сгенерированных произведений исключительно в личных некоммерческих це-

лях. Любое коммерческое использование допускается только при условии предварительного согласования с Яндексом.

Таким образом, соглашение об условиях использования сервиса «Шедевр» устанавливает, что именно ООО «Яндекс» является лицензиаром в отношении всех генерируемых сервисом результатов, что означает принадлежность компании исключительных прав на такие результаты.

Между тем, встает следующий вопрос: имеют ли юридическую силу положения в Пользовательском соглашении об использовании ИИ сервиса, которые определяют правообладателя сгенерированного контента и пределы его использования? Ведь права на произведения возникают на основании закона, а не соглашения. В силу п. 3 ст. 1228 ГК РФ исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. И как уже отмечалось ранее, в рассматриваемой ситуации, генерируемые искусственным интеллектом произведения, в создании которых участие человека ограничилось исключительно вводом текстового запроса – не отвечают критериями охраноспособности и соответственно, не являются результатами интеллектуальной деятельности, не могут иметь автора и, следовательно, исключительное право на такие произведения не возникает [2].

В пользовательском соглашении об использовании ИИ сервиса можно установить условия о передаче только имеющегося исключительного права и предоставить право использования произведения в определенных пределах. В связи с чем, положения соглашения, которые определяют возникновение исключительных прав на генерируемые искусственным интеллектом произведения, представляются ничтожными.

Автор настоящей работы солидарен с позицией, выраженной в работе В.А. Дозорцева: «результаты, полученные как итог функционирования технических средств, неохраноспособны. Автором такого результата не может быть признана ни бездушная машина, неспособная к творчеству, ни ее создатель, ни автор программы (в случае ЭВМ), на основании которой получен результат, ни оператор технического средства или его собственник» [1].

Правительство Российской Федерации также признает, что «существующий правовой режим не обеспечивает правовую охрану результатов деятельности систем искусственного интеллекта, полученных без творческого вклада человека, а потенциальная "неохраноспособность" результатов деятельности, полученных с использованием систем искусственного интеллекта и робототехники, может дестимулировать разработку и внедрение таких систем» [3].

Заключение. Таким образом, к настоящему моменту сложилась ситуация, при которой результаты, созданные искусственным интеллектом автономно, без творческого участия человека, не признаются объектами интеллектуальной собственности. Действующий правовой режим не предоставляет им охраны, поскольку традиционное авторство требует творческого вклада личности.

Такая правовая неопределенность создает серьезные риски. Отсутствие гарантий охраны и возможности распоряжения результатами, сгенерированными ИИ, может замедлить темпы разработки и внедрения передовых технологий,

так как инвесторам и разработчикам неясен правовой режим и коммерческий потенциал таких продуктов.

В связи с этим представляется необходимым разработать специальный правовой режим. Его целью должно стать признание и регулирование оборота результатов интеллектуальной деятельности, полученных с использованием систем искусственного интеллекта без непосредственного творческого вмешательства человека. Это позволит не только защитить инвестиции в данную сферу, но и создать четкие правила для их дальнейшего развития и коммерциализации.

Список литературы

1. Дозорцев В.А. Интеллектуальные права: Понятие. Система. Задачи кодификации: Сб. статей. М., 2005.
2. Колобова Е. Ю. Проблемы гражданско-правовой защиты прав на произведения, созданные с помощью нейросетей // Молодой ученый. 2025. № 2 (553). С. 214–216.
3. Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // Собрание законодательства РФ. 2020, № 35, ст. 5593.
4. Соглашение об использовании сервиса GigaChat для физических лиц (ред. от 19.08.2025). URL: <https://developers.sber.ru/docs/ru/policies/gigachat-agreement/individuals> (дата обращения 08.09.2025).
5. Пользовательское соглашение об использовании Сервиса Kandinsky. URL: <https://www.sberbank.com/common/img/uploaded/files/promo/kandinskiy-terms/kandinskiy-terms-of-use.pdf> (дата обращения 08.09.2025).
6. Условия использования сервиса «Шедеврум» (редакция от 24.06.2025г.). URL: https://yandex.ru/legal/shedevrum_termsfuse/ru/ (дата обращения 08.09.2025).
7. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16,190, 16,192 (Mar. 16, 2023) (“AI Registration Guidance”).
8. U.S. Copyright Office, Copyright and Artificial Intelligence, Part 2: Copyrightability. URL: <https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf>
9. Copyright Office, Compendium of U.S. Copyright Office Practices (3d ed. 2014). § 313.2. URL: <https://www.copyright.gov/comp3/docs/compendium-12-22-14.pdf>
10. Second Request for Reconsideration for Refusal to Register Théâtre D’opéra Spatial (SR # 1-11743923581; Correspondence ID: 1-5T5320R). URL: <https://www.copyright.gov/rulings-filings/review-board/docs/Theatre-Dopera-Spatial.pdf>

А. С. Кочеткова,

студент,

Брянский государственный университет
имени академика И. Г. Петровского,

П. А. Петухова

студент,

Брянский государственный университет
имени академика И. Г. Петровского

Использование виртуальной аутопсии в расследовании преступлений

Аннотация. В статье рассматривается феномен виртуального вскрытия как инновационного метода в системе уголовного судопроизводства и судебной медицины, формирующегося на стыке цифровых технологий и правоприменительной практики. Авторы анализируют понятие и сущность виртуальной аутопсии, ее преимущества и ограничения, а также актуальные проблемы правового регулирования в условиях отсутствия прямого нормативного закрепления в российском законодательстве. Особое внимание уделено вопросам допустимости результатов виртуального вскрытия в качестве доказательств, этическим и культурным нормам, а также проблемам технической и организационной реализуемости данной методики применительно к российским реалиям.

Ключевые слова: виртуальное вскрытие, виртуальная аутопсия, цифровизация, судебная медицина, уголовное судопроизводство, доказательства, судебно-медицинская экспертиза, уголовно-процессуальное право, 3D-томография, правовое регулирование

A. S. Kochetkova,

student,

Bryansk State University
named after academician I. G. Petrovsky,

P. A. Petukhov

student,

Bryansk State University
named after Academician I. G. Petrovsky

The use of virtual autopsy in crime investigation

Abstract. The article examines the phenomenon of virtual autopsy as an innovative method in the system of criminal proceedings and forensic medicine, which is formed at the intersection of digital technologies and law enforcement practice. The authors analyze the concept and essence of virtual autopsy, its advantages and limitations, as well as current problems of legal regulation in the absence of direct regulatory consolidation in Russian legislation. Particular attention is paid to the admissibility of the results of virtual autopsy as evidence, ethical and cultural norms, as well as

problems of technical and organizational feasibility of this technique in relation to Russian realities.

Keywords: virtual autopsy, virtual autopsy, digitalization, forensic medicine, criminal proceedings, evidence, forensic medical examination, criminal procedure law, 3D tomography, legal regulation

Введение. В последнее время с быстротечным развитием научно-технического прогресса в нашу жизнь активно внедряются цифровые технологии [1]. Вопросы внедрения инновационных решений в деятельность правоохранительных органов сегодня также актуальны.

Цифровизация – это процесс перехода от аналоговых форм хранения, обработки и передачи информации к цифровым, предполагающий использование современных технических средств и программного обеспечения для автоматизации и повышения эффективности деятельности государственных структур. Одним из проявлений цифровизации, затрагивающим сферу уголовного судопроизводства и судебной медицины, является использование технологий виртуального вскрытия (также известного как «виртуальная аутопсия» или «виртопсия»).

Под виртуальными технологиями в данном контексте понимаются специализированные цифровые решения, применяемые для дистанционного, неинвазивного или визуализированного анализа объектов и процессов, включая 3D-сканирование, томографию, цифровую реконструкцию и другие методики.

На сегодняшний день виртуальные технологии занимают все более важное место в расследовании преступлений, судебной экспертизе и криминалистике. Их применение позволяет повысить точность собираемой информации, минимизировать человеческий фактор и ошибки, ускорить процедуры расследования и обеспечить дополнительную объективность принимаемых решений. Технология виртуального вскрытия как один из аспектов цифровизации уголовного судопроизводства представляет собой метод неинвазивного исследования тела умершего с использованием современных средств визуализации, таких как компьютерная томография (КТ), магнитно-резонансная томография (МРТ) и трехмерное моделирование. В отличие от традиционного патологоанатомического вскрытия, виртуальная аутопсия не требует физического вмешательства в тело, что может иметь принципиальное значение как с медицинской, так и с этической и правовой точки зрения.

В.А. Дударев отмечает, что современные глобальные изменения, экспоненциальное развитие науки и техники, изменение социальных укладов ускорили преобразования и в праве. Новые тенденции активно внедряются и применяются в уголовном судопроизводстве. Цифровые технологии не только внедряются в уголовный процесс, но и активно его развивают и даже преобразуют [2. С. 112–113].

Основная часть. Применение технологии виртуальной аутопсии актуально по следующим факторам.

Во-первых, наблюдается растущая потребность в более точных и оперативных методах установления причины смерти, особенно в условиях, когда

традиционное вскрытие невозможно или затруднено по религиозным, культурным или юридическим причинам.

Во-вторых, виртуальные технологии могут стать действенным инструментом повышения эффективности расследования преступлений, связанных с насильственной смертью, профессиональными и медицинскими ошибками, дорожно-транспортными происшествиями и другими случаями. Как отмечает А.Р. Хаметова виртуальное вскрытие представляет собой относительно новое направление в сфере судебной медицины и судебной экспертизы. Метод был впервые апробирован в конце XX века в Швейцарии, а к началу XXI века получил широкое распространение в странах Европы, США, Японии, Израиле. Его основой является высокоточная визуализация тела с помощью современных средств медицинской томографии, с последующим построением трехмерной модели, доступной для анализа экспертами. Такая методика позволяет с высокой степенью достоверности определить причины смерти, механизмы получения повреждений, их локализацию, а также выявить другие важные признаки, имеющие значение для следствия [8. С. 299].

В России применение виртуального вскрытия пока не получило широкого распространения, хотя научные исследования в этом направлении ведутся с начала 2010-х годов. Появление первых пилотных проектов в крупных медицинских и судебно-экспертных учреждениях свидетельствует о растущем интересе к методике со стороны профессионального сообщества. Однако, несмотря на очевидные преимущества, применение виртуальной аутопсии в следственной практике по-прежнему остается эпизодическим, что обусловлено как техническими ограничениями, так и отсутствием четкой нормативной регламентации.

С правовой точки зрения использование виртуального вскрытия должно оцениваться с позиции норм Конституции РФ, уголовно-процессуального законодательства, законодательства о судебно-экспертной деятельности и законодательства в области здравоохранения.

Статьей 21 Конституции Российской Федерации [5] установлен запрет на унижение человеческого достоинства, что приобретает особую значимость при производстве вскрытия тел умерших, особенно в случаях, когда традиционная процедура вызывает неприятие со стороны родственников по религиозным или этическим основаниям. В этом контексте виртуальная аутопсия может рассматриваться как альтернатива, обеспечивающая более гуманное отношение к телу умершего и правам его семьи.

Статьей 178 Уголовно-процессуального кодекса Российской Федерации (далее – УПК РФ) [6] предусмотрена возможность назначения судебно-медицинской экспертизы в целях установления причины смерти, а также в случае необходимости – проведения вскрытия тела. Однако в УПК РФ отсутствует прямое упоминание или легитимация методов виртуального вскрытия, что создает правовую неопределенность. Статья 195 УПК РФ определяет общее содержание постановления о назначении экспертизы, в том числе указание методов исследования, однако конкретизация применяемых методик остается за экспертом.

Кроме того, в соответствии с Федеральным законом от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской

Федерации» [7], эксперт имеет право использовать современные научно-технические средства и методы, однако они должны быть признаны научно обоснованными и соответствовать установленным стандартам. На практике это означает необходимость официального признания виртуальной аутопсии в качестве допустимого экспертного метода, что пока не получило отражения в нормативных актах Минздрава или Минюста Российской Федерации.

Существуют и иные правовые проблемы, связанные с применением виртуального вскрытия. В частности, возникает вопрос допустимости использования таких результатов в качестве доказательств в уголовном процессе. Согласно статье 74 УПК РФ, доказательствами по делу могут быть любые данные, полученные в соответствии с законом. Следовательно, если виртуальная аутопсия будет признана легитимным и научно обоснованным методом, ее результаты могут иметь доказательственное значение.

Наряду с этим необходимо учитывать, что проведение виртуального вскрытия требует наличия дорогостоящего оборудования – в первую очередь, компьютерных томографов, магнитно-резонансных томографов и специализированного программного обеспечения для обработки и визуализации полученных данных. Большинство региональных судебно-медицинских учреждений в России в настоящее время не располагают необходимыми техническими средствами, что существенно ограничивает возможность повсеместного внедрения данной методики.

Это поднимает вопрос не только о правовой допустимости виртуального вскрытия, но и о технической и организационной готовности системы здравоохранения и уголовного судопроизводства к ее практическому применению.

Следует также отметить, что вопрос допустимости виртуальной аутопсии неразрывно связан с этическими и культурными аспектами. В ряде религиозных конфессий существует категорический запрет на вскрытие тела после смерти, что нередко становится источником конфликтов между следственными органами и родственниками умершего. В таких случаях виртуальное вскрытие может выступать как компромиссное решение, позволяющее соблюсти требования закона и одновременно уважить религиозные чувства граждан. Конституционные принципы свободы совести и вероисповедания, закрепленные в статье 28 Конституции Российской Федерации, а также гарантии охраны личной и семейной тайны, закрепленные в статье 23, поддерживают необходимость поиска таких альтернатив.

Кроме того, вопросы применения новых цифровых методов в уголовном процессе должны решаться с учетом принципа допустимости доказательств и обеспечения состязательности сторон. Применение виртуального вскрытия не должно нарушать право стороны защиты на ознакомление с методикой исследования, возможность поставить перед экспертом вопросы и представить альтернативное заключение.

Соответственно, необходимо не только законодательно закрепить допустимость такого вида экспертизы, но и создать четкие процессуальные механизмы обеспечения прав участников уголовного судопроизводства при использовании данных технологий.

Положительным примером в этом контексте может служить зарубежная практика. Так, в Швейцарии, где и была впервые апробирована методика виртуальной аутопсии, подобные исследования проводятся с 2000-х годов на базе университетских клиник и судебно-медицинских учреждений. В ряде случаев виртуальное вскрытие проводится как самостоятельное исследование, а в иных – как предварительный этап перед традиционным вскрытием. В Германии, Австрии, Великобритании и других странах также сформировалась практика использования КТ и МРТ в качестве части судебно-медицинской экспертизы. Особенно активно технология используется в случаях авиакатастроф, террористических актов, массовых поражений, когда необходимо оперативно идентифицировать тела, установить причины и механизмы повреждений, не прибегая к классическому вскрытию каждого погибшего.

В России наиболее заметные шаги в направлении внедрения виртуальной аутопсии предпринимаются в рамках научных и пилотных проектов. Так, в Институте судебной медицины Сеченовского университета в Москве проводятся исследования возможностей применения компьютерной томографии в судебно-медицинской практике. На базе отдельных учреждений также разрабатываются программы интеграции цифровой визуализации в судебно-экспертные процедуры. Однако до сих пор отсутствует единый порядок проведения виртуального вскрытия, его процессуальный регламент, а также система оценки достоверности и допустимости получаемых результатов. Это создает риски произвольного толкования и ограничивает сферу практического применения технологии.

Виртуальная аутопсия обладает рядом преимуществ: высокой точностью, возможностью сохранения и повторного анализа результатов, а также этической нейтральностью. В отличие от классического вскрытия, данные в цифровом формате могут быть представлены в суде и использованы при возникновении новых обстоятельств, что повышает объективность и снижает риск ошибок. Однако ее внедрение требует комплексного правового регулирования: признания виртуального вскрытия как допустимого метода судебной экспертизы, определения критериев допустимости доказательств, закрепления технических стандартов и единого протокола проведения. Будущее виртуальной аутопсии в России зависит от готовности властей внести соответствующие изменения в законодательство. При наличии необходимой правовой базы и технологической поддержки она может стать частью уголовного судопроизводства, особенно в ситуациях, когда традиционное вскрытие затруднено или невозможно.

Таким образом, виртуальное вскрытие становится важным инструментом расследования, позволяя обеспечить гуманность, точность и воспроизводимость результатов. Для его эффективного применения необходимо создать прозрачный и юридически определенный механизм проведения таких процедур.

Так, согласно статье 195 УПК РФ, судебная экспертиза может быть назначена по уголовному делу для установления обстоятельств, имеющих значение для дела, если для этого необходимы специальные знания в области науки, техники, искусства или ремесла. Из содержания данной нормы следует, что законодатель не ограничивает методы, которые могут применяться экспертами при проведении исследования. Следовательно, использование современных техно-

логий, таких как компьютерная томография и магнитно-резонансная томография, в рамках судебно-медицинской экспертизы допустимо, если они направлены на достижение целей, предусмотренных статьей 195 УПК РФ. Более того, в соответствии с частью 1 статьи 196 УПК РФ, обязательное назначение судебно-медицинской экспертизы предусмотрено в случае необходимости установления причин смерти. Статья 178 УПК РФ также допускает производство эксгумации для установления причин смерти в случае необходимости.

Таким образом, с правовой точки зрения не существует запрета на использование альтернативных методов исследования, в том числе и неинвазивных, при условии, что они обеспечивают достоверность, полноту и объективность выводов эксперта.

Согласно статье 17 Конституции Российской Федерации права и свободы человека признаются в соответствии с международными нормами. Европейский суд по правам человека в ряде решений подчеркивает необходимость соблюдения баланса между интересами расследования и уважением к телу умершего. В частности, в деле *Jalloh v. Germany* указано, что вмешательства в тело должны быть обоснованными, пропорциональными и сопровождаться правовыми гарантиями. Это позволяет рассматривать виртуальное вскрытие как гуманную альтернативу, при наличии соответствующего нормативного регулирования [3].

Отдельного внимания требует вопрос допустимости результатов виртуальной аутопсии в качестве доказательств. В соответствии со статьей 74 УПК РФ, доказательствами могут быть заключения экспертов, если они соответствуют требованиям закона. Статья 80 УПК РФ уточняет, что такое заключение признается доказательством при наличии научной обоснованности и соблюдении установленного порядка. Следовательно, признание результатов виртуального вскрытия требует привлечения квалифицированных специалистов, использования утвержденных методик и надлежащего оформления заключения. Для этого необходимо разработать методические рекомендации Минздрава и Минюста, обеспечивающие единообразие процедуры. Только при таких условиях можно говорить о формировании устойчивой судебной практики, признающей результаты виртуальной аутопсии допустимыми доказательствами.

Несмотря на все потенциальные преимущества виртуальной аутопсии, ее широкое распространение в российской правоприменительной практике следует сказать и о минусах.

Во-первых, это проблема кадрового обеспечения. Проведение и интерпретация результатов томографического исследования требует высокой квалификации специалистов не только в области судебной медицины, но и в области радиологии, информационных технологий и трехмерной реконструкции. Существующая система подготовки судебно-медицинских экспертов, как правило, не включает в себя достаточный объем учебных курсов, направленных на работу с такими технологиями. Это требует реформирования образовательных стандартов и создания специализированных программ повышения квалификации [4. С. 188].

Во-вторых, развитие и внедрение виртуального вскрытия требует координации между Минздравом, МВД, Следственным комитетом, Минюстом и судебной системой, поскольку эта технология затрагивает здравоохранение, су-

дебно-экспертную деятельность, уголовное судопроизводство и защиту персональных данных. Поэтому нормативное регулирование должно учитывать интересы всех участников и обеспечивать согласованность правовой базы.

Заключение. Таким образом, виртуальное вскрытие – важный этап цифровизации уголовного процесса и модернизации судебной медицины. Оно повышает точность установления причин смерти, учитывает права человека, этические, культурные и религиозные аспекты, особенно в случаях, когда традиционное вскрытие невозможно или затруднено. Виртуальное вскрытие – это не просто инновация, а инструмент повышения эффективности и гуманизма уголовного судопроизводства. Его интеграция требует адекватного правового регулирования, соответствующего уровню технологического развития и поддерживаемого государством, экспертами и профессиональным сообществом.

Список литературы

1. Дударев В. А. Опыт цифровизации уголовного судопроизводства в зарубежных странах и Российской Федерации / В. А. Дударев // Международное уголовное право и международная юстиция. 2022. № 2. С. 15–17.

2. Дударев В. А. Влияние цифровых технологий на проведение допроса несовершеннолетних: проблемные вопросы / В. А. Дударев // Высокотехнологичное право: современные вызовы: материалы IV Международной межвузовской научно-практической конференции, Москва–Красноярск, 17–20 февраля 2023 года. Том Часть 1. Красноярск: Красноярский государственный аграрный университет, 2023. С. 112–119.

3. ЕСПЧ: Решение властей о кремации тела и тайном захоронении террориста нарушает права его близких // Адвокатская газета Орган Федеральной палаты адвокатов РФ: [сайт]. URL: <https://www.advgazeta.ru/novosti/espch-reshenie-vlastey-o-krematsii-tela-i-taynom-zakhoronении-terrorista-narushaet-prava-ego-blizkikh/> (дата обращения: 01.08.2025).

4. К вопросу об использовании результатов виртуальной аутопсии (виртопсии) в ходе расследования преступлений: научный обзор / А.Б. Оракбаев, Ж.К. Курмангали, Е.Н. Бегалиев [и др.] // Судебная медицина. 2023. Т. 9, № 2. С. 183–192.

5. Конституция Российской Федерации: (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства Российской Федерации. 2014. № 4. Ст. 445.

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 24.12.2001. № 52. Ст. 4921.

7. Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» от 31.05.2001 № 73-ФЗ (ред. от 22.07.2024) // Собрание законодательства РФ. 04.06.2001. № 23. Ст. 2291

8. Хаметова А.Р. Виртопсия – инновация в мире криминалистики / А.Р. Хаметова // Закон и право. 2024. № 5. С. 298–304.

**Право на цифровое забвение после смерти:
пробелы правового регулирования и пути их устранения**

Аннотация. В статье исследуется проблема реализации «права на забвение» после смерти субъекта персональных данных в российском законодательстве. Целью исследования является выявление правовой коллизии между нормами, регулирующими посмертную обработку персональных данных, и механизмом удаления информации из поисковой выдачи, а также разработка предложений по ее устранению. Методологическую основу составили формально-юридический, системный и сравнительно-правовой методы. В ходе исследования Федерального закона «Об информации, информационных технологиях и о защите информации», регулирующего вопросы информационной сферы, цифровых технологий и обеспечения информационной безопасности была рассмотрена статья 10.3. Данная законодательная норма устанавливает исключительную компетенцию физического лица в отношении требования об исключении интернет-ссылок, не допуская передачи подобных полномочий третьим сторонам. Выявлено противоречие с нормой статьи 9 Федерального закона «О персональных данных», наделяющей наследников правом давать согласие на обработку данных умершего, но не предоставляющей им права требовать их удаления. В результате сравнительного анализа рассмотрен опыт ЕС и США. Основным результатом работы являются конкретные предложения по внесению изменений в действующее законодательство, направленные на предоставление наследникам права требовать прекращения выдачи ссылок на информацию об умершем. Практическая значимость заключается в возможности использования предложенных поправок в законотворческой деятельности для защиты чести, достоинства и памяти умерших граждан в цифровой среде.

Ключевые слова: право, цифровые технологии, персональные данные, право на забвение, цифровая смерть, информационное право, правовое регулирование, цифровое наследие, защита персональных данных, наследники

S.V. Kravtsova,
student,
University of prosecutor's office
of the Russian Federation

The right to digital oblivion after death: regulatory gaps in the federal law on personal data and ways to eliminate them

Abstract. The article examines the problem of implementing the "right to be forgotten" after the death of a personal data subject in Russian legislation. The research aims to identify the legal conflict between the norms governing post-mortem processing of personal data and the mechanism for removing information from search engine results, as well as to develop proposals for its resolution. The methodological basis includes formal-legal, systemic, and comparative-legal methods. Article 10.3 of the Federal Law "On Information, Information Technologies, and Information Protection," which grants the right to remove links only to the citizen themselves, is analyzed. A contradiction is identified with Article 9 of the Federal Law "On Personal Data," which empowers heirs to consent to the processing of the deceased's data but does not grant them the right to demand its deletion. A comparative analysis of the EU and US experience is conducted. The main result of the work is specific proposals for amending the current legislation to grant heirs the right to demand the cessation of issuing links to information about the deceased. The practical significance lies in the potential use of the proposed amendments in legislative activities to protect the honor, dignity, and memory of deceased citizens in the digital environment.

Keywords: law, digital technologies, personal data, right to be forgotten, digital death, information law, legal regulation, digital legacy, personal data protection, heirs

Введение. В эпоху цифровизации жизнедеятельность человека оставляет глубокий и долговечный след в информационном пространстве. Смерть субъекта не означает исчезновения его виртуального присутствия, сформированного накопленными в процессе жизнедеятельности личными сведениями, которые продолжают функционировать в глобальной компьютерной сети. Подобная совокупность информационных следов охватывает профили на платформах социального взаимодействия, авторские материалы, упоминания в средствах массовой информации и тематических дискуссионных площадках. Данные массивы сохраняют доступность для широкой общественности на протяжении значительных временных периодов, измеряемых десятилетиями. Актуальность данного исследования обусловлена нарастающим объемом таких «посмертных» данных и отсутствием в российском законодательстве четкого механизма, позволяющего наследникам или иным заинтересованным лицам управлять этим цифровым наследием, в частности, реализовывать право на удаление неактуальной, недостоверной или порочащей честь и достоинство умершего информации.

Основная часть. Исследование базируется на правовом механизме забвения персональных данных, который нормативно зафиксирован в части 10.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149-ФЗ) [2], регулирующего вопросы информационного оборота, технологических процессов обработки данных и обеспечения информационной безопасности граждан. Рассматриваемое правовое положение предоставляет физическому лицу возможность обращаться к администратору поискового интернет-ресурса с требованием об исключении из результатов поиска гиперссылок, ведущих к материалам, содержащим сведения о заявителе. Однако конструкция нормы недвусмысленно указывает, что заявителем может быть только сам гражданин, что создает правовой вакуум после его смерти.

Целью настоящей статьи является анализ правовых пробелов в регулировании посмертного «права на забвение» и разработка конкретных законодательных предложений для их устранения.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать действующие нормы российского законодательства в сфере ПДн и «права на забвение».

2. Выявить и обосновать правовую коллизию, препятствующую реализации «права на забвение» после смерти субъекта ПДн.

3. Провести сравнительно-правовой анализ зарубежного опыта регулирования данного вопроса.

4. Сформулировать предложения по внесению изменений в Федеральный закон «О персональных данных» и Федеральный закон «Об информации, информационных технологиях и о защите информации».

Методологическую основу исследования составляют формально-юридический метод, метод системного анализа правовых норм, а также сравнительно-правовой метод для изучения зарубежных моделей правового регулирования.

Основная часть. Анализ действующего российского законодательства и выявление правовых пробелов.

Российское законодательство оперирует двумя ключевыми законами в рассматриваемой сфере: Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ) [1] и ФЗ № 149-ФЗ [2].

Институт «права на забвение» введен в российское правовое поле статьей 10.3 ФЗ № 149-ФЗ.

Первая часть указанной статьи устанавливает обязанность субъекта, управляющего поисковой системой, приостановить предоставление гиперссылок на сведения, касающиеся конкретного лица, подавшего соответствующее обращение. Данная обязанность возникает при условии, что размещенная информация характеризуется отсутствием достоверности, потерей актуальности, утратой практической ценности для субъекта обращения или нарушением действующих правовых норм при ее распространении.

Законодательная конструкция, определяющая субъекта как "гражданин (физическое лицо)", наряду со специальными требованиями к составлению за-

явления, включающими предоставление паспортной информации заявителя и его персонального согласия на процедуры обработки персональных данных, недвусмысленно свидетельствует об индивидуальном характере рассматриваемого правомочия.

Подобная регламентация процедурных аспектов подчеркивает персональную природу предоставляемой правовой защиты, поскольку требует непосредственного участия заинтересованного субъекта в процессе инициирования механизма удаления нежелательной информации из результатов поисковой выдачи.

Правоспособность гражданина прекращается с его смертью (ст. 17 ГК РФ), следовательно, и право на обращение к оператору поисковой системы угасает вместе с ним.

В то же время ФЗ № 152-ФЗ признает возможность обработки персональных данных после смерти субъекта. Ключевой нормой здесь является часть 7 статьи 9, которая гласит: «В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни» [1]. Эта норма создает парадоксальную ситуацию: наследники наделены правом легитимировать продолжение обработки ПДн умершего, но лишены сопутствующего права требовать их уточнения, блокирования или уничтожения в той же мере, в какой это мог делать сам субъект при жизни.

Таким образом, налицо правовая коллизия:

1. Право на управление данными: ФЗ № 152-ФЗ признает за наследниками ограниченное право на управление ПДн умершего (дача согласия на обработку).

2. Право на удаление ссылок: ФЗ № 149-ФЗ трактует «право на забвение» как сугубо личное, непередаваемое право, которое прекращается со смертью гражданина.

В результате информация об умершем, даже если она является недостоверной или порочит его память, может продолжать свободно распространяться в сети «Интернет» через поисковые системы, а у наследников отсутствуют эффективные правовые инструменты для противодействия этому. Они могут обратиться в суд с иском о защите чести и достоинства умершего, однако это более сложная и длительная процедура по сравнению с механизмом, предусмотренным статьей 10.3 ФЗ № 149-ФЗ.

Сравнительно-правовой анализ зарубежного опыта. Проблема цифрового забвения после смерти не является уникальной для России. Зарубежные правовые порядки также ищут баланс между свободой информации, правом на память и защитой частной жизни умерших.

Европейский союз. Общий регламент по защите данных (GDPR) не содержит прямых норм о персональных данных умерших лиц, оставляя этот вопрос на усмотрение государств-членов (преамбула) [4]. Некоторые страны ЕС разработали собственное регулирование. Наиболее показателен пример Франции, где в 2016 году был принят «Закон о цифровой республике» (*Loi pour une République numérique*). Он предоставил гражданам право заранее определять

директивы относительно своих данных после смерти, а также наделил наследников правом требовать от операторов удаления данных или их обновления для «организации и урегулирования памяти умершего» [5]. В Италии, напротив, судебная практика пошла по пути признания за наследниками права на доступ к данным умершего для защиты его памяти и семейных интересов [6].

США. В Соединенных Штатах отсутствует федеральный закон о «праве на забвение». Регулирование цифровых активов после смерти осуществляется на уровне штатов, большинство из которых приняли Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA). Этот акт в первую очередь ориентирован на предоставление фидуциариям (исполнителям завещания, попечителям) доступа к цифровым активам умершего для управления наследственной массой, а не на удаление информации [7]. Вопросы приватности и репутации остаются на втором плане.

Сравнительный анализ показывает наличие различных подходов (табл. 1), однако общая тенденция движется в сторону признания за наследниками определенных прав в отношении цифрового следа умершего.

Таблица 1. Сравнительный анализ подходов к посмертному праву на забвение [1]

Юрисдикция	Правовая основа	Субъект права после смерти	Объем прав
Российская Федерация	ФЗ-152-ФЗ, ФЗ-149-ФЗ	Наследники	Только дача согласия на обработку ПДн, право на удаление ссылок отсутствует
ЕС (общий подход)	GDPR (оставляет на усмотрение стран)	Не определено	Не определено
Франция (в рамках ЕС)	Loi pour une République numérique	Наследники, назначенные лица	Доступ, обновление, удаление данных для защиты памяти
США (типовой подход)	RUFADAA	Фидуциарии (исполнители завещания)	Преимущественно доступ к цифровым активам, а не удаление информации

Как видно из таблицы, российская модель является одной из наиболее ограниченных, не предоставляя наследникам действенных инструментов для управления репутационными рисками, связанными с цифровым наследием умершего.

Предложения по совершенствованию российского законодательства. Для устранения выявленного правового пробела и гармонизации норм двух федеральных законов предлагается внести следующие точечные изменения.

1. Изменения в Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Предлагается дополнить статью 10.3 новой частью 1.1 следующего содержания:

«1.1. В случае смерти гражданина, указанного в части 1 настоящей статьи, права заявителя могут быть реализованы его наследниками. К требованию наследника, помимо сведений, предусмотренных пунктами 2–5 части 2 настоящей статьи, должны быть приложены копии документов, подтверждающих факт смерти гражданина и вступление в права наследования».

Данная поправка позволит распространить механизм «права на забвение» на наследников, определив четкий перечень документов для подтверждения их полномочий. Это создаст простой и понятный для операторов поисковых систем алгоритм действий, аналогичный существующему порядку работы с заявлениями от живых граждан.

2. Изменения в Федеральный закон № 152-ФЗ «О персональных данных».

Предлагается изложить часть 7 статьи 9 в новой редакции:

«7. В случае смерти субъекта персональных данных его наследники вправе давать согласие на обработку его персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни, а также осуществлять иные права субъекта персональных данных, предусмотренные настоящим Федеральным законом, включая право на отзыв согласия на обработку персональных данных, право требовать уточнения, блокирования или уничтожения персональных данных в порядке, установленном настоящим Федеральным законом. Полномочия наследников подтверждаются в соответствии с законодательством Российской Федерации».

Эта поправка расширит права наследников, прямо закрепив за ними не только право давать согласие, но и право отзываться его, а также требовать удаления или исправления данных. Она гармонизирует положения ФЗ № 152-ФЗ с предлагаемыми изменениями в ФЗ № 149-ФЗ, создавая единую и непротиворечивую систему посмертного управления персональными данными.

Заключение. Цифровая эпоха поставила перед правом новые вызовы, одним из которых является юридическая судьба персональных данных после смерти человека. Действующее российское законодательство демонстрирует явный пробел в этой области: наследники, имея право дать согласие на обработку данных умершего, лишены возможности требовать удаления ссылок на неактуальную или порочащую информацию через механизм «права на забвение».

Предложенные в настоящей статье поправки в статью 10.3 ФЗ № 149-ФЗ и статью 9 ФЗ № 152-ФЗ направлены на устранение этой правовой коллизии. Их принятие позволит:

- наделить наследников четко определенным правом на обращение к операторам поисковых систем с требованием прекратить выдачу ссылок на информацию об умершем;
- создать правовой механизм для защиты посмертной чести, достоинства и деловой репутации в цифровой среде;
- гармонизировать российское законодательство с прогрессивными международными тенденциями в области управления «цифровым наследием».

Реализация данных предложений станет важным шагом в адаптации российского информационного права к реалиям цифрового общества и обеспечит более полную защиту прав граждан и их памяти после ухода из жизни.

Список литературы

1. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 28.02.2025) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.06.2025) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

3. Александрова А. С. Актуальные проблемы реализации права на забвение В Российской Федерации // Российский научный вестник. 2025. № 1. URL: <https://cyberleninka.ru/article/n/aktualnye-problemy-realizatsii-prava-na-zabvenie-v-rossiyskoy-federatsii> (дата обращения: 30.07.2025).

4. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. L 119/1. 4.5.2016.

5. LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (1) // Journal Officiel de la République Française. 2016. № 0235. Texte 1.

6. Hamulak, O., Kocharyan, H., Kerikmae, T. The contemporary issues of post-mortem personal data protection in the EU after GDPR entering into force [Рабочий документ]. 2021. URL: https://www.researchgate.net/profile/Ondrej-Hamulak/publication/343084219_THE_CONTEMPORARY_ISSUES_OF_POST-MORTEM_PERSONAL_DATA_PROTECTION_IN_THE_EU_AFTER_GDPR_ENTERING_INTO_FORCE/links/5f15f3c192851c1eff21ca7c/THE-CONTEMPORARY-ISSUES-OF-POST-MORTEM-PERSONAL-DATA-PROTECTION-IN-THE-EU-AFTER-GDPR-ENTERING-INTO-FORCE.pdf

7. Johnson C. J., McLaughlin J., Pinedo A. T. Corporate Finance and the Securities Laws / Charles J. Johnson Jr., Joseph McLaughlin, Anna T. Pinedo. Wolters Kluwer Law & Business, 2023. 1726 p.

А. В. Кулагина,

магистрант,

Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

**Автоматизированное увольнение:
границы допустимости и судебная практика**

Аннотация. В данной статье рассматривается проблема правовой допустимости и последствий применения алгоритмов и систем искусственного интеллекта для принятия решений об увольнении работников без участия человека. Анализируется действующее зарубежное законодательство, включая ограничения, установленные статьей 22 GDPR. Рассматриваются ключевые риски, возникающие при отсутствии повторной проверки алгоритмического решения человеком, в частности, нарушение трудового законодательства, нарушение принципа недискриминации, признания увольнения незаконным в судебном порядке. Проведен обзор актуальной судебной практики, отражающей стремление к защите работника при использовании автоматизированных систем увольнения.

Ключевые слова: автоматизированное увольнение, искусственный интеллект, алгоритм, автоматизация, обработка данных, непрозрачность, эффект «черного ящика», нарушение трудовых прав, дискриминация

A.V. Kulagina,

undergraduate student,

Moscow State Legal
University named after O. E. Kutafina (MSUA)

Automated dismissal: limits of admissibility and judicial practice

Abstract. This article examines the problem of using artificial intelligence algorithms and systems that make decisions about dismissing employees without human involvement. It analyzes current foreign legislation, including the restrictions established by Article 22 of the GDPR. It examines the risks arising from the absence of human review of algorithmic decisions: encouraging discrimination, violating employees' labor rights, and recognizing dismissals as unlawful. Examples of current court practice are provided, reflecting the desire to protect employees when using automated dismissal systems.

Keywords: automated dismissal, artificial intelligence, algorithm, automation, data processing, non-transparency, black box effect, violation of labor rights, discrimination

Введение. Для каждого работника, полагаем неприятным, услышать известие о внезапном расторжении трудового договора и необходимости искать новое место. Вдвойне неприятным оно кажется, если подобное решение принял алгоритм или искусственный интеллект.

В последнее время все чаще появляются тревожные новости, что новые технологии не только могут заменить работника с успехом и меньшими затратами для работодателя исполнять трудовую функцию, но и о том, что алгоритм может самостоятельно принять решение о том, что с определенным работником стоит прекратить трудовые отношения.

Так, согласно статистическим данным, а именно опроса, проведенного среди руководителей и менеджеров среднего звена сайтом Resume Builder, шесть из десяти опрошиваемых указали, что прибегают к мнению и помощи больших языковых моделей (LLM), принимая важные кадровые решения [8]. Чаще всего в качестве помощника по кадровым вопросам используются ChatGPT (53%), Microsoft Copilot (29%) и Google Gemini (16%) [11].

А 66% респондентов признались, что обращались к таким LLM как ChatGPT и прочие для консультации по поводу увольнения работников и расторжения трудовых договоров. При этом почти каждый пятый опрошиваемый оставлял окончательное решение за нейросетью и уже воплощал решение языковой модели на практике.

Основная часть. Описанный механизм автоматизированного увольнения еще с 2015 года начал внедряться в компании Amazon. Пока он действует в отношении водителей-курьеров, то есть наименее защищенной категории с неопределенным правовым статусом (в США на данный момент пока не установлена на законодательном уровне обязанность заключать с курьерами, водителями и иными лицами, занятыми на платформе трудовой договор).

Так, Amazon активно использует технологию Flex, анализирующую эффективность и производительность водителя [19]. Flex фиксирует ряд различных параметров, например, он обращает внимание на скорость доставки, опоздания курьера и пр. При оценке работы также учитывается тот факт, оставил ли курьер посылку под дверью или дождался заказчика [5. Р. 75].

При этом алгоритмом совершенно не учитываются внешние объективные факторы. Согласно опросам уволенных, почти четверть из них считают свое увольнение незаслуженным и явно необоснованным. К примеру, одному курьеру поручили доставить посылки на закрытую территорию, попасть туда он так и не смог, вследствие чего его эффективность была оценена как низкая. На основании полученного массива данных искусственный интеллект определяет, кого из водителей не стоит оставлять на работе

Вскоре после этого водитель получил электронное письмо, где его уведомили об увольнении. Водитель неоднократно пытался обжаловать решение, но получал стандартные отписки или письма вовсе оставались без ответа. В итоге его уволили несмотря на то, что он так и не смог «вживую» пообщаться с другим человеком.

Другой водитель имел безупречный рейтинг, но однажды у него повредилось колесо. После обращения в службу поддержки система посоветовала вернуться на базу. Водитель вернулся, однако сразу после этого рейтинг резко упал. Через несколько дней было получено уведомление об увольнении [1].

Таким образом, когда алгоритм принимает решение оставить водителя или курьера без работы, ему незамедлительно блокируется доступ к приложению Flex,

где он получает заказы на доставку товаров. При этом при составлении рейтинга алгоритм не учитывает различные внешние форс-мажорные обстоятельства, в связи с чем многие работники несправедливо теряют место работы.

Бывшие работники также сообщали о неидеальности и непрозрачности работы алгоритмов. Применяемый инструмент не учитывает реальные условия труда курьеров и водителей, не исправляет показатели из-за влияния форс-мажорных обстоятельств. При этом, по сообщениям, руководство осведомлено о предвзятости алгоритмов и распространенности несправедливых увольнений. Опрошенные утверждают, что людей увольняют с молчаливого согласия компании, потому что, легче довериться искусственному интеллекту, чем расследовать случаи ошибочных увольнений.

Не менее показательным кейсом служит отношение к водителям небезызвестной компании Uber. Так, исходя из документов, представленных в суд, компания Uber не соблюдает требования Европейского союза к прозрачности алгоритмов и использует механизма автоматизированного увольнения.

Один из водителей сообщил о деталях своего увольнения следующее: рейтинг мужчины составлял 4.94, когда он как обычно вышел на смену, ему пришло уведомление о том, что доступ в систему запрещен. После обращения в службу поддержки, бывшему водителю объявили, что аккаунт был заблокирован в связи с мошенническими действиями [18]. Несмотря на его попытки связаться с представителями компании, доказательств мошенничества и более подробного разъяснения причин отключения аккаунта так и не было предоставлено.

Поскольку вышеописанная проблема начала приобретать массовый характер, группа бывших водителей Uber из Великобритании и Португалии подала в суд на компанию Uber с требованием предоставить доступ к их данным и оспорить дисциплинарные меры (автоматическое увольнение), которые, с точки зрения человека, принимаются исключительно алгоритмом.

Основная позиция истцов заключается в ненадлежащем исполнении статьи 22 GDPR (General Data Protection Regulation – Общий регламент по защите данных), которая гласит, что *«Субъект данных имеет право не подвергаться принятию решений, основанных исключительно на автоматизированной обработке данных, включая профилирование, которое влечет за собой юридические последствия в отношении него или оказывает на него аналогичное существенное влияние»* [10].

Иными словами, в случае, если решение об увольнении принимается автоматически, только с помощью новых технологий, то согласно Общему регламенту по защите данных, у работодателя должны быть законные основания для использования такой технологии, и существует обязанность предоставить водителям возможность оспорить автоматическое решение.

Позиция Uber базировалась на том, что аккаунты водителей были деактивированы (то есть фактически расторгнуты трудовые отношения) только после ручной проверки человеком. Более того, поскольку многие аккаунты блокировались из-за якобы мошеннических действий, о которых сообщило их программное обеспечение, это не позволяет ссылаться на статью 22. Только полностью автоматизированные дисциплинарные процедуры подпадают под действие

статьи 22, а запрашиваемые работники сведения об участии человека и данных, приведших к решению об отключении аккаунта, составляют предмет коммерческой тайны.

Также Uber ссылался на весьма спорное мнение TIGRR (Целевой группы по инновациям, экономическому росту и регуляторной реформе), утверждавшей, что решение об увольнении работника должно соответствовать действующему режиму защиты данных, но при этом не должно предусматриваться какое-то конкретное право обжалование решения, поскольку это будет являться значительным снижением уровня защиты субъектов данных [7].

Весь происходящий процесс весьма емко и точно описал президент АСДУ Профсоюз водителей и курьеров, использующих приложения (ACDU), Ясин Аслам: *«Uber годами безнаказанно нарушал трудовое законодательство, и теперь мы видим проблеск оруэлловского мира труда, где у работников нет прав, а всем управляет машина. Если Uber не приструнить, такая практика станет нормой для всех»* [17].

Суд Амстердама постановил, что Uber Technologies Inc. должен восстановить уволенных водителей и аннулировать решения об отключении аккаунта [13]. Суд отметил, что решения, принятые ответчиком в связи с предполагаемыми мошенническими действиями истцов, должны рассматриваться как решения, основанные исключительно на автоматизированной обработке, и которые имеют юридические последствия для истцов или иным образом существенно затрагивают их права.

Далее в 2023 году было инициировано новое судебное разбирательство уже при участии двух уволенных водителей в отношении компании Uber и Ola. Бывшие водители, чьи аккаунты были заблокированы алгоритмом, требовали предоставить доступ к обработанным данным, связанным с предполагаемым увольнением, указать причины, по которым они были уволены. Компании настаивали, что предоставление запрашиваемого массива данных приведет к раскрытию коммерческой тайны и, тем самым, лишит смысла все использование новых технологий для борьбы с мошенничеством если водителям предоставят полную информацию о том, как они функционируют. Суд постановил, что платформы не вправе ссылаться на коммерческую тайну, чтобы скрыть и отказать водителям в доступе к данным о такого рода решениях, принимаемых с помощью искусственного интеллекта [9].

Исходя из вышенаписанного, можно обозначить несколько существенных проблем:

1) Проблема черного ящика и непрозрачности. Используемые алгоритмы и системы искусственного интеллекта потенциально могут сопоставлять и обрабатывать любые имеющиеся данные для формирования вывода о необходимости прекращения трудовых отношений [4. С. 47]. Работодатель в отдельных случаях может вообще не знать, как именно работает алгоритм, на какие критерии он опирается, не может расшифровать результаты анализа данных и объяснить принцип действия ни суду, ни самому работнику [7]. Тем самым невозможность раскрыть истинную информацию о принципах работы алгоритма и

логике принятия решения демонстрирует актуальность проблемы черного ящика и непрозрачности [3. С. 142].

2) Злоупотребление крупными корпорациями положениями GDPR. В приведенных судебных делах Uber ссылаясь, что проверка водителей на мошеннические действия не подпадает под понятие дисциплинарных процедур и соответственно регулируется статьей 22. Однако такое вольное толкование и подмена понятий недопустимо, так как ставит в неравное положение работодателя и работника, фактически лишая последнего право на понимание и разъяснения механизма работы алгоритмов и проведения проверок, права на прозрачность.

3) Отсутствие повторной проверки результатов алгоритмического анализа человеком. Поскольку алгоритм может содержать непреднамеренные ошибки или преднамеренную скрытую предвзятость, то без ручной проверки человека это приводит к необоснованному или очевидно незаконному увольнению лица (например, в период беременности женщины, увольнению без согласования с представителями профсоюзной организации и пр.) только на основе агрегированных данных. При автоматизированном увольнении единственным «основанием», подтверждающим убежденность работодателя в необходимости увольнения, являются данные алгоритма без дальнейшего их анализа работником.

Поскольку обеспокоенность вышеописанными проблемами и явно несправедливыми увольнениями все возрастает, в отдельных странах уже предпринимают попытку создать четкое законодательное регулирование.

Так, в Калифорнии, США, в марте 2025 года был представлен законопроект «No Robo Bosses Act», основная цель которого заключается в том, чтобы запретить работодателям использовать ИИ для принятия ключевых и важнейших кадровых решений, таких как прием на работу, увольнение или повышение в должности, без контроля и последующей перепроверки со стороны человека. В пояснительной записке сделан акцент на том, что окончательное решение должно оставаться за человеком, а искусственный интеллект – это всего лишь инструмент, который призван помогать людям и быть управляемым ими, а не наоборот [16].

Схожие инициативы реализуются и в Европейском союзе. В Регламенте (ЕС) 2024/1689 Европейского парламента и Совета от 13.06.2024 закрепляются гармонизированные правила в области искусственного интеллекта [15]. В документе регламентируется, что системы ИИ, влияющие на условия трудовых отношений, в том числе их прекращение и предназначенные для принятия решений классифицируются как системы ИИ с высоким уровнем риска, что подчеркивает необходимость соблюдения осторожности при их использовании.

Кроме того, в трудовом законодательстве Португалии использование алгоритмов и ИИ регулируется Законом № 13/2023, который гарантирует, что условия труда не могут быть ущемлены или ухудшены, а вопросы заключения и расторжения трудовых договоров полностью урегулированы в результате принятия решений на основе алгоритмов или других систем ИИ [14]. Одновременно с этим устанавливается право работников на представление и раскрытие информации о принципах и критериях работы алгоритма, который непосредственно влияет на их трудовую деятельность.

Данный закон стал дополнительной гарантией от законодателя в ответ на резонансный судебный процесс по поводу массового увольнения работников португальской авиакомпании. Компания разработала алгоритм для отбора сотрудников, которых стоит уволить в ближайшее время. Алгоритмические системы учитывали стаж работы, квалификацию, затраты на сотрудника, количество отсутствия на рабочем месте и пр., на основании чего принимал решение о необходимости уволить работника [6].

Апелляционный суд Лиссабона пришел к выводу, что подобные критерии в силу того, что они сформулированы крайне размыто и основаны на неизвестных работнику переменных, не позволяют сотруднику понять, почему он был включен в список коллективного увольнения. Ответчик попытался определить критерии и параметры лиц, с которыми необходимо прекратить трудовые отношения, но он использовал излишне общие и абстрактные термины, не учитывая индивидуальные особенности каждого работника. Таким образом, суд постановил, что критерии, по которым алгоритм определяет список для массового увольнения, должен позволять затронутым лицам четко определить причину, которая привела к их увольнению.

Помимо законопроектов также полагаемым необходимым корректировать работу управленцев и кадровиков, непосредственно опирающихся на решения алгоритмов и искусственного интеллекта при принятии кадровых решений.

Несмотря на то, что ошибки или потенциальные факторы дискриминации могут быть заложены на этапе разработки, апробации алгоритма и иных этапах, невозможно не согласиться с позицией о том, что формально решение «было принято» алгоритмом самостоятельно, однако именно менеджер по работе с персоналом окончательно определяет, насколько объективно решение искусственного интеллекта и стоит ли действительно расторгать трудовой договор [12]. В указанной ситуации не стоит забывать о личностном факторе, так как менеджеры также могут быть предвзяты и интерпретировать предоставленный алгоритмом массив данных не в пользу работников.

Однако вопреки приведенной неутешительной статистике и громким судебным процессам, алгоритмы могут весьма успешно и эффективно использоваться в сопровождении процесса увольнения. В частности, представляется разумным поручать алгоритму проверять отключение увольняемого от корпоративных ресурсов, блокировку его аккаунта, удаление оставленной информации, своевременной передаче необходимых сведений в государственные органы, например, в Социальный фонд.

Заключение. В данной статье был рассмотрен феномен автоматизированного увольнения работников, то есть увольнения основанного исключительно на данных, собранных алгоритмами и искусственным интеллектом. Был сделан вывод о том, что в большинстве случаев такой способ таит в себе существенные риски дискриминации и последующего судебного оспаривания.

Правоприменительная практика по данному вопросу однозначно указывает, что бесконтрольное использование новых технологий для принятия решения об увольнении лица не соответствует положениям Общего регламента по защите данных, грубо вмешивается в трудовую деятельность работника, несет зна-

чительные юридические последствия, нарушает его право на прозрачность, судебную защиту.

На данный момент говорить о безупречности применения новых технологий преждевременно, справедливое, но полностью автоматизированное решение об увольнении кажется невозможным [2. С. 23]. Для их приведения в соответствии с требованиями национального законодательства и соблюдения прав более слабой сторон трудовых отношений требуется долгая и тщательная работа. Тем не менее алгоритмы и искусственный интеллект имеют весьма положительные перспективы для сопровождения процесса увольнения, для выполнения рутинных технических задач.

Список литературы

1. В Amazon роботы начали принимать решения об увольнении людей, даже если они ни в чем не виноваты. URL: https://www.cnews.ru/news/top/2021-06-29_roboty_nachali_uvolnyat (дата обращения: 01.08.2025).

2. Жильцов М.А., Жильцова Ю.В. Применение искусственного интеллекта при регулировании трудовых отношений // Трудовое право в России и за рубежом. 2023. №3. С. 22–24.

3. Кутейников Д. Л., Ижаев О. А., Зенин С. С., Лебедев В. А. Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика» // Lex russica. 2020. Т. 73. № 6. С. 139–148.

4. Марченко А. Ю. Правовой анализ новейшего законодательства ЕС о применении технологий искусственного интеллекта: дис. ... канд. юрид. наук. М., 2022. С. 47.

5. Alimahomed-Wilson Jake, Reese Ellen. The Amazonification of Logistics: E-Commerce, Labor, and Exploitation in the Last Mile. // The Cost of Free Shipping: Amazon in the Global Economy. Pluto Press. 2020. Pp. 69–84.

6. Américo Oliveira Fragoso, Marta Presas, Carolina Cordeiro dos Santos. Automated dismissals and AI: The balance between efficiency and rights. // Lexology. URL: <https://www.lexology.com/library/detail.aspx?g=ad0f6cc4-815f-455e-bb87-4c1c81ee9170> (дата обращения: 01.08.2025).

7. Automated Dismissal Decisions, Data Protection and The Law of Unfair Dismissal. // UK Labour Law Blog. URL: <https://uklabourlawblog.com/2021/10/19/automated-dismissal-decisions-data-protection-and-the-law-of-unfair-dismissal-by-philippa-collins/> (дата обращения: 01.08.2025).

8. Bosses Are Using AI to Decide Who to Fire. URL: <https://futurism.com/managers-using-ai-fire> (дата обращения: 01.08.2025).

9. ECLI:NL:GHAMS:2023:793. URL: Amsterdam Court of Appeal rules Uber violated data protection rights | Court ruling | Eurofound Platform Economy Repository (дата обращения: 01.08.2025).

10. General Data Protection Regulation (GDPR) Art. 22 GDPR Automated individual decision-making, including profiling. URL: <https://gdpr.eu.org/art/22/> (дата обращения: 01.08.2025).

11. Half of Managers Use AI To Determine Who Gets Promoted and Fired. URL: <https://www.resumebuilder.com/half-of-managers-use-ai-to-determine-who-gets-promoted-and-fired/> (дата обращения: 01.08.2025).
12. Hill Dickinson. Exploring workplace discrimination in the age of AI. // Lexology. URL: <https://www.lexology.com/library/detail.aspx?g=3473c145-7598-4d36-9b1f-5144a78cd168> (дата обращения: 01.08.2025).
13. In Case C / 13/696010/ HA ZA 21-81. URL: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/696010/_/HA_ZA_21-81 (дата обращения: 01.08.2025).
14. Lei n.º 13/2023, de 3 de abril. URL: <https://diariodarepublica.pt/dr/detalhe/lei/13-2023-211340863> (дата обращения: 01.08.2025).
15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32024R1689> (дата обращения: 01.08.2025).
16. SB-7 Employment: automated decision systems. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202520260SB7 (дата обращения: 01.08.2025).
17. Uber faces GDPR lawsuit over 'robo-firing' algorithm. URL: <https://www.itpro.com/business-strategy/automation/357553/uber-gdpr-lawsuit-robo-firing> (дата обращения: 01.08.2025).
18. Uber sued by drivers over 'automated robo-firing'. URL: <https://www.bbc.com/news/business-54698858> (дата обращения: 01.08.2025).
19. Why you should be a delivery driver with Amazon Flex. URL: <https://flex.amazon.com/why-flex> (дата обращения: 01.08.2025).

С. В. Ларцина,
аспирант, ассистент
Государственный институт русского языка
имени А. С. Пушкина,
Московский педагогический государственный университет,
Московский университет имени С. Ю. Витте

**«Чей туфля»? Право на сгенерированную интеллектуальную
собственность в практике китайских разработчиков**

Аннотация. Статья посвящена анализу проблем правового регулирования интеллектуальной собственности относительно материалов, созданных с помощью генеративного искусственного интеллекта. Цель исследования заключается в выявлении подходов разработчиков зарубежных нейросетей к определению авторства и распределению ответственности за сгенерированные материалы. На основе анализа пользовательских соглашений MiniMax, DeepSeek и Qwen показано, что отсутствует универсальный подход к определению правового статуса такого контента: одни компании отказываются от притязаний на авторство, но сохраняют обширные лицензии на использование данных, другие предоставляют пользователю практически полные права на результаты генерации, а некоторые ограничиваются лишь упоминанием общих правил использования сервиса. Сделан вывод о том, что неопределенность в вопросах авторства и прав на сгенерированный контент требует разработки единого механизма регулирования, который обеспечил бы поддержание баланса между интересами разработчиков, пользователей и правообладателей.

Ключевые слова: право, цифровые технологии, искусственный интеллект, генеративные модели, авторское право, интеллектуальная собственность, пользовательское соглашение, нейросети

S. V. Lartsina,
Postgraduate Student, Assistant,
Pushkin State Russian Language Institute,
Moscow Pedagogical State University,
Moscow Witte University

**«Who owns the shoe?»: the right to generated intellectual property
in the practice of chinese developers**

Abstract. This article examines the challenges of legal regulation concerning intellectual property for materials generated by generative artificial intelligence. The study aims to identify the approaches employed by foreign neural network developers in determining authorship and allocating responsibility for AI-generated content. Based on an analysis of the user agreements of MiniMax, DeepSeek, and Qwen, it is demonstrated that no universal approach exists regarding the legal status of such content: some companies disclaim authorship while retaining broad licenses to use user data; others grant users nearly full rights to the generated output; and some merely reference

general terms of service without addressing ownership. The article concludes that the current ambiguity surrounding authorship and rights to AI-generated content necessitates the development of a unified regulatory framework capable of ensuring a balanced protection of the interests of developers, users, and rights holders.

Keywords: law, digital technologies, artificial intelligence, generative models, copyright, intellectual property, user agreement, neural networks

Введение. Словосочетание «искусственный интеллект» и связанные с ним (нейросеть, чат-бот, ИИ) успели коснуться многих сфер человеческой жизни. По данным ресурса «Грамота.ру», в число наиболее употребительных слов в области информационных технологий вошли «промт», «дипфейк», «чат-бот» и др. По данным от Государственного института русского языка им. А. С. Пушкина, в финал «Слова года» вошло, помимо прочих, «искусственный интеллект». Все это свидетельствует о том, что нейросети преобразуют многие сферы человеческой жизни, с каждым годом усиливая свое влияние на них.

Основная часть. Несмотря на возрастающее внимание научного сообщества к влиянию нейросетевых технологий на различные аспекты человеческой деятельности, в том числе на вопросы интеллектуальной собственности [2, 3, 5], многие аспекты правового регулирования в данной сфере остаются неразрешенными. Особенно остро стоит проблема определения авторства и закрепления прав на результаты интеллектуальной деятельности, созданные при помощи генеративного искусственного интеллекта, поскольку действующее законодательство Российской Федерации не предусматривает юридически однозначного механизма распределения прав на подобный контент. Как отмечает П. М. Морхат, традиционные юридические категории, такие как «автор» и «субъект права», требуют переосмысления применительно к алгоритмическим системам, что напрямую связано с коллизиями в сфере авторского права на сгенерированные материалы [1]. В условиях активного технологического развития в Китае представляется актуальным проанализировать практики китайских разработчиков генеративных систем, в частности их подходы к определению правового статуса сгенерированных материалов, распределению ответственности между пользователем и разработчиком, а также правовому оформлению авторства в рамках пользовательских соглашений.

Целью настоящего исследования является анализ подходов зарубежных разработчиков нейросетей к вопросам определения авторства и ответственности за сгенерированные материалы, включая права пользователей на такой контент и их потенциальную ответственность.

1. *MiniMax*.

Исходя из условий использования нейросети «MiniMax», становится очевидным, что компания Nanonoble Pte. Ltd. (Сингапур) стремится максимально обезопасить себя, при этом предоставляя пользователям определенные, но строго ограниченные права на генерируемый контент. В разделе «User Contributions and User Generated Content» прямо указано: «We do not claim ownership of User Contributions or User Generated Content». Это означает, что компания не претендует на то, чтобы быть владельцем созданного вами текста, аудио или видео.

Это фундаментальный принцип, который отличает MiniMax от некоторых других платформ, где авторство может быть более размытым или даже полностью принадлежать разработчику. Пользователь, вводя свои «User Contributions» (иными словами, запросы, инструкции) и получая «User Generated Content» (сгенерированный материал), по умолчанию остается его владельцем.

Сразу же после заявления об отсутствии претензий на владение сгенерированными материалами, следует обширный пункт о лицензировании. Пользователь, используя сервис, предоставляет MiniMax, аффилированным лицам и правопреемникам «широкую, бессрчную, безотзывную, всемирную и неисключительную лицензию» (royalty-free, perpetual, irrevocable, worldwide, non-exclusive right) на использование сгенерированного контента. Это может привести к формированию закрытых экосистем, где разработчик фактически монополизирует поток данных и производные продукты, что подрывает принципы справедливого творчества и свободного обмена, о чем писал С. Гульямов [4].

При решении вопроса об ответственности пользователя за сгенерированные материалы MiniMax исходит из позиции, что ответственность полностью возлагается на пользователя. В том случае, если сгенерированный контент нарушает чьи-либо права интеллектуальной собственности (в частности, авторские права), то вся ответственность лежит на пользователе. На пользователе в том числе лежит ответственность за возмещение убытков компании в случае каких-либо претензий, причиной которым послужило нарушение пользователем условием пользования сервисов. Пользователь несет полную ответственность за все генерируемые им материалы. Предполагается, что он будет крайне внимателен к соблюдению всех стандартов контента.

2. DeepSeek.

С нейросетью DeepSeek ситуация упрощенная. Разработчики языковой модели в разделе 4.2 лицензионного соглашения указывают, что предоставляют все материалы, полученные при предоставлении услуги пользования нейросетью, пользователю. Разработчики утверждают, что пользователи имеют право использовать выходные данные в личных целях, для научных исследований, для разработки производных продуктов и даже для обучения других моделей. Разработчики DeepSeek оставляют за собой право использовать входные и выходные данные с целью улучшения работы нейросетевой технологии. Пользователь может отказаться от предоставления разработчикам такой возможности, запретив в настройках сервиса соответствующие действия.

Внедрение подобных дополнительных настроек отмечается только у нейросети DeepSeek среди всех проанализированных китайских сервисов нейросетевых технологий. Примечательно, что в таком случае за пользователем закрепляется право принимать участие в урегулировании правовых отношений.

3. Qwen AI.

В пользовательском соглашении Qwen в разделе «Proprietary rights» указывается, что все содержимое сайта защищено авторским правом. Пользователю разрешается использовать сайт (и, соответственно, функционирующую на его базе нейросетевую технологию) исключительно в личных некоммерческих целях. Запрещается систематическое извлечение данных (т. е. parsing).

В разделе «Use of this website» подчеркивается, что пользователь несет полную ответственность за загружаемый контент и может быть привлечен к ответственности за нарушение прав третьих лиц. Компания оставляет за собой право редактировать, удалять или не публиковать любой контент, но не предоставляет пользователю четких гарантий в отношении его прав на сгенерированные материалы.

Анализ пользовательских соглашений MiniMax, DeepSeek и Qwen наглядно демонстрирует, что на сегодняшний день вопрос авторства и прав на контент, созданный с помощью искусственного интеллекта, остается спорным моментом. В связи с этим, отмечается отсутствие единообразия в разрешении этого вопроса. Так, MiniMax формально отказывается от претензий на владение сгенерированным контентом, но пунктом ниже указывает, что имеет практически абсолютную лицензию на использование как входных, так и выходных данных. Пользователь, хотя и признается единственным автором, по сути, теряет контроль над результатами своего взаимодействия с чат-ботом, в ходе которого и был создан сгенерированный продукт. DeepSeek, с другой стороны, передает все права на выходные данные пользователю, который может использовать их в любых целях без ограничений. Qwen придает пользователю статус полноправного участника правовых отношений, наделяя его возможностью разрешать или запрещать разработчикам совершать определенные действия со сгенерированным материалом. Дополнительно в соглашении Qwen указывается, что использование сайта ограничивается исключительно личными некоммерческими целями. Запрещено копирование, извлечение данных с целью обучения собственных моделей.

Заключение. Проблема авторства над сгенерированными материалами остается на данный момент неразрешенной на законодательном уровне. В связи с этим пользовательские соглашения современных нейросетей регулируют проблему авторства на свое усмотрение. Разработка универсального подхода к определению авторства на материалы, созданные ИИ, остается насущной задачей, решение которой необходимо для формирования справедливой и предсказуемой правовой среды в эпоху массового распространения генеративных технологий.

Список литературы

1. Морхат П. М. Искусственный интеллект: правовой взгляд. Москва: КТ "Буки-Веди", 2017. 257 с.
2. Begemann M., Hutson J. Navigating Copyright in AI-Enhanced Game Design: Legal Challenges in Multimodal and Dynamic Content Creation // Journal of Information Economics. 2025. Vol. 3 (1). P. 1–14.
3. Bharati R. K. AI and intellectual property: Legal frameworks and future directions // International Journal of Law Justice and Jurisprudence. 2024. Vol. 4 (2). P. 207–215.
4. Gulyamov S. AI Authorship and Ownership of Intellectual Property in Industrial Power and Control Systems / S. Gulyamov. // Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA). 2023. PP. 217–221.
5. Hutson A. The Evolving Role of Copyright Law in the Age of AI-Generated Works // Journal of Digital Technologies and Law. 2024. Vol. 2 (4). PP. 886–914.

В. С. Луценко,
стажер–исследователь,
Национальный исследовательский университет
«Высшая школа экономики»

Правовое регулирование искусственного интеллекта в Республике Корея

Аннотация. Цель исследования состоит в анализе особенностей регулирования и развития искусственного интеллекта в Республике Корея. В статье рассматриваются стратегические документы и инициативы государства, направленные на формирование национальной AI-экосистемы, развитие инфраструктуры и привлечение кадров. Особое внимание уделено правовому регулированию: отсутствие единого закона о ИИ компенсируется системой «мягкого права», отраслевыми актами, этическими стандартами и механизмами «регуляторных песочниц». Подчеркивается ключевая роль государства и крупных корпораций (Samsung, LG, SK Hynix) в финансировании и внедрении ИИ-технологий, а также активное участие Южной Кореи в международных инициативах (ОЭСР, GPAI, Hiroshima AI Process). При этом выделяются структурные вызовы: демографический спад, «утечка мозгов», доминирование чеболей и разрыв между быстрыми технологическими изменениями и правовым регулированием. Сделан вывод о необходимости баланса между инновационным развитием, социальной ответственностью и защитой прав граждан.

Ключевые слова: Республика Корея, искусственный интеллект, правовое регулирование, цифровые технологии, этический искусственный интеллект, национальная стратегия, международное сотрудничество

V. S. Lutsenko,
Research Assistant,
National Research University
Higher School of Economics

Legal regulation of artificial intelligence in the Republic of Korea

Abstract. The purpose of this study is to analyze the specific features of artificial intelligence regulation and development in the Republic of Korea. The article examines strategic policy documents and governmental initiatives aimed at shaping a national AI ecosystem, expanding infrastructure, and fostering talent. Attention is devoted to legal regulation: the absence of a comprehensive AI law is compensated by a system of “soft laws,” sectoral acts, ethical standards, and regulatory sandbox mechanisms. The decisive role of the state and major corporations (Samsung, LG, SK Hynix) in financing and implementing AI technologies is highlighted, alongside South Korea’s active participation in international initiatives (OECD, GPAI, Hiro-

shima AI Process). At the same time, several structural challenges are identified, including demographic decline, brain drain, the dominance of chaebols, and the widening gap between rapid technological change and legal frameworks. The study concludes that striking a balance between technological innovation, social responsibility, and the protection of citizens' rights is essential.

Keywords: Republic of Korea, artificial intelligence, legal regulation, digital technologies, ethical AI, national strategy, international cooperation

Введение. Южная Корея стремится войти в число мировых лидеров в области искусственного интеллекта (далее – ИИ), что отражается в ее стратегических документах и программах. Развитие ИИ является национальным приоритетом и рассматривается как ключевой фактор Четвертой промышленной революции и будущего экономического роста. В 2019 году была принята Национальная стратегия по искусственному интеллекту, определившая три направления: формирование глобально конкурентной ИИ-экосистемы, подготовка кадров и развитие человеко-ориентированных технологий [12].

Эти приоритеты закреплены в последующих инициативах – «Новом цифровом курсе» (2020, обновлен в 2022 г.), программе «120 ключевых национальных задач» (2022) [1], а также в стратегиях по науке, технологиям и кибербезопасности. Центральную роль играет государство, координируя взаимодействие с академическим сектором и бизнесом [2]. В 2024 году при президенте был создан Национальный комитет по ИИ для развития государственно-частного партнерства [20].

Южная Корея активно внедряет ИИ в различных сферах – от умных городов и обороны до здравоохранения и индустрии развлечений. При этом общественное восприятие остается противоречивым: высокие ожидания сочетаются с обеспокоенностью рисками кибербезопасности и вытеснения рабочих мест [6. С. 55–56]. Важную роль играют и частные компании, особенно чеболи (Samsung, SK Hynix, LG), а также стартапы, развивающие нишевые инновации. Согласно Индексу развития ИИ Tortoise Media (2023), Южная Корея занимает шестое место в мире и третье в Азии [16]. Однако наряду с успехами сохраняются вызовы – демографический спад, пробелы в регулировании и доминирование крупных корпораций.

Основная часть.

Регулирование искусственного интеллекта. Южная Корея, стремясь к лидерству в области искусственного интеллекта, выработала модель регулирования, основанную на принципах «мягкого права» и акценте на государственно-частном партнерстве. Такой подход, с одной стороны, стимулирует инновации, но, с другой, порождает ряд вызовов. Исторически укоренившийся акцент на информационных технологиях как двигателе экономического роста привел к тому, что Южная Корея приоритетно развивает ускоренное внедрение ИИ [8. С. 316–327]. Эти устремления отражаются в активном участии страны в глобальных дискуссиях о регулировании ИИ. Как член ОЭСР, Республика Корея вносит вклад в разработку принципов и рекомендаций по этичному и ответственному использованию ИИ. Кроме того, страна участвует в Глобальном

партнерстве по искусственному интеллекту (GPAI) и процессе Хиросимы по ИИ, цель которых – выработка международных подходов к управлению рисками, связанными с ИИ.

В настоящее время в Южной Корее отсутствует специализированный закон об ИИ. Регулирование основывается на отраслевых законодательных актах, механизмах саморегулирования, отраслевых руководствах, а также на совокупности консультативных и стимулирующих документов. Широко используется практика «регуляторных песочниц», что позволяет ускорять внедрение инноваций в сфере ИИ и тестировать новые технологии под надзором государства. В 2020 году Министерство науки и ИКТ совместно с Корейским институтом развития информационного общества разработали Этические стандарты в сфере ИИ. Они базируются на принципах человеческого достоинства, общественной пользы и технологической адекватности и включают гарантии прав человека, защиту конфиденциальности, уважение к разнообразию, запрет причинения вреда, обеспечение общественной пользы и солидарности, управление данными, подотчетность, безопасность и прозрачность [17].

Тем не менее, законодательные вызовы в Южной Корее тесно связаны с национальной моделью развития ИТ и ИИ, которая часто отдает приоритет экономической конкурентоспособности в ущерб минимизации социальных рисков. Это отражает более широкий дискурс, в рамках которого продвижение и регулирование новых технологий рассматривается как диалектический выбор между сохранением глобальной конкурентоспособности и реагированием на непредсказуемые последствия их применения. В итоге отсутствие комплексного законодательства может привести к недостаточной защите прав граждан и бизнеса в сфере ИИ. Более того, стремительное развитие технологий ИИ опережает существующие регуляторные механизмы, что делает их недостаточными для ответа на возникающие вызовы и риски.

Финансирование и инфраструктура как условия для реализации регулирования. Южная Корея активно инвестирует в сектор искусственного интеллекта, используя как государственные, так и частные источники финансирования. В последние годы правительство демонстрирует повышенный интерес к развитию ИИ, выделяя значительные средства на поддержку исследований и разработок в этой области. Несмотря на общее сокращение расходов на НИОКР в 2024 году, вложения в ИИ выросли. Бывшая администрация президента Юн Сок Ея планировала выделить 6,9 млрд долларов на развитие технологий ИИ [20], а Министерство науки и ИКТ – направить 3,7 млрд долларов на стратегические национальные технологии, из которых 777,2 млн будет инвестировано непосредственно в ИИ [7]. Особое внимание уделяется секторам стратегической значимости, в частности полупроводникам.

Однако экономическая ситуация, характеризующаяся замедлением роста ВВП, негативно сказывается на финансировании НИОКР. Так, в 2024 году государственный бюджет на исследования и разработки был сокращен на 14,8% и составил 26,5 трлн вон [7]. Дополнительные препятствия создают мировые экономические вызовы и торговые споры с другими странами. Южная Корея сталкивается с жесткой конкуренцией со стороны Китая, Тайваня и США в сфере

высоких технологий, при этом производство отдельных компонентов для инфраструктуры ИИ остается зависимым от импорта из Китая и Японии. Позиции страны в мировой торговле также ослабли: ее доля в глобальном экспорте высокотехнологичной продукции снизилась со второго на пятое место в 2018–2022 гг [10]. Более того, торговые барьеры, включая меры со стороны США, создают дополнительные трудности для корейского экспорта.

Крупные южнокорейские конгломераты играют ключевую роль в финансировании ИИ. Их инвестиции в приоритетные исследования зачастую значительно превышают государственные вложения [14]. Это способствует быстрой коммерциализации инноваций, адаптированных под потребности частного сектора. Однако акцент частных компаний на прикладных разработках приводит к недостаточному вниманию к фундаментальным исследованиям, которые необходимы для прорывных технологий. Кроме того, зависимость от частного финансирования не всегда соответствует интересам малых и средних предприятий. Несмотря на активность корейских стартапов, доминирование чеболей в распределении ресурсов усугубляет трудности МСП, которые и так ограничены в доступе к капиталу.

Одним из ключевых преимуществ Южной Кореи в сфере ИИ является развитая инфраструктура, обеспечивающая как научные исследования, так и коммерциализацию технологий. Страна занимает лидирующие позиции на мировом рынке высокопроизводительной памяти: компании SK Hynix и Samsung совместно контролируют 91% рынка. Это серьезное конкурентное преимущество, поскольку микросхемы памяти играют центральную роль в развитии ИИ и больших данных. Samsung также производит 31% мирового объема логических чипов, а доля Южной Кореи в мировом производстве DRAM и NAND-памяти составляет 50,3% и 27,1% соответственно [5]. Для поддержания этого сектора в 2021 году был запущен проект «K-Semiconductor Belt», предусматривающий создание промышленных кластеров для производства, исследований и разработок полупроводников [13].

В стране также создана передовая инфраструктура дата-центров, доступная как государственным, так и частным организациям для исследований в области ИИ. Национальный суперкомпьютерный центр оказывает поддержку ведущим научным институтам, таким как KISTI и ETRI. Один из мощнейших корейских суперкомпьютеров – Nurion – используется для обучения масштабных моделей глубокого обучения и проведения межотраслевых исследований. Крупные корпорации, включая Naver и Kakao, также активно строят собственные дата-центры. Государство стимулирует развитие инновационной среды через технопарки и стартап-хабы, включая Pango Techno Valley («Силиконовую долину Кореи»), цифровой медиацентр (DMC) в Сеуле и международный бизнес-дистрикт Сонгдо в Инчхоне.

Наука и исследования, кадровый потенциал как факторы, влияющие на успешность регулирования и внедрения стандартов. Южная Корея выделяет значительные средства на НИОКР, которые составляют 4,8% ВВП – один из самых высоких показателей в мире [19]. Однако значительная часть этих расходов приходится на частные компании. Страна занимает первое место в мире

по числу ИИ-патентов в расчете на 100 тыс. человек. Лидером является Samsung, зарегистрировавшая 700 патентов в 2010–2021 гг., за ней следует LG с 593 патентами [11. С. 15]. Кроме крупных корпораций, значительный объем патентов принадлежит университетам и исследовательским центрам, особенно в областях машинного обучения, компьютерного зрения и обработки естественного языка.

Корейские исследователи активно публикуют научные работы по ИИ. В зависимости от методики подсчета их количество составляет от 14 тыс [9]. до 68 404 статей [11. С. 24]. что обеспечивает Южной Корее 11-е место в мире. Примечательно, что 31% публикаций подготовлены в соавторстве с зарубежными исследователями, что подтверждает высокий уровень международного сотрудничества [11. С. 26]. Вместе с тем в последнее время усилились опасения по поводу утечек данных в высокотехнологичных отраслях, что частично связывается с участием иностранных специалистов в научных и производственных процессах.

Ведущие университеты страны – Сеульский национальный университет, Йонсей и KAIST – играют центральную роль в развитии науки и технологий. KAIST и Корейский институт искусственного интеллекта (KIAI) являются ведущими центрами ИИ-исследований, а институты KISTI и ETRI вносят значимый вклад в инновации в сфере ИИ.

Правительство и частный сектор активно инвестируют в развитие образования в сфере ИИ, открывая новые академические программы и исследовательские центры. Десять ведущих университетов страны предлагают магистерские программы по ИИ, а также специализированные краткосрочные курсы и программы переподготовки. Южная Корея занимает третье место в мире по числу специалистов в области ИИ, уступая лишь Израилю и Сингапуру [4].

Тем не менее, страна сталкивается с серьезными демографическими проблемами, включая низкую рождаемость и сокращение населения, что приводит к дефициту квалифицированных кадров. Несмотря на усилия правительства, нехватка специалистов остается острой. С 2018 года рост кадрового потенциала застопорился, а отток специалистов за рубеж превышает приток. Особенно остро это проявляется у выпускников, получивших образование в США: 75% из них не планируют возвращаться в Корею [18]. Основные причины «утечки мозгов» – лучшие условия труда, более высокая зарплата и карьерные перспективы за рубежом, а также недостаток финансирования науки и нестабильность рынка труда в самой Корее.

Корейская молодежь испытывает сильную неопределенность в сфере занятости. Это снижает мотивацию к обучению и профессиональной деятельности. Низкая заработная плата, корпоративная культура с высоким уровнем стресса и традиционные социальные нормы усугубляют ситуацию. Например, сильное влияние конфуцианских ценностей способствует гендерному неравенству на рынке труда, что сказывается и на сфере ИИ, где число женщин-специалистов заметно уступает числу мужчин [11. С. 35].

Заключение. Таким образом, Южная Корея обладает значительными преимуществами для продвижения в сфере искусственного интеллекта, включая

развитую технологическую инфраструктуру, глобальное лидерство в полупроводниковой отрасли и активное участие государства в финансировании ИИ-проектов. Существенную роль играют развитый сектор научных исследований, крупные корпорации и потенциал «умных городов», формирующих инновационную экосистему.

В то же время страна сталкивается с вызовами, которые напрямую затрагивают сферу правового регулирования: демографический спад и «утечка мозгов» усугубляют кадровый дефицит, а приоритет экономической конкурентоспособности приводит к недооценке этических и социальных рисков. Экономическая стагнация и доминирование чеболей создают препятствия для развития малых и средних предприятий в секторе ИИ. В этих условиях формирование комплексной нормативно-правовой базы, обеспечивающей баланс между технологическим прогрессом, защитой прав граждан, социальной ответственностью и устойчивым развитием кадрового потенциала, становится необходимым условием сохранения и укрепления позиций Южной Кореи в глобальной гонке ИИ.

Опыт Республики Корея показывает, что в условиях стремительного технологического прогресса государства вынуждены искать баланс между стимулированием инноваций и формированием правовой среды, способной минимизировать социальные и этические риски. Отсутствие единого закона об ИИ компенсируется комбинацией «мягкого права», отраслевых актов и международного сотрудничества, что позволяет гибко реагировать на вызовы. Однако этот подход сопряжен с риском правовых пробелов и недостаточной защитой гражданских прав. Следовательно, глобальная тенденция заключается в необходимости разработки комплексных и согласованных нормативных решений, которые одновременно поддерживали бы технологическое развитие и обеспечивали защиту прав человека.

Список литературы

1. 120 대 국정과제 [120 национальных задач] // 대한민국 대통령실 [Офис президента Республики Корея]. 2022. URL: https://www.president.go.kr/affairs/gov_project (дата обращения: 17.08.2025).

2. 4 차산업혁명위원회의 설치 및 운영에 관한 규정 [Положение о создании и деятельности Комитета 4-й промышленной революции] // 국가법령정보센터 [Национальный юридический информационный центр]. 2021. URL: <https://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=228675&lsId=012976&chrClsCd=010202&urlMode%20=lsInfoP&viewCls=lsInfoP&efYd=20210112&vSct=인공지능%20ancYnChk=0&efGubun=#0000> (дата обращения: 17.08.2025).

3. Artificial Intelligence Index Report 2024 // HAI Stanford University. 2024. URL: https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf (дата обращения: 25.08.2025).

4. Assessing South Korea's AI Ecosystem // CSET. 2023. URL: <https://ai.gov.ru/knowledgebase/investitsionnaya->

ak-

tivnost/2023_ocenka_ekosistemy_iskusstvennogo_intellekta_v_yughnoy_koree_asse
ssing_south_korea_s_ai_ecosystem_cset/ (дата обращения: 20.08.2025).

5. Gillespie N., Lockey S., Curtis C., Pool J., Akbari A. Trust in Artificial Intel-
ligence. A global study // KPMG and The University Of Queensland. 2023. P. 55–56.

6. High-technology exports (current US\$) – Korea, Rep. // The World Bank.
URL: <https://data.worldbank.org/indicator/TX.VAL.TECH.CD?locations=KR> (дата
обращения: 20.08.2025).

7. Kim J. Defining risk in AI legislation: perspectives and implications in the
Korean context // Communication Research and Practice. 2024. Vol.10. №3. P. 316–
327.

8. KISTEP R&D and Beyond // KISTEP. URL:
<https://www.kistep.re.kr/board.es?mid=a20404000000&bid=0049> (дата обращения:
25.08.2025).

9. Lee Jeong-gu, Yeom Hyun-a. S. Korea's 6 key high-tech industries face 25.5
% export market share decline // The Chosun daily. 2024.
URL:[https://www.chosun.com/english/industry-
en/2024/01/21/KWTFMCJTLBGIDO7MCURTLA7S7Q/](https://www.chosun.com/english/industry-en/2024/01/21/KWTFMCJTLBGIDO7MCURTLA7S7Q/) (дата обращения:
20.08.2025).

10. McFaul C., Chahal H., Gelles R., Konaev M. Assessing South Korea's AI
Ecosystem. Data Brief // CSET. 2023. P. 15.

11. National Strategy for Artificial Intelligence // MSIT. URL:
<https://www.msit.go.kr/bbs/view.do?sCode=eng&nttSeqNo=9&bbsSeqNo=46&mId=10&mPid=9> (дата обращения: 17.08.2025).

12. Plan to make Korea 'top semiconductor power' by 2030 // Korea.net. 2021.
URL: <https://www.korea.net/NewsFocus/policies/view?articleId=198152> (дата об-
ращения: 20.08.2025).

13. Samsung Accounts for Half of Korea's Total R&D Spending // The Chosun
Daily. 2023. URL: [https://www.chosun.com/english/industry-en/2023/07/26/
VZ4IZJ5VAA2B6XMROPE3Y63A7A/](https://www.chosun.com/english/industry-en/2023/07/26/VZ4IZJ5VAA2B6XMROPE3Y63A7A/) (дата обращения: 20.08.2025).

14. Science ministry to spend \$3.7 bil. on key strategic technologies this year // TheKoreaTimes. 2024. URL: [https://www.koreatimes.co.kr/www/tech/2024/01/
133_367778.html](https://www.koreatimes.co.kr/www/tech/2024/01/133_367778.html) (дата обращения: 20.08.2025).

15. The Global AI Index // Tortoise Media. URL:
<https://www.tortoisemedia.com/intelligence/global-ai> (дата обращения:
18.08.2025).

16. The National Guidelines for AI Ethics // AI Ethics Communication Channel.
2020. URL: <https://ai.kisdi.re.kr/eng/main/contents.do?menuNo=500011> (дата об-
ращения: 18.08.2025).

17. Zwetsloot R., Feldgoise J., Dunham J. Trends in U.S. Intention-to-Stay
Rates of International Ph.D. Graduates Across Nationality and STEM Fields // CSET.
2020. URL: [https://cset.georgetown.edu/publication/trends-in-u-s-intention-to-
stay-rates-of-international-ph-d-graduates-across-nationality-and-stem-fields/](https://cset.georgetown.edu/publication/trends-in-u-s-intention-to-stay-rates-of-international-ph-d-graduates-across-nationality-and-stem-fields/)
(дата обращения: 25.08.2025).

18. 박영민 신약개발단장 "한국 R&D 비용 적어...선택과 집중해야" [Пак Ен Мин, руководитель группы по разработке новых лекарств: «Затраты на НИОКР в Корее низкие... Нам нужно выбирать и концентрироваться»] // Yonhap News. 2024. URL: <https://www.yna.co.kr/view/AKR20240320083400017?section=search> (дата обращения: 25.08.2025).

19. 윤 "민관역량 총결집 '국가 AI 컴퓨팅센터' 구축...2027 년 AI 'G3' 도약"(종합) [Юн: «Создание «Национального вычислительного центра ИИ» путем объединения возможностей государственного и частного секторов... Переход к ИИ «G3» к 2027 году»] // NEWSIS. 2024. URL: https://www.newsis.com/view/NISX20240926_0002900325 (дата обращения: 18.08.2025).

Д. В. Маслова,
студент,
Белорусский государственный университет транспорта,
А. И. Морочковская,
студент,
Белорусский государственный университет транспорта

Роль чат-ботов в системе правовой поддержки населения

Аннотация. В статье рассматриваются особенности применения чат-ботов в юридической сфере в контексте цифровизации профессиональной деятельности. Описаны этапы функционирования чат-ботов, их классификация по функциональному назначению, а также выделены основные преимущества и риски, связанные с их внедрением. Наряду с этим анализируются ограничения, связанные с интерпретацией правового контекста, отсутствием юридической ответственности, угрозами конфиденциальности и нормативной неопределенностью. Представленный материал может быть полезен для специалистов в области права, информационных технологий и государственного регулирования.

Ключевые слова: чат-бот, юриспруденция, цифровизация, правовая помощь, конфиденциальность, нормативное регулирование, RuGPT

D. V. Maslova,
student,
Belarusian State University of Transport,
A. I. Morochkovskaya,
student,
Belarusian State University of Transport

The role of chatbots in the system of legal support for the population

Abstract. The article explores the use of chatbots in the legal field within the broader context of digital transformation in professional practice. It outlines the stages of chatbot operation, their classification by functional purpose, and highlights key advantages and risks associated with their implementation. The analysis also addresses limitations such as challenges in interpreting legal context, lack of legal accountability, threats to confidentiality, and regulatory uncertainty. This material may be useful for professionals in law, information technology, and public administration.

Keywords: chatbot, jurisprudence, digitalization, legal assistance, confidentiality, normative regulation, RuGPT

Введение. Юридический рынок, традиционно ассоциирующийся с обширным документооборотом, значительным объемом бумажной работы и длительными судебными заседаниями, в настоящее время переживает масштабную цифровую трансформацию. Внедрение искусственного интеллекта (ИИ), чат-ботов и автоматизированных решений меняет устоявшиеся представления

о функционировании юридических служб, адвокатских практик и корпоративных юридических отделов. По состоянию на 2025 год эти изменения приобретают не только трендовый, но и прикладной характер, оказывая непосредственное влияние на организацию правовой деятельности.

Основная часть. Одним из наиболее распространенных инструментов цифровизации выступают **чат-боты** – программные интерфейсы, способные вести диалог с пользователем в текстовой или голосовой форме. Благодаря способности обрабатывать типовые запросы, чат-боты позволяют существенно сократить затраты на техническую поддержку и административные функции, частично заменяя соответствующих сотрудников.

Работа чат-бота строится на последовательной обработке пользовательского запроса, включающей следующие ключевые этапы:

1. Распознавание запроса. На первом этапе бот анализирует входящее сообщение с использованием технологий обработки естественного языка (Natural Language Processing, NLP). Целью анализа является выявление пользовательского намерения (например, «узнать», «записаться», «оформить») и извлечение релевантных данных.

2. Поиск релевантного ответа. В зависимости от архитектуры чат-бота применяются различные подходы:

- Скриптовые боты осуществляют поиск ответа в заранее заданной базе сценариев и шаблонов.

- ИИ-боты формируют ответ на основе обученных моделей машинного обучения, что позволяет учитывать контекст и вариативность запросов.

3. Формирование и передача ответа. Сформированный ответ может быть представлен в различных форматах – текстовом, графическом, голосовом или интерактивном (например, кнопки, ссылки), в зависимости от интерфейса взаимодействия.

Классификация чат-ботов по функциональному назначению:

1. Информационные (FAQ-боты). Предоставляют справочную информацию, отвечают на типовые вопросы.

2. Консультативные. Ориентированы на помощь в выборе продукта или услуги, предоставляют рекомендации на основе пользовательских запросов.

3. Операционные. Выполняют конкретные действия: бронирование, оформление заказа, регистрация, оплата.

4. Образовательные. Используются для обучения, тестирования, интерактивного освоения материала.

5. Развлекательные. Ведут неформальный диалог, рассказывают шутки, участвуют в играх [6].

Среди достоинств применения чат-ботов в юриспруденции можно выделить следующие:

1. **Повышение доступности правовой помощи.** Чат-боты обеспечивают круглосуточный доступ к базовым юридическим консультациям без необходимости личного обращения к специалисту. Это особенно актуально для граждан, проживающих в регионах с ограниченной инфраструктурой правовых услуг.

2. Снижение нагрузки на специалистов. Обработка типовых запросов с помощью чат-ботов позволяет юристам сосредоточиться на более сложных и нестандартных задачах, тем самым повышая общую эффективность работы юридических отделов и служб поддержки.

3. Оптимизация документооборота. Автоматизированное составление договоров, заявлений и жалоб сокращает время подготовки документов, снижает вероятность технических ошибок и способствует ускорению внутренних процессов.

4. Стандартизация обработки запросов. Использование чат-ботов обеспечивает единообразие в предоставлении информации и соблюдение внутренних регламентов, что критически важно для юридической точности и корпоративного соответствия.

5. Интеграция с LegalTech-инфраструктурой. Чат-боты могут быть интегрированы с базами нормативных данных, CRM-системами и платформами электронного документооборота, становясь частью единой цифровой экосистемы юридической практики [1].

Также необходимо отметить, что существуют и некоторые риски:

1. Ограниченное понимание контекста. Даже при использовании ИИ чат-боты могут некорректно интерпретировать сложные правовые формулировки, особенно при неструктурированных запросах.

2. Отсутствие юридической ответственности. Бот не является субъектом права, а его рекомендации не имеют юридической силы. Ошибки могут привести к принятию неверных решений пользователем.

3. Риски конфиденциальности. Работа с персональными и юридически значимыми данными требует соблюдения высоких стандартов безопасности. Нарушения могут повлечь ответственность для владельца системы.

4. Ограниченность функционала. Чат-бот не способен заменить профессиональное суждение, оценить риски или стратегические последствия. Он выполняет вспомогательные задачи в рамках алгоритмической обработки.

5. Нормативная неопределенность. Во многих странах отсутствует четкое регулирование использования чат-ботов в правовой сфере, что затрудняет их официальную интеграцию в юридическую практику [1].

6. Для более подробного ознакомления с возможностями чат-ботов в сфере правовой поддержки населения, был рассмотрен один из наиболее доступных и используемых инструментов – ruGPT, русскоязычный чат-бот, работающий на базе модели GPT-4o.

RuGPT способен не только генерировать осмысленные тексты по юридическим темам, но и отвечать на вопросы граждан, анализировать документы, прогнозировать исходы судебных дел и адаптироваться к различным сценариям развития событий [5].

К основным преимуществам чат-бота можно отнести:

- Быстрая обработка запросов.
- Готовые шаблоны.
- Доступ без VPN – работает стабильно на территории Российской Федерации и Республики Беларусь».
- Бесплатный доступ.

Несмотря на доступность, функционал бесплатной версии RuGPT ограничен:

Количество запросов в сутки ограничено;

Полный и глубокий анализ документов и прогнозирование судебных решений доступны только по подписке.

Для проверки практической эффективности RuGPT был составлен тестовый запрос, представленный на рисунке 1. В нем описывалась ситуация, связанная с досрочным расторжением договора аренды нежилого помещения по инициативе арендодателя.

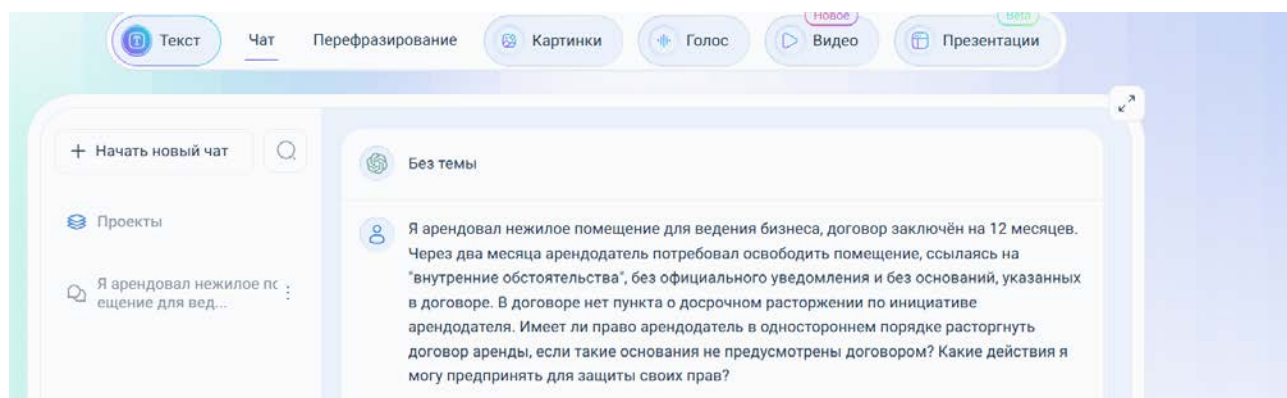


Рис. 1. Текстовый запрос

RuGPT обработал запрос и выдала ответ, представленный на рисунках 2 и 3. Ответ содержал следующие пункты:

ссылки на статьи ГК РФ, регулирующие порядок расторжения договора;
пояснение о правах арендатора и арендодателя;

рекомендации по действиям, включая возможность подачи претензии или обращения в суд;

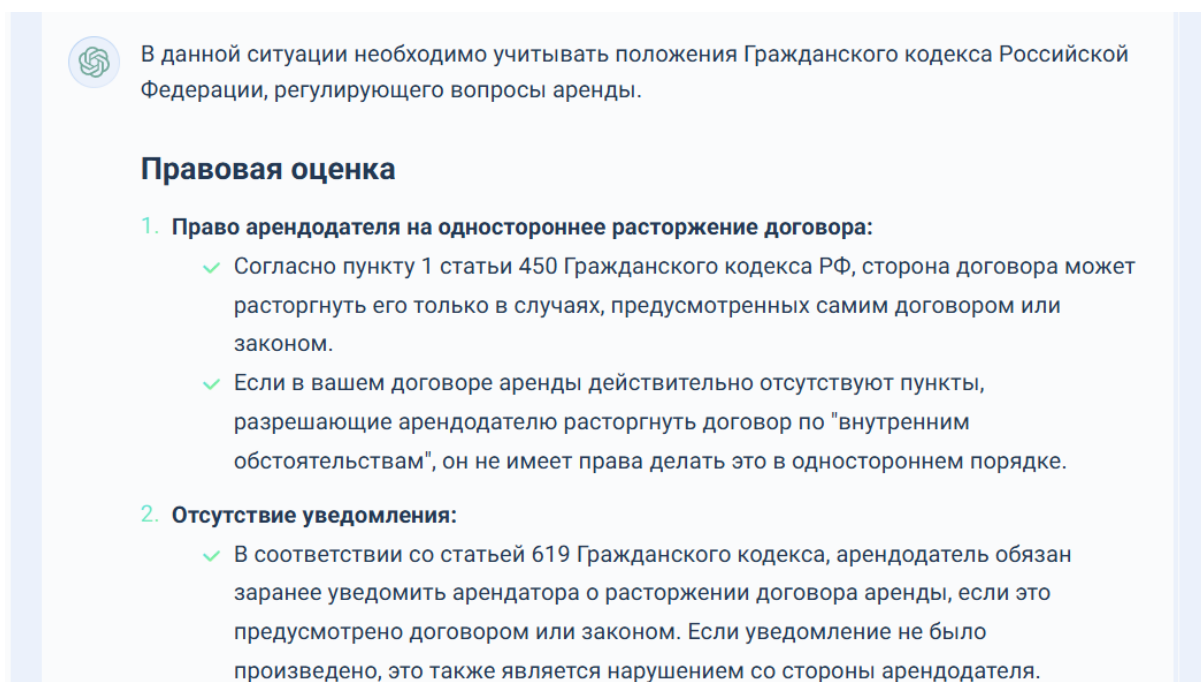


Рис. 2. Ответ ruGPT

Возможные действия для защиты прав

1. Договориться с арендодателем:

- ✓ Попробуйте провести переговоры с арендодателем для выяснения ситуации и поиска компромиссного решения, если это возможно.

2. Письменное уведомление:

- ✓ Направьте арендодателю письменное уведомление о том, что вы отказываетесь освободить помещение, так как расторжение договора без достаточных оснований и уведомления является неправомерным.

3. Обращение в суд:

- ✓ Если арендодатель не изменит свое решение, вы можете подать иск в суд о признании действий арендодателя неправомерными и о сохранении права на аренду помещения до истечения срока договора.
- ✓ Также вы можете требовать компенсацию убытков, если они возникли в результате действий арендодателя.

4. Консультация юриста:

- ✓ Рекомендуется обратиться к квалифицированному юристу для подготовки и подачи иска, а также для получения консультаций по вашим правам и обязанностям.

Заключение

Вы имеете законные основания для продолжения использования арендованного помещения до истечения срока аренды, если арендодатель не исполняет условия договора. Ваши действия должны быть юридически обоснованными и документально оформленными для защиты своих интересов.

Рис. 3. Ответ ruGPT

RuGPT показал, что способен давать понятные и обоснованные юридические ответы, опираясь на нормы действующего законодательства.

Это подтверждает, что нейросеть может быть полезна как инструмент для первичной правовой помощи – особенно, когда нужно быстро сориентироваться и понять, какие шаги предпринять.

Заключение. Таким образом, чат-боты на базе нейросетей делают правовую помощь доступной, быстрой и понятной. Они помогают гражданам ориентироваться в законах и получать консультации. При этом чат боты остаются вспомогательным инструментом – не заменяя профессиональную защиту, а дополняя ее.

Список литературы

1. Как ИИ и чат-боты меняют юридический рынок в 2025 году? URL: <https://tatarpravo.ru/blog/tpost/sbxatpr8f1-kak-ii-i-chat-boti-menyayut-yuridicheski> (дата обращения: 04.09.2025).

2. Как юридические чат-боты могут улучшить доступ к правосудию URL: <https://investinfo.pro/view?url=kak-yuridicheskie-chat-boty-mogut-uluchshity-dostup-k-pravosudiyu-&id=52223> (дата обращения: 04.09.2025).

3. Лучшие нейросети для юридических консультаций в 2025 году. URL: <https://vc.ru/id2581788/1845105-luchshie-neiroseti-dlya-yuridicheskikh-konsultacii-v-2025-godu> (дата обращения: 04.09.2025).

4. Нейросеть для решения юридических задач. URL: <https://rugpt.io/nejroset-dlya-resheniya-yuridicheskikh-zadach?categoryId=ce122089-d680-4e68-83dc-0b49db27154c&chatId=2969b378-810d-4b50-b328-04a141d3997c> (дата обращения: 04.09.2025).

5. Нейросети для юристов. URL: <https://epicai.ru/professions/4-yuristy> (дата обращения: 04.09.2025).

6. Что такое чат-боты и зачем они нужны? FAQ по видам, целям и сценариям текстов. URL: <https://petr-panda.ru/chto-takoe-chat-boty-faq> (дата обращения: 04.09.2025).

А. Г. Мухатдинова,
студент,
Санкт-Петербургский государственный университет

Правовые аспекты использования регуляторных «песочниц» (regulatory sandboxes)

Аннотация. В условиях цифровой трансформации традиционные правовые механизмы сталкиваются с необходимостью адаптации к новым технологическим вызовам. Цель исследования заключается в анализе правовых аспектов функционирования регуляторных «песочниц» как инструмента экспериментального регулирования. В работе рассматривается генезис данного института, начиная с практики Британского управления по финансовому регулированию и надзору (UK Financial Conduct Authority, FCA), проводится сравнение зарубежных моделей и отечественного опыта, включая соотношение с экспериментально-правовыми режимами. Особое внимание уделено проблемам выбора модели регулирования, а также вопросу пределов реализации регуляторных песочниц. Выявлены преимущества и ограничения их внедрения в российское правовое пространство, а также возможности дальнейшей эволюции. Сделан вывод о значимости данного института как эффективного механизма стимулирования инноваций при условии учета национальной специфики и обеспечения баланса между свободой эксперимента и защитой публичных интересов.

Ключевые слова: право, цифровые технологии, экспериментально-правовой режим, регуляторная песочница, экспериментальное регулирование, инновации, правовой эксперимент

A. G. Mukhatdinova,
student,
St. Petersburg State University

Legal aspects of usage of regulatory sandboxes

Abstract. In the context of digital transformation, traditional legal mechanisms are faced with the need to adapt to new technological challenges. The aim of the study is to analyse the legal aspects of the functioning of regulatory sandboxes as a tool for experimental regulation. The article examines the genesis of this institution, starting with the practice of the FCA, and compares foreign models and national experience, including the connection with experimental legal regimes. Particular attention is paid to the problems of choosing a regulatory model, as well as the issue of the limits of implementing regulatory sandboxes. The advantages and limitations of introducing sandboxes into the Russian legal space are identified, as well as the possibilities for their further evolution. A conclusion is made about the importance of sandboxes as an effective mechanism for stimulating innovation, provided that na-

tional specifics are taken into account and a balance is ensured between freedom of experimentation and the protection of public interests.

Keywords: law, digital technologies, experimental legal regime, regulatory sandbox, experimental regulation, innovation, legal experiment

Введение. Современная эпоха цифровой трансформации характеризуется стремительной интенсификацией информационных технологий и их интеграцией в общественно-экономические сферы, что требует адаптации правовых механизмов для обеспечения баланса между стимулированием инноваций и защитой публичных интересов. В этой связи все более распространенным становится экспериментальное правовое регулирование, включающее различные инструменты. Одним из них являются регуляторные (регулятивные) «песочницы» (от англ. regulatory sandboxes), которые постепенно приобретают значимость по всему миру.

Основная часть. Создание института регуляторных «песочниц» (далее также – песочницы) было инициировано FCA в ноябре 2015 г. с целью поддержки финтех-компаний [9. С. 4]. За 10 лет было объявлено о разработке более 190 регуляторных песочниц в сферах информационных технологий, искусственного интеллекта (ИИ), медицины, финансов и т. д. [8]. По данным исследований, 7 регуляторных песочниц установлены на международном уровне [11. С. 6]. Кроме того, данный специфический правовой режим создан при поддержке Банка России и в отечественной системе [3].

Первоначально FCA определила «регуляторные песочницы» как «некое «безопасное пространство», в котором предприятия могут тестировать инновационные продукты, услуги, бизнес-модели и механизмы их реализации, не сталкиваясь при этом со всеми обычными регуляторными последствиями, связанными с осуществлением данной деятельности» [10. С. 6]. Банк России дает следующую дефиницию: «Регулятивная «песочница» Банка России – это механизм для пилотирования, моделирования процессов новых финансовых сервисов и технологий в изолированной среде, требующих изменения правового регулирования» [3]. Обобщая, можно сказать, что «регуляторная песочница» – это инструмент нормативно-правового регулирования, представляющий исключения из стандартного законодательно установленного режима отдельным субъектам в целях развития передовых технологий и инновационных продуктов.

Данное понятие закреплено на законодательном уровне во многих странах, например, Сингапуре, Норвегии, Южной Корее, США и иных [7. С. 217–296]. Кроме национальных систем, регуляторные песочницы установлены и в международных актах: наиболее ярким примером служит European Union Artificial Intelligence Act [4].

Экспериментальное регулирование, в том числе песочницы, преследует две основные цели. В краткосрочной и среднесрочной перспективе достигается по большей части экономическая цель: разработка инновационных технологий, а также поддержка предпринимательского сообщества, которое способствует данному прогрессу. В долгосрочной перспективе достигается цель, связанная с правотворческим потенциалом регулирования: стратегическое формирование

гибкой нормативной среды таким образом, чтобы она соответствовала темпам общественного развития [6. С. 4]. Стремительное распространение регуляторных песочниц свидетельствует о них, как об эффективном средстве достижения данных целей.

В качестве основных субъектов регуляторных песочниц стоит выделить регулятора и самих участников экспериментального режима. Регулятором является специально уполномоченный государственный орган, осуществляющий регулирование в определенной сфере: финансово-экономической, технологической и др. К участникам относятся субъекты предпринимательской деятельности. Кроме того, в работу регуляторной песочницы могут быть включены и иные субъекты: профильные научные и этические советы, наднациональные органы, граждане и т.д.

Создание песочниц влечет за собой не только преимущества, но и некоторые риски и проблемы. Во-первых, возникает вопрос о модели управления экспериментального режима. Можно предположить три основных концепта:

1. Государственно-центрированное регулирование. Регулятор осуществляет самостоятельное администрирование, включающее контроль и мониторинг за деятельностью участников регуляторных песочниц и иных субъектов на всех этапах пилотирования проектов;

2. Делегированное (частное) регулирование. Участники экспериментального режима действуют в основном самостоятельно с минимальным влиянием регулятора, что может выражаться в различных формах: отбор участников, установление общих принципов деятельности, оценка результатов и т.д.;

3. Гибридное регулирование. Такая модель предполагает действие участников песочницы и регулятора в равной степени.

Каждый подход обуславливает различные юридические последствия: например, субъекты юридической ответственности, гибкость нормотворчества и прозрачность принятия решений (табл. 1).

Таблица 1

Сравнение моделей управления регуляторной песочницей

Критерий сравнения / модель управления	Государственно-центрированная	Делегированная (частная)	Гибридная
Субъекты юридической ответственности	Определяются регулятором. Чаще всего ответственность несут участники	Определяются участниками при возможном вмешательстве регулятора	Ответственность распределяется между участниками и регулятором (а также, возможно, иными субъектами)
Гибкость нормотворчества	Нормотворчество, в основном, негибкое. Регулятор собирает эмпирические данные, а изменение	Гибкое нормотворчество, поскольку участники и иные субъекты могут оказывать	Относительно гибкое нормотворчество. Участник могут вносить предложения законодательных

Критерий сравнения / модель управления	Государственно- центрированная	Делегированная (частная)	Гибридная
	регулирование происходит лишь в долгосрочной перспективе	значительное влияние на результаты деятельности регуляторной песочницы, в том числе и на изменение отдельных норм в соответствии с такими результатами	изменений, преобразуя нормы совместно с регулятором
Прозрачность принятия решений	Высокая транспарентность, что обусловлено публичностью деятельности регулятора как органа государственной власти	Присутствует риск снижения прозрачности по причине множественности лиц, ответственных за принимаемые решения	Относительно высокая прозрачность, поскольку регулятор может осуществлять контроль за принятием итоговых решений

Наиболее распространенным в данный момент является государственно-центрированный подход, что обусловлено характером песочниц как подвида экспериментальных режимов (примеры стран: Россия, Норвегия, Малайзия, Индия и др.). В первую очередь это исключение из законодательно установленного регулирования, в связи с чем за ним должны осуществляться более внимательное наблюдение и контроль. Однако перспективной также стоит признать и гибридную модель (черты гибридного регулирования присущи регуляторным песочницам в США) [10. С. 6]. Она позволит снизить административные барьеры и повысить адаптированность правового регулирования, что может стимулировать развитие инновационных технологий и законодательной системы.

С выбором концепта управления также связана и вторая проблема – пределы реализации регуляторных песочниц. В государственно-центрированной модели, как правило, действие песочниц значительно ограничено регулятором. Несмотря на то, что его полномочия не могут быть всеобъемлющими, на практике они, как правило, не являются исчерпывающими и не содержат точного перечня, что создает пространство для широкого толкования. Регулирующие органы во многих случаях занимаются деятельностью, которая не оговорена явно, что, тем не менее, вызывает вопросы относительно «нормативности такого порядка действий» [12. С. 5].

С одной стороны, это позволяет обеспечить стабильность системы, гарантировать правовую определенность, осуществить контроль за регуляторной песочницей и предупредить возможные риски, связанные с ней. С другой стороны, такие пределы не позволяют свободно реализовывать многие прорывные идеи в силу недостаточной целесообразности, высоких административных барьеров и стоимости участия или крайне ограниченной свободы субъектов. Видится, что наиболее оптимальным решением вопроса пределов стало бы уstra-

нение их унифицированности в различных секторах. К примеру, регуляторные песочницы в сфере медицины или финансов могут иметь более жесткие режимы, так как иное повлекло бы множество рисков [5. С. 4]. А песочницы в сфере ИИ и иных технологических разработок могут получить больше преимуществ от гибкого режима и расширенных пределов.

Как уже было упомянуто ранее, в России также создана регулятивная песочница под руководством Банка России. Тем не менее, данный институт не так распространен, как «экспериментальные правовые режимы» (далее – ЭПР), установленные федеральным законодательством в 2021 г. [1]. В отечественной доктрине существует мнение о том, что это взаимозаменяемые понятия, поскольку «они сущностно не отличаются и обладают тождественными признаками» [2. С. 5]. Однако даже в законодательстве между ними существуют различия.

Во-первых, для ЭПР в соответствии с законом установлена жесткая формализованная процедура с более длинными сроками рассмотрения инициативы. Требования регулятивной песочницы упрощены: заявка подается через онлайн платформу, и не требует детальной информации о проекте. Во-вторых, ЭПР позволяет полноценно реализовать проект и преодолеть некоторые правовые нормы на основании официального статуса. Регулятивная песочница предполагает только пилотные проекты (прототипы), не включающие реальных клиентов и операций, что негативно сказывается на объективности и достоверности результатов проекта. В-третьих, срок действия ЭПР составляет 3 года, а фаза активного пилотирования проекта в регулятивной песочнице длится около 30 дней.

Заключение. Таким образом, у каждого из институтов есть свои преимущества и недостатки. ЭПР характеризуется большей стабильностью и возможностями, но имеет значительные административные барьеры и ограничения. Регулятивная песочница отличается более гибким режимом, однако подходит для небольших проектов и не предоставляет привилегий.

Регуляторные песочницы обладают потенциалом развития в рамках национальной системы как разновидность ЭПР. Установление более свободного регулирования позволило бы обеспечить стимулирование инновационных разработок, международное сотрудничество, дифференцированный режим управления, а также дать большую свободу инициаторам. Однако адаптация зарубежных практик должна быть разумной, с учетом особенностей отечественной правовой системы, рисков и целей международной кооперации.

Список литературы

1. Федеральный закон от 31.07.2020 № 258-ФЗ (ред. от 31.07.2025) «Об экспериментальных правовых режимах в сфере цифровых и технологических инноваций в Российской Федерации» // СПС «КонсультантПлюс». URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=511291&dst=1000000001&cacheid=4D33186B76D40DA5624EA59048FDAC4B&mode=splus&rnd=unjn0wUamdU5YbYN#mOon0wUWgI8uIQYq1>.

2. Земляникова А. В. Экспериментальные правовые режимы как механизм внедрения цифровых инноваций // Вестник Университета имени ОЕ Кутафина. 2025. № 4 (128). С. 197–203.
3. Регуляторная песочница // Банк России URL: https://www.cbr.ru/fintech/regulatory_sandbox/ (дата обращения: 06.09.2025);
4. Artificial Intelligence Act (P9_TA(2024)0138) // European Parliament. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf (дата обращения: 06.09.2025).
5. Kim J. AP Regulatory Fintech Quick Guide / J. Kim, S. Lee, A. K. M. Shafique et al // Baker McKenzie. January 2018. URL: https://www.bakermckenzie.com/-/media/files/insight/publications/2018/01/qrg_ap_regulatoryfintech_jan18.pdf (дата обращения: 06.08.2025).
6. Mateusz Bonca, Jolanta Jabłońska-Bonca. «Regulatory Sandboxes – Two Perspectives». // Krytyka Prawa 3:304–327. 2024;
7. OECD Regulatory Policy Outlook 2021 // OECD (2021). OECD Publishing, Paris. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/oecd-regulatory-policy-outlook-2021_c5274577/38b0fdb1-en.pdf (дата обращения: 06.09.2025).
8. Portal on Regulatory Sandboxes: research project // Centre for Competition Policy [Электронный ресурс]. URL: <https://competitionpolicy.ac.uk/research-projects/portal-on-regulatory-sandboxes/> (дата обращения: 06.09.2025);
9. Regulatory sandboxes and fintech funding: evidence from the UK // Bank for International Settlements. October 2020 (revised April 2023). URL: <https://www.bis.org/publ/work901.pdf> (дата обращения: 06.09.2025).
10. Regulatory sandboxes for digital health // World Bank Group. URL: <https://documents1.worldbank.org/curated/en/099011825011040830/pdf/P175075-0c729174-1c7a-4f04-9bb2-4127f301c037.pdf> (дата обращения: 06.09.2025);
11. Sandboxes for AI: Tools for a new frontier // Datasphere Initiative (2025). URL: <https://www.thedatasphere.org/wp-content/uploads/2025/02/Report-Sandboxes-for-AI-2025.pdf> (дата обращения: 06.09.2025).
12. Vladimír Sharp, Gabriela Blahoudková. «Setting up the Legislative Framework for the Introduction of a Regulatory Sandbox: the Czech Perspective» // Acta Universitatis Carolinae Iuridica 2:35–48. 2024.

Общедоступные данные в регулировании обучения ИИ-моделей

Аннотация. Целью исследования является комплексный анализ правовой природы «общедоступных данных» применительно к обучению искусственного интеллекта, а также выявление ограничений и рисков использования открытых источников в подготовке обучающих наборов. В статье рассматриваются нормы российского законодательства (ФЗ–152), положения Общего регламента по защите данных (GDPR) и Регламента ЕС об искусственном интеллекте (AI Act). Отдельное внимание уделяется понятию данных, разрешенных субъектом для распространения, а также механизмам прозрачности и оценки воздействия (DPIA, FRIA) при скрейпинге и повторном использовании информации. Делается вывод, что «общедоступность» не устраняет правовых обязанностей оператора, а напротив, требует дополнительного COMPLIANCE в части правовых оснований, информирования субъектов и исключения недопустимых практик обучения, прямо запрещенных AI Act.

Ключевые слова: право, цифровые технологии, искусственный интеллект, персональные данные, GDPR, AI Act, биометрия, DPIA, FRIA

А. А. Olifirenko,

Master's student,

Saratov State Law Academy

Publicly available data in the regulation of ai model training

Abstract. The purpose of the study is to provide a comprehensive analysis of the legal nature of «publicly available data» in the context of artificial intelligence training, as well as to identify the limitations and risks of using open sources in the preparation of training datasets. The article examines the provisions of Russian legislation (Federal Law No. 152–FZ), the General Data Protection Regulation (GDPR), and the EU Artificial Intelligence Act (AI Act). Particular attention is paid to the concept of data disclosed by the subject for dissemination, as well as to mechanisms of transparency and impact assessment (DPIA, FRIA) in cases of scraping and reuse of information. The conclusion is drawn that «public availability» does not remove the operator's legal obligations but, on the contrary, requires additional compliance in terms of legal grounds, subject notification, and the exclusion of inadmissible training practices explicitly prohibited by the AI Act.

Keywords: law, digital technologies, artificial intelligence, personal data, GDPR, AI Act, DPIA, FRIA

Введение. Понятие «общедоступные данные» часто используется в бытовой речи, однако с юридической точки зрения оно является неоднозначным и способно вводить в заблуждение. Российский законодатель заменил представ-

ление о «данных, доступных всем» специальной категорией – персональными данными, «разрешенными субъектом для распространения» (ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ) [1]). Для их обработки необходимо отдельное, информированное и детализированное согласие, в котором субъект вправе установить запреты и условия дальнейшего использования информации третьими лицами. Несоблюдение этих условий делает обучение моделей незаконным, даже если технический доступ к источнику открыт.

Основная часть. Общие принципы обработки закреплены в ст. 5 ФЗ №152-ФЗ (законность, справедливость, целевое ограничение, соразмерность), а правовые основания установлены в ст. 6. Для специальных категорий и биометрических данных действуют усиленные требования (ст. 10–11), а оператор обязан обеспечить безопасность обработки и учет действий с данными (ст. 18–19). В праве Европейского союза Общий регламент по защите данных (GDPR) [2] прямо указывает, что публичная доступность источника не лишает информацию статуса персональных данных и не освобождает от соблюдения принципов ст. 5, наличия правового основания по ст. 6 и ограничений ст. 9 для специальных категорий. Если сбор осуществляется не у самого субъекта, информирование в соответствии со ст. 14 является обязательным, а исключение о «непропорциональных усилиях» не освобождает от внедрения защитных мер и обеспечения базовой прозрачности. Дополнительный уровень регулирования вносит AI Act [3], который вводит запреты на практики «неприемлемого риска», включая создание или расширение баз данных распознавания лиц через нетаргетированный скрейпинг изображений из интернета и систем видеонаблюдения. Кроме того, AI Act устанавливает требования к качеству и управляемости обучающих данных для систем высокого риска и к прозрачности для моделей общего назначения, распространяя действие норм и на случаи, когда использование модели происходит в ЕС независимо от места ее обучения.

DPIA и FRIA интегрируются в эту систему как обязательные или рекомендуемые элементы оценки добросовестности обработки. DPIA (Data Protection Impact Assessment) представляет собой формализованную оценку воздействия на защиту данных, предусмотренную ст. 35 GDPR. Она включает описание операций и целей обработки, характеристику категорий данных и субъектов, анализ необходимости и соразмерности, оценку рисков для прав и свобод, а также меры по снижению рисков – как технические, так и организационные. Результатом является вывод о допустимости остаточного риска, а при необходимости проводится консультация с надзорным органом. Для проектов обучения ИИ проведение DPIA необходимо при масштабном мониторинге публичных пространств, обработке специальных категорий, массовом скрейпинге, внедрении новых технологий и в случаях вероятности значительного ущерба для субъектов данных.

FRIA (Fundamental Rights Impact Assessment) – это инструмент более широкого характера, направленный на оценку воздействия на фундаментальные права. Он активно развивается в доктрине, руководствах регуляторов и методических документах, связанных с применением AI Act. FRIA охватывает не только защиту

данных и приватность, но также свободу выражения, недопущение дискриминации, равный доступ к услугам, трудовые и образовательные права, а также право на эффективные средства правовой защиты. Методология FRIA предполагает: определение затрагиваемых прав, описание возможных механизмов причинения вреда при обучении и использовании модели, оценку вероятности и серьезности последствий, проектирование мер по снижению рисков (ограничение источников, фильтрация, де-идентификация, внедрение принципа «privacy by default» и «privacy by design»), оценку остаточного риска и определение критериев его приемлемости, а также разработку плана независимого аудита и процедур для обжалования решений лицами, права которых могут быть затронуты [4].

В экосистеме AI Act FRIA органично связана с требованиями к управлению рисками и документацией для систем высокого риска, а также с кодексами практики для моделей общего назначения GPAI (General-Purpose AI). Этот инструмент позволяет соединить защиту фундаментальных прав с инженерными параметрами моделей. Следует подчеркнуть, что в рамках европейских требований GPAI – это не любая модель, а именно та, которая предназначена для многоцелевого применения и способна создавать значительные риски для прав человека и безопасности.

Запретные практики в отношении общедоступных источников определены напрямую. AI Act относит к недопустимому риску создание или расширение баз распознавания лиц посредством нетаргетированного скрейпинга изображений из интернета и систем видеонаблюдения. С 2 февраля 2025 года такие практики запрещены к размещению на рынке, вводу в эксплуатацию и использованию, независимо от того, каким образом собирались изображения и были ли они общедоступны. Даже если модель формально не является системой распознавания лиц, обучение на таком корпусе может поставить под сомнение законность ее применения, особенно в случаях, когда модель способна извлекать или усиливать биометрические шаблоны. В рамках GDPR регуляторы государств-членов уже квалифицировали подобные практики как незаконные из-за отсутствия правовых оснований и нарушений принципов ст. 5, 6, 9 и 14, что согласуется с новой системой ограничений, установленной AI Act.

Управление качеством и происхождением данных перестало быть факультативной рекомендацией и превратилось в юридически обязательное требование. Для систем высокого риска AI Act предусматривает проверяемую управляемость данных (ст. 10): провайдер обязан документировать источники, подтверждать репрезентативность, полноту и релевантность наборов, обеспечивать точность и устойчивость моделей, описывать меры кибербезопасности, а также фиксировать версии и трассируемость данных. Для GPAI в главе V вводятся обязательства по раскрытию информации и реализации кодексов практики (ст. 56), которые формируют стандарты прозрачности обучающих наборов и уравнивают интерес к защите коммерческой тайны с необходимостью общественной подотчетности. Эта система документирования тесно связана с DPIA и FRIA: выявление источникового риска, анализ смещений и дискриминационных эффектов, применение мер минимизации и проверка их эффективности должны быть зафиксированы в досье на систему и в отчетности по процессу обучения [5].

Заключение. Можно заключить, что «общедоступные данные» – это характеристика канала распространения, а не правовое основание для обучения ИИ. Российский режим ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» делает распространение контролируемой сферой: субъект определяет запреты и условия, а оператор обязан их соблюдать наряду с общими принципами и основаниями обработки. Европейский режим GDPR не рассматривает «публичность» как освобождение от требований законности, минимизации и прозрачности; при масштабных обучающих операциях обязательна оценка воздействия на защиту данных, а при наличии рисков для фундаментальных прав и недопущения дискриминации необходима также оценка воздействия на права человека. AI Act устраняет неопределенности: некоторые практики обучения на общедоступных источниках прямо запрещены; для систем высокого риска и GPAI вводятся требования к управляемости данными, документированию, раскрытию и кодексам практики, а сфера действия распространяется и на международные цепочки разработки, если результаты используются в ЕС. Практический вывод: допустимость обучения на открытых источниках определяется связанной оценкой по указанному закону и GDPR, проведением DPIA/FRIA и соответствием AI Act, а не самим фактом доступности ресурса в сети; чем масштабнее скрейпинг, чувствительнее категории данных и дальше цели обучения от исходного контекста публикации, тем строже должен быть набор правовых оснований, уведомлений, технических мер и ограничений по источникам.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451; 2025. № 26 (ч. 1). Ст. 3486.
2. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // Official Journal of the European Union. OJ L 119. 04.05.2016. P. 1–88.
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008, (EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) // Official Journal of the European Union. OJ L 2024/1689. 12.07.2024.
4. Novelli C., Casolari F., Hacker P., Spedicato G., Floridi L. Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity // Computer Law & Security Review. 2024. Vol. 55. Article 106066.
5. Kattinig M., Angerschmid A., Reichel T., Kern R. Assessing trustworthy AI: Technical and legal perspectives of fairness in AI // Computer Law & Security Review. 2024. Vol. 55. Article 106053.

К. С. Павлова,

курсант,

Санкт-Петербургский университет МВД России

**Влияние цифровизации судебной деятельности на доступность
и эффективность правосудия в условиях современной правовой системы**

Аннотация. Данная статья раскрывает фундаментальные преобразования судебной системы в эпоху цифровых инноваций, акцентируя внимание на уникальной роли технологий в трансформации правосудия. Рассматривается внедрение электронных платформ, искусственного интеллекта и автоматизированных процессов. Предлагаются новые концептуальные подходы к оценке эффективности цифровизации, подчеркивая необходимость комплексного перехода судебной системы к инновационной модели, основанной на прозрачности и интерактивном взаимодействии с гражданами.

Ключевые слова: право, цифровизация, судебная деятельность, электронное правосудие, модернизация правовой системы, правовая трансформация, виртуальные судебные заседания

K. S. Pavlova,

student,

St. Petersburg University of the Ministry of Internal Affairs of Russia

**The impact of digitalization of judicial activities on the accessibility
and effectiveness of justice in the context of the modern legal system**

Abstract. This article explores the fundamental transformations of the judicial system in the era of digital innovation, emphasizing the unique role of technology in the transformation of justice. The article discusses the introduction of electronic platforms, artificial intelligence, and automated processes. It proposes new conceptual approaches to assessing the effectiveness of digitalization, emphasizing the need for a comprehensive transition of the judicial system to an innovative model based on transparency and interactive communication with citizens.

Keywords: law, digitalization, judicial activities, electronic justice, modernization of the legal system, legal transformation, virtual court sessions

Введение. Современная правовая система претерпевает интенсивные трансформации под влиянием цифровых технологий, которые кардинально меняют способы предоставления судебных услуг и взаимодействия с правосудием. По данным Счетной палаты России за 2025 год, общий уровень внедрения цифровых технологий в судах оценивается в 8,81 балла из 10. В период с 19 марта по 11 мая 2020 года суды рассмотрели 3,4 млн дел и материалов, из них более

13 тыс. – с использованием системы видео–конференц–связи, а электронные сервисы государственной автоматизированной системы «Правосудие» были использованы свыше 300 млн раз. Это подтверждает важную роль цифровизации в обеспечении непрерывности, доступности и прозрачности правосудия.

Основная часть. Научные исследования различных аспектов цифровизации судебной деятельности становятся все более интенсивными, изобилуют непривычными юристам словами и категориями, но, как представляется, ограничиваются лишь отдельными институтами [1. С. 154]. Цифровизация судебной деятельности подразумевает системное внедрение информационно-коммуникационных технологий (ИКТ) с целью переосмысления традиционных процедур правосудия. Это не просто перевод документов в электронный формат, а создание комплексной технологической среды, включающей электронные системы делопроизводства, цифровые платформы для взаимодействия сторон, автоматизированные решения для мониторинга судебных процессов и внедрение элементов искусственного интеллекта. Основные цели цифровизации:

- 1) обеспечение открытости и прозрачности судопроизводства через электронный доступ к информации и публичным реестрам;
- 2) ускорение рассмотрения дел за счет автоматизации процессов и снижения процедурных издержек;
- 3) упрощение доступа к судебным услугам, особенно для жителей отдаленных регионов и маломобильных групп населения, благодаря дистанционным технологиям;
- 4) снижение бумажного документооборота.

Важной составляющей является развитие единой информационной системы судов, которая интегрирует все компоненты судебной деятельности, облегчая взаимодействие между судами, участниками процесса и государственными органами.

Цифровые технологии значительно расширяют возможности доступа граждан к правосудию. Один из аспектов принципа доступности, как отмечает Г.А. Жилин, заключается в создании реальной возможности быть допущенным к процессуально–правовому механизму в целях защиты нарушенного или неправомерно оспариваемого права [2. С. 148]. В свою очередь электронные сервисы позволяют подавать иски онлайн, получать мгновенный доступ к судебным материалам и участвовать в судебных заседаниях через видеоконференцсвязь, что особенно важно для жителей отдаленных регионов, инвалидов и социально уязвимых групп. Это снижает необходимость физического присутствия, что экономит время и средства.

Также автоматизация снижает вероятность коррупционных проявлений и ошибок, связанных с ручной обработкой документов, что повышает общественное доверие к судебной системе. Ее внедрение способно резко сократить проявления любых форм коррупции в сфере правосудия, поскольку физические и юридические лица будут лишены возможности лично контактировать сотрудниками государственных учреждений, что автоматически означает невозможность использования личных договоренностей в процессе принятия решений в пользу той или иной стороны [3. С. 140]. Электронное правосудие обеспечивает про-

зрачность, позволяя контролировать ход процесса и своевременность рассмотрения дел. Внедрение цифровых платформ способствует интеграции информации и унификации процедур на разных уровнях судебной системы, что улучшает качество правовой помощи и способствует более справедливым решениям.

Цифровизация оказывает значительное влияние на эффективность всей судебной системы. Электронные системы управления делами позволяют ускорять обработку информации, обеспечивать прозрачный контроль сроков рассмотрения и оперативно контролировать исполнение судебных решений. Это приводит к существенному снижению затягивания процессов и повышению оперативности работы судов.

Использование аналитических инструментов на базе искусственного интеллекта помогает выявлять типичные ошибки и управлять рисками, такими как затягивание рассмотрения дел. Искусственный интеллект также выступает в роли вспомогательного инструмента для судей, помогая анализировать большие объемы информации и прогнозировать возможные исходы, при этом сохраняя роль человека в принятии решения.

Кроме того, цифровизация снижает рутинную нагрузку на судей и сотрудников аппарата, освобождая их время для решения более сложных и важных задач, что в итоге повышает качество судебных решений и работу всей судебной системы.

Несмотря на очевидные преимущества, внедрение цифровых технологий в судебной системе сопровождается значительными вызовами и проблемами:

1) неравномерный доступ к интернету и современным цифровым устройствам.

2) недостаточная подготовка кадров и низкий уровень цифровой грамотности судей, сотрудников аппарата судов и участников процесса порождают трудности при использовании новых технологий.

3) вопросы информационной безопасности, защита персональных данных и обеспечение конфиденциальности судебных процессов становятся критически важными в условиях возросших киберугроз.

4) недостаточное нормативно-правовое регулирование цифровых аспектов судебной деятельности.

5) этические и юридические вопросы, связанные с использованием искусственного интеллекта и автоматизированных систем в принятии решений, включая риски ограничения права на справедливое судебное разбирательство и обеспечение независимости судей.

Заключение. Перспективы цифровизации судебной деятельности тесно связаны с комплексным подходом к развитию технологий, кадровой подготовки и правового регулирования. Для успешной цифровой трансформации необходимо:

1) улучшение технического оснащения судов и обеспечение равного доступа к цифровым инструментам для всех участников процесса;

2) повышение квалификации судей и сотрудников с акцентом на навыки работы с новыми технологиями и цифровую этику;

3) создание и совершенствование нормативно-правовой базы, регулирующей цифровые процессы в судах, включая стандарты информационной безопасности и защиты персональных данных;

4) акцент на повышении правовой грамотности граждан для эффективного использования электронных сервисов;

5) внедрение контролируемых и прозрачных систем искусственного интеллекта, обеспечивающих помощь в анализе, но не замену человеческого фактора в вынесении решений;

6) разработка единой стратегии цифровизации судебной системы с учетом зарубежного опыта и современных тенденций в области цифрового правосудия.

Такой подход позволит не только повысить доступность и эффективность правосудия, но и укрепить доверие общества к судебной системе, сохраняя при этом основные принципы справедливого и независимого судопроизводства.

Список литературы

1. Курочкин С. А. Цифровые технологии и эффективность правосудия // Lex Russica. 2022. №10 (191). URL: <https://cyberleninka.ru/article/n/tsifrovye-tehnologii-i-effektivnost-pravosudiya> (дата обращения: 12.08.2025).

2. Долотин Р.Р. Электронное правосудие как средство реализации принципа доступности гражданского судопроизводства // Учен. Зап. Казан. Ун-та. Сер. Гуманит. Науки. 2021. №2. URL: <https://cyberleninka.ru/article/n/elektronnoe-pravosudie-kak-sredstvo-realizatsii-printsipa-dostupnosti-grazhdanskogo-sudoproizvodstva> (Дата обращения: 12.08.2025).

3. Мирошниченко О.И., Филоненко Т.В. Цифровые технологии как фактор снижения коррупционных проявлений в судебной системе // Legal Concept. 2020. №2. URL: <https://cyberleninka.ru/article/n/tsifrovye-tehnologii-kak-faktor-snizheniya-korrupcionnyh-proyavleniy-v-sudebnoy-sisteme> (дата обращения: 12.08.2025).

**Криптовалюта в Российской Федерации:
проблемы правового режима и перспективы регламентации**

Аннотация. Актуальность настоящего исследования обусловлена отсутствием единого подхода к регулированию криптовалюты и возникающей, в связи с этим неопределенностью субъектов права в защите своих прав на нее. В статье изучается природа криптовалюты при помощи анализа действующего законодательства и научных работ. Для выявления пробелов в правовом регулировании сопоставляются отечественные и зарубежные судебные дела, в которых фигурирует исследуемый объект, отмечается неоднородность судебной практики. Определяется место криптовалюты в системе объектов гражданских прав с учетом анализа нормативного и научного материала. В работе выдвигается ряд предложений по введению новых законодательных положений для решения поставленной проблемы.

Ключевые слова: цифровизация, криптовалюта, правовая природа, кибермошенничество, блокчейн, майнинг, перспективы регламентации

A. O. Isakova,

Student,

Far Eastern Federal University

**Cryptocurrency in the Russian Federation:
problems of the legal regime and prospects for regulation**

Abstract. The relevance of this study is due to the lack of a unified approach to the regulation of cryptocurrency and the resulting uncertainty among legal entities in protecting their rights to it. The article examines the nature of cryptocurrency through an analysis of current legislation and scientific works. To identify gaps in legal regulation, domestic and foreign court cases involving this object are compared, and the heterogeneity of judicial practice is noted. The article determines the place of cryptocurrency in the system of objects of civil rights, taking into account the analysis of regulatory and scientific material. The paper presents a number of proposals for introducing new legislative provisions to address this issue.

Keywords: digitalization, cryptocurrency, legal nature, cyber fraud, blockchain, mining, prospects for regulation

Введение. Цифровая трансформация влечет внедрение новых технологий в различные сферы жизнедеятельности людей, в результате чего они начинают активно фигурировать в их правоотношениях, оказывая влияние на их содержа-

ние. В частности, это проявляется в возникновении новых объектов правоотношений. Одним из них является цифровая валюта, а именно, ее вид – криптовалюта, получившая правовое закрепление в 2020 году в Федеральном законе от 31 июля 2020 г. № 259-ФЗ "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" (далее – Закон о ЦФА) [12]. Однако на сегодняшний день правовой режим данного объекта окончательно не урегулирован – он различается в зависимости от того, предметом какого вида правоотношений выступает: по общему правилу криптовалюта не является объектом права, но в ряде институтов гражданского и уголовного права она признается имуществом. Таким образом, отсутствует единообразие в подходе к регулированию криптовалюты, что создает неопределенность в ее обращении для субъектов права. Обозначенная проблема явилась предметом исследования ряда ученых. С учетом анализа их научных работ стоит выделить несколько устоявшихся точек зрения по этому вопросу: криптовалюта – это средство платежа; она не входит в круг объектов прав; она входит в категорию «иного имущества». В рамках данной статьи мы рассмотрим варианты отнесения криптовалюты к различным видам объектов прав и выясним, какие можно выделить перспективы ее правовой регламентации.

Основная часть. Перед анализом правовой природы криптовалюты следует установить, является ли она разновидностью цифровой валюты, и начать следует с легального определения последней, закрепленного в Законе о ЦФА. Так, согласно ч. 3 ст.1 цифровая валюта – это совокупность электронных данных, которые содержатся в информационной системе и предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей. Исходя из понятия можно сделать вывод, что цифровая валюта не производна от обыкновенной, не является ее разновидностью, так как она не представляет собой денежную единицу. На данный момент законодатель прямо не устанавливает перечень видов цифровой валюты, в связи с чем в научной среде существует мнение, что криптовалюта вовсе не производна от цифровой валюты, так как она не является законным средством платежа в России. Для устранения неопределенности в этом вопросе стоит обратиться к положениям вышеуказанного закона, где отмечено, что цифровая валюта предлагается или может быть принята средством платежа, в отличие от обыкновенной валюты, которая законодательно признается таковой, поэтому не следует отождествлять эти понятия. Кандидат юридических наук Зазулин А.И. в своей статье «Цифровые валюты. Цифровые права» приводит еще один аргумент в поддержку позиции об отличиях цифровой валюты от криптовалюты, утверждая, что для признания криптовалюты цифровой, она должна быть выпущена сертифицированным государством оператором, который ведет реестр пользователей и имеет возможность точно идентифицировать лицо, владеющее криптовалютой [4. С.3.]. В соответствии с ч. 5 ст. 14.2 Закона о ЦФА операторами информационных систем могут быть индивидуальные предприниматели и юридические лица только после включения в соответствующий реестр. Однако субъектам, осуществляющим майнинг (добывающим криптовалюту), законодатель дает относительную свободу в этом плане: физические лица, при соблюдении ограниче-

ний по энергопотреблению, установленных в ч. 2 данной статьи, имеют право осуществлять ее получение без предоставления сведений в реестр. Приобрести данный цифровой объект можно не только путем майнинга, а также путем покупки. В этом случае законодатель не устанавливает обязанностей для сторон сделки направлять сведения о себе в государственный орган. Таким образом, идентифицировать субъектов, участвующих в обороте криптовалюты, практически невозможно. Причиной этого является не только отсутствие императивного законодательного регулирования, но и специфика платформы, на которой осуществляется обращение с криптовалютой: в ее основе лежат децентрализованные технологии блокчейн, которые маскируют IP-адреса и затрудняют отслеживание источника транзакции. С учетом проведенного анализа законодательства можно сделать вывод, что криптовалюта является разновидностью цифровой валюты, однако ее отличие заключается в меньшем контроле со стороны государства. Так, цифровой рубль, введение которого планируется осуществить в ближайшее время, согласно Федеральному закону от 24.07.2023 N 340-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации" [13] признается в качестве средства платежа, выпускается одним оператором – Банком России, пользование им не анонимно – возможно после открытия счета и заключения договора с оператором, а криптовалюта обладает противоположными характеристиками: она не является средством платежа, требование к идентификации пользователей–физических лиц не всегда предъявляется, но тем не менее она входит в понятие «цифровой валюты», так как не противоречит положениям закона и отвечает признакам, предъявляемых его положениями. Установив, что криптовалюта является разновидностью цифровой валюты, раскроем ее сущность, определив понятие и характерные черты.

«Крипто» в переводе с греческого означает «тайный», или «скрытый», «валюта» происходит от итальянского *valuta* – «стоимость, монета». Этимология слова объясняет специфику данного объекта: криптовалюта защищена благодаря использованию криптографии, которая включает в себя способы обеспечения безопасности и целостности данных при помощи шифрования. Согласно обзору Центрального Банка по криптовалютам от декабря 2017 года, криптовалюта представляет собой децентрализованную виртуальную валюту, основанную на математических алгоритмах и защищенную методами криптографии [6. С.4.]. В научной литературе выделяют еще одно понятие, в котором под криптовалютой понимается цифровая валюта, основанная на применении криптографии для создания и контроля новых единиц валюты и осуществления транзакций [3. С.132.]. Объяснить понятие можно путем рассмотрения признаков криптовалюты. Часть из них уже была изучена нами ранее – это те черты, которые присущи цифровой валюте, их можно назвать «родовыми»:

- 1) представляет собой совокупность электронных данных (цифрового кода или обозначения);
- 2) содержится в информационной системе;
- 3) не является денежной единицей в Российской Федерации.

Вместе с этим можно выделить существенные признаки криптовалюты, то есть те, которые характерны только для нее:

- 1) не имеет статуса законного платежного средства;
- 2) имеет относительную свободу от государственного контроля;
- 3) их оборот является анонимным.

Первый признак предполагает, что криптовалюта не признается законодательством в качестве официального платежного средства в России. Согласно п.1 ст.140 ГК РФ единственным законным платежным средством в нашей стране является рубль, в т.ч. в цифровой форме [2]. Это характерно и для других государств, где данный объект признается цифровым активом/иностранной валютой/имуществом/платежным средством, но тем не менее, не является законным средством платежа, ввиду того, что криптовалюта не имеет единого эмитента, который бы гарантировал и обеспечивал ее выпуск, в связи с чем повышен риск операций с ней: государство не может гарантировать надежность и безопасность обращения с тем средством платежа, которое неподконтрольно ему. Однако можно привести в пример Сальвадор, первую страну, в которой принятый 9 июня 2021 года «Закон о биткоинах» признал биткоин, разновидность криптовалюты, в качестве законного средства платежа [16]. Принятие данного закона вызвало отрицательную реакцию Международного валютного фонда (финансовой организации ООН), члены Исполнительного совета которого указали, что использование биткоина в качестве законного платежного средства связано с крупными рисками для финансовой стабильности. В связи с этим, в рамках соглашения с фондом, 30 января 2025 года Конгресс Сальвадора одобрил законопроект об упразднении официального статуса биткоина. Вторым признаком является то, что операции с криптовалютой в меньшей степени подконтрольны государственным органам, несмотря на то, что с каждым годом законодатель вводит новые требования и ограничения относительно их оборота. Тем не менее, стоит отметить, что операции с криптовалютой не настолько детально регламентированы законодателем, в отличие от тех же цифровых финансовых активов. Третий признак предполагает отсутствие возможности идентифицировать пользователя криптовалюты, ввиду использования криптографии для обеспечения безопасности и анонимности транзакций, а также для создания новых единиц валюты.

При рассмотрении правовой природы криптовалюты следует дать ответ на ключевой вопрос: какое место она занимает среди объектов прав? Этот вопрос остается дискуссионным ввиду того, что нормативная основа данного объекта крайне незначительна и неоднородна. В последнее десятилетие возникало множество точек зрения по этому поводу, мы анализируем самые преобладающие. Объекты гражданского права включают в себя материальные и нематериальные блага. Некоторые ученые считают, что криптовалюта представляет собой нематериальное благо, выраженное в стоимостном эквиваленте. Однако данная позиция противоречит доктрине гражданского права, в которой существенным признаком личных неимущественных прав является неотчуждаемость от личности и отсутствие экономического содержания, чего о криптовалюте сказать нельзя, поэтому будем рассматривать только возможность причисления данного объекта к какому-либо виду материальных благ. Материальными благами согласно ст. 128 ГК РФ являются вещи, иное имущество (в т.ч. имуще-

ственные права), результаты работ и оказание услуг. Последние два объекта не вызывают интереса, так как криптовалюта как объект прав не содержит обязательственного элемента в себе и может предполагать просто ее принадлежность определенным субъектам. Можно ли на исследуемый объект распространять правовой режим вещей? Для того, чтобы дать ответ на этот вопрос следует обратиться к некоторым существенным признакам вещей: материальность и индивидуальность. Криптовалюта, в отличие от вещи, нематериальна, так как она представляет собой совокупность электронных данных, которые не облечены в физическую форму. Мы уже выяснили, что оборот данного объекта из-за децентрализованного учета преимущественно анонимный (если пользователи-физические лица не будут предоставлять сведения в реестр), поэтому криптовалюта по общему правилу не индивидуализирована. Таким образом, она не является вещью. Данная позиция подтверждается судебной практикой: Савеловский районный суд в своем решении от 03.12.2021 по делу № 02-2888/2021 отказал в требовании истца о виндикации части криптовалюты, которую он передал ответчику в доверительное управление, после чего последний отказался ее возвращать [10]. Объектом виндикационного иска является индивидуально-определенная вещь, существующая в натуре, имеющая физическую форму. Невозможность признания цифрового объекта в качестве вещи стала одной из причин того, что суд отказал истцу в требовании ввиду ненадлежащего объекта иска. Помимо этого, суд указал, что права истца не могут быть защищены в силу ч. 6 ст. 14.2 Закона о ЦФА, где прямо указано, что в случае, если лицо не проинформировало налоговый орган об обладании цифровой валютой, то его требование не подлежит удовлетворению. Исходя из толкования ст. 128 ГК РФ перечень иного имущества является открытым – это может быть обусловлено тем, что с научно-техническим прогрессом появляются новые объекты гражданских прав, большая часть из которых не имеет физической формы, не может быть отнесена к категории движимых или недвижимых вещей, однако обладает ценностью. В этой связи допустимым вариантом представляется распространять на криптовалюту правовой режим «иного имущества».

Закон о ЦФА ст. 20–26 вводит дополнения в иные законы, в связи с чем криптовалюта признается имуществом только в двух институтах гражданского права: в делах о банкротстве (включение ее в конкурсную массу должника) и по части возмещения ущерба при легализации (отмывании) имущества. Однако на практике суды признают ее имуществом при заключении договора купли-продажи. Так, Верховный суд в определении по делу № 44-КГ20-17-К7 признал криптовалюту имуществом [8]. Обстоятельства дела были таковы, что потерпевшая являлась клиентом ПАО «Сбербанк» (истца) и в один день мошенниками были совершены переводы денежных средств в размере 930 700 рублей с ее счета на номер ответчика. Ответчик пояснил, что считал, будто денежные средства ему поступили в результате совершения ряда сделок купли-продажи криптовалюты. Он полагал, что потерпевшая является покупателем и не подозревал о мошенничестве со стороны неустановленных лиц. Истец потребовал взыскания с ответчика данных денежных средств в пользу потерпевшей в качестве неосновательного обогащения и его требование было частично удовлетво-

рено апелляционной инстанцией, с этим согласился кассационный суд. Как пояснили суды, у ответчика отсутствовало правовое основание для получения денежных средств. Однако Верховный суд указал, что у ответчика были правовые основания для получения денежных средств, поскольку «передав свое имущество (криптовалюту) взамен полученных денежных средств», у него была определенная экономическая цель, в которой не содержится ничего неправомерного. Таким образом, на данном примере мы видим, как влияет правовая природа криптовалюты на защиту прав граждан. Еще одно дело в подтверждение тезиса о том, что на криптовалюту стоит распространять правовой режим иного имущества, содержится в зарубежной судебной практике. В Англии все объекты права делятся на три вида: недвижимое имущество, личное имущество и интеллектуальная собственность. Впервые после завершения судебного разбирательства Высокий суд Англии и Уэльса в деле Д'Алоя против Неустановленных лиц, Bitkub и других (D'Aloia v Persons Unknown, Bitkub and others (2024) EWHC 2342 (Ch)), подтвердил, что криптовалюта, в частности USD Tether (сокращенно – USDT), может считаться личной собственностью в соответствии с английским законодательством [15]. Так как в англо-саксонской правовой системе среди источников права преобладает судебный прецедент, суд сослался на раннее вынесенное судебное решение Высокого суда Англии и Уэльса в деле AA против Неустановленных лиц (AA v Persons Unknown (2019) EWHC 3556 (Comm)), в котором было указано, что криптоактивы, такие как биткоин, могут рассматриваться как имущество [14]. Данные решения были вынесены по делам о мошенничестве, в которых была произведена кража криптовалюты. Заместитель судьи Ричард Фарнхилл в своем решении по делу от 2024 года описал USDT как «довольно уникальную форму собственности, которая не зависит от основных юридических прав», что делает ее подлежащей отслеживанию и способной составлять трастовую собственность, как и другие активы. В решении от 2019 года, на которое ссылался судья, Апелляционным судом было отмечено, что криптоактивы соответствуют критериям имущества, установленным в решении Национального банка Англии по делу Эйнсворт (National Provincial Bank Ltd v Ainsworth, 1965):

- 1) их можно идентифицировать;
- 2) они могут быть предметом владения третьих лиц;
- 3) они имеют некоторую степень постоянства и стабильности [17].

Первый критерий может показаться спорным, так как ранее мы выяснили, что оборот криптовалюты может быть анонимным. Однако в рассмотренных судебных делах истцы-владельцы подтвердили свое право на данный объект – это является важным условием для защиты их права на криптовалюту как на имущество. С учетом анализа теории объектов гражданского права и отечественной и зарубежной судебной практики можно сделать вывод о том, что признание криптовалюты в качестве «иного имущества» в гражданско-правовых спорах имеет потенциал.

Проблема определения места криптовалюты в системе объектов гражданских прав неразрывно связана с вопросом о квалификации преступлений, совершенных с ее использованием. Поскольку Уголовный кодекс не раскрывает

понятие «имущества» как предмета посягательства, в связи с чем возникает необходимость руководствоваться гражданским законодательством. На сегодняшний день криптовалюта на законодательном уровне была признана имуществом лишь в двух составах преступлений, а именно – легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем и приобретенных лицом в результате совершения им преступления (ст. 174, 174.1 УК РФ) [11]. В развитие положения, введенного Законом о ЦФА (ст. 17 Закона), в постановлении Пленума Верховного Суда РФ от 26.02.2019 N 1 было разъяснено, что предметом преступления могут являться денежные средства, преобразованные из криптовалюты, приобретенной в момент совершения преступления [9]. Возникает неопределенность относительно того, будет ли криптовалюта являться предметом иных преступлений, совершенных против права собственности, к примеру мошенничества (ст. 159 УК РФ), вымогательства (ст. 163 УК РФ). Логично, что если прямого указания законодателя на это нет, то и суды в случае рассмотрения деяния, совершенного с использованием криптовалюты и не связанного с легализацией доходов, добытых преступным путем, не должны его квалифицировать как преступление по вышеуказанным статьям из-за отсутствия объекта в составе преступления. Более того, в постановлениях пленума Верховного суда, разъясняющих составы данных преступлений, определено содержание предмета посягательства и криптовалюты там нет. Однако на практике суды, разрешая дела о мошенничестве и вымогательстве, признают ее в качестве предмета посягательства. Так, Восьмой кассационный суд признал обвиняемого виновным в совершении мошенничества по ч. 4 ст. 159 УК РФ. Обвиняемый с иными лицами, представившись сотрудником правоохранительных органов и введя потерпевшего в заблуждение, потребовал от него передачи биткоинов. В кассации обвиняемый просит суд отменить решение, поскольку криптовалюта, согласно действующему законодательству, не является предметом хищения. Суд не удовлетворил его требование, указав, что данный цифровой объект имеет материальную ценность и вывод нижестоящих инстанций об отнесении ее к имуществу является обоснованным [1]. Аналогичный вывод сделал Третий кассационный суд по делу о вымогательстве, указав, что криптовалюта может быть принята в качестве средства платежа и относиться к иному имуществу, следовательно, является объектом хищения [5]. Таким образом, из-за наличия пробела в правовом регулировании криптовалюты и отсутствия прямого указания закона на признание ее в качестве иного имущества в гражданском законодательстве, отнесение рассматриваемого объекта к предмету посягательства в преступлениях остается полностью на усмотрение судей, которые истолковывают ст. 128 ГК РФ в пользу потерпевших.

Отнесение криптовалюты к иному имуществу в первую очередь создаст правовое основание для ее владения и устранил неопределенность в вопросе удовлетворения требований истцов о защите их прав. Однако для этого следует ввести меры принуждения для исполнения лицами обязанности по уведомлению Федеральной налоговой службы о факте владения криптовалютой, в том случае, если они являются собственниками в результате ее майнинга – это явля-

ется необходимым условием для того, чтобы подтвердить их право. Так как в данный момент информирование государственных органов является правом, а не обязанностью, то и защита прав не во всех случаях удовлетворяется судами. Помимо этого, если криптовалюта перестанет быть анонимной и будет признана имуществом, то это позволит определить ее как предмет сделки (например, в случае заключения договора купли–продажи) и предоставит возможность сторонам приводить доказательства в пользу действительности сделки. В противном случае, недобросовестные участники гражданского оборота, покупая криптовалюту, требуют с продавцов возврата денежных средств, ссылаясь на нормы о неосновательном обогащении, и суды удовлетворяют их требования, мотивируя тем, что отношения с использованием криптовалюты не урегулированы законодательно, в связи с чем установить предмет сделки и доказательства ее совершения невозможно. С другой стороны, можно выделить отрицательное последствие признания криптовалюты имуществом. Распространенными являются дела о мошенничестве с криптовалютой, в которых от имени и за счет потерпевших неизвестные лица совершают сделки купли–продажи криптовалюты, в результате чего истцы просят суд взыскать с ответчиков их денежные средства ввиду неосновательного обогащения. В деле, рассматриваемом Верховным судом (С. 4–5), со счета потерпевшей мошенниками был списан почти миллион рублей, и частично эта сумма была взыскана с ответчика в качестве неосновательного обогащения в Апелляционном суде, однако Верховный суд направил дело на пересмотр, указав, что ответчик получил их от неустановленных лиц на правомерном основании, так как предоставлением по договору купли–продажи является имущество (цифровая валюта). Таким образом, потерпевшие лишаются возможности возмещения причиненного им материального ущерба ввиду неосновательного обогащения.

Также стоит рассмотреть перспективы наследования криптовалюты. Хотя на сегодняшний день это не распространенное явление в России, однако учитывая, что с каждым годом рост обладателей цифровой валюты растет (по данным обзора финансовой стабильности Центрального Банка объем криптовалюты на кошельках пользователей за 2024–2025 год увеличился на 27% и достиг 827 млрд рублей), то можно предположить, что рано или поздно встанет вопрос о возможности ее наследования [7. С. 76]. Сейчас юристы отмечают, что наряду с отсутствием причисления криптовалюты к каким-либо объектам прав в гражданском кодексе причиной, по которой ее нельзя включить в наследство, является ее анонимность и защищенность. Решением первой проблемы может служить предоставление в качестве доказательств права собственности выписки с криптовалютной биржи, которая подтвердит сделку купли–продажи, совершенную наследодателем, либо выписки из реестра о майнинге. Далее, после подтверждения прав на криптовалюту, для того, чтобы обеспечить доступ наследников к ней, им должен быть предоставлен ключ доступа к криптокошельку. При соблюдении последовательности данных действий представляется возможным включить данный объект в наследственную массу.

Если криптовалюта найдет свое правовое закрепление как имущество в гражданском праве, то будет логично внести изменения и в некоторые статьи

уголовного кодекса, устанавливающие ответственность за преступления против собственности, а также в акты толкования, разъясняющие, что подразумевается под имуществом в том или ином составе. Данные изменения следует внести в главу 21 кодекса, но не во все составы, а в те, в которых в качестве предмета посягательства упоминается имущество. При этом необходимо учитывать специфику криптовалюты, так как она имеет не физическую, а цифровую форму. Так, в правовом регулировании будет устранен пробел и суды в своих решениях будут ссылаться на прямое указание закона, а обвиняемые в совершении преступления с использованием криптовалюты будут лишены оснований подавать апелляционную жалобу из-за отсутствия данного объекта в числе имущества.

Заключение. В результате проведенного исследования было установлено, что правовое регулирование криптовалюты окончательно не сформировалось. Хотя оно значительно продвинулось с принятием Закона о ЦФА, который стал распространять на данный объект в ряде правовых институтов правовой режим имущества, тем не менее, вопросов в разрешении гражданских и уголовных споров возникло еще больше ввиду оставшихся пробелов в правовом регулировании. В зарубежной и отечественной судебной практике по разрешению дел, связанных с оборотом криптовалюты, наблюдается общая тенденция признания судами исследуемого объекта в качестве имущества. С учетом анализа правовой природы криптовалюты представляется возможным закрепить ее в качестве «иного имущества» в гражданском кодексе, а также внести разъяснения по вопросу определения предмета посягательства в преступлениях против собственности в уголовном кодексе и включить в содержание имущества криптовалюту.

Список литературы

1. Восьмой кассационный суд общей юрисдикции: Кассационное определение № 77–5316/2023 от 21.12.2023 // СПС «Клерк». URL: <https://www.klerk.ru/doc/631676/> (дата обращения: 23.05.2025).
2. Гражданский кодекс Российской Федерации. Часть первая, 30 ноября 1994 г. № 51-ФЗ // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 23.05.2025).
3. Егорова М.А., Ефимова Л.Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex russica. 2019. № 7. С.132.
4. Зазулин А.И. Цифровые валюты и права и др. в российском законодательстве и судебной практике // Экономика и жизнь. 2022. № 14 (1215). С.3.
5. Кассационное определение № 77–1578/2022 от 02.06.2022 Третьего кассационного суда общей юрисдикции // СудебныеРешения.рф [Электронный ресурс]. URL: <https://судебныерешения.рф/69166360> (дата обращения: 25.05.2025).
6. Обзор по криптовалютам, ICO (Initial Coin Offering) и подходам к их регулированию // Сайт Банка России. URL: https://cbr.ru/content/document/file/36009/rev_ico.pdf (дата обращения: 30.05.2025).
7. Обзор финансовой стабильности. IV квартал 2024 – I квартал 2025 года // Сайт Банка России. URL: https://cbr.ru/Collection/Collection/File/55878/4q_2024_1q_2025.pdf (дата обращения: 06.06.2025).

8. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 02.02.2021 N 44-КГ20-17-К7, 2-2886/2019 // Юридическая информационная система «Легалакт – законы, кодексы и нормативно-правовые акты Российской Федерации». URL: <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-02022021-n-44-kg20-17-k7-2-28862019/> (дата обращения: 03.06.2025)

9. Постановление Пленума Верховного Суда РФ от 26.02.2019 N 1 "О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года N 32 // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_319191/ (дата обращения: 11.06.2025).

10. Решение Савеловского районного суда от 03.12.2021 по делу № 02-2888/2021 // Официальный портал судов общей юрисдикции города Москвы. URL: <https://mos-gorsud.ru/rs/savyolovskij/services/cases/civil/details/c71e4241-6b8a-11eb-a99b-83b5cc923d6f> (дата обращения: 29.05.2025)

11. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 31.07.2025) // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 07.06.2025).

12. Федеральный закон "О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации" от 31.07.2020 № 259-ФЗ (последняя редакция) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения: 01.06.2025).

13. Федеральный закон "О внесении изменений в отдельные законодательные акты Российской Федерации" от 24.07.2023 № 340-ФЗ (последняя редакция) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_452645/ (дата обращения: 10.06.2025).

14. AA v Persons Unknown [2019] EWHC 3556 (Comm) // Ikigai Law. URL: <https://www.ikigailaw.com/wp-content/uploads/2020/03/Aa-v-Persons-Unknown-Who-Demanded-Bitcoin-on-10th-and-11th-October-2019-Persons-Unknown-Who-Own-Control-Specified-Bitcoin-iFINEX-trading-as-Bitfinex-BFXWW-Inc-trading-as-Bitfinex.pdf> (дата обращения: 24.05.2025)

15. D'ALLOIA V PERSONS UNKNOWN [2024] EWHC 2342 (Ch) // Appleby Law Firm. URL: <https://www.applebyglobal.com/wp-content/uploads/DAlloia-v-Persons-Unknown-2024.pdf> (дата обращения: 30.05.2025)

16. El Salvador's Bitcoin Law: Full English Text // Foundation for Research on Equal Opportunity (FREOPP). URL: <https://freopp.org/whitepapers/el-salvadors-bitcoin-law-full-english-text/> (дата обращения: 26.05.2025).

17. National Provincial Bank v Ainsworth // My Law Tutor. 2024. URL: <https://www.mylawtutor.net/cases/national-provincial-bank-v-ainsworth/> (дата обращения: 11.06.2025)

А. А. Подъячева,

студент,

Тульский государственный университет

**Концепция «Smart notary»:
цифровая трансформация нотариальной деятельности в России**

Аннотация. В статье рассматривается концепция цифровой трансформации нотариата в России через внедрение технологий искусственного интеллекта, блокчейна, квантовой связи и метавселенных. Автор анализирует текущее состояние Единой информационной системы нотариата и выявляет правовые и организационные проблемы, связанные с цифровизацией. Особое внимание уделяется рискам использования дипфейков, необходимости аудио- и видеофиксации действий, а также регулированию онлайн сервисов нотариусов. Предлагаются конкретные меры по интеграции перспективных технологий при сохранении баланса между инновациями и традиционными принципами нотариата. Автор подчеркивает важность активной роли нотариата в построении цифрового правопорядка, модернизации законодательства и развития ИТ-компетенций нотариусов.

Ключевые слова: цифровая трансформация, нотариальная деятельность, искусственный интеллект, блокчейн, квантовые технологии, метавселенные, кибербезопасность

A. A. Podyacheva,

student,

Tula State University (TSU)

**«The Smart notary» concept:
digital transformation of notary activities in the Russian Federation**

Abstract. The article examines the concept of digital transformation of the notary system in Russia through the introduction of artificial intelligence, blockchain, quantum communication, and metaverses. The author analyzes the current state of the Unified Information System of the Notary System and identifies legal and organizational challenges related to digitalization. Special attention is given to the risks of using deepfakes, the need for audio and video recording of actions, and the regulation of online presence of notaries. The article proposes specific measures to integrate promising technologies while maintaining a balance between innovation and traditional notary principles. The work emphasizes the importance of the notary's active role in building a digital legal system. It highlights the need for modernizing legislation and developing the IT competencies of notaries.

Keywords: digital transformation, notarial activity, artificial intelligence, blockchain, quantum technologies, blockchain, metaverses, cybersecurity

Введение. Понятие цифровизации предполагает внедрение цифровых технологий. Ее зачастую путают с информатизацией, которая является более широким понятием, включающим создание условий для удовлетворения всеобщей потребности в сборе, обработке, хранении, передаче информации при помощи информационно-коммуникационных технологий. Цифровая трансформация – изменение всего алгоритма работы, а не только внедрение цифровых технологий. Таким образом, концепция цифровой трансформации нотариальной деятельности предполагает не простое внедрение новых технологий, а изменение самой работы нотариуса, включая трансформацию нотариальных действий и даже появление новых их видов.

Основная часть. В юриспруденции в целом уже происходят структурные сдвиги, которые выводят на первый план цифровую обработку данных. В судах апробируют технологии искусственного интеллекта для автоматизированного изготовления судебных приказов [11], юристы анализируют судебную практику с использованием технологий big data для создания прогнозов по конкретному делу [12], налоговая служба создала систему машиночитаемых доверенностей на основе блокчейн-платформы [18]. Есть и иные примеры цифровой трансформации юридической деятельности. В связи с этим вызывает научный и практический интерес, что цифровизация дает нотариальной системе России.

Нотариусы одним из первых внедрили в свою деятельность сложные информационные системы обработки данных. Единая информационная система нотариата или ЕНОТ, представляет собой централизованную цифровую платформу, обеспечивающую электронный документооборот, ведение реестров нотариальных действий (включая реестр уведомлений о залоге движимого имущества, реестр наследственных дел и др.), а также взаимодействие нотариусов с государственными органами (ФНС, Росреестр, МВД) в рамках системы межведомственного электронного взаимодействия (СМЭВ). ЕНОТ позволяет нотариусам оперативно проверять юридически значимые сведения (например, данные ЕГРН или сведения о банкротстве), удостоверять сделки в электронной форме с использованием усиленной квалифицированной электронной подписи и официальные сайты нотариальных палат субъектов Российской Федерации, которые позволяют гражданам и организациям – дистанционно подавать документы через личный кабинет на официальных сайтах нотариальных палат субъектов Российской Федерации. Данные сайты функционируют как ключевые информационные порталы, предоставляя доступ к сервисам поиска нотариусов, проверки подлинности документов через QR-коды [1] и онлайн-записи на прием. Однако, несмотря на технологическую продвинутость системы, ее эффективность зависит от качества интеграции с государственными информационными системами, уровня цифровой грамотности.

Правовая регламентация работы с системой ЕНОТ достаточно общая, что на практике вызывает различные споры и непонимание у нотариального сообщества. Например, только в 2024 году был разъяснен вопрос о выдаче из ЕНОТ сведений третьим лицам [6]. До этого каждый нотариус решал этот вопрос по своему усмотрению. Функционирование ЕНОТ также не исключает технических сбоев. Именно поэтому критически важно не только регулярно повышать

юридические компетенции нотариусов, но и активно развивать их ИТ-навыки. Например, дистанционно проводить ежегодное обучение нотариуса информационным технологиям с постоянно обновляемой программой такого обучения.

Данная концепция внедрения информационных технологий в нотариальную деятельность порождает ряд правовых и организационных проблем, поэтому остановиться стоит на самых актуальных, приближенных к текущим реалиям.

1. Онлайн оказания услуг нотариусами и удаленные нотариальные действия в условия развития технологии – дипфейков (от англ. deepfake). В России ст. 152.1 ГК РФ защищает изображение гражданина от любого незаконного использования [13]. Дипфейк позволяет воспроизводить изображение и голос гражданина, что создает угрозу совершения нотариальных действий удаленно. Использовать технологию злоумышленник может по-разному. Например, вместо нотариуса участвовать в виртуальном взаимодействии, видоизменяя свое лицо, голос для внешнего соответствия личности нотариуса. Это позволит наследнику имитировать нотариальное действие для лица, которое желает изменить завещание, исключив из него наследника. В данном случае юридические последствия весьма интересны, так как уголовной ответственности наследник в рамках действующего законодательства может избежать, а помещать нотариальному действию и скомпрометировать нотариуса он вполне способен.

Для самого нотариуса наибольшую опасность представляют поддельные аудио- и видеозаписи, которые могут использоваться для фальсификации доказательств или манипуляций при удостоверении сделок. В этой связи необходимо внедрить технологию фактчекинга – автоматизированных систем проверки подлинности мультимедийных материалов с помощью искусственного интеллекта и развитие доступных сервисов верификации. Это позволит определять достоверность видео и аудио без специальных технических навыков. В связи с этим предлагается внести изменения в процедуру совершения нотариального действия удаленно, обязав нотариусов использовать технологии фактчекинга при совершении подобных нотариальных действий.

2. Аудио- и видеозапись нотариальных действий, так же как и видеофиксация протоколов нотариальных действий являются важным инструментом повышения прозрачности нотариальной деятельности и защиты добросовестных участников гражданского оборота. Сегодня нотариус вправе фиксировать нотариальные действия таким способом. При этом порядок создания и хранения таких записей утвержден Федеральной нотариальной палатой [9]. В подготовленном Минюстом проекте закона «О нотариате нотариальной деятельности в Российской Федерации» [10] (далее – Проект закона «О нотариате»), который может вступить в силу с 01.01.2026 закладывается обязательная аудио- и видеофиксация нотариусом удостоверения сделок по отчуждению недвижимости. Вероятно, было бы разумным распространить данную обязанность на все нотариальные действия, совершаемые вне нотариальной конторы. Также целесообразно пересмотреть существующий порядок. В нем, например, только пункты

10 и 11 посвящены мерам по защите данных, полученных в ходе видеофиксации. Этого явно недостаточно в условиях развития киберпреступности.

3. В подготовленном Минюстом проекте закона о нотариате есть часть 10 статьи 67: «Нотариус обязан информировать граждан и юридических лиц о своем месте нахождения и режиме работы, в том числе посредством размещения при входе в здание или помещение нотариальной конторы вывески, указателей, а также посредством официального сайта нотариуса в информационно-телекоммуникационной сети «Интернет».

Сайт в сети «Интернет» – «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет» [3]. Представляется, что после принятия законопроекта, все нотариусы будут вынуждены делать официальные собственные сайты. Это явно не рационально, так как не всегда хватает специальных знаний в данном вопросе для составления технического задания. Помимо создания сайта, необходимо на постоянной основе обеспечивать его функционирование, что создаст дополнительные проблемы. Более рациональным выглядит создание странички нотариуса на официальном сайте Региональной нотариальной палаты. Однако из буквального толкования законопроекта это недопустимо. В связи с этим считаем важным, оперативно направить замечания на законопроект в данной части от нотариального сообщества.

4. Учитывая активное присутствие нотариусов в социальных сетях, отсутствие четких профессиональных рекомендаций по их ведению может создавать риски нарушения этических норм, конфиденциальности и репутации нотариата, что делает актуальным разработку специализированных правил. Нотариусам, как и судьям, следует придерживаться строгих этических норм при ведении социальных сетей, избегая публикации профессиональных подробностей, обсуждения клиентских дел и любой информации, которая может подорвать доверие к профессии. Рекомендуется ограничиваться нейтральным контентом – новостями законодательства, общими правовыми советами и официальными объявлениями, не нарушая конфиденциальности без согласия нотариальной палаты. По аналогии с судебными органами нотариальные палаты могли бы разработать единые рекомендации по ведению публичных страниц, поскольку нотариусы, так или иначе, присутствуют в медиапространстве, и важно минимизировать риски репутационных потерь и профессиональных конфликтов, исходя из закрепленного ст.6.1 ФЗ «О нотариате» кодекса профессиональной этики нотариуса.

Вышеизложенное будет способствовать дальнейшей успешной информатизации нотариальной деятельности, чтобы перейти к цифровизации, нотариат должен внедрить цифровые технологии, к которым относят: искусственный интеллект; системы распределенного реестра; квантовые технологии; новые производственные технологии; компоненты робототехники и сенсорики; технологии беспроводной связи; технологии виртуальной и дополненной реальностей [5].

1. Самой перспективной, безусловно, выглядит интеграция нотариатом систем искусственного интеллекта (далее – ИИ). ИИ – 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 [4]. Известен прецедент, когда в нотариальной практике ИИ, созданный компанией Smart Engines, как сканер с множеством механизмов проверок смог успешно выявить все классы подделок паспорта РФ в системе нотариального делопроизводства «Экспресс», которую используют более 7 тыс. нотариусов по всей стране. Вся процедура распознавания паспортных данных и проверки подлинности занимает около секунды за счет использования сверхлегких 4.6-битных нейросетей, но закрывает риски преступлений фальсификаций и обеспечивает защиту интересов граждан и бизнеса при совершении нотариальных действий [19].

На ближайшем этапе становление ИИ могло бы предстать поэтапным внедрением его в рутинные процессы (проверка реквизитов документов, выявление подделок, анализ типовых сделок) с сохранением за нотариусом окончательного контроля и принятия юридически значимых решений, еще разработка федеральных стандартов валидации алгоритмов и создание защищенной ИИ-платформы нотариата с обязательным аудитом принимаемых системой решений, т.е. подвергаемая самоанализу. Это позволит повысить эффективность работы нотариусов без ущерба для надежности нотариальных действий и быстро составлять сводку по коэффициенту так называемых «ошибок» – неверных алогичных решений, принятых ИИ, противоречащих закону, и «плюсов» – корректных и отвечающих требованиям законодательства решениям. Искусственный интеллект обучаем, но пока в его работе будут проявляться погрешности и неточности, то он может служить нотариусам помощником в работе с массивами данных и алгоритмами проверок документов, совершенствуясь для более объемных задач.

2. Квантовая коммуникация, основанная на принципах квантового распределения ключей (QKD), может стать ключевым инструментом обеспечения информационной безопасности в нотариате. Угрозы, связанные с появлением квантовых компьютеров, способных взломать современные криптографические алгоритмы, требуют перехода на новые методы защиты данных. Сегодня QKD защищает данные в финансовой, оборонной, коммунальной сферах и здравоохранении. Внедрение QKD в нотариальную практику позволит гарантировать абсолютную криптографическую стойкость передачи данных при удостоверении сделок, хранение электронных документов и взаимодействия с государственными реестрами, исключая риски перехвата или подделки информации.

Учитывая, что нотариат играет критическую роль в обеспечении юридической чистоты сделок и превентивного правосудия, использование квантовых технологий может быть интегрировано в Единую информационную систему нотариата (ЕИС). Это повысит лояльность к электронным нотариальным действиям и подготовит нотариат к будущим вызовам цифровой эпохи. Пилотные проекты, подобные линии квантовой связи между Москвой и Санкт-Петербургом (2021 г.), демонстрируют готовность инфраструктуры РФ к таким решениям, однако требуют адаптации нормативной базы, включая экспериментальные правовые режимы для апробации технологий [14]. Особое значение имеет син-

хронизация этих мер с разработкой постквантовых алгоритмов шифрования, что обеспечит комплексную защиту как передаваемых данных, так и хранимой информации. Такой подход позволит нотариату РФ не только противостоять будущим квантовым угрозам, но и стать как минимум федеральным лидером в области безопасных цифровых юридических услуг.

3. Если рассматривать шире, то пока не урегулированным объектом виртуальных пространств являются метавселенные [15], формирующие цифровую идентичность и взаимодействие пользователей виртуальных пространств с элементами дополненной и смешанной реальности, открывают новые возможности для нотариата РФ, особенно в контексте фиксации цифровых активов и доказательств. Например, нотариальный осмотр сайта для выявления диффамации может быть дополнен технологиями метавселенных, позволяя фиксировать не только текстовый или мультимедийный контент, но и его виртуальное представление, включая взаимодействие пользователей с таким контентом в 3D-среде. Это особенно актуально для случаев, когда диффамация проявляется через интерактивные элементы или динамически изменяющиеся данные.

Для внедрения таких решений нотариальным палатам следует обратить внимание на разработку стандартов фиксации данных в метавселенных, включая использование NFT для удостоверения подлинности цифровых доказательств. Это потребует обновления нормативной базы, например включения метавселенных в перечень технологий для экспериментальных правовых режимов или создания новых юридических норм, как это уже предложено для квантовых коммуникаций. Подобные инновации не только повысят точность нотариальных действий, но и фактически создадут новое нотариальное действие, в котором Россия сможет стать мировым лидером.

4. Современное законодательство постепенно адаптируется к использованию распределенных реестров и блокчейн-технологий в правоприменительной практике. Так, в соответствии с Письмом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 февраля 2024 г. № П15-13439 «Об информационной системе хранения машиночитаемой доверенности» [7] распределенные реестры признаются допустимым способом фиксации данных при соблюдении требований безопасности. Налоговые органы уже применяют эту технологию для машинночитаемых доверенностей [8], что создает прецедент для ее внедрения в нотариальную деятельность.

Использование блокчейна в нотариате способно обеспечить неизменность и прозрачность записей, что соответствует требованиям ст. 34.1 ФЗ «О нотариате» в части достоверности реестровых данных. Технология распределенного хранения исключает риски фальсификации и упрощает межведомственное взаимодействие, как это уже происходит в налоговой сфере. При этом данная статья прямо предусматривает возможность применения электронных технологий, что открывает путь для легализации блокчейн-решений в нотариальной практике при условии их соответствия стандартам Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» [2].

Заключение. Следует отметить, что ключевым вызовом для нотариата сегодня является сохранение баланса между технологическим прогрессом и фун-

даментальными принципами нотариата – легитимностью, конфиденциальностью и человеческим контролем над критически важными решениями. Успешная трансформация возможна только через синтез инновационных технологий с обновленной правовой доктриной, где нотариат станет не пассивным наблюдателем, а активным архитектором цифрового правопорядка.

Цифровая трансформация нотариальной деятельности – неизбежный процесс, диктуемый развитием технологий и потребностями современного общества, поэтому для перехода от концепта-идеи до реализации важно заручиться поддержкой нотариального сообщества и увеличить содействие различных правоохранительных и оказывающих правовую помощь институтов в РФ для обмена практическим опытом по внедрению тех или иных технологий. Впоследствии внедрение ИИ в верификацию сделок, квантово-защищенное шифрование документов и нотариальные услуги в метавселенных повысят эффективность и доступность юридических услуг. Однако для этого необходима модернизация законодательства, новые стандарты кибербезопасности и четкое определение юрисдикции в виртуальных средах.

Список литературы

1. Федеральный закон «О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации» от 27.12.2019 № 480-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_341788/3d0cac60971a511280cbba229d9b6329c07731f7/ (дата обращения: 28.04.2025)
2. Федерального закона «Об электронной подписи» от 06.04.2011. № 63-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_112701/f13f7dcdaabebfa823ec8e7fe6697c835617bb6b/ (дата обращения: 31.08.2025)
3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.
4. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 2019. № 41. Ст. 5700.
5. Постановление Правительства РФ от 03.05.2019 № 551 «О государственной поддержке программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий» // Собрание законодательства РФ. 2019. № 19. Ст. 2307.
6. Письмо ФНП от 05.08.2024 № 6450/06–15–2 «О порядке предоставления сведений, содержащихся в единой информационной системе нотариата (ЕИС)». URL: <https://www.garant.ru/products/ipo/prime/doc/410280559/?ysclid=mbbwr0ievc927463965> (дата обращения: 31.08.2025).
7. Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15 февраля 2024 г. № П15–13439 «Об информационной системе хранения машиночитаемой доверенности». URL:

<https://www.garant.ru/products/ipo/prime/doc/408610339/?ysclid=mbbz26ift1943446587> (дата обращения: 31.08.2025).

8. Письмо Федеральной налоговой службы от 28 марта 2024 г. № ЕА-2-26/4778@ «О машиночитаемой доверенности». URL: <https://www.garant.ru/products/ipo/prime/doc/408711579/?ysclid=mbbz2pevov508841710> (дата обращения: 31.08.2025).

9. Порядок использования нотариусами средств видеофиксации и хранения материалов видеофиксации (утв. решением Правления ФНП, протокол от 17.11.2015 № 15/15). URL: <https://www.garant.ru/products/ipo/prime/doc/71158864/> (дата обращения: 31.08.2025).

10. Проект Федерального закона «О нотариате и нотариальной деятельности в Российской Федерации» (подготовлен Минюстом России, ID проекта 02/04/02-25/00154552) / КонсультантПлюс, 2025. URL: <https://www.consultant.ru/law/hotdocs/88312.html> (дата обращения: 31.08.2025).

11. Афанасьев С. Ф., Кружалова А. В. Искусственный интеллект в приказном производстве // Вестник Университета имени О. Е. Кутафина. 2025. № 2 (126). С. 64–70.

12. Махмадиев Р.З. Можно ли предсказать исход судебного заседания с помощью ИИ? Да! // Первая полоса. 2023. № 5 (154). С. 7–9. URL: <https://alventa.ru/blog/materialy-pervoy-polosy/mozhno-li-predskazat-iskhod-sudebnogo-zasedaniya-s-pomoshchyu-ii-da/>

13. Добробаба М. Б. Дипфейки как угроза правам человека // Lex Russica. 2022. №11 (192). С. 112–119.

14. Евсиков К. С. Информационная безопасность цифрового государства в квантовую эпоху // Вестник Университета имени О. Е. Кутафина. 2022. №4 (92). С. 46–58.

15. Холодная Е. В. О правовой концепции метавселенных // Lex Russica. 2024. №3 (208). С. 116–128.

16. Mayana, R. F., & Santika, T. (2021). Legalitas Tanda Tangan Elektronik: Posibilitas Dan Tantangan Notary Digitalization Di Indonesia. Acta Diurnal Jurnal Ilmu Hukum Kenotariatan Dan Ke-PPAT-An, 4(2), 244–262. <https://doi.org/10.23920/acta.v4i2.517>

17. Menezes L., Araújo L. V., Nishijima M. Blockchain and smart contract architecture for notaries services under civil law: a Brazilian experience // International Journal of Information Security. 2023. Vol. 22. P. 872–873. DOI: <https://doi.org/10.1007/s10207-023-00673-3>

18. Нотариат присоединился к эксперименту по обмену машиночитаемым через блокчейн-платформу ФНС России и электронными доверенностями. URL: https://www.nalog.gov.ru/rn77/news/activities_fts/12136179/ (дата обращения: 31.08.2025).

19. URL: <https://www.comnews.ru/content/235272/2024-09-18/2024-w38/1011/moskovskiy-notarius-pervym-rossii-nachal-ispolzovat-ii-smart-engines-dlya-borby-moshennikami> (дата обращения: 31.08.2025)

Д. И. Рябина,
студент,
Белорусский государственный университет транспорта,
А. А. Сидорова,
студент,
Белорусский государственный университет транспорта

**Блокчейн в государственных реестрах:
опыт и проблемы внедрения**

Аннотация. Статья посвящена исследованию потенциала и проблем внедрения технологии блокчейн в систему государственных реестров. Целью работы является анализ международного опыта, выявление ключевых преимуществ, систематизация технологических, правовых и организационных барьеров, а также предложение комплексных путей их преодоления. На примере кейсов Калифорнии, Грузии, Швеции и других стран демонстрируется, как блокчейн способен повысить прозрачность, безопасность и эффективность регистрации прав. В результате обосновывается необходимость экосистемного подхода, сочетающего развитие правовой базы, использование гибридных моделей, внедрение стандартов и подготовку кадров для успешной цифровой трансформации.

Ключевые слова: блокчейн, государственные реестры, цифровая трансформация, смарт-контракты, нормативное регулирование, защита данных, доверие, публичная администрация, цифровое государство

D. I. Ryabina,
student,
Belarusian State University of Transport,
A. A. Sidorova,
student,
Belarusian State University of Transport

**Blockchain in government registries:
implementation experience and challenges**

Abstract. The article explores the potential and challenges of implementing blockchain technology in government registry systems. The aim of the work is to analyze international experience, identify key benefits, systematize technological, legal, and organizational barriers, and propose comprehensive ways to overcome them. Using case studies from California, Georgia, Sweden, and other countries, the study demonstrates how blockchain can enhance the transparency, security, and efficiency of rights registration. The results justify the necessity of an ecosystem approach that combines the development of a legal framework, the use of hybrid models, the im-

plementation of standards, and personnel training for a successful digital transformation.

Keywords: blockchain, government registries, digital transformation, smart contracts, regulatory framework, data protection, trust, public administration, digital governance

Введение. Современные государства активно стремятся к цифровой трансформации ключевых институтов, среди которых особое место занимают государственные реестры. Эти системы, будь то земельные кадастры, реестры прав на недвижимость, регистры транспортных средств или удостоверений личности, служат фундаментом для фиксации прав, регистрации сделок и обеспечения законности в цифровую эпоху. В этом контексте технология блокчейн возникает как потенциально революционное решение, предлагающее возможности для повышения прозрачности, неизменности данных, безопасности и уровня доверия к работе государственных институтов, а также для автоматизации процессов через смарт-контракты.

Основная часть. Однако внедрение распределенных реестров в сферу государственного управления сопряжено с комплексом серьезных вызовов. Технологические проблемы масштабируемости и энергоэффективности, правовые вопросы юридической силы записей в блокчейне и защиты персональных данных, а также организационное сопротивление изменениям создают существенные барьеры на пути реализации проектов. Настоящая статья рассматривает международный опыт внедрения блокчейн-решений в государственные реестры, выявить ключевые преимущества и преимущества, систематизировать возникающие проблемы и предложить практические пути для их преодоления.

Мировой опыт внедрения технологии блокчейн в системы государственных реестров демонстрирует разнообразие подходов, мотиваций и достигаемых результатов. Еще в 2016 году аналитическое агентство Gartner включило блокчейн в десятку ключевых мировых технологических трендов, а Всемирный экономический форум прогнозировал, что к 2025 году до 10% мирового ВВП будет храниться с использованием этой технологии [5. С. 123–127]. Пионерами в этой области выступили как развитые страны, стремящиеся оптимизировать существующие бюрократические процессы и повысить уровень доверия граждан, так и развивающиеся государства, которые увидели в распределенных реестрах возможность совершить технологический «прыжок» и построить более прозрачные и эффективные институты с чистого листа. Анализ ключевых кейсов позволяет выделить несколько устойчивых тенденций: доминирование разрешенных (permissioned) блокчейн-сетей, ориентированных на взаимодействие между государственными органами и уполномоченными коммерческими организациями; приоритетность сфер земельного кадастра и регистрации прав собственности; а также растущая роль цифровой идентификации как краеугольного камня для всех остальных цифровых сервисов.

Ярким примером масштабного внедрения в развитой экономике является проект Департамента транспортных средств (DMV) штата Калифорния, США. В 2023 году DMV объявил о партнерстве с платформой Avalanche с целью пере-

вода 42 миллионов записей об автомобильных титулах (vehicle titles) на блокчейн. Основными драйверами данного проекта стали борьба с мошенничеством (поддельными титулами и клонированием VIN-номеров) и кардинальное упрощение процедуры купли-продажи автомобилей. Реализация позволяет гражданам через мобильное приложение безопасно и практически мгновенно передавать права собственности, минимизируя необходимость личных визитов в отделения DMV, что значительно экономит время и ресурсы как граждан, так и самого государственного органа. Ключевым аспектом является выбор публичного, но высокопроизводительного и масштабируемого блокчейна Avalanche, что подчеркивает стремление государства использовать уже опробованные на рынке решения, способные выдерживать экстремальные нагрузки.

Европа демонстрирует комплексный подход, где проекты по реестрам прав собственности постепенно интегрируются в более широкую архитектуру цифрового доверия.

- Грузия является признанным мировым лидером, запустившим одну из первых в мире блокчейн-систем для земельного кадастра еще в 2016 году совместно с компанией Bitfury. Особенностью грузинской модели является гибридный подход: основная база данных работает в высокопроизводительной закрытой разрешенной сети (Exonum), а ее криптографические хэши (отпечатки данных) регулярно записываются в публичный блокчейн Bitcoin. Это обеспечивает беспрецедентный уровень доказательства подлинности и неизменности записей, делая практически невозможными задним числом какие-либо коррупционные изменения в реестре без обнаружения. Успех проекта в Грузии стал катализатором для многих других стран.

- Швеция пошла путем тщательного многоэтапного тестирования. Управление земельного кадастра Lantmäteriet с 2016 года исследует возможность переноса процесса торговли недвижимостью на блокчейн (проект на базе платформы Corda). Процесс, который traditionally involved множество посредников (банки, риелторы, юристы, государственные регистраторы) и занимал недели, с помощью смарт-контрактов может быть автоматизирован и сокращен до дней или даже часов. Исследования указывают на потенциальную экономию до \$106 млн в год за счет снижения административных издержек, уменьшения бумажного документооборота и минимизации рисков мошенничества.

- Великобритания в лице HM Land Registry также активно экспериментирует в рамках исследовательской программы «Digital Street». Цель – понять, как технология распределенного реестра может трансформировать не только регистрацию прав, но и весь жизненный цикл недвижимости, включая аренду, ипотеку и плановое обслуживание. Проект ориентирован на создание открытых стандартов и интерфейсов (API) для будущей экосистемы цифровых услуг.

- На наднациональном уровне выделяется инициатива Европейского союза – European Blockchain Services Infrastructure (EBSI). EBSI нацелена на создание общеевропейской инфраструктуры доверия для проверки и хранения официальных документов (дипломов, прав на вождение, свидетельств о рождении), управления цифровой идентификацией и оптимизации трансграничных процессов для бизнеса и граждан. Это самый амбициозный проект, который

призван заложить основу для межгосударственного взаимодействия на основе блокчейна.

Для ряда стран внедрение блокчейна – это не оптимизация, а создание принципиально новой, прозрачной системы там, где ранее реестры были неполными, коррумпированными или вовсе отсутствовали.

– Руанда реализует программу полной цифровизации земельного кадастра к 2023 году. Блокчейн-система позволяет регистрировать права на землю для миллионов граждан, обеспечивая юридическую защиту и создавая основу для развития рыночных отношений (использование земли в качестве залога для кредитов). Это способствует экономическому росту и социальной стабильности.

– Китай демонстрирует системный государственный подход. В декабре 2023 года была запущена национальная система децентрализованных идентификаторов (DID) – RealDID. Она позволяет гражданам аутентифицироваться на интернет-платформах, не раскрывая своих персональных данных, что является решением на стыке регистров населения и защиты приватности. Пилотные проекты, запущенные в Гонконге, подтверждают практическую применимость решения для мегаполисов.

– В Беларуси пока нет полноценных государственных блокчейн-реестров, однако технологическая база для их внедрения уже существует. Принятый в 2017 году Декрет №8 «О развитии цифровой экономики» создал правовую основу для работы с криптовалютами и смарт-контрактами, а Парк высоких технологий стал центром компетенций в этой области [3. С. 33–41]. Белорусские ИТ-компании разрабатывают блокчейн-решения для зарубежных заказчиков, что позволяет при необходимости адаптировать эти наработки для государственных нужд. Потенциальными направлениями пилотных проектов могут стать: единый реестр недвижимости с защитой от подделок, система электронного голосования для местных выборов, а также платформа для прозрачных государственных закупок с автоматическим контролем целевого расходования средств.

– В России применение блокчейна в государственном управлении также развивается, но пока точечно. В образовании Финансовый университет при Правительстве РФ начал хранить сведения о дипломах в распределенных реестрах. В государственных закупках предлагалось использовать технологию для «окрашивания» бюджетных средств и автоматического блокирования при их нецелевом расходовании. В Москве на портале «Активный гражданин» блокчейн применялся для защиты результатов электронных голосований, а в 2017 году был запущен эксперимент по использованию распределенного реестра для мониторинга достоверности данных ЕГРН [11. С. 301–309].

Таким образом, зарубежный опыт не является однородным, но он единогласно указывает на то, что блокчейн-технология перешла из стадии теоретических обсуждений в стадию практических пилотов и даже полноценной реализации. Основные успехи достигнуты в областях, где критически важны неизменность данных, прозрачность истории изменений и автоматизация многошаговых процессов между различными сторонами. Этот опыт служит ценным источником понимания для анализа возникающих проблем, о которых пойдет речь далее.

Внедрение технологии блокчейн в системы государственных реестров предлагает не просто эволюционное улучшение, а потенциал для радикальной трансформации взаимодействия между государством, гражданами и бизнесом. Преимущества этой технологии проистекают из ее фундаментальных характеристик – децентрализации, криптографической безопасности, неизменности и прозрачности. Эти свойства позволяют решить системные проблемы традиционных централизованных реестров, такие как уязвимость к несанкционированному доступу и манипуляциям, высокие операционные издержки, непрозрачность процессов и необходимость постоянного посредничества государственных органов. Анализ международного опыта позволяет систематизировать ключевые преимущества в несколько взаимосвязанных групп [1. С. 66–74].

1. Гарантированная неизменность и повышенная прозрачность.

Ключевым преимуществом блокчейна является обеспечение неизменности (иммутабельности) данных. Каждая запись (транзакция) о регистрации права, изменении статуса или проведении сделки криптографически подписывается, добавляется в блок и связывается с предыдущими записями, образуя хронологическую цепочку. После внесения информация не может быть изменена или удалена без согласия всех участников сети, а любая попытка подделать данные в одном блоке потребует изменения во всех последующих блоках, что вычислительно невозможно.

– Борьба с мошенничеством и коррупцией: Это свойство напрямую противодействует фальсификациям и «задним датировкам». В Грузии и Руанде это свело на нет риски коррупционного изменения записей о землевладельцах. В Калифорнии система на блокчейне Avalanche исключает возможность подделки автомобильных титулов или существования нескольких оригиналов документа на один автомобиль (проблема «клонирования»), так как в реестре существует лишь одна уникальная и верифицируемая запись.

– Аудит и доверие: Прозрачность истории изменений (которая в разрешенных блокчейнах может быть избирательной и не раскрывать конфиденциальные данные) позволяет любому уполномоченному участнику – аудитору, суду, заинтересованной стороне – провести полный и независимый аудит всей истории операций с активом. Это кардинально повышает доверие к системе в целом, так как государство не является единственным хранителем и контролером информации, а лишь одним из валидаторов ее подлинности.

2. Автоматизация процессов и рост эффективности.

Вторым революционным преимуществом является возможность использования смарт-контрактов – самоисполняющихся программных кодов, которые автоматически выполняют заранее прописанные условия при их наступлении.

– Устранение посредников и бюрократии: Смарт-контракты позволяют автоматизировать сложные многоступенчатые процессы, которые традиционно требуют ручного вмешательства чиновников и взаимодействия между различными ведомствами. Например, сделка купли-продажи недвижимости может быть запрограммирована как смарт-контракт, который автоматически проверит наличие прав у продавца, получит цифровые подписи сторон, инициирует перевод денежных средств через интегрированную платежную систему и момен-

тально регистрирует переход права к новому владельцу в реестре. Это устраняет необходимость в бумажных документах, многократных визитах в МФЦ и длительных ожиданиях проверок.

- Ускорение транзакций: Процессы, занимавшие недели и месяцы, могут быть сокращены до часов или минут. Проект в Швеции нацелен именно на такую автоматизацию цепочки от заключения договора до регистрации. Аналогично, платформа COAATChain в Испании автоматизирует процесс согласования архитектурно-кадастровой документации, исключая задержки, связанные с человеческим фактором.

3. Значительное снижение операционных затрат.

Автоматизация и повышение эффективности напрямую трансформируются в существенную экономию финансовых и административных ресурсов.

- Сокращение административных расходов: Государственные органы экономят на содержании бумажных архивов, физической инфраструктуры для приема граждан, ручной обработке документов и устранении последствий ошибок и мошеннических схем. Оценка шведского земельного кадастра, предсказывающая экономию до \$106 млн в год, – яркий пример этого эффекта.

- Косвенная экономия: снижаются затраты и для конечных пользователей системы. Граждане и бизнес экономят время и деньги на транспорте, нотариальных услугах (их функции частично заменяются криптографической подписью и смарт-контрактами) и временных издержках. В Калифорнии снижение потребности в личных визитах в офисы DMV высвобождает ресурсы госоргана для решения более сложных задач, не связанных с рутинной регистрацией.

4. Усиление доверия граждан и новый уровень доступности услуг.

Технология меняет саму парадигму взаимодействия «гражданин–государство», переводя ее из модели «проситель–распределитель» в модель равноправного участия в защищенной цифровой экосистеме.

- Контроль над данными: В системах с продвинутой цифровой идентификацией (как в проекте EBSI ЕС или китайской RealDID) гражданин получает больший контроль над своими персональными данными. Он может дистанционно предоставлять доступ к своим реестровым записям (например, подтверждать право собственности при аренде квартиры или получении кредита) без необходимости запрашивать и пересылать бумажные справки.

- Удобство и инклюзивность: Круглосуточный удаленный доступ к сервисам через мобильные приложения или веб-порталы делает государственные услуги более доступными, особенно для жителей удаленных районов или людей с ограниченной мобильностью. Прозрачность и невозможность произвольного изменения записей со стороны чиновника восстанавливает и укрепляет доверие к государственным институтам, что является ключевым нематериальным активом. Как показывает опыт Руанды, наличие гарантированного и защищенного права собственности, которое можно легко проверить, само по себе стимулирует экономическую активность и социальную стабильность.

Таким образом, преимущества блокчейна выходят далеко за рамки простой «оцифровки» бумажных носителей. Технология предлагает комплексное решение для создания более безопасных, эффективных, дешевых и доверитель-

ных систем регистрации прав, что в конечном итоге способствует не только оптимизации государственного управления, но и экономическому развитию и повышению уровня социального благополучия.

Несмотря на значительный потенциал и очевидные преимущества, широкое внедрение блокчейн-технологий в систему государственных реестров сталкивается с комплексом серьезных вызовов. Эти проблемы носят междисциплинарный характер, лежащий на стыке технологий, юриспруденции, управления и социологии. Их игнорирование или недооценка на этапе планирования проекта неизбежно приводит к провалам, потере инвестиций и подрыву доверия к самой технологии. Анализ международной практики позволяет выделить наиболее критичные барьеры [8. С. 386–402].

1. Нормативно-правовые и регуляторные барьеры.

Наиболее фундаментальным препятствием является правовая неопределенность. Национальные законодательства большинства стран не успевают за технологическим развитием, что создает правовой вакуум.

- Юридическая сила записей: Ключевой вопрос – признают ли суды и государственные органы записи в блокчейне в качестве полноценных и достаточных доказательств права собственности. Отсутствие прямых указаний в законах делает любую сложную сделку, оспоренную в суде, крайне уязвимой.

- Статус смарт-контрактов: Не определен их юридический статус. Является ли код юридически обязывающим документом? Как интерпретировать результаты выполнения или ошибки в коде? Как примирить принцип «код – это закон» с традиционными правовыми нормами, предусматривающими возможность оспаривания и толкования условий договора?

- Ответственность и атрибуция: В случае ошибки или мошенничества сложно определить субъекта ответственности: разработчика смарт-контракта, оператора узла, государственный орган или самого пользователя. Эта неясность отпугивает как госорганы, так и граждан.

2. Технологические и инфраструктурные сложности.

Интеграция инновационных децентрализованных систем с существующей ИТ-инфраструктурой государства (legacy systems) – крайне сложная и дорогостоящая задача.

- Интеграция с Legacy-системами: Государственные реестры десятилетиями работают на централизованных базах данных (Oracle, SQL и т. д.). Их интеграция с блокчейном требует создания сложных промежуточных слоев (API-шлюзов, оракулов), что увеличивает сложность, стоимость и создает новые точки отказа, потенциально нивелируя преимущества децентрализации.

- Проблемы масштабируемости и производительности: Публичные блокчейны (например, ранние версии Ethereum) часто сталкиваются с низкой пропускной способностью (low throughput) и высокими задержками (latency). Обработка десятков тысяч транзакций в секунду, необходимых для национального реестра, – нетривиальная задача. Хотя разрешенные блокчейны (например, Hyperledger Fabric, Corda) решают эту проблему, они требуют тщательного проектирования архитектуры сети.

- Энергопотребление: Модель консенсуса Proof-of-Work (PoW), используемая в Bitcoin и Ethereum 1.0, критикуется за чрезмерное энергопотребление, что неприемлемо для государственных экологических и экономических программ. Переход на более эффективные алгоритмы (Proof-of-Stake, PoA) является необходимым, но требует дополнительных исследований и аудита безопасности.

3. Вызовы конфиденциальности и соответствие регуляториям.

Принцип неизменности данных вступает в прямой конфликт с современными законами о защите персональных данных, прежде всего с Общим регламентом по защите данных (GDPR) в ЕС.

- «Право на забвение»: Статья 17 GDPR предоставляет субъекту данных право требовать полного удаления своих персональных данных. Однако неизменность блокчейна технически делает это невозможным. Решения (например, хранение в цепочке только хэшей данных или использование механизмов «забывания» нулевого знания) являются сложными и пока не стандартизированы.

- Определение контролера данных: В децентрализованной сети сложно идентифицировать субъекта, ответственного за соблюдение GDPR (контролера данных). Является ли им каждый узел сети? Оператор платформы? Государственный орган? Эта неопределенность создает значительные правовые риски.

4. Управленческие, кадровые и социокультурные барьеры.

Технологические инновации часто упираются в человеческий фактор и организационную инертность.

- Нехватка квалифицированных кадров: Острый дефицит специалистов, обладающих одновременно глубокими знаниями в области блокчейна и пониманием специфики государственного управления, сдерживает развитие проектов. Требуется масштабная программа переобучения и повышения квалификации государственных служащих.

- Организационное сопротивление: Внедрение блокчейна угрожает сложившимся бюрократическим процедурам и может встречать скрытое или явное сопротивление со стороны сотрудников, опасющихся за свои jobs или не желающих осваивать новые процессы. Успех проекта критически зависит от поддержки со стороны высшего руководства.

- Недоверие и низкая осведомленность общества: Широкая публика может ассоциировать блокчейн исключительно с криптовалютами и их спекулятивным характером, скептически относясь к его использованию в госуправлении. Необходима масштабная разъяснительная кампания о реальных преимуществах и механизмах защиты приватности.

- Угрозы централизации и безопасности.

- Ирония заключается в том, что многие государственные блокчейн-проекты, стремясь к эффективности, воссоздают централизованные модели.

- Централизация в консорциумных сетях: Разрешенные блокчейны, управляемые консорциумом государственных органов, могут воспроизводить существующие властные отношения. Если небольшая группа узлов получает чрезмерный контроль, это подрывает саму суть децентрализации и доверия, создавая риски сговора.

– Новые векторы атак: Хотя блокчейн защищает данные от несанкционированного изменения, он не защищает от уязвимостей в смарт-контрактах, компрометации приватных ключей пользователей или атак 51% в публичных сетях. Безопасность системы становится заботой не только централизованного оператора, но и каждого участника.

Таким образом, проблемы внедрения носят системный характер и требуют не только технологических, но и комплексных правовых, организационных и социокультурных изменений. Преодоление этих барьеров является необходимым условием для успешной реализации потенциала блокчейн-технологий в сфере государственных реестров.

Преодоление барьеров на пути внедрения блокчейна в государственные реестры требует не изолированных технических решений, а комплексного стратегического подхода. Успешные кейсы демонстрируют, что ключ к успеху лежит в создании сбалансированной экосистемы, где технология, право, управление и общество взаимодействуют синхронно. Это предполагает отказ от поиска универсального решения в пользу гибких моделей, поэтапного внедрения и постоянного диалога со всеми заинтересованными сторонами.

Фундаментальным решением является восприятие блокчейна не как точечного приложения, а как новой цифровой инфраструктуры для доверия. Это означает параллельное развитие нормативной базы, определяющей юридический статус записей и смарт-контрактов, и создание технических стандартов, обеспечивающих совместимость и взаимодействие различных систем как на национальном, так и на международном уровне. Разработка открытых протоколов и API позволяет интегрировать новые блокчейн-решения с существующими устаревшими системами (legacy systems), обеспечивая плавный переход и защищая государственные инвестиции.

В технологическом плане наиболее практичной моделью для государств оказывается использование разрешенных (permissioned) или гибридных блокчейнов. Такие платформы, как Hyperledger Fabric, Corda или Quorum, предоставляют необходимый баланс между децентрализацией и контролем. Они позволяют государственным органам управлять доступом к конфиденциальным данным, обеспечивая при этом прозрачность и проверяемость для уполномоченных участников, таких как суды, нотариусы или финансовые институты. Гибридная модель, где хэши данных хранятся в публичном блокчейне для обеспечения неизменности, а сами данные – в защищенном закрытом реестре, эффективно решает проблему конфликта с GDPR, так как позволяет при необходимости удалять или анонимизировать персональные данные, не затрагивая сам хэш-доказательство [4. С. 33–41].

Для обеспечения конфиденциальности и соответствия регуляторным требованиям необходимо активное внедрение усовершенствованных криптографических технологий, таких как zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) и других протоколов с нулевым разглашением. Эти технологии позволяют проверять подлинность данных и соблюдение условий сделки, не раскрывая самих конфиденциальных данных, что является прорывом в области защиты приватности.

Однако ни одна технология не будет эффективной без организационной и кадровой поддержки. Критически важным является формирование компетенций внутри государственного аппарата через образовательные программы и партнерства с академическими институтами и технологическими компаниями. Подготовка руководящих кадров, способных артикулировать цели и преимущества проекта, управлять изменениями и бороться с бюрократической инерцией, так же важна, как и подготовка технических специалистов. Одновременно с этим необходима просветительская работа с обществом, направленная на формирование реалистичных ожиданий и доверия к новой системе, разъяснение ее механизмов и выгод для каждого гражданина.

Таким образом, успешное внедрение блокчейна – это длительный эволюционный процесс, а не разовая революция. Он требует поэтапного подхода, начинающегося с пилотных проектов в ограниченных доменах (например, реестр нотариальных действий или цифровые дипломы), последующего анализа, доработки и только затем – масштабирования. Только такой комплексный и взвешенный путь позволит реализовать потенциал технологии для создания более прозрачных, эффективных и заслуживающих доверия государственных институтов.

Технология блокчейн представляет собой мощный инструмент для фундаментальной трансформации государственных реестров, предлагая беспрецедентный уровень прозрачности, автоматизации и безопасности. Международный опыт, накопленный в таких юрисдикциях, как Калифорния, Грузия и Швеция, наглядно демонстрирует ее потенциал в борьбе с мошенничеством, снижении операционных издержек и укреплении доверия граждан к государственным институтам. Однако путь внедрения сопряжен с комплексом взаимосвязанных вызовов, включая нормативно-правовую неопределенность, технические сложности интеграции с устаревшими системами, проблемы масштабируемости, обеспечение соответствия требованиям по защите персональных данных, а также преодоление организационной инерции и кадрового дефицита.

Заключение. Для успешной реализации этого потенциала необходим не точечный, а экосистемный подход, предполагающий синхронное развитие технологической, правовой и образовательной инфраструктуры. Ключевыми элементами успеха являются адаптация гибридных моделей, сочетающих преимущества децентрализации с необходимым уровнем контроля, разработка единых стандартов, активное внедрение механизмов защиты конфиденциальности и масштабная работа по подготовке квалифицированных кадров. Стратегия внедрения должна быть поэтапной – начинаться с реалистичных пилотных проектов, а затем, по мере накопления опыта и устранения барьеров, аккуратно масштабироваться. Дальнейшие усилия как исследователей, так и практиков должны быть сосредоточены на всесторонней оценке экономической эффективности таких решений, глубоком анализе их влияния на уровень общественного доверия и разработке надежных моделей для их устойчивого копирования в различных национальных контекстах.

Список литературы

1. Клечиков А. В., Пряников М. М., Чугунов А. В. Блокчейн-технологии и их использование в государственной сфере // International Journal of Open Information Technologies. 2017. № 12. С. 123–127.
2. e-Estonia. The Digital Society. Tallinn: e-Governance Academy, 2019. С. 14–20. Алферов, А. П. Криптография: основы современной защиты информации / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин. 3-е изд. СПб.: БХВ-Петербург, 2021. – 576 с.
3. Atzei N., Bartoletti M., Cimoli T. A survey of attacks on Ethereum smart contracts // Future Generation Computer Systems. 2018. P. 66–74.
4. European Union Blockchain Observatory and Forum. Legal and regulatory framework of blockchains and smart contracts [Электронный ресурс]. Brussels, 2020. С. 33–41. URL: <https://www.eublockchainforum.eu> (дата обращения: 06.09.2025).
5. IBM Institute for Business Value. Building trust in government through blockchain. New York: IBM, 2019. С. 210–218.
6. Mougayar W. The Business Blockchain. Hoboken: Wiley, 2018. С. 101–109.
7. Ølnes S., Ubacht J., Janssen M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing // Government Information Quarterly. 2017. Vol. 34, № 3. P. 77–85.
8. Swan M. Blockchain: Blueprint for a New Economy. Sebastopol: O'Reilly Media, 2015. С. 386–402.
9. Tapscott D., Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin, 2018. С. 12–18.
10. World Bank. Blockchain and Emerging Digital Technologies for Enhancing Post-2020 Climate Markets. Washington, DC: World Bank, 2018. С. 55–63.
11. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends // IEEE International Congress on Big Data. 2017. P. 301–309.

Вопросы обучения больших языковых моделей и авторского права в России и в мире

Аннотация. Широкое внедрение больших языковых моделей класса GPT/LLaMA и мультимодальных генеративных систем обострило вопросы законности использования охраняемых произведений в обучающих корпусах. В статье кратко рассмотрены технические аспекты обучения (сбор данных, архитектура, типы данных), проанализированы положения российского авторского права (ГК РФ, ч. 4) и сравнительные подходы США (fair use) и ЕС (исключения для text and data mining, TDM). Обобщена ключевая судебная практика (Authors Guild v. Google; Authors Guild v. HathiTrust; Doe v. GitHub (Copilot)), а также рамочные международные договоры (Бернская конвенция, ТРИПС, WCT). Показано, что в России отсутствует специальное исключение для TDM, вследствие чего массовое копирование произведений для обучения ИИ, как правило, требует разрешения правообладателей. В США преобладает гибкая оценка трансформативности и влияния на рынок в рамках fair use; в ЕС действует прямое законодательное исключение для TDM (с опцией opt-out). Сформулированы рекомендации по модернизации российского законодательства: внедрение TDM-исключения, механизма opt-out и прозрачности источников, развитие коллективного управления правами и национальных дата-хабов, а также прояснение статуса ИИ-генераций. Материал адресован исследователям, юристам, регуляторам и разработчикам ИИ.

Ключевые слова: большие языковые модели, искусственный интеллект, авторское право, text and data mining (TDM), fair use, ГК РФ, Бернская конвенция, TRIPS, WIPO

T. B. Sabitov,

Student,

Russian State University of Justice

Questions of teaching large language models and copyright in Russia and the world

Abstract. The rapid expansion of large language models (LLMs) and multi-modal generative systems has intensified legal debates over the lawful use of copyrighted works in training corpora. This paper outlines the technical background of LLM training (data collection, model architecture, data types), and analyzes Russian copyright law (Civil Code Part IV), alongside comparative approaches in the U.S. (fair use) and the EU (text and data mining–TDM–exceptions). It surveys landmark case law (Authors Guild v. Google; Authors Guild v. HathiTrust; Doe v. GitHub (Co-

pilot)) and key international instruments (Berne Convention, TRIPS, WCT). We show that Russia lacks a specific TDM exception, thus large-scale copying for AI training typically requires rightholder authorization. The U.S. applies a flexible, case-by-case assessment focusing on transformative use and market impact; the EU provides statutory TDM exceptions (with rightholders' opt-out). We propose legislative updates for Russia: introducing a TDM exception, opt-out and transparency duties, expanding collective rights management, building national data hubs, and clarifying the legal status of AI-generated outputs. The paper targets researchers, lawyers, regulators, and AI developers.

Keywords: large language models, artificial intelligence, copyright, text and data mining (TDM), fair use, Russian Civil Code, Berne Convention, TRIPS, WIPO, EU Directive 2019/790

Введение. Быстрый прогресс генеративного ИИ базируется на обучении моделей на масштабных корпусах текстов, кода и изображений. Это породило значимую правовую неопределенность: допускается ли использование охраняемых произведений для обучения без согласия правообладателей и в каких пределах? Цель настоящей работы – систематизировать технические и правовые аспекты обучения БЯМ, сопоставить российское регулирование с подходами США и ЕС и предложить направления для совершенствования национального законодательства.

Основная часть

Технические аспекты обучения БЯМ

2.1. Сбор и подготовка данных. Обучающие корпуса формируются из публично доступных источников (веб-скрейпинг, открытые датасеты, открытые репозитории кода, оцифрованные издания и др.). Такие процессы часто автоматизированы (поисковые роботы, краулеры). На этапе подготовки применяются очистка и токенизация, а данные агрегируются в обучающие выборки с приоритизацией качества и разнообразия.

2.2. Архитектура и обучение. Современные модели основаны на архитектуре Transformer, обучаются по парадигме самообучения (self-supervised) на задаче предсказания следующего токена [1]. Качество модели существенно зависит от объема и разнообразия данных.

2.3. Типы данных. Помимо текстов, широко используются исходные коды ПО (часто под открытыми лицензиями) и изображения/видеокадры для мультимодальных моделей. Вопросы правомерности использования стилей, художественных приемов и т.п. следует отличать от правомерности копирования защищенных экземпляров: стили как таковые охраной обычно не пользуются, тогда как копирование произведений для обучения подпадает под режим авторского права.

2.4. Результат обучения. Обученные БЯМ выполняют генерацию текста, кода, изображений и др. При корректной настройке результат должен быть «новым» и не воспроизводить произведения из обучающего корпуса, однако риски дословных «регургитаций» сохраняются и требуют технических и организационных мер контроля.

Российское авторское право

3.1. Общие положения. Исключительные права на произведения включают, среди прочего, воспроизведение (в т.ч. запись в память ЭВМ), распространение, доведение до всеобщего сведения и др. [2]. Массовое копирование произведений для обучения без разрешения правообладателя, как правило, рассматривается как использование, требующее согласия.

3.2. Личное воспроизведение. Допускается воспроизведение «в личных целях» без согласия автора (ст. 1273 ГК РФ), но с жесткими ограничениями (запрет полного копирования книг и нотных текстов, программ, баз данных и др.) [2]. Эти исключения не покрывают промышленное обучение ИИ.

3.3. Свободное использование и цитирование. Разрешено цитирование в научных, критических, учебных целях «в объеме, оправданном целью» при указании автора и источника (ст. 1274 ГК РФ). По объему и целям эта норма не позволяет массовую загрузку произведений для предобучения [2].

3.4. Библиотечные и образовательные исключения. Разрешены единичные копии для сохранности фондов и научного доступа (ст. 1275 ГК РФ), а также ограниченное использование отрывков в образовательном процессе [2]. Эти положения не дают правовой базы для широкомасштабного TDM корпусов.

3.5. Программы и базы данных. Программы защищаются как литературные произведения; для их правомерного использования применяются специальные нормы ст. 1280 ГК РФ (для законного пользователя). Базы данных защищаются как объекты авторского права и/или смежные права составителя [2]. Специального TDM-исключения российское право не содержит.

Вывод по РФ: при нынешнем регулировании обучение БЯМ на охраняемых произведениях без лицензии или иного правового основания несет высокие риски нарушения исключительных прав.

Международные подходы

4.1. США: доктрина fair use. 17 U.S.C. § 107 предусматривает «добросовестное использование» по четырем факторам (цель/характер, природа произведения, объем, влияние на рынок) [3]. В контексте цифровых библиотек и поиска суды признали трансформативность значимой:

Authors Guild v. Google (2015): оцифровка книг для полнотекстового поиска и показа «сниппетов» признана fair use (трансформативная цель; отсутствие замещения рынка) [8].

Authors Guild v. HathiTrust (2014): оцифровка для поиска и доступности для людей с инвалидностью – также fair use [9].

Doe v. GitHub (Copilot, 2024): суд N.D. Cal. отклонил большинство исков; истцы не доказали дословное копирование сгенерированными фрагментами; претензии по CMI/DMCA частично неприменимы на предъявленных фактах [10].

Эти решения подтверждают: анализ больших массивов и трансформативные сервисы могут подпадать под fair use, при условии отсутствия вреда рынку и недословной репликации. При этом иски против разработчиков генеративного ИИ (СМИ против OpenAI/Meta и др.) продолжают рассматриваться; единообразная практика формируется.

4.2. ЕС: исключения для TDM. Директива (ЕС) 2019/790 ввела два исключения [4]:

Статья 3: обязательное исключение для исследовательских организаций и культурных учреждений при наличии законного доступа.

Статья 4: общее исключение TDM для любых лиц при законном доступе, с возможностью предварительного «резервирования прав» правообладателем (opt-out) «подходящим образом», например в метаданных или условиях использования.

Исключения имплементированы в национальные законы (напр., Германия – UrhG § 44b [12]). На практике opt-out ограничивает применение ст. 4 в коммерческих сценариях и требует процедур проверки источников.

4.3. Международные договоры. Бернская конвенция, ТРИПС и WCT устанавливают минимальные стандарты охраны и допускают исключения, соответствующие «трехступенчатому тесту» (узкое исключение; не мешает нормальному использованию; не наносит неоправданного ущерба законным интересам автора) [5–7]. Вопрос обучения ИИ прямо не урегулирован и отнесен к компетенции национального права.

Судебная практика, релевантная обучению ИИ

Authors Guild v. Google, 804 F.3d 202 (2d Cir. 2015) – признана трансформативность цифрового индексирования [8].

Authors Guild v. HathiTrust, 755 F.3d 87 (2d Cir. 2014) – поддержаны цели доступности и поиска [9].

Doe v. GitHub, Inc., No. 4:22-cv-06823-JST (N.D. Cal., 11.07.2024) – ключевые требования истцов отклонены; вопрос о прямой репликации исходников не подтвержден доказательствами [10].

Примечание по Великобритании и Канаде. В ряде юрисдикций Содружества действует доктрина fair dealing (более узкая, чем fair use). В Великобритании существует исключение для TDM в некоммерческих исследовательских целях (CDPA 1988, s.29A) [11]; попытка расширения на коммерческий TDM была отозвана в 2022–2023 гг. Информация о конкретных судебных решениях, прямо запрещающих генерацию изображений как производных работ вне статутных исключений, требует аккуратной верификации на дату публикации; известные крупные дела (например, Getty Images v. Stability AI в Англии и Уэльсе) по состоянию на 2024 г. еще находились в процессе рассмотрения.

Сравнительный анализ (Россия – США – ЕС)

Россия: узкий набор исключений (ст. 1273–1275 ГК РФ), отсутствие TDM-исключения; масштабное копирование для обучения требует согласия правообладателей или иного правового основания. Это сдерживает формирование легальных больших корпусов данных.

США: казуистическое регулирование через fair use с акцентом на трансформативность и отсутствие рыночного вреда; обучение ИИ не является per se незаконным и может квалифицироваться как fair use при соблюдении факторов и отсутствии регургитации.

ЕС: законодательные TDM-исключения (ст. 3, 4 Директивы 2019/790) при законном доступе; правообладатель может «забронировать права» (opt-out) для ст. 4, что требует у разработчиков процедур проверки и управления источниками.

Рекомендации для развития законодательства РФ

Ввести специальное TDM-исключение в ГК РФ (по модели ст. 3/4 DSM): разрешить воспроизведение произведений в целях анализа данных при законном доступе, с ограничениями и гарантиями (например, запрет на использование для замещения рынков, требования к хранению и безопасности копий).

Предусмотреть механизм opt-out и прозрачность: право правообладателя резервировать права «надлежащим образом» (метаданные/robots.txt/условия использования); требования к раскрытию основных источников обучения и политик фильтрации регургитаций.

Развить коллективное управление правами и модель лицензирования массивов: отраслевые соглашения (extended collective licensing), «единые окна» лицензирования, тарифы/компенсации за коммерческий TDM.

Создать и поддерживать национальные дата-хабы с правово-чистыми наборами данных (включая государственные данные, открытые лицензии, произведения с истекшим сроком охраны).

Прояснить статус результатов ИИ-генерации и распределение ответственности: закрепить, что авторское право возникает при наличии творческого вклада человека; определить правила для служебных/коммерческих сценариев и гарантии для пользователей.

Заключение. Обучение БЯМ ставит перед правом классические вопросы в новой плоскости. В России на данный момент отсутствует явное исключение, позволяющее безопасно осуществлять TDM охраняемых произведений; в США суды склоняются к признанию трансформативного обучения как fair use; в ЕС действует позитивное регулирование через исключения для TDM с механизмом opt-out. Для стимулирования инноваций и защиты интересов правообладателей целесообразно скорректировать российское законодательство, опираясь на международный опыт и «трехступенчатый тест», а также внедрить прозрачные и воспроизводимые практики доступа к данным.

Список литературы

1. Vaswani A., Shazeer N., Parmar N., et al. Attention Is All You Need // Advances in Neural Information Processing Systems. 2017. Vol. 30. URL: https://papers.nips.cc/paper_files/paper/2017/hash/3f5ee243547dee91fbd053c1c4a845aa-Abstract.html

2. Гражданский кодекс Российской Федерации (часть четвертая): федер. закон от 18.12.2006 № 230-ФЗ. Доступ из СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_64629/

3. United States Code. Title 17 – Copyrights. § 107. Limitations on exclusive rights: Fair use. 2018. URL: <https://www.law.cornell.edu/uscode/text/17/107>

4. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market // Official

Journal of the European Union. 2019. L 130. P. 92–125. URL: <https://eur-lex.europa.eu/eli/dir/2019/790/oj>

5. Berne Convention for the Protection of Literary and Artistic Works (Paris Act 1971, as amended on 28 September 1979). Geneva: WIPO, 1979. URL: <https://www.wipo.int/treaties/en/ip/berne/>

6. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Marrakesh, 15 Apr. 1994. URL: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

7. WIPO Copyright Treaty (WCT), 1996. Geneva: WIPO. URL: <https://www.wipo.int/treaties/en/ip/wct/>.

8. Authors Guild v. Google, Inc., 804 F.3d 202 (2d Cir. 2015). URL: <https://law.justia.com/cases/federal/appellate-courts/ca2/13-4829/13-4829-2015-10-16.html>

9. Authors Guild, Inc. v. HathiTrust, 755 F.3d 87 (2d Cir. 2014). URL: <https://law.justia.com/cases/federal/appellate-courts/ca2/12-4547/12-4547-2014-06-10.html>

10. Doe v. GitHub, Inc., United States District Court, N.D. California, No. 4:22-cv-06823-JST. Order on motions to dismiss, 11 July 2024. URL: <https://www.courtlistener.com/docket/66681230/doe-v-github-inc/>

11. United Kingdom. Copyright, Designs and Patents Act 1988. Section 29A: Copies for text and data analysis for non-commercial research. URL: <https://www.legislation.gov.uk/ukpga/1988/48/section/29A>

12. Urheberrechtsgesetz (UrhG). § 44b Datenanalyse. BGBl. I, 2019; m.w.N. URL: https://www.gesetze-im-internet.de/urhg/__44b.html

А. Э. Сеитова,
студент,
Казанский инновационный университет
имени В. Г. Тимирязова

Взаимосвязь между интернет-зависимостью и предрасположенностью к преступному поведению

Аннотация. Исследование имеет своей целью рассмотрение взаимосвязи совершения преступлений и наличие у криминального субъекта интернет-зависимости. В работе освещаются признаки интернет-зависимости, дается их краткая характеристика, рассматривается проблема алкоголизма и наркомании и их влияния на совершение преступления, проводится сравнение интернет-зависимости с зависимостями от алкоголя и наркотических веществ, выделяются особенности интернет-зависимости у молодежи. Отмечается, что на формирование интернет-зависимости может повлиять недостаточное воспитательное воздействие родителей, а также особенности психики и поведения несовершеннолетних. Констатируется, что нет прямой зависимости между вовлеченностью в интернет-активность и совершением преступлений.

Ключевые слова: интернет-зависимость, преступное поведение, информационная сеть, зависимость, социальные сети, информационные технологии, социальные факторы

E. Seitova,
student,
Kazan Innovative University named after V.G. Timiryasov

The relationship between internet addiction and criminal behavior

Abstract. The purpose of the study is to examine the relationship between the commission of crimes and the presence of Internet addiction in a criminal subject. The paper highlights the signs of Internet addiction, gives a brief description of them, examines the problem of alcoholism and drug addiction and their impact on the commission of a crime, compares Internet addiction with addiction to alcohol and narcotic substances, highlights the features of Internet addiction among young people. It is noted that the formation of Internet addiction can be influenced by the insufficient educational influence of parents, as well as the peculiarities of the psyche and behavior of minors. It is stated that there is no direct relationship between involvement in Internet activity and the commission of crimes.

Keywords: Internet addiction, criminal behavior, information network, addiction, social networks, information technology, social factors

Введение. Интернет является неотъемлемой частью жизни современного человека, в настоящее время даже трудно представить себе ребенка, который не знал бы, что такое интернет и как им пользоваться. Каждый день миллионы людей заходят в сеть с целью узнать погоду, проверить уровень пробок на дороге, посмотреть короткие видео за завтраком, ответить друзьям на сообщения, оценить «истории» в социальных сетях. Современный человек настолько сильно привязан и связан с глобальной информационной сетью, что невольно хочется сказать об этом, как о самой настоящей зависимости. Несмотря на пользу, удобство и упрощение жизни человека, интернет также стал средой, в которой начала развиваться своя преступность. Из вышесказанного следует, что вопрос взаимосвязи интернет-зависимости и предрасположенности к преступному поведению является актуальным и в настоящее время.

Целью работы является рассмотрение влияния глобальной сети «Интернет» на личность в ее стремлении к совершению общественно опасного деяния. Для достижения поставленной цели необходимо решить следующие задачи, а именно: раскрыть понятие интернет-зависимости, указать признаки и последствия интернет-зависимости и определить взаимосвязь интернет-зависимости и преступного поведения.

Основная часть. Интернет-зависимость – устойчивое нарушение поведения и состояние, при котором человек не может контролировать проведенное в интернете время; данное состояние сопровождается сильным влечением к использованию информационной сети в ее различных проявлениях, а также проявляются сопутствующие психофизиологические, поведенческие и эмоциональные изменения.

В 1995 году нью-йоркский психиатр Айвен Голдберг впервые дал определение понятию интернет-зависимости: в понимании Айвена Голдберга интернет-зависимость – это «дезадаптивная схема пользования интернетом, ведущая к клинически значимым нарушениям или дистрессу».

Интернет-зависимость обладает своими признаками, которые находят свое выражение в следующем:

1. Страх оказаться без мобильного устройства даже на непродолжительное время;
2. Высокий уровень тревожности и дискомфорта при разряженном электронном устройстве;
3. Компульсивное стремление к проверке своего телефона (сообщений, новостей из социальных сетей, количества людей, просмотревших выставленную «историю» и пр.);
4. «Жизнь в сети» – постоянное пребывание на связи в социальных сетях и мессенджерах;
5. Синдром рассеянного внимания – невозможность сосредоточиться на актуальных задачах и длительное время удерживать фокус деятельности (клиповое восприятие действительности) [11. С. 64].

Таким образом, можно сделать вывод о том, что тема интернет-зависимости продолжает развиваться, так как современный мир не стоит на месте, постоянно появляются новые разработки, приложения, внедряются новые

технологии, которые призваны упростить жизнь человека, но вместе с этим возникает ряд определенных проблем, решать которые необходимо уже сейчас.

Для того чтобы ответить на вопрос, влияет ли интернет-зависимость на предрасположенность к совершению преступлений, необходимо сперва уточнить проблему влияния зависимости в целом на поведение человека. Для этого предлагается рассмотреть влияние алкогольной и наркотической зависимостей на поведение человека.

Для полноты исследования рассматриваемой темы видится необходимым дать определение такому явлению, как зависимость – это навязчивая потребность в определенном объекте или деятельности, которая может проявляться на физическом, психологическом и эмоциональном уровнях. У зависимого человека удовлетворение тяги выходит на первый план, а невозможность удовлетворить ее характеризуется повышением тревожности, страданиями и даже негативной физической реакцией. Зависимость не всегда пагубно влияет на человека, его поведение и его взаимодействие с окружающим миром и людьми как, например, зависимость от чужого мнения. Если же говорить о пьянстве и наркомании, то такие зависимости чаще сопряжены с социальными отклонениями, и могут подкрепляться информацией из интернет и социальных сетей [4. С. 150].

«Пьянство и алкоголизм, как отклоняющееся поведение, способно влиять на совершение преступления. В состоянии алкогольного опьянения человек не может контролировать себя, его нормальная реакция на внешние раздражители притупляется, искажается восприятие мира, алкоголь отрицательно сказывается на течении психических процессов, расстраивает сознание и волю» [3. С. 148]. Это все влияет на саморегуляцию человека, вследствие чего, в сознании пьяного стираются границы дозволенного; совесть, чувство долга, моральные принципы, уважение к закону исчезают, что приводит к антиобщественному, а нередко и преступному поведению. Как отмечает А.А. Култасов, «среди субъективных факторов алкоголизма определенное место занимает психологический фактор. Существует точка зрения, согласно которой психологический фактор является ведущим в распространении пьянства и алкоголизма» [3. С. 149]. Желание испытать приятное ощущение составляет неотъемлемую часть человеческой психики.

Преступность и наркомания вот уже долгое время неразрывно между собой связаны. В качестве причины, способствующей развитию зависимости от наркотических веществ у человека, можно выделить его неудовлетворенность своей жизнью, уровнем благосостояния, отсутствия ресурсов для закрытия каких-либо потребностей. Здесь также стоит отметить психологический фактор, на который уже указывалось выше при рассмотрении зависимости от алкоголя, а именно желание расшевелить или же расслабить свою нервную систему, испытать приятные ощущения [3. С.150].

Важным проблемой является простая доступность пользования интернетом: чтобы открыть и начать пользоваться глобальной сетью достаточно телефона. Доступ в интернет ничем не ограничивается, не важен даже возраст пользователя.

Интернет-зависимости более подвержены подростки, причиной этому могут быть разные факторы, например, проблемы в общении со сверстниками и семьей, поиски себя как личности [12. С. 480], отсутствие надзора со стороны взрослых [1. С. 18]. Подростки больше подвержены влиянию со стороны разнообразных факторов в силу возрастных особенностей, неустоявшихся взглядов, особенностей подростковой психики. У подростков больше свободного времени, чем у взрослого работающего человека, поэтому они являются наиболее активными пользователями интернета [9. С. 3].

В силу общедоступности, анонимности, отсутствия возрастного ценза и других ограничивающих факторов, интернет становится идеальным местом для времяпровождения. В таком пространстве стирается необходимость регулировать свое поведение, манеру общения, ощущается вседозволенность [10. С. 155]. Здесь могут потреблять контент любого характера, начиная от коротких видео длиной в 10 секунд, до сериалов и игр, чье прохождение и просмотр будет занимать сотни, а то и тысячи человекочасов. Компьютерные игры, в силу особенностей своего содержания и упоминавшейся выше анонимности, также могут способствовать совершению преступлений, формируя отклоняющееся поведение и одобряя его [5. С. 260; 6. С. 112] как своим сюжетом, так и поведением участников (которые часто имеют анонимные клички с оскорбительным содержанием, и в переписке часто употребляют нецензурные выражения или даже совершают оскорбительные действия против аватаров иных участников. К сожалению, именно интернет может стать источником насаждения и продвижения не только отклоняющегося или преступного поведения, но и привести к нарушению полового поведения или изменить гендерное понимание своей половой принадлежности, нарушив, тем самым, репродуктивные права несовершеннолетних [7. С. 398].

Заключение. Подводя итоги вышесказанному, можно выделить общие особенности у таких явлений, как зависимость от алкоголя и наркотиков: влияние социальных факторов (снижение уровня жизни, общая неудовлетворенность, отсутствие возможности закрыть, в связи с этим, какие-либо потребности), психологический фактор (желание испытать приятные ощущения), но самое важное – влияние физических веществ (алкогольной продукции, наркотических препаратов) материального мира на организм и психику человека путем употребления или введения внутрь.

Опираясь на сделанные выводы, можно сказать, что интернет-зависимость отличается от привычных нашему пониманию проявлений такого явления как «зависимость». В случае интернет-зависимости человеку, чтобы удовлетворить свое навязчивое желание, достаточно зайти в социальную сеть, полистать «ленту», кому-то будет необходимо открыть мобильное приложение любимого маркетплейса или же запустить привычную онлайн-игру. Как мы видим, чтобы закрыть свою «потребность», в таком случае не нужно принимать препараты, употреблять что-либо внутрь, достаточно просто переключить свое внимание на цифровую реальность [2. С. 280].

Вопрос влияния интернет-зависимости на предрасположенность к преступному поведению является открытым. Интернет-зависимость, как явление

относительно новое, еще продолжает изучаться. Не все ученые и обычные люди считают, что интернет-зависимость – это болезнь, и с ней необходимо бороться; многие не видят в этом проблемы [8. С. 105].

Общественности уже известны случаи проявления насилия, совершения преступлений со стороны подростков и взрослых, у которых просматривалась интернет-зависимость. Также есть мнение ученых, которое связывает интернет-зависимость, как причину девиантного поведения. Интернет, в действительности, оказывает негативное влияние на преступность [13. С. 205]. Интернет-зависимость действительно может влиять на поведение и поступки человека, но может ли такая зависимость стать причиной предрасположенности к преступному поведению, сказать однозначно нельзя. У подростков, активно пользующихся глобальной сетью, отсутствует внутренняя саморегуляция, нет четкого понимания последствий выбранных действий, они не видят возможного наказания или негативного примера за подобный выбор поведения. Нельзя также забывать, что лица подросткового возраста более уязвимы и нестабильны, поэтому вопрос психического здоровья не должен оставаться в стороне при рассмотрении данной проблемы.

Несмотря на все изложенные факты, думается, что выделить интернет-зависимость как единственную причину к совершению преступления будет неправильным. Наличие самой зависимости не делает из человека преступника. Интернет-зависимость по своей сути отличается от алкоголизма и наркомании, поэтому требует совершенно иного подхода к рассмотрению ее взаимосвязи со склонностью к совершению преступных деяний.

Список литературы

1. Анисимова Ю. Н. Социально–психологический тренинг как метод коррекции зависимого поведения подростков // Современная наука: актуальные проблемы теории и практики. Серия: Познание. 2024. № 4. С. 15–20.
2. Демидова Е. Е. Влияние процесса цифровизации на нормы и девиации современной молодежной среды // Ежегодная богословская конференция Православного Свято–Тихоновского гуманитарного университета. 2020. № 30. С. 277–282.
3. Култасов А.А. Классификация социальных отклонений при совершении преступления // Вестник Евразийского национального университета им. Л.Н. Гумилева. Серия: Право. 2024. № 1(146). С. 147–157.
4. Латыпова Э.Ю. О влиянии средств массовой информации на профилактику и предупреждение зависимости от алкоголизма и наркомании / В сборнике: Уголовно-правовая превенция в сфере оборота наркотических средств или психотропных веществ, алкогольной и спиртосодержащей продукции (региональный аспект). Сборник материалов Всероссийской научно-практической конференции. Чебоксары: Изд-во Чувашского гос. ун-та, 2015. С. 148–152.
5. Латыпова Э.Ю., Бадрутдинов Р.Р. Преступления, совершаемые в сфере компьютерных игр, и их основные характеристики / В сборнике: Цифровые технологии и право: сборник научных трудов III Международной научно-

практической конференции (г. Казань, 20 сентября 2024 г.) / под ред. И.Р. Бегишева и др. В 6 т. Т. 6. – Казань: Изд-во «Познание» Казанского инновационного ун-та, 2024. С. 256–263. EDN: EIVHER. http://DX.DOI.ORG/10.21202/978-5-8399-0846-8_6

6. Латыпова Э.Ю., Гильманов Р.Э., Бадрутдинов Р.Р. Роль правоохранительных органов и специальных служб в борьбе с преступлениями, совершаемыми в сфере компьютерных игр, и технические решения для их предотвращения // Правопорядок: история, теория, практика. 2024. № 2 (41). С. 109–114. DOI: 696X-2024-39-4-109-114

7. Латыпова Э.Ю., Гильманов Р.Э. Посягательства на репродуктивные права как угроза национальной демографической безопасности / В сборнике: Обеспечение безопасности современного общества и государств в условиях многополярного мир. Сборник материалов X Международной научно-практической конференции. Чебоксары: Изд-во Чувашского гос. ун-т, 2025. С. 393–402.

8. Латыпова Э.Ю., Клейн М.С., Гильманов Р.Э. Антропологические подходы к изучению преступности: история и современное состояние // *Oeconomia et Jus*. 2024. № 1. С. 95–109. DOI: 10.47026/2499-9636-2024-1-95-109

9. Сметанкина Л.В. Интернет-зависимость: медицинский, социальный и юридический признаки // Социально-экономические процессы современного общества: материалы Всероссийской научно-практической конференции, Чебоксары, 16 мая 2025 года. Чебоксары: Общество с ограниченной ответственностью «Издательский дом «Среда», 2025. С. 93–95.

10. Степнова Л. А. Особенности субъективного переживания одиночества среди студентов в зависимости от уровня интернет-зависимости // Современные психотехнологии в управлении, политике, бизнесе, образовании и искусстве: Материалы Четвертой Международной научно-практической конференции, Москва, 01–02 июня 2023 года, Москва: Общество с ограниченной ответственностью "Русайнс", 2024. – С. 477–487.

11. Толстогузов С.Н., Елифанов А.В., Машкина С.А., Найда Ю.В. Психологические особенности молодых людей с признаками интернет-зависимости // Экспериментальная психология. 2024. Т. 17, № 1. С. 61–75.

12. Lubis M. The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity // *Procedia Computer Science*. 2022. Vol. 197. P. 151–161.

13. Шутова А. А. Современные тенденции использования информационно-телекоммуникационной сети в процессе совершения преступления // Проблемы в российском законодательстве. 2015. № 4. С. 205–208. EDN UZFDRT.

К. А. Сергеева,

магистрант,

Дальневосточный федеральный университет

**Новые объекты интеллектуальной собственности:
перспективы правового регулирования**

Аннотация. Целью исследования является выявление и анализ проблем правового регулирования новых объектов интеллектуальной собственности – цифрового контента, NFT, объектов, созданных с использованием технологий искусственного интеллекта, геймплеи, массивы данных и др. Автор приходит к выводу о необходимости постепенного развития законодательства в целях сохранения технологической нейтральности и избежания излишней регламентации ввиду динамичного развития цифровых технологий.

Ключевые слова: интеллектуальная собственность, NFT, цифровые права, смарт-контракт, искусственный интеллект, авторское право, правосубъектность, цифровизация

К. А. Sergeeva,

master's degree,

Far Eastern Federal University

New intellectual property objects: prospects for legal regulation

Abstract. The purpose of the study is to identify and analyze the problems of legal regulation of new intellectual property objects, such as digital content, NFTs, objects created using artificial intelligence technologies, games, data sets, and others. The author concludes that it is necessary to gradually develop legislation to maintain technological neutrality and avoid excessive regulation due to the dynamic development of digital technologies.

Keywords: intellectual property, NFT, digital rights, smart contract, artificial intelligence, copyright, legal personality, digitalization

Введение. Цифровой контент стал одной из ключевых экономических категорий – к нему относятся любые результаты творческой деятельности, существующие в цифровой форме – тексты, изображения, аудио- и видеоконтент, программное обеспечение, игровые объекты, трехмерные модели и пр. Многие из этих объектов, по сути, являются традиционными произведениями и охраняются действующим правом интеллектуальной собственности, но их цифровая природа упрощает их копирование и распространение, создавая новые вызовы для правовой охраны.

Кроме того, появляются уникальные виды цифровых объектов, характерных именно для сетевого пространства. Например, эксперты отмечают, что гейм-

плеи, массивы больших данных – это порождения цифровой среды, которые уже сейчас имеют коммерческую ценность и являются оборотоспособным активом, однако прямо не отнесены к объектам интеллектуальной собственности.

Основная часть. Одним из наиболее обсуждаемых феноменов последних лет стали NFT (non-fungible tokens) – уникальные записи в блокчейне (платформенные решения на базе технологии распределенных реестров), которые удостоверяют право собственности на определенный цифровой объект (изображение, музыкальный файл, коллекционный предмет и т. д.). NFT фактически выступает цифровым сертификатом, привязанным к конкретному объекту; это способ совершения сделки с новым, переработанным из существующего цифровым объектом в сети блокчейн, посредством смарт-контракта и электронного кошелька.

В 2022 году был внесен законопроект, предлагающий расширить перечень ст. 1225 ГК РФ и включить NFT-токены в число охраняемых результатов интеллектуальной деятельности. Авторы этой инициативы обосновывали ее необходимостью юридически закрепить понятие NFT и обеспечить правовую защиту правообладателей, указывая, что «NFT-токен – это цифровой сертификат на право собственности, поэтому он сам является объектом интеллектуальной собственности».

Однако объектом интеллектуальных прав могут быть только сами результаты творческой деятельности или средства индивидуализации, но не права на них. NFT по своей сути – запись в распределенном реестре, удостоверяющая определенное право (например, право владения конкретным экземпляром цифрового артефакта) [1. С. 11]. Такой токен не создается творческим трудом и не обладает самостоятельной творческой оригинальностью; он лишь подтверждает связь между владельцем и цифровым объектом [2. С. 116].

NFT имеют деловую и репутационную значимость, но, приобретая NFT, субъект не обязательно получает авторские права на само произведение – он получает «цифровую метку» на блокчейне, а авторские права остаются у создателя контента (если иное не оговорено договором) [3. С. 98]. Более правильным видится регулировать NFT как особый вид цифровых активов (цифровых прав).

Российский законодатель уже ввел в 2019 году понятие «цифровых прав» (ст. 141.1 ГК РФ) – это обязательственные и иные права, содержание и условия осуществления которых определяются в информационной системе (например, права из токенов). NFT-токены логично рассматривать именно как цифровые права, удостоверяющие имущественные интересы. При совершении сделок с NFT следует четко договориться о правах на исходный цифровой объект (например, лицензирование авторских прав на изображение, связанное с NFT), поскольку само по себе приобретение NFT не передает право собственности на интеллектуальные результаты, лежащие в основе токена, отсутствует творческая составляющая для создания непосредственно нового объекта.

Зарубежная практика показывает, что цифровые технологии (NFT, блокчейн, нейросети) рассматриваются через призму авторского права и товарного знака: суды США применяют общие принципы, лишь учитывая новые формы эксплуатации (см. например, *Hermès International v. Mason Rothschild* № 22-CV-

384–JSR, 2023). Никаких особых правовых режимов для NFT не сформировано. Если NFT содержат материал, охраняемый авторским или смежным правом, его использование без разрешения считается нарушением.

Если на основе оригинального объекта был создан его цифровой аналог, который будет реализовываться в качестве NFT-токена, то цифровой аналог может считаться производным произведением к оригиналу, соответственно, если права на оригинал не принадлежат создателю цифровой версии, без согласия правообладателя и без выплаты вознаграждения использование такого производного произведения запрещено [4. С. 5].

Исходя из анализа представленных позиций, целесообразно обязать участников рынка зарегистрированных объектов, цифровые версии которых передаются при помощи NFT-токенов, регистрировать отчуждение права (заключение лицензионного договора) и на реальный зарегистрированный объект. В качестве альтернативы видится обоснованным создание единого реестра NFT-токенов, что позволит упростить процедуру регистрации.

Далее рассмотрим алгоритмы – это упорядоченные последовательности действий или логических операций, лежащие в основе программного кода и работы программных продуктов. В эпоху цифровизации алгоритмы и модели данных приобретают огромную экономическую значимость (например, алгоритмы ранжирования поисковых результатов, рекомендательные системы, модели машинного обучения).

Действующее законодательство РФ исходит из того, что алгоритм как таковой не охраняется патентом или авторским правом, если рассматривается абстрактно, в отрыве от конкретной реализации. В частности, патентное право прямо устанавливает, что научные теории и математические методы не являются изобретениями. Алгоритм, по сути, представляет собой математический метод или правило, поэтому не может быть запатентован сам по себе (патентоспособна лишь техническая реализация алгоритма, применение его для решения конкретной технической задачи). Также и авторское право не защищает идеи, методы и принципы – оно охраняет только форму выражения.

Поэтому исходный код программы (в котором выражен алгоритм) защищается как литературное произведение, но идея алгоритма – нет. Тем не менее, на практике разработчики защищают ценные алгоритмы и модели с помощью режима коммерческой тайны (ноу-хау): держат их в секрете или предоставляют по лицензии с запретом раскрытия. В российском перечне объектов интеллектуальной собственности секреты производства (ноу-хау) прямо поименованы, и алгоритм, имеющий коммерческую ценность при условии конфиденциальности, может квалифицироваться как ноу-хау.

Таким образом, алгоритмы выступают важным объектом интеллектуальных прав в широкой трактовке (как часть программ для ЭВМ или как ноу-хау). В условиях развития искусственного интеллекта и сложных программных систем все острее встает вопрос, нужна ли дополнительная правовая охрана для алгоритмов (например, особый режим патентования программного обеспечения или расширение возможностей авторского права).

В ряде юрисдикций идут дискуссии о целесообразности патентования программных решений (США и Европа позволяют патенты на изобретения, реализованные компьютером, но при условии технического характера решения). В России тоже предпринимались шаги к стимулированию патентования в IT-сфере, но в целом принцип остается прежним: алгоритм охраняется правом опосредованно (через код или режим секрета), а не напрямую как самостоятельный объект интеллектуальной собственности.

Стремительное развитие технологий искусственного интеллекта создает перед правом интеллектуальной собственности новые вызовы – появляются изобретения, созданные полностью или частично при участии систем искусственного интеллекта. Ситуация беспрецедентна: появляется объект без традиционного субъекта, т. е. результат творчества, полученный без непосредственного творческого участия человека.

В Государственной Думе Российской Федерации осенью планируется обсуждение законопроекта, предусматривающего внесение изменений в статью 1259 Гражданского кодекса РФ, направленных на формальное закрепление авторских прав на произведения, созданные с участием нейросетевых технологий.

Искусственный интеллект, как одна из цифровых «сквозных» технологий (согласно Дорожной карте развития «сквозной» цифровой технологии «Нейротехнологии и искусственный интеллект»), способная выполнять функции, ассоциирующиеся с интеллектом человека (согласно Приказу Росстандарта от 22 сентября 2016 г. № 1189–ст) все сильнее получает распространение во всех сферах. Однако современный этап развития инноваций и правового регулирования не позволяет утверждать о самостоятельной возможности систем искусственного интеллекта вступать в правоотношения.

Исследования, изучающие правовую концепцию и характеристику искусственного интеллекта, в целом определяют взятое во внимание понятие как сложную техническую систему (что связано с термином «искусственный», то есть синтетический, не встречающийся в природе), характеризующуюся способностью к логическому мышлению, самообучению и самореферентному принятию решений в случае изменения внешних условий [5. С. 97]. Иными словами, это результат деятельности человека с указанными «разумными» чертами.

Если рассматривать искусственный интеллект с точки зрения узкого подхода, под ним стоит понимать способность системы достичь определенной цели способом, близким к уровню человеческих возможностей. Однако рассматривая данное понятие шире, стоит отметить способность не только достигать поставленных целей, но и самостоятельно ставить новые, развиваться на основе заложенных алгоритмов и самостоятельно принимать взвешенное решение.

Ряд авторов, развивая позицию законодателя, отмечает когнитивные или даже эмоциональные функции искусственного интеллекта, подобные человеческим (анализ, восприятие, распознавание, оценка, моделирование информации), в связи с чем данные системы подразделяются на сильные (автономные, практически в полном объеме соответствуют разуму человека или превосходят его) и слабые (действуют в рамках заложенного алгоритма) [6. С. 56]. Указанная классификация имеет условный характер.

Применение технологий искусственного интеллекта позволяет создавать объекты авторского права (литературные и художественные произведения, музыка, изобразительное искусство и др.), которые могут генерироваться алгоритмами искусственного интеллекта, изобретения, программы для ЭВМ и т. д. В целом, технологии искусственного интеллекта могут быть задействованы при создании практически всех категорий результатов интеллектуальной деятельности. Это расширяет творческие и изобретательские возможности, но порождает серьезные вопросы правового режима таких результатов.

Сложно согласиться с тезисом о наличии у искусственного интеллекта способности к творчеству или сознания, основанном на схожем с человеческим мозгом принципом работы данных систем. В основе работы искусственного интеллекта лежат безэмоциональные, статистически вероятные результаты, которые генерируются без перестройки имеющихся представлений, взглядов и мировоззрения робота.

Правоприменительная практика в настоящее время тоже сталкивается с необходимостью определения набора функций, присущих искусственному интеллекту. В основном споры связаны с некачественной разработкой систем, обладающих способностью к самообучению и обработке определенных данных. Например, в деле № А40-161176/23-27-1165 вопрос функциональности итогового алгоритма выступил решающим при взыскании арбитражным судом компенсации по лицензионному договору (см. постановление Девятого арбитражного апелляционного суда от 18.06.2024 № 09АП-26642/24 по делу № А40-161176/2023).

Представляется необходимым в данном аспекте разграничивать самообучающиеся алгоритмы искусственного интеллекта, формируемые системой на основе имеющейся информации, от индивидуальных черт, присущих человеку (например, самосознание, психика, воображение). Способности искусственного интеллекта не свидетельствуют о самостоятельной разумной идентификации – это продукт деятельности человека.

Некоторые авторы определяют сущность искусственного интеллекта в качестве «электронной личности» [7. С. 67], что обосновывается подходом Европейского Парламента о необходимости наделения автономных роботов статусом электронных лиц, которые несут ответственность за свои действия и могут независимо принимать решения и взаимодействовать с обществом [8].

Стоит согласиться с позицией ученых о том, что данный комплекс технологий не может быть абстрагирован от умственной деятельности человека ни на стадии определения общих условий его функционирования, ни при вступлении в конкретные гражданские правоотношения [9]. Искусственный интеллект не обладает свободой воли, что исключает возможность определения субъективной стороны (осознания вредных последствий деяния) [10. С. 775], в связи с чем вопросы ответственности могут быть сосредоточены лишь на традиционной юридической ответственности, например, разработчика, оператора, владельца, пользователя и т. д.

На международном уровне подобная позиция отражена в Рекомендации Парламентской Ассамблеи Совета Европы № 2102 от 2017 года, в которой от-

мечено, что несмотря на независимость решений систем искусственного интеллекта, ответственности подлежит деятельность создателей, владельцев и операторов (п. 9.1.1).

Дополнительно необходимо заметить, что в настоящее время в правовой действительности отсутствуют критерии допустимого правового воздействия искусственного интеллекта на правовое поле, «рамки» его деятельности, что исключает возможность установления его ответственности за неправомерное поведение.

Однако в литературе встречается позиция о том, что регулирование поведения искусственного интеллекта в целом не должно существенно отличаться от правовой регламентации деятельности человека [11. С. 15]. В случае поддержки данного подхода искусственный интеллект «претендует» на равные правовые возможности с иными субъектами права. Представляется справедливым квалифицировать искусственный интеллект как особый объект правового регулирования, результаты работы которого требуют специальных правил распределения прав между людьми (авторами данных, авторами алгоритмов, пользователями).

Основным вопросом настоящего исследования выступает способность искусственного интеллекта быть правообладателем результатов интеллектуальной деятельности, созданных им или с его использованием. Статья 1257 ГК РФ закрепляет, что автором произведения науки, литературы или искусства признается гражданин, творческим трудом которого оно создано. Такой подход не препятствует признанию автором произведений, созданных с помощью систем искусственного интеллекта, человека, внесшего творческий вклад в их создание. С развитием технологий искусственного интеллекта данная «монополия» ставится под сомнение в юридической науке.

В ряде резолюций и докладов Европейского Союза подчеркивалось, что автономное творение искусственного интеллекта не обладает оригинальностью, которая требуется для охраны авторским правом (см. например п. 15 Резолюции Европейского парламента от 20.10.2020 о правах интеллектуальной собственности на разработку технологий искусственного интеллекта (2020/2015(INI)).

В судебной практике главенствует подход, согласно которому произведения, созданные с применением технологии искусственного интеллекта, являются интеллектуальной собственностью человека, ввиду презумпции авторства лица, указанного на оригинале произведения либо иным образом (постановление Тринадцатого арбитражного апелляционного суда от 06.02.2024 № 13АП-37912/2023 по делу № А42-3966/2023), что также свидетельствует об отсутствии необходимости и возможности наделения искусственного интеллекта признаками правосубъектности. В Постановлении Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» подчеркивалось, что творческий характер деятельности не исключает возможности использовать технические средства (абз. 5 п. 80) при наличии творческого вклада человека, который будет признаваться автором данного произведения.

ЮНЕСКО подходит к этому вопросу с этико-правовой стороны. В ноябре 2021 года была принята Всеобщая рекомендация по этике искусственного интеллекта, в которой затронуты в том числе и аспекты интеллектуальной собственности. Данный документ не дает прямых указаний, а предлагает вырабатывать политику на основе дальнейшего анализа влияния искусственного интеллекта на права авторов и правообладателей, подчеркивая, что внедрение искусственного интеллекта не должно умалять роль человеческого творчества и культурного многообразия.

Действительно, простого ввода текстового запроса («prompt») может быть недостаточно, чтобы признать возникшее изображение результатом интеллектуальной деятельности. Именно такой подход сейчас прослеживается в зарубежной практике. Например, Ведомство по авторским правам США подтверждает, что произведения искусственного интеллекта охраняются авторским правом только при наличии достаточного человеческого творчества в их формировании. Данный подход стремится сохранить центральную роль человеческого творчества, что соответствует потребностям общества.

Стоит отметить относительную состоятельность и иной позиции о том, что права на результаты интеллектуальной деятельности, созданные искусственным интеллектом, принадлежат обладателям исходных данных или контента для обучения искусственного интеллекта [12. С. 11], так как алгоритмы генерируют новое на базе больших массивов существующих произведений, то есть создатели исходного контента так или иначе сохраняют контроль над производными генерациями. Такой подход сталкивается с трудностями установления конкретного вклада каждого правообладателя, так как алгоритм может состоять из массы объектов обучения, повлиявших на итоговое произведение.

Обобщая вышеизложенное, стоит сделать вывод о том, что прямо сейчас искусственный интеллект не может быть признан ни автором, ни иным правообладателем результата творчества, созданного в результате его использования. Любое произведение, полностью созданное автономным искусственным интеллектом без участия человека, формально не подходит под критерии охраняемого объекта. Стоит констатировать отсутствие исчерпывающего определения понятия искусственного интеллекта, что, в частности, вызывает споры в вопросе признания его в качестве субъекта права.

Говоря о вопросе включения в современной правовой действительности категории правосубъектности искусственного интеллекта, стоит отметить его преждевременность. На современном этапе развития систем искусственного интеллекта нет оснований для отнесения его к числу субъектов авторских прав. По нашему мнению, искусственный интеллект – это лишь объект, цифровое решение, используемое человеком для автоматизации процессов в различных сферах жизни общества, не обладающее правосубъектностью. Отсутствие четко установленного правового статуса искусственного интеллекта является существенной проблемой, ввиду неизбежного отставания правовой материи от научно-технического развития.

Хочется верить, что творчество человека при использовании искусственного интеллекта не будет носить лишь технический характер, включающее в себя лишь создание команды, на основании которой искусственный интеллект генерирует объекты, и внесение изменений в конечный результат.

Представляется, что введение общих норм о правах на результаты интеллектуальной деятельности, созданные искусственным интеллектом, в любом случае должно подчеркнуть, что правообладателями выступают физические или юридические лица (например, разработчики или пользователи), действующие законно и с соблюдением прав тех, чьи материалы могли использоваться для обучения искусственного интеллекта.

Как уже отмечалось, право интеллектуальной собственности в конечном счете служит развитию культуры, науки и прогресса для блага человечества, и искусственный интеллект должен стать инструментом в этих руках, а не конкурентом. В долгосрочной перспективе видится необходимым определение судьбы объектов интеллектуальной собственности, созданных при помощи искусственного интеллекта. Один из вариантов – признать, что при отсутствии автора-гражданина исключительное право принадлежит лицу, запустившему и проконтролировавшему процесс создания такого произведения (в частности, разработчику программы). Однако такой подход может ослабить оригинальность охраняемых произведений ввиду упрощения их защиты.

Альтернативой указанной фикции может выступить создание особого права на объекты интеллектуальной собственности, созданные искусственным интеллектом, что создает возможность правовой охраны указанных произведений без искажения концепции авторства. Этот подход, возможно, преждевременен, ввиду отсутствия попыток адаптации уже существующих правовых конструкций.

Совершенствуя правовой режим объектов интеллектуальной собственности, созданных с помощью искусственного интеллекта, законодатель обеспечивает баланс между поощрением инноваций и сохранением основополагающих принципов права интеллектуальной собственности, что позволит безопасно интегрировать новые технологии в правовое поле.

Заключение. В целом, расширять перечень ст. 1225 ГК РФ следует очень осторожно. Например, цифровой контент – это, по сути, произведение, база данных. Прямое добавление каждой новой технологии в перечень охраняемых результатов интеллектуальной деятельности может привести к чрезмерной регламентации. Вместо этого целесообразно прибегнуть к разъяснениям и точечным поправкам: например, охраняемыми произведениями могут быть в том числе произведения, созданные с использованием компьютерных технологий (то есть цифровая форма не препятствует их охране). Новые средства индивидуализации (например, хештеги брендов, аккаунты в соцсетях) могут защищаться как товарные знаки или коммерческие обозначения при определенных условиях, без создания отдельной категории объектов. То есть, технологическая нейтральность законодательства об интеллектуальной собственности видится на современном этапе развития общества наиболее целесообразным.

Список литературы

1. Лазарева Ю. А. NFT: проблема определения правовой природы и перспективы законодательства // Журнал Суда по интеллектуальным правам. 2023. № 5. С. 10–15.
2. Ходова М. Т. Технологии NFT как способ защиты прав интеллектуальной собственности // Юридическая наука. 2022. № 8. С. 111–126.
3. Рожкова М. А. NFT и иные токены: право на запись и право из записи // Журнал Суда по интеллектуальным правам. 2022. № 11. С. 96–99.
4. Berlia A. Intellectual Property Rights in Sports Law: The Role of NFTs in Copyright Protection and Trademarks // Journal of Legal Aspects of Sport. 2022. № 32(1). С. 3–15.
5. Хисамова З. И., Бегишев И. Р. Сущность искусственного интеллекта и проблема определения правосубъектности // Московский юридический журнал. 2020. № 2. С. 96–100.
6. Регулирование робототехники: введение в «робоправо». Правовые аспекты развития робототехники и технологий искусственного интеллекта / под ред. А.В. Незнамова. Москва: НОРМА, 2018. 110 с.
7. Морхат П. М. Юнит искусственного интеллекта как электронное лицо // Московский юридический журнал. № 2. 2018. С. 61–72.
8. Резолюция Европейского парламента от 16.02.2017 с рекомендациями Комиссии по гражданско-правовым нормам в области робототехники [Электронный ресурс]. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата обращения: 11.06.2025).
9. Олейник Е.В., Шевченко О.М. Понятие и правовое регулирование цифровой корпорации // Предпринимательское право. 2023. № 2. С. 31–33.
10. Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12. № 6. С. 771–775.
11. Морхат П. М. Искусственный интеллект с точки зрения международного гуманитарного права // Право и государство: теория и практика. № 10 (154). 2017. С. 10–15.
12. Григорян К. Г. Проблема определения авторства при создании произведений с помощью программ искусственного интеллекта // Весенние дни науки : сборник докладов Международной конференции студентов и молодых ученых (Екатеринбург, 20–22 апреля 2023 г.). Екатеринбург: Издательский Дом «Ажур», 2023. С. 13–14.

**Проблемы собирания и оценки электронных доказательств
в уголовном процессе**

Аннотация. Цифровизация общества приводит к тому, что у большинства людей имеется доступ к электронным ресурсам и гаджетам. На почве этого человеческое взаимодействие переходит в информационную среду, включая совершение преступлений и иных правонарушений, в связи с чем различные цифровые устройства (телефоны, планшеты, компьютеры, ноутбуки, жесткие диски и т.п.) могут нести важную для предварительного расследования и суда информацию, однако извлечь ее удастся только при помощи специалистов. Однако вопрос их применения все еще не разрешен. В данной статье будут рассмотрены особенности употребления термина "электронные доказательства", а также проблемы их извлечения.

Ключевые слова: право, доказательства, уголовный процесс, электронные доказательства, электронный носитель информации, режим инкогнито, VPN

K.S. Seu,

Student,

National Research University

Higher School of Economics

**Problems of collecting and assessing electronic evidence
in criminal proceedings**

Abstract. The digitalization of society leads to the fact that most people have access to electronic resources and gadgets. As a result, human interaction is transferred to the information environment, including the commission of crimes and other offenses, which means that various digital devices (phones, tablets, computers, laptops, hard drives, etc.) can contain important information for preliminary investigations and courts, but it can only be extracted with the help of specialists. However, the issue of their use is still not resolved. This article will explore the use of the term "electronic evidence" and the challenges associated with its retrieval.

Keywords: law, evidence, criminal proceedings, electronic evidence, electronic media, incognito mode, VPN

Введение. Современный этап развития общества характеризуется экспоненциальным ростом количества и разнообразия электронных устройств, а также проникновением цифровых сервисов во все сферы человеческой деятельности. Широкое распространение смартфонов, планшетов, систем «умный дом», интернета вещей (IoT), а также повсеместный доступ к высокоскоростному интернету кардинально трансформируют способы коммуникации, работы и досуга. Однако эта тотальная цифровизация имеет и обратную сторону: виртуальное пространство становится новой ареной для противоправной деятельности. В связи с этим наблюдается закономерный и стремительный рост количества преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, либо тех, в которых цифровые следы являются ключевыми для установления истины по делу. Киберпреступность, мошенничества в сети, распространение запрещенного контента, утечки данных, а также традиционные преступления, подготовка и сокрытие которых фиксируются в цифровой среде, – все это формирует новый вызов для системы уголовной юстиции. Таким образом, увеличение объема цифровой информации напрямую коррелирует с ростом ее доказательственного значения, что актуализирует необходимость совершенствования механизмов работы с электронными доказательствами.

Актуальность темы настоящего исследования обусловлена всеобщей цифровизацией общества, в условиях которой электронные устройства и информационные технологии стали неотъемлемой частью повседневной жизни и, как следствие, инструментом и средой для совершения преступлений. Это приводит к тому, что значительный объем информации, имеющей критически важное значение для раскрытия и расследования уголовных дел, содержится на цифровых носителях – от персональных смартфонов и компьютеров до удаленных серверов в информационно-телекоммуникационной сети «Интернет». Однако процессуальный механизм работы с такими данными в российском уголовном процессе отстает от технологических реалий, что порождает комплекс теоретических и практических проблем, связанных с их сбором, фиксацией, оценкой и использованием в качестве доказательств.

Целью данной статьи является комплексный анализ проблем собирания и оценки электронных доказательств в уголовном судопроизводстве.

Для достижения поставленной цели в работе решаются следующие **задачи**:

1. Раскрыть понятие и виды доказательств в уголовном процессе в соответствии с действующим законодательством Российской Федерации.
2. Проанализировать дискуссионные вопросы, связанные с использованием термина «электронные доказательства», и определить их правовую природу.
3. Исследовать специфические проблемы, возникающие на практике при извлечении информации с электронных носителей, в том числе связанные с использованием веб-приложений, режима инкогнито и VPN-технологий.
4. Сформулировать выводы о необходимости развития процессуальных и криминалистических средств работы с цифровыми данными для нужд правосудия.

Основная часть

Понятие и виды доказательств в уголовном процессе. Под доказательством в уголовном процессе в соответствии со ст. 74 УПК РФ понимаются «любые сведения, на основе которых суд, прокурор, следователь, дознаватель в порядке, определенном данным Кодексом, устанавливает наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела» [13]. Тем не менее часть 2 данной статьи предусматривает *numerus clausus* (закрытый перечень) доказательств, принимаемых в рамках уголовного процесса, а именно:

- показания подозреваемого, обвиняемого;
- показания потерпевшего, свидетеля;
- заключение и показания эксперта;
- заключение и показания специалиста;
- вещественные доказательства;
- протоколы следственных и судебных действий;
- иные документы.

Таким образом, все доказательства можно обобщить до 5 видов: показания, заключения, вещественные доказательства, протоколы и иные документы [3. С. 490].

В качестве основных характеристик любых показаний Л.В. Головки выделяет:

- 1) субъективный личный характер, т.е. происхождение данной информации от определенного лица;
- 2) вербальный характер;
- 3) возможность получения их только в ходе определенного следственного действия.

Если говорить про заключения, то они могут принадлежать только специалисту или эксперту, однако они всегда носят дополнительный характер по отношению к данным другими участниками процесса показаниям.

Протоколы, в свою очередь, делятся на те, что осуществляются в рамках досудебного производства – то есть протоколы следственных действий – и те, что применяются в рамках судебного производства – то есть протоколы судебно-следственных действий.

Рассуждая об электронных доказательствах, становится понятно, что отнести к какому-то определенному виду их довольно сложно, поскольку существует проблема определения того, что этимологически и практически под ними понимается. Более подробно поговорим про это далее.

Использование термина “Электронные доказательства”. Несмотря на то, что в научном поле доказательства, закрепленные в электронной или цифровой форме, называют электронными, по мнению ряда ученых, данный термин является не совсем корректным, поскольку при использовании его правовая природа подобных доказательств не принимается во внимание [7. С. 150–151]. Под электронной частью доказательства подразумевается то, что информация, имеющая значение для предварительного расследования или суда, передается

посредством электронных приборов, то есть объектов, работающих за счет электричества. При этом количество используемых электротоков настолько незначительно, что человек не способен ощутить его посредством контактов. Таким образом, под электронными приборами понимают часть электрических приборов, не способных навредить человеку ввиду использования в них деталей, работающих на небольшой силе тока, что означает, что слово “электрические” уже является термином, а потому не может быть применимо в качестве описания доказательств, передающихся посредством подобных приборов, так как сами доказательства не состоят из определяющих данный термин деталей [5. С. 3586–3590].

Тем не менее Р.И. Оконенко отмечает, что важной характеристикой электронных данных является то, что они созданы не только посредством человеческого вмешательства, но и путем создания алгоритмов разработчиками и повторения определенных программ, несмотря на то что в конечном итоге приходит к выводу о том, что “электронные доказательства” как состоявшаяся категория позитивного права еще не сформировалась, а использование в УПК РФ термина “электронный носитель информации”, введенного в соответствии с Федеральным законом от 28.07.2012 143-ФЗ [14], является лишь промежуточным этапом в Российском уголовно-процессуальном праве до появления термина “электронные доказательства” [9. С. 120–123].

Так к характерным чертам цифровых устройств можно отнести:

1. Способность хранить значительный объем сведений.
2. Легкость копирования сведений, содержащихся на электронном устройстве.
3. Возможность получения информации, содержащейся как в памяти самого устройства, так и в информационно-телекоммуникационной сети “Интернет”.
4. относительность и неочевидность содержания цифровых данных

Несмотря на весьма определенные и узко сформулированные особенности данных устройств, возникает вопрос относительно того, насколько реально получить доступ к информации, содержащейся вне памяти самого устройства. То есть если даже электронное устройство, или “электронный носитель информации”, было изъято в рамках следственных действий, на данном этапе этот объект может быть рассмотрен исключительно в качестве вещественного доказательства, однако после получения доступа к информации посредством собирания, исследования, фиксации и ее оценки в зависимости от содержания информации она может быть также отнесена к текстовому доказательству. Однако проблемы, вызванные отсутствием информации в памяти устройства будут рассмотрены в следующей главе.

Рассуждая об изъятии, передаче, хранении, использовании сведений, содержащих цифровую информацию, необходимо руководствоваться принципами, закрепленными Международной организацией по цифровым доказательствам (IOCE), а также использовать определения и понятия, данные ею, о чем пишет Е.И. Галяшина [2. С. 139–140]. Наиболее ключевым из них является определение цифрового доказательства, то есть информации, сохраненной или переданной в бинарной форме, которая может быть использована в суде. Таким обра-

зом, Международная организация по цифровым доказательствам названные в отечественном праве электронные доказательства называет цифровыми, что еще раз может подтвердить позицию С.В.Калитина по этому поводу.

П.С. Пастухов в свою же очередь считает, что в УПК РФ не стоит вводить термины “электронные доказательства” или “электронный носитель информации” в качестве нового источника [12. С. 700–706], поскольку электронные сведения могут быть в виде электронной информации, что в свою очередь может восприниматься в качестве вещественного доказательства или документа [11. С. 558–564]. Однако данная позиция автора нам кажется спорной, поскольку в таком случае важно разграничивать, что именно имеет значение для дела – сам электронный носитель или информация, передаваемая посредством его, как минимум потому, что следственные действия, проводимые в отношении разных видов доказательств также будут различны, что предопределяет набор допустимых средств и методов.

Таким образом, мнение ученых-юристов сильно разнится в вопросе применения термина “электронные доказательства”: кто-то оспаривает использование самого термина, кто-то считает, что выделение таких доказательств в отдельную категорию не обосновано. Я склонна думать, что в научном поле должны вестись дискуссии насчет более детального определения “электронных доказательств” как информации, необходимой для предварительного расследования и использования в рамках судебного процесса, а не источника, посредством которого данная информация передается, тем самым закрепляя приоритет содержания над формой источника. При этом важно отметить, что в таком случае важно разделять электронные доказательства как вещественные и как документы, поскольку в таком случае для нас будет иметь предопределяющее значение либо сам электронный носитель, а информация на нем содержащаяся не будет иметь как такового значения, либо сама информация, содержащаяся в нем, независимо от того, что передается посредством электронного носителя.

Проблемы извлечения электронных доказательств. Придя к выводу о том, что использование термина “электронные доказательства” не является корректным в полной мере, а скорее употребляется в таком значении, в каком оно возникло из практики, мы приходим к еще одной проблеме, в частности, трудности извлечения информации, передаваемой посредством электронных носителей. такую информацию можно разделить на ту, что содержится в памяти устройства и ту, что в ней не содержится.

К информации, содержащейся в памяти устройства относятся данные, которые представлены в виде, понятном и доступном для процессора устройства. Они физически записаны в ячейки памяти в форме бинарного кода (последовательностей нулей и единиц). Более того, данная информация структурирована (источник знает, по какому адресу лежит необходимая информация), она читаема процессором и понятна ему, а также она готова к использованию, т.е. в любой момент может быть открыта, передана другому источнику, отображена на экране и т. д.

Если говорить про информацию, не содержащуюся в памяти устройства, то это те данные, которые не могут быть обработаны устройством, поскольку не

содержатся в его памяти в привычном для него бинарном коде. Для того чтобы такая информация была передана в память устройства, необходимо произвести определенные действия, которые бы оцифровали информацию в понятный для устройства вид.

Одним из примеров обоих видов информации могут послужить кросс-платформенные мессенджеры, которые могут быть открыты на устройствах либо через приложение, которое загружается в память устройства, либо через поисковый сервис, а именно через веб версию приложения, которая не сохраняется в памяти компьютера, подобно приложению. Проблема использования подобной платформы заключается в том, что несмотря на сохранение метаданных в системе, большая часть информации, передаваемой через веб приложения, сохраняется не в памяти устройства, а непосредственно на серверах, принадлежащих тому или иному приложению. Это приводит к тому, что собирание доказательной информации может быть осложнено или недоступно для следственных органов вообще, в случае если данная информация передавалась через веб приложения, поскольку цифровые следы от использования данных приложений, если и будут сохранены в устройстве, то передавать саму информацию, имеющую существенное значение для расследования, они не будут.

Еще одной причиной, значительно усложняющей процесс получения доказательной информации, является возможность использования режима инкогнито, или "режима приватного просмотра", при котором не сохраняется локальная история в браузере [4. С.75–76]. В случае использования данного режима, метаданные сохраняются и передаются провайдеру, т.е. он может видеть адрес сайта, на который заходил пользователь, время осуществления запроса, тип браузера и операционной системы, используемые гражданином, примерный объем данных и другую информацию [6. С. 60–64], однако сами действия, которые осуществлялись на сайте или информация, полученная или переданная пользователем сети на данном сайте, остается скрытой. Безусловно, правоохранительные органы могут запросить у провайдера метаданные, созданные в ходе использования пользователем сети режима "инкогнито", однако эти данные скорее помогут следственным органам понять, какие действия могли быть осуществлены лицом, нежели будут являться достаточным и полным доказательством.

Еще одной причиной невозможности получения доступа к электронным доказательствам может стать использование VPN [1. С.191–192]. Связано это с тем, что в случае использования VPN-серверов весь трафик можно безопасно маршрутизировать через сервер, находящийся в другой точке земли, что позволит скрыть реальный адрес интернет протокола с веб сайтов, т.е. провайдер не сможет отследить, на какие сайты заходил пользователь, какой объем информации передал, а также когда было совершено подключение, а, следовательно, и в случае запроса информации о метаданных следственными органами, провайдер не сможет предоставить эти данные, что повышает возможность сокрытия доказательств, передаваемых посредством электронных носителей [8. С. 60–68].

Заключение. В конечном итоге если пользователь объединяет все вышеперечисленные способы шифрования информации, риск сокрытия доказа-

тельств, передаваемых на электронных носителях, значительно повышается, а так как и рост использования данного вида доказательств увеличивается [10], то и способы, позволяющие обнаруживать такие доказательства, должны активно использоваться следственным органам, что представляется возможным только в случае повсеместного информирования о подобных способах сокрытия передаваемой информации.

Список литературы

1. Бадиков Д.А., Батуева А.Б. Проблемные вопросы раскрытия и расследования преступлений, совершенных с использованием VPN и проху-серверов // Закон и право. 2025. №1. URL: <https://cyberleninka.ru/article/n/problemnye-voprosy-raskrytiya-i-rassledovaniya-prestupleniy-sovershennyh-s-ispolzovaniem-vpn-i-proxu-serverov> (дата обращения: 03.09.2025).
2. Галяшина Е. И. Оценка достоверности цифровых фонограмм в уголовном процессе // Доказывание и принятие решений в современном уголовном судопроизводстве: материалы Междунар. науч.-практ. конференции, посвящ. памяти д-ра юрид. наук, проф. Полины Абрамовны Лупинской : сборник науч. трудов. М.: Элит, 2011. С. 139–140.
3. Головки Л.В. Курс уголовного процесса / под ред. д.ю.н., проф. Л.В. Головки. 2-е изд., испр. М.: Статут, 2018. 490 с.
4. Дерюгин Р. А. Некоторые аспекты исследования цифровых следов в процессе расследования мошенничеств, совершаемых с использованием сведений о пользователях средств сотовой связи // Вестник Уральского юридического института МВД России. 2023. №4 (40). URL: <https://cyberleninka.ru/article/n/nekotorye-aspekty-issledovaniya-tsifrovyyh-sledov-v-protssesse-rassledovaniya-moshennichestv-sovershaemyh-s-ispolzovaniem-svedeniy-o> (дата обращения: 25.08.2025).
5. Калитин С. В. Доказательства электронные и цифровые // Научно-методический электронный журнал «Концепт». 2014. Т. 20. С. 3586–3590. URL: <http://e-koncept.ru/2014/54981.htm> (Дата обращения: 08.09.2024)
6. Карпов Д.С., Ибрагимова З.А. Способы и средства обеспечения анонимности в глобальной сети Интернет // Правовая информатика. 2021. №3. URL: <https://cyberleninka.ru/article/n/sposoby-i-sredstva-obespecheniya-anonimnosti-v-globalnoy-seti-internet> (дата обращения: 23.07.2025).
7. Кольчурин А.Г., Садырина Л.В. Электронные доказательства в уголовном процессе // Гуманитарные, социально-экономические и общественные науки. 2022. №9. URL: <https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-ugolovnom-protssesse> (дата обращения: 01.07.2025).
8. Николахин А. Ю. Использование технологии vpn для обеспечения информационной безопасности // Экономика и качество систем связи. 2018. №3 (9). URL: <https://cyberleninka.ru/article/n/ispolzovanie-tehnologii-vpn-dlya-obespecheniya-informatsionnoy-bezopasnosti> (дата обращения: 24.08.2025).
9. Оконенко Р. И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные

проблемы российского права. 2015. №3. URL: <https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-kak-novoe-napravlenie-sovershenstvovaniya-rossiyskogo-ugolovno-protssessualnogo-prava> (дата обращения: 21.08.2025).

10. От буллинга до плагиата: как печать нотариуса помогает выиграть суд // Федеральная нотариальная палата. 2025. URL: <https://notariat.ru/ru-ru/news/ot-bullinga-do-plagiata-kak-pechat-notariusa-pomogaet-vyigrat-sud-2506> (дата обращения: 24.08.2025)

11. Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // СПС «КонсультантПлюс».

12. Пастухов П. С. "Электронные доказательства" в нормативной системе уголовно-процессуальных доказательств // Пермский юридический альманах. 2019. №2. URL: <https://cyberleninka.ru/article/n/elektronnye-dokazatelstva-v-normativnoy-sisteme-ugolovno-protssessualnyh-dokazatelstv> (дата обращения: 03.11.2024).

13. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 24.12.2001. № 52 (ч. I). Ст. 4921.

14. Федеральный закон "О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации" от 28.07.2012 № 143-ФЗ // Собрание законодательства РФ. 30.07.2012. N 31. Ст. 4332.

Особенности охраны и защиты цифровых прав.

Способы защиты цифровых прав

Аннотация. В настоящей статье проанализированы способы защиты прав, применительно к цифровым правам. Разобраны общие способы защиты прав и затронуты специальные способы защиты. Одновременно рассмотрен вопрос о применимости и относительности обязательственно-правовых и вещно-правовых исков в области защиты цифровых прав. Сделано заключение о преимуществах в применении юрисдикционных и неюрисдикционных средств защиты.

Ключевые слова: юрисдикционные и неюрисдикционные способы защиты, цифровые права, право требования, вещно-правовые и обязательственно-правовые иски, утилитарные цифровые права

Features of protection and defense of digital rights.

Ways of protection of digital rights

Abstract. This article analyzes the ways to protect rights in relation to digital rights. The general methods of protection of rights are analyzed and special methods of protection are affected. At the same time, the question of the applicability and relativity of mandatory and substantive lawsuits in the field of digital rights protection was considered. A conclusion is made about the advantages of using jurisdictional and non-jurisdictional remedies.

Keywords: jurisdictional and non-jurisdictional methods of protection, digital rights, rights of claim, property and contractual claims, and utilitarian digital rights

Введение. Активное внедрение в законодательное регулирование концепта цифровых прав создает для юридического сообщества целый ряд проблем, которые заключаются не только в интерпретации сущности цифровых прав и необходимости применения к ним стандартных норм права, но и возможности их защиты.

Разработка механизмов защиты любого права – это одна из основополагающих задач юриспруденции, как науки, а также дальнейшее внедрении таких механизмов в действующее законодательство. Несмотря на это, до настоящего времени, четкая позиция законодательных органов по вопросам охраны и защиты цифровых прав не выработана. Гражданский кодекс Российской Федерации [4] (далее – ГК РФ) иллюстрирует нам лишь общие меры защиты, применительно ко всем правам. Как правило, это связано с нежеланием законодателя

излишне расширять нормативно-правовые акты новыми терминами и понятиями. Однако, учитывая особенности цифровых прав, а именно, их обращение строго в рамках информационного поля, дает нам наставление о необходимости применения к ним специальных способов защиты, не свойственных, к примеру, вещам или иному материально выраженному имуществу.

Тема исследования является малоизученной и актуальной, в связи с тем, что цифровые права в последнее время становятся все более ликвидным активом и неотъемлемой частью предпринимательского оборота.

Основная часть. Как правило, теория и практика всегда «сопровождают» друг друга, однако, в случае с цифровыми правами, теория «шагнула» дальше. Законодательная база не успевает формироваться в условиях быстроразвивающихся цифровых технологий. Вопросы защиты цифровых прав законодателем своевременно не прорабатываются, чем ставят судебные органы в затруднительное положение и вынуждают, в отсутствии достаточной правовой базы, применять аналогия закона или права.

Ученые сходятся во мнении, что «защита цифровых прав допускает использование гражданско-правовых способов защиты, с учетом особенностей объекта цифровых прав и специфики конкретного нарушения в том или ином случае» [2. С 160]. Между тем, некоторые из них считают, что нагромождение в законодательство новых видов защиты для тех или иных видов прав будет излишним и полагают, что поиск и определение специальных способов защиты для цифровых прав – это прерогатива правовой доктрины.

С такой точкой зрения не согласен Д.Н. Кархалев, в своем исследовании профессор подчеркивает, что «способы защиты цифровых прав можно разделить на две группы: общие и специальные. Общие способы предусмотрены ГК РФ – это признание цифрового права, восстановление положения, существовавшего до нарушения цифрового права, пресечение действий, нарушающих цифровое право или создающих угрозу его нарушения, признание сделок недействительными и применение последствий их недействительности (реституция), самозащита цифровых прав и др.» [6. С. 137]. В той же работе он поднимает вопрос о необходимости применения специальных средств защиты к цифровым правам и обязательное включение их в действующее законодательство.

Тем временем Н.С. Бочарова высказывает предложение «о необходимости формирования своей системы рассмотрения споров, которая будет внедрена в платформу на основании технологии блокчейн и использоваться сторонами при возникновении спора» [3. С. 64]. Вместе с тем она, скептически относясь к стандартным способам защиты цифровых прав, одобряет применение неюрисдикционных средства защиты. Н.М. Ковязина, напротив, полагается больше на меры судебной защиты и признает «существование современного механизма гражданско-правовой защиты, включающего в себя меры цифровой защиты» [7. С. 53]. Д.А. Павлова в диссертации резюмирует, что «среди специальных юрисдикционных способов защиты цифровых прав возможна подача декларативного иска о признании цифровых прав» [11. С. 162]. В то же время, в целях судебной защиты цифровых прав, она предлагает приме-

нять «иск о возврате (восстановлении) доступа к учетной записи пользователя» [1. С. 162].

В целом, в российском законодательстве традиционно разделяют обязательственно-правовые и вещно-правовых способов защиты.

Среди вещно-правовых способов защиты привычно выделяют виндикационные, негаторные и иски о признании права собственности. Отдельные ученые, например, Е.Н. Абрамова [1] рассматривают возможность применить указанные способы защиты к цифровым правам и предлагают выстраивать защиту цифровых прав по аналогии с вещно-правовыми исками, а Крысанова-Кирсанова И.Г. [8. С. 150] так и вовсе проводит тождественную параллель между вещными и цифровыми правами.

Впрочем, при внимательном анализе вещно-правовых способов защиты, нацеленных на защиту абсолютного вещного права – права собственности, разрешить их применение к цифровым правам не допустимо, более того, это будет идти в разрез с российским законодательством.

Обращаясь к определению цифровых прав, которыми в соответствии со ст. 141.1 ГК РФ «...признаются названные в таком качестве в законе обязательственные и иные права...», можно с полной уверенностью говорить об их обязательственной природе. Следовательно, к ним априори должны быть применимы обязательственно-правовые способы защиты.

Если вспомнить про аналогию закона, то применению обязательственно-правовых исков к цифровым правам, вполне может предшествовать образование задолженности по утилитарным цифровым правам, в соответствии с Федеральным законом от 2 августа 2019 г. № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» [9], таких как «право требовать передачи вещи (вещей); право требовать передачи исключительных прав на результаты интеллектуальной деятельности; право требовать выполнения работ и (или) оказания услуг». В том числе сюда же можно отнести и денежные требования.

Вместе с тем, вполне целесообразно применение исков «к оператору информационной системы, в которой осуществляется выпуск цифровых финансовых активов», в соответствии с Федеральным законом от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [10] о возмещении убытков данным оператором владельцу цифровых прав.

По этой же эгидой, в соответствии со ст. 1103 ГК РФ к цифровым правам вполне законно применить кондикционные иски (иски о возврате неосновательного обогащения).

Кроме того, ученые-юристы выделяют в отдельный подкласс специальные способы защиты, такие как, иски о восстановлении данных учета цифровых прав; о признании цифровых прав; о восстановлении доступа к учетной записи субъекта.

Заключение. Таким образом, особенностями защиты цифровых прав являются учет и обращение их в информационной системе, а также комплексная

структура, включающий не только законодательные и юридические меры, но и технические.

Разброс мнений ученых по вопросам защиты цифровых прав находится в широком диапазоне, тем не менее из всех проанализированных источников позиция Д. А. Павловой видится одной из наиболее прогрессивных [11], так как она наиболее точно описала механизмы защиты цифровых прав.

На основе проведенного исследования автор настоящей работы приходит к выводу, что в отношении цифровых прав вполне целесообразно использовать стандартные защитные процедуры, отраженные в отечественных нормативно-правовых актах, в частности в ГК РФ. По общему правилу способы защиты делятся на юрисдикционные и неюрисдикционные.

Одновременно с этим необходимо подчеркнуть, что для цифровых прав более действенны юрисдикционные меры защиты, в виде различных исков. Как выяснилось, гораздо эффективнее использовать обязательственно-правовые способы защиты, в силу обязательственной природы цифровых прав. Между тем сделано заключение, что вещно-правовые способы защиты к цифровым правам не применимы, так как вызывают противоречия с действующим законодательством.

Вместе с тем защита цифровых прав может осуществляться и неюрисдикционными способами, под которыми понимается совокупность действий, осуществляемых правообладателем самостоятельно, без обращения в государственные органы. Такими средствами защиты могут выступать самозащита, ведение досудебной претензионной работы, обращение в третейские суды и т.п.

Список литературы

1. Абрамова Е. Н. Форма ценной бумаги: эволюционное развитие юридической конструкции от бумажного документа к цифровому. Санкт-Петербург: Изд-во СПбГЭУ. 2022. 260 с.
2. Блинкова Е. В., Кошелюк Б. Е. Особенности защиты цифровых прав // Вестник Тюменского государственного университета. Социально-экономические и правовые исследования. 2024. Т. 10. № 3(39). С. 158–173.
3. Бочарова Н.С. Защита цифровых прав // Учение о гражданском процессе: настоящее и будущее: сборник докладов на I Международной научной конференции памяти М.К. Треушникова. М.: Зерцало-М, 2022. С. 63–70.
4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 31.07.2025) // СЗ РФ. 1994. №32. (ч. I). Ст. 3301.
5. Казанцева Е. В. Способ защиты цифровых прав, предусмотренных законодательством РФ // Актуальные проблемы частного права: Материалы всероссийской научно-практической конференции. Омск: 2023. С. 10–13.
6. Кархалев Д.Н. Цифровые права в гражданском обороте // Сибирское юридическое обозрение. 2022. № 2. С. 134–141.
7. Ковязина Н.М. О вопросе защиты цифровых прав // Юрист. 2022. № 1. С. 49–54.

8. Крысанова–Кирсанова И.Г., Гук В.А., Звездкина А.С. Отдельные аспекты признаков цифровых прав // Государственная служба и кадры. 2024. №2. С. 150–153.

9. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 2 авг. 2019 г. № 259-ФЗ (ред. от 08.08. 2024 г.) // СЗ РФ. № 31. Ст. 4418.

10. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 г. № 259-ФЗ (ред. от 25.10.2024) // СЗ РФ. № 31 (ч. I). Ст. 5018.

11. Павлова Д.А. Цифровые права как объект частноправового регулирования: специальность 5.1.3 «Частно–правовые (цивилистические) науки»: дис. ... канд. юрид. наук. СПб. 2025. 210 с.

12. Степанова Т. А. Способы защиты цифровых прав // Научный альманах Центрального Черноземья. 2022. № 1–9. С. 363–368.

Д. В. Терещенко,

студент,

Российский государственный университет
имени В. М. Лебедева

Смарт-контракты в страховании космических запусков и миссий

Аннотация. Современное освоение космоса переживает бум: растет число коммерческих запусков и разворачиваются огромные спутниковые группировки. Это резко увеличивает страховые риски и возможные финансовые потери из-за аварий и сбоев. Традиционное космическое страхование при этом сталкивается с серьезными трудностями: урегулирование убытков часто проходит долго и сложно, процессы непрозрачны, операционные издержки высоки, а риск споров велик. Цель статьи – проанализировать, как смарт-контракты могут оптимизировать страхование космических миссий. Мы рассмотрим основы космического страхования, его участников и виды покрытия, уделив особое внимание параметрическому страхованию, где выплата автоматически срабатывает при наступлении объективно измеряемого события.

Ключевые слова: космическое страхование, смарт-контракты, блокчейн, управление рисками, автоматизация выплат

D. V. Tereshchenko,

student,

Russian State University of Justice named after V. M. Lebedev

Smart contracts in space launch and mission insurance

Abstract. Modern space exploration is booming: the number of commercial launches is growing and huge satellite groups are being deployed. This dramatically increases insurance risks and possible financial losses due to accidents and disruptions. At the same time, traditional space insurance faces serious difficulties: loss settlement is often lengthy and difficult, processes are opaque, transaction costs are high, and the risk of disputes is high. The purpose of the article is to analyze how smart contracts can optimize insurance for space missions. We will look at the basics of space insurance, its participants and types of coverage, paying special attention to parametric insurance, where the payment is automatically triggered upon the occurrence of an objectively measurable event.

Keywords: space insurance, smart contracts, blockchain, risk management, payment automation

Введение. Современный этап освоения космического пространства характеризуется стремительным ростом коммерческой космической деятельности. Активное участие частных компаний, широкое распространение относительно недорогих малых космических аппаратов и развертывание масштабных мега-созвездий спутников приводят к значительному увеличению числа запусков.

Этот количественный рост, в свою очередь, обуславливает резкое возрастание уровня страховых рисков, связанных как с самими запусками, так и с эксплуатацией космических аппаратов на орбите. При этом крайне высокая стоимость разработки, производства и запуска космических миссий, характерная даже для малых спутников в рамках созвездий, многократно увеличивает потенциальные финансовые потери в случае аварий или сбоев. Необходимость разработки современных подходов и решений в этой области становится все более очевидной и востребованной.

Основная часть. Несмотря на возрастающую актуальность страхования космической деятельности, традиционные модели и практики сталкиваются с рядом существенных проблем, ограничивающих их эффективность. Во-первых, процесс урегулирования убытков отличается исключительной сложностью и длительностью. Это обусловлено необходимостью привлечения узкоспециализированных экспертов-аджастеров, проведения глубоких технических расследований причин аварий (зачастую в труднодоступной космической среде) и оценки уникальных повреждений, что неизбежно затягивает сроки выплат и увеличивает неопределенность для страхователей [17]. Во-вторых, наблюдается значительная непрозрачность ключевых процессов – от точной методологии оценки рисков до деталей расследования претензий и расчета окончательных выплат – для всех вовлеченных сторон, включая самих страхователей. Эта закрытость подрывает доверие и затрудняет понимание реальной стоимости и условий страхового покрытия. В-третьих, система характеризуется высокими операционными издержками. Затраты на услуги международных аджастеров и технических экспертов, сложность администрирования полисов, охватывающих многоэтапные космические миссии, и значительные комиссионные отчисления приводят к существенному удорожанию страховой защиты для конечных потребителей [2. С. 93–94]. В-четвертых, совокупность сложности, длительности и непрозрачности создает высокий потенциал для возникновения споров между страховщиками, перестраховщиками и страхователями относительно причин убытка, объема ответственности и размера компенсации, что нередко выливается в длительные и ресурсоемкие судебные разбирательства.

Целью данной статьи выступает анализ потенциала, преимуществ, вызовов и перспектив внедрения смарт-контрактов для оптимизации процессов страхования космических запусков и миссий.

Космическое страхование – это комплексная защита от рисков, связанных с работой в космосе. Оно объединяет разные виды страховок, чтобы покрыть возможные проблемы на всех этапах космической деятельности. Для страховщиков наблюдение за запуском – всегда очень напряженный и зрелищный момент, буквально история в прямом эфире. Алексей Галахов из «Ингосстраха» поясняет, что современный космический аппарат может стоить 250 миллионов евро и больше, что превышает 20 миллиардов рублей. Обеспечить страховое покрытие на такие суммы в одиночку невозможно. Поэтому компании объединяют собственные финансовые резервы с ресурсами зарубежных партнеров и перестраховщиков по всему миру. Мощностей одного российского рынка здесь обычно не хватает [7]. Страховое покрытие в космосе со временем стало значи-

тельно шире. Первые российские полисы защищали в основном риски запуска и выхода на орбиту. Сейчас стандартом стало страхование всего жизненного цикла миссии – от создания аппарата до завершения его работы в космосе. Конкретные риски всегда зависят от задачи. Например, при запуске корабля «Союз МС-19» с киноэкипажем на МКС в 2021 году, где участвовал «Ингосстрах», страховка покрывала потерю имущества от старта ракеты до открытия люка после стыковки с МКС. Такой подход давно устоялся для пилотируемых полетов к станции. В целом, полис обычно включает: сам космический аппарат и его обслуживание, наземную инфраструктуру (включая стартовые комплексы), гражданскую ответственность (на случай ущерба третьим лицам или окружающей среде), а также жизнь и здоровье членов экипажа [15].

Страхованию в сфере космической деятельности подлежат ключевые активы: разнообразные автоматические космические аппараты, ракеты-носители, пилотируемые корабли, орбитальные комплексы, системы выведения, а также обеспечивающие их функционирование наземные сооружения, центры управления и аналогичные объекты [14. С. 381–382].

Космическое страхование опирается на четко структурированный список участников. Центральными фигурами выступают страховые компании (страховщики), чьи функции охватывают комплексную экспертизу рисков, расчет потенциального ущерба, сбор страховых премий и исполнение обязательств по выплатам при реализации страховых событий. Учитывая экстраординарную величину космических рисков, их принятие фокусируется в руках ограниченного круга ведущих страховщиков (традиционно 3–4 ключевых игрока), которые диверсифицируют свою ответственность через механизм сострахования [8. С. 215]. Именно страховые компании являются основными рискодержателями. Страховые брокеры (среди них Marsh, Heath Group, AON Group) выполняют критически важную посредническую и консультативную роль: они проводят глубокий анализ угроз, специфичных для конкретного космического аппарата, совместно со страхователем определяют оптимальные параметры покрытия, согласовывают детали страховой программы со страховщиками, обеспечивают администрирование договора и содействуют в урегулировании убытков. Круг субъектов страхования (страхователей) динамичен и определяется фазой космического проекта – от инвесторов и разработчиков космической техники до производителей и организаций, ответственных за запуски. На международной арене значимыми партнерами признаны синдикаты Ллойда, перестраховочные общества (Мюнхенское, Ганноверское, UIB) и глобальные брокерские группы (Marsh, Heath Group) [10. С. 14].

Смарт-контракт – это договор в виде программы, созданный для автоматизации сделок. Он переводит договорные условия в программный код, который работает сам по себе на протяжении всего срока действия контракта. Когда наступают заранее прописанные условия (например, нужно внести платеж), код автоматически запускает нужное действие. Такие контракты особенно удобны для рутинных, часто повторяющихся операций в бизнесе, где постоянное согласование каждого шага между партнерами не требуется. Чтобы превратить обычный бумажный договор в «умный» цифровой код, используется специаль-

ное программное обеспечение – Contractware. Оно бывает разным: от уже привычных решений вроде систем для оформления страховок или платежей до более сложных платформ, специализирующихся именно на цифровом исполнении договоров [9. С. 244–245]. Особенно мощным инструментом здесь становится технология блокчейн, которая позволяет смарт-контрактам работать надежно – выполнять условия честно, даже если стороны изначально не доверяют друг другу, так как контроль обеспечивается самой системой, а не посредником вроде банка. При этом внедрению смарт-контрактов мешают серьезные сложности. Главная из них – осторожность бизнеса: многие компании пока сомневаются в надежности блокчейна и считают его использование для договоров лишним усложнением привычных процессов [18. С. 100].

Введение инновационного подхода к управлению рисками, известного как параметрическое страхование (Parametric Insurance), было осуществлено компанией Descartes в 2018 году. Принципиальное отличие данной методологии от традиционных страховых механизмов заключается в устранении необходимости проведения сложных и длительных процедур установления факта и оценки размера убытка. Ключевая сущность параметрического страхования состоит в активации страховой выплаты исключительно при наступлении заранее определенного и объективно измеримого события природного или техногенного характера (такого как наводнение, циклон, землетрясение, достигшие заданной интенсивности). Выплата инициируется при достижении событием порогового значения строго заданного параметра или индекса, что исключает потребность в трудоемкой верификации фактических убытков на местности [15]. При рассмотрении контекста инновационных страховых продуктов актуальным представляется также вопрос страхования космических рисков, представляющего собой узкоспециализированную отрасль, нацеленную на защиту финансовых интересов субъектов хозяйствования в космической сфере. Данная отрасль предлагает комплексное покрытие, включающее страхование предпусковых рисков (защита от ущерба на этапе подготовки к запуску вследствие аварий, стихийных бедствий или ошибок сборки), страхование рисков запуска (покрытие убытков от неудачного вывода на орбиту, включая потерю ракеты-носителя и полезной нагрузки) и страхование рисков эксплуатации на орбите (покрытие ущерба от отказов бортового оборудования, столкновений с космическими объектами, воздействия радиации и иных факторов космической среды в течение срока активного существования аппарата) [4].

Спутники на низких орбитах живут недолго – всего несколько лет. После окончания службы они сходят с орбиты, сгорают в атмосфере, и, к сожалению, иногда их фрагменты могут достичь Земли. Этот факт создает реальный, хоть и небольшой, риск для людей и имущества на планете. Возникает важный вопрос: кто будет нести ответственность, если такой обломок причинит вред? Похожие сложности с определением виновника возникают, если один космический аппарат повредит другой прямо в космосе. Первым делом в таких ситуациях смотрят на законы страны, где произошел ущерб. Представим: обломок упал в Германии. В этом случае будут применяться немецкие законы – специальные разделы авиационного законодательства о космической деятельности и общие нормы Граж-

данского кодекса (параграф 823) [3. С. 190]. Ключевой момент для пострадавших: по немецкому праву владелец или оператор спутника несет абсолютную ответственность. Это означает, что людям или организациям, которым причинен вред, не нужно доказывать вину оператора. Сам факт, что ущерб причинен космическим объектом, обязывает к выплате компенсации. Размер выплат при этом может зависеть от того, сколько объектов запустила ответственная сторона.

Однако ситуация резко усложняется, если космический объект одной страны причиняет ущерб на территории другой страны или ее имуществу в космосе. Разбираться в таких спорах только через национальные суды очень трудно, потому что необходимо: доказать точную связь между конкретным объектом и ущербом на большом расстоянии, преодолеть различия в законах разных стран о пределах страховой ответственности, добиться исполнения решения суда одной страны в другой. Чтобы решить эти проблемы и обеспечить справедливость для всех, страны мира договорились о единых международных правилах. Главными из них являются два документа:

Космический Договор (1967 г.), как основополагающий документ, впервые установил принцип: если государство запускает объект в космос (само или с его территории), оно несет международную ответственность за любой ущерб, который этот объект или его части причинят другому государству-участнику Договора или его гражданам – будь то на Земле, в воздухе или в космосе (Статья VII). Это создало основу для коллективной ответственности.

Конвенция об ответственности (1972 г.). Эта Конвенция придала практическое содержание принципам Договора 1967 года. Самое важное в Конвенции 1972 года – ее практический подход к защите людей и имущества на Земле: за ущерб на поверхности Земли (или воздушному судну в полете) запускающее государство несет строгую (абсолютную) ответственность (Статья II). Это значит: если спутник или его обломок упал и причинил вред, пострадавшим не нужно доказывать ошибку или вину запустившего государства. Факта ущерба достаточно для требования компенсации. За ущерб в космосе (например, столкновение спутников) ответственность наступает, только если будет доказана вина запускающего государства (Статья III) [12].

Космическое страхование выступает надежным партнером для компаний, работающих на орбите и за ее пределами. Его основная ценность – в защите от значительных финансовых потерь, которые могут возникнуть из-за непредвиденных событий. Покрытие распространяется на широкий спектр рисков: от повреждения или уничтожения дорогостоящего спутника еще на земле до аварии ракеты-носителя, неудачного вывода аппарата на орбиту или других критических сбоев на разных этапах миссии. Одно из ключевых преимуществ – минимизация финансовых рисков для компании. Наличие страховки позволяет бизнесу сохранять устойчивость и операционную непрерывность даже после серьезных инцидентов, которые в ином случае могли бы поставить под угрозу само существование проекта или компании. Страховой полис также способствует снижению стоимости привлекаемого капитала. Инвесторы, видя, что их вложения защищены от форс-мажорных обстоятельств в высокорисковой космической сфере, охотнее финансируют проекты и могут предлагать более вы-

годные условия. Более того, наличие страхования часто становится обязательным условием для получения крупных кредитов или инвестиций от специализированных банков и финансовых институтов, работающих с космическими инициативами. Наконец, и это особенно важно, космическое страхование обеспечивает защиту людей – главной ценности отрасли. Речь идет о жизни и здоровье космонавтов, а также персонала, работающего на наземных космических объектах. Страховщик гарантирует финансовую поддержку – выплату компенсации самому застрахованному лицу или его наследникам в случае трагической гибели, получения инвалидности или иной потери трудоспособности вследствие несчастного случая при исполнении профессиональных обязанностей. Это не просто финансовая мера, а проявление ответственности перед теми, кто осваивает космос [8. С. 215–217].

Смарт-контракты, функционирующие в распределенных реестрах, представляют собой критически важные, но потенциально уязвимые компоненты блокчейн-инфраструктуры. Наличие ошибок в их реализации способно привести к необратимым финансовым потерям, компрометации данных и системным сбоям, что обуславливает необходимость обязательного независимого аудита безопасности перед развертыванием в продуктивной среде. Следует выделить следующие категории уязвимостей, представляющих наибольшую угрозу [6]:

Реентерабельность (Re-entrancy) – эксплуатация возможности повторного вызова функции до завершения предыдущей операции и обновления состояния контракта. Данный вектор атаки, продемонстрированный в инциденте с The DAO, позволяет злоумышленнику инициировать рекурсивный вывод активов.

Целочисленное переполнение/исчерпание (Integer Overflow/Underflow) – возникает при выполнении арифметических операций за пределами диапазона допустимых значений переменной, что вызывает некорректное изменение состояния (например, необоснованное увеличение баланса).

Неконтролируемые внешние вызовы (Unchecked External Calls) – передача управления непроверенным или враждебным контрактам в процессе межконтрактного взаимодействия, что может привести к неавторизованному изменению данных или блокировке средств.

Дефекты бизнес-логики (Business Logic Flaws) – семантические ошибки, при которых корректный с синтаксической точки зрения код реализует ошибочные операционные потоки (например, нарушение принципов распределения вознаграждений или некорректные механизмы управления доступом).

Проведение комплексного аудита безопасности является неотъемлемым элементом жизненного цикла разработки блокчейн-решений. Данная процедура включает статический и динамический анализ кода, формальную верификацию, моделирование угроз и пентестинг. Целью является выявление не только технических уязвимостей, но и концептуальных противоречий в архитектуре. Пренебрежение аудитом создает неприемлемые правовые, финансовые и репутационные риски для всех участников экосистемы. Рекомендуется привлекать специализированные организации, соответствующие международным стандартам кибербезопасности (таким как OWASP SAMM, NIST SP 800–115), для обеспечения всесторонней экспертизы до публикации контракта в основной сети блокчейна [11].

Правовое положение смарт-контрактов сегодня напоминает зыбкую почву – единого международного подхода к их регулированию не существует. Несмотря на то, что по своей сути смарт-контракты представляют собой форму договорных обязательств, автоматизированных кодом, большинство стран мира пока не создали для них специальной законодательной базы, оставляя участников рынка в зоне правовой неопределенности. Международное сообщество предпринимает определенные шаги: такие документы, как Конвенция ООН об использовании электронных сообщений в договорах и Типовой закон ЮНСИТРАЛ об электронной торговле, устанавливают общие рамки для сделок, заключенных электронным способом. Эти акты теоретически могут быть применимы и к смарт-контрактам как к частному случаю электронных соглашений. Однако в них критически не хватает конкретики, необходимой именно для смарт-контрактов. Как гарантированно идентифицировать стороны контракта в анонимной или псевдонимной среде блокчейна; как фиксировать предмет сделки и ценовые условия так, чтобы это было понятно и суду, и исполняющему коду; как распределять ответственность, если исполнение кода привело к ущербу из-за ошибки или внешнего вмешательства: все эти вопросы, которые стандартны для бумажного договора, становятся сложнейшей головоломкой в мире смарт-контрактов. На фоне глобального правового вакуума отдельные юрисдикции пытаются найти свои ответы. В США, например, несколько штатов приняли законы, прямо признающие смарт-контракты. Яркий пример – Теннесси, где законодательно закреплено право использования смарт-контрактов в электронных сделках, при условии, что такие контракты обладают юридической силой и могут быть основанием для иска. Это важный шаг, но он охватывает лишь часть страны [13]. В России ситуация иная. Отечественное законодательство пока плохо приспособлено к регулированию смарт-контрактов. Определенные надежды вселил законопроект Минэкономразвития РФ, представленный в 2020 году и предлагавший внести изменения в часть 4 Гражданского кодекса РФ. Этот документ предполагал легализацию «типовых смарт-контрактов» – шаблонов для управления определенными цифровыми правами с автоматической проверкой исполнения условий [1]. Однако даже этот проект, фокусируясь на узком сегменте (цифровые права), не решал комплексно всех перечисленных выше проблем: идентификации, фиксации условий, ответственности. Его судьба и дальнейшее развитие законодательства в этой сфере остаются предметом дискуссий.

Пилотные инициативы в области блокчейн-страхования демонстрируют растущий практический интерес отрасли к распределенным технологиям. Стартап Etherisc создал децентрализованную платформу на базе Ethereum, где пассажиры могут приобретать полисы от задержек авиарейсов с автоматическими выплатами при наступлении страхового случая – как криптовалютой, так и традиционными средствами. Компания также разрабатывает решения для страхования сельхозкультур от погодных рисков, защиты от ураганов и даже страхования цифровых активов. В секторе морских перевозок платформа Insurwave использует блокчейн для автоматизации страховых транзакций, повышения точности оценки рисков и создания неизменяемого реестра данных о грузоперевозках, что существенно снижает операционные издержки [16]. Значительный им-

пульс развитию придают отраслевые консорциумы: RiskStream Collaborative, объединяющий десятки страховщиков, внедрил блокчейн-систему для мгновенной верификации автостраховых полисов при ДТП и автоматизации уведомлений об убытках. Платформа OpenIDL, разработанная при участии Американской ассоциации страховых услуг, фокусируется на повышении прозрачности отчетности через защищенный обмен данными между участниками рынка и регуляторами. Ключевую роль в формировании индустриальных стандартов играют профильные альянсы – такие как B3i, оптимизирующий кросс-корпоративные процессы на базе Hyperledger Fabric, или инициатива европейских гигантов в лице Allianz, Zurich и Munich Re, совместно создающих новые страховые продукты на блокчейне [5]. Эти проекты иллюстрируют общую тенденцию: от автоматизации выплат до создания доверенных экосистем данных, где распределенные реестры становятся технологическим фундаментом для трансформации традиционных бизнес-моделей.

Заключение. Смарт-контракты обладают значительным потенциалом для трансформации страхования космических рисков, прежде всего за счет автоматизации выплат по параметрическим продуктам. Их внедрение сулит существенные преимущества: повышение скорости расчетов, снижение операционных издержек, обеспечение прозрачности и неизменности условий договора. Однако ключевым условием для масштабирования этой технологии является решение двух фундаментальных проблем: технологической (включая надежность оракулов для верификации космических событий) и правовой (устранение регуляторных пробелов в статусе смарт-контрактов). Успешное преодоление этих барьеров способно стать катализатором устойчивого роста коммерческой космонавтики, обеспечив надежную защиту многомиллиардных инвестиций в отрасль. Для реализации этих перспектив критически важно продолжение прикладных исследований, запуск пилотных проектов в реальных условиях и формирование конструктивного диалога между индустрией, технологическими компаниями и регуляторами для разработки сбалансированной правовой базы.

Список литературы

1. Федеральный закон от 31 июля 2020 г. № 262-ФЗ «О внесении изменений в часть четвертую Гражданского кодекса Российской Федерации» (документ не вступил в силу) // СПС «Гарант.ру». URL: <https://www.garant.ru/products/ipo/prime/doc/74351020/> (дата обращения: 14.08.2025)
2. Алифанов Е. В. Исследование методологических особенностей страхования космических рисков // ТДР. 2011. №1. С. 93–95.
3. Бонн В. Б., Суханов Е. А. Германское право. Ч. 1. Гражданское уложение: пер. с нем. Исследовательский центр частного права, 1996.
4. В бесконечность и за ее пределы: 10 европейских космических стартапов // PROXIMA. URL: https://gisproxima.ru/10_startapov (дата обращения: 12.08.2025).
5. Запущена блокчейн-платформа для страховых компаний // InScience URL: <https://inscience.news/ru/article/blockchain/5959> (дата обращения: 15.08.2025).

6. Как можно взломать смарт-контракт // BINANCE SQUARE. URL: <https://www.binance.com/ru/square/post/425358> (дата обращения: 13.08.2025).
7. Как устроено космическое страхование – десять главных вопросов // РБК Тренды. URL: <https://trends.rbc.ru/trends/industry/61a759259a79476cae99dc0> (дата обращения: 11.08.2025).
8. Камолов С. Г., Красноштанова Т. А. Страхование космических рисков как фактор коммерциализации космической деятельности // Инновации и инвестиции. 2019. №4. С. 213–218.
9. Крыцула А. А. Правовой режим смарт-контрактов: код или договор // Вестник Пермского университета. Юридические науки. 2022. № 56. С. 239–267.
10. Максимова Е. С. Риски высокого полета // Страховой случай. 2014. №12. С. 14.
11. Нейросеть для аудита смарт-контрактов: Как ИИ находит уязвимости и защищает ваши активы // Радиоточка Плюс ИИ Магия. URL: <https://radiotochki.net/blog/ai-magic/neyroset-dlya-audita-smart-kontraktov-kak-ii-nahodit-uyazvimosti-i-zashchishchaet-vashi-aktivy.html> (дата обращения: 13.08.2025).
12. Ответственности перед третьими лицами за ущерб, причиненной РКТ // ЦЭНКИ. URL: <https://www.russian.space/puskovye-uslugi/strakhovanie-riskov/otvetstvennosti-pered-tretimi-litsami-za-ushcherb-prichinennoy-rkt.html> (дата обращения: 12.08.2025).
13. Правовые аспекты смарт-контрактов // BITTEAM. URL: <https://bit.team/blog/ru/pravovye-aspekty-ispolzovaniya-smart-kontraktov/> (дата обращения: 14.08.2025).
14. Степанова Я. Д. Страхование космических рисков // Управление организационно-экономическими системами: сборник трудов научного семинара студентов и аспирантов института экономики и управления. 2023. №23. С. 381–385.
15. Страхование космических рисков: обзор рынка // Ek-top. URL: <https://ek-top.ru/articles/finansovaya-gramotnost/protect-space-investments/> (дата обращения: 11.08.2025).
16. Страхование на основе блокчейна: лучшие решения, меняющие отрасль // PLISIO. URL: <https://plisio.net/ru/blog/blockchain-insurance> (дата обращения: 15.08.2025).
17. Услуги лосс аджастера. Урегулирование убытков при наступлении страхового случая // Независимое агентство сюрвея и аджастинга. URL: https://nasa-service.ru/services/uregulirovanie_ubytkov_loss_adjusting.html (дата обращения: 11.08.2025).
18. Шушканов П. А., Ряховская Я. О. Смарт-контракты в российской правовой системе // Право и управление. 2022. №10 С. 99–105.

А. А. Тесленко,

магистрант,

Воронежский государственный университет

Метавселенные как вызов для правового регулирования

Аннотация. Статья посвящена анализу вызовов и проблем, которые метавселенные представляют для современного правового регулирования. Рассмотрены вопросы определения понятия и правовой природы метавселенной и анализируются два основных подхода к регулированию данного объекта информационно-правовых отношений: централизованный и децентрализованный, особое внимание уделяется проблемам установления юрисдикции в отношении метавселенных и сложностям квалификации преступлений, совершаемых в них. Автором предложена гибридная модель правового регулирования, которая сочетает в себе элементы государственного регулирования и децентрализованного самоуправления, также исследуются возможные принципы определения юрисдикции в отношении метавселенных.

Ключевые слова: метавселенная, цифровые технологии, правовое регулирование, централизованный подход, децентрализованный подход, юрисдикция, квалификация преступлений

A. A. Teslenko,

Master's student,

Voronezh State University

Metaverse as a challenge for legal regulation

Abstract. The article is devoted to the analysis of the challenges and problems that metaverses pose for modern legal regulation. The issues of defining the concept and legal nature of a metaverse are considered and two main approaches to the regulation of this object of information and legal relations are analyzed: centralized and decentralized, with special attention paid to the problems of establishing jurisdiction over metaverses and the difficulties of qualifying crimes committed in them. The author proposes a hybrid model of legal regulation, which combines elements of state regulation and decentralized self-government, and explores possible principles for determining jurisdiction over metaverses.

Keywords: metaverse, digital technologies, legal regulation, centralized approach, decentralized approach, jurisdiction, qualification of crimes

Введение. Развитие Интернета прошло большой путь от статического Web 1.0 к интерактивному Web 2.0, однако в настоящий момент мы стоим на пороге новой иммерсивной реальности, название которой «metaverse» (метавсе-

ленная). Впервые понятие «metaverse» было использовано в фантастическом романе «Лавина», автором которого является Нил Стивенсон. Кто бы мог подумать, что это понятие будет определять целую концепцию интерактивной трехмерной вселенной.

Основная часть. Метавселенная сочетает в себе широкий спектр технологий, таких как блокчейн, VR/AR, искусственный интеллект, 3D-реконструкция и IoT [3]. Таким образом, метавселенная будет являться не просто глобальной платформой, а полноценной экосистемой виртуальной коммуникации, где люди смогут обучаться, работать, общаться и вести бизнес в режиме реального времени. В отчете Bloomberg 2023 года анализируются перспективы внедрения технологий метавселенной, по данным исследования к 2030 году рынок metaverse может достичь 615 миллиардов долларов [1].

Метавселенные – это новый этап в развитии цифровых технологий, в рамках которого появляются новые формы общественного взаимодействия, которые требуют переосмысления существующих правовых подходов и механизмов регулирования, так как в настоящее время, развитие метавселенных создает беспрецедентный правовой вызов.

Проблема определения понятия «metaverse» является одним из фундаментальных препятствий для ее правового регулирования. Понятие «метавселенная» не имеет общепринятой дефиниции, а также официального закрепления в нормативно-правовых актах или международных документах, однако есть много научных исследований, которые изучают и рассматривают ее правовую природу.

Мэтью Болл – бывший топ-менеджер Amazon Studios, венчурный капиталист и, как многие его называют, пророк метавселенной, в своей книге «Метавселенная и то, как она изменит все» охарактеризовал metaverse следующим образом: «Метавселенная – это масштабная и совместимая сеть трехмерных виртуальных миров, отображаемых в режиме реального времени, в которых практически неограниченное число пользователей могут находиться синхронно и постоянно, ощущая свое присутствие и имея доступ к непрерывным данным, таким как личность, история, права, объекты, коммуникации и платежи» [6]. Исходя из указанного определения, метавселенная это не одна единственная система, которая принадлежит одной организации, а сложная структура, которая позволит различным компаниям создавать внутри метавселенной собственные виртуальные среды. Российские ученые, например, К.С. Евсиков, под «метавселенной» понимает информационную систему с присущими ей технологическими компонентами [10], Н.Н. Ковалева утверждает, что разработанные технологии метавселенных знаменуют новый этап развития мировой экономики, который предполагает создание новой виртуальной экосистемы, и определяет метавселенную как цифровое пространство в сочетании технического и экономического подходов [14]. В своей работе Е.В. Холодная указывает на то, что метавселенная – это направление развития цифровых технологий по созданию цифрового пространства для определенных видов деятельности с имитацией личного присутствия [19].

Все определения отражают и технологические, и экономические, и социальные составляющие концепции метавселенной. Однако есть ряд причин, по которым выработка единого правового определения исследуемого понятия представляет сейчас сложную задачу. Во-первых, метавселенная не имеет финальной формы, на данный момент, по мнению аналитиков компании Gartner, занимающихся технологическим прогнозированием, метавселенная находится на первой фазе развития – зарождающейся [4]. Тем самым динамика эволюции метавселенных создает проблему в разработке единого правового определения. Во-вторых, метавселенная это не одна платформа, а совокупность множества виртуальных пространств, которая в итоге представляет собой их взаимосвязанную сеть. В-третьих, технологическая амбивалентность, что подразумевает под собой сочетание разных технологий в «строении» метавселенной, создает сложности для формирования и сочетания правовых режимов каждой из таких технологий [13].

Таким образом, исходя из анализа научных публикаций, можно предложить следующее определение: метавселенная – это непрерывно действующая, взаимосвязанная сеть иммерсивных миров, которая обеспечивает массовое и синхронное взаимодействие пользователей в реальном времени, которая создает новое цифровое пространство для реализации экономических (цифровая экономика) и социальных отношений.

Отсутствие легального определения метавселенной является лишь вершиной айсберга существующих на данный момент вызовов ее правового регулирования. В рамках работы мы рассмотрим такие вызовы как: дуализм подходов к регулированию применения метавселенных, проблемы установление юрисдикции в отношении метавселенных и сложности квалификации преступных действий в данных сетях.

Существующие вызовы правового регулирования метавселенной обусловлены ее комплексной и многогранной природой, которая создает уникальный правовой и технологический прецедент для цифровой трансформации общества. В связи с этим первостепенное значение приобретает выбор применения централизованного или децентрализованного подходов к регулированию метавселенной [5, 16]. Указанные подходы имеют ряд отличий по ключевым аспектам, а именно различия в архитектуре управления, защите данных и модели регулирования взаимодействия субъектов отношений, возникающих в метавселенных.

Так, суть централизованного подхода заключается в том, что контроль над архитектурой метавселенной (над ее стандартами, развитием и др.) осуществляет один центр (одна организация). Это можно проследить на примере игровой онлайн-платформы Roblox, которая управляется одной компанией Roblox Corporation. Сущность централизованного подхода состоит в том, государство регулирует не саму метавселенную, а взаимодействует с ее владельцем в случае нарушения закона [12]. У такого подхода есть явные преимущества: установление единообразных правил для всех участников; снижение рисков относительно неопределенности ответственных лиц; обеспечение безопасности данных; упрощение контроля со стороны регуляторов. Однако, такой подход не способен

решить проблемы нарушений конфиденциальности (приватности), монополизации рынка данных, ограничений инноваций, а также манипуляции цифровым контентом. Например, крупные корпорации, такие как Meta Platforms Inc⁸ получают полный контроль над данными своих пользователей, что создает не только риск утечек данных, но и позволяет использовать их для манипулирования поведением, таргетированной рекламой и, что еще немало важно, способствует формированию определенного общественного мнения.

Децентрализованный подход (в основе которого распределенная архитектура управления, реализуемая с помощью технологии блокчейна, например, Decentraland, The Sandbox), с одной стороны, решает указанные выше проблемы, но при этом создает новые, такие как: неопределенность субъекта юридической ответственности, разрозненность национальных законодательств, которым должно будет соответствовать функционирование технологий метавселенной. В частности, указанные выше платформы управляются децентрализованными автономными организациями (DAO) [2], что существенно усложняет установление ответственного лица при совершении противоправных действий. В таком случае ответственность размыта между разработчиками протокола, владельцами токенов управления и членами DAO. А также децентрализация порождает необходимость принятия норм международного характера по причине невозможности соответствия такой организационной формы национальному законодательству той или иной страны (в условиях текущих международных отношений). В результате несогласованность законодательных требований различных юрисдикций создает хаос и затрудняет сотрудничество между метавселенными.

Таким образом, централизованный подход не учитывает транснациональную природу метавселенных, а децентрализованный создает правовой вакуум в сфере юридической ответственности. Следовательно, создание гибридной модели регулирования метавселенных станет наиболее эффективным решением – сочетание лучших черт каждого подхода. Так, наднациональная координация, то есть создание международно-правового регулирования на основе соответствующих конвенций и соглашений, которые определяли бы общие принципы работы метавселенных (использование блокчейна, обеспечение конфиденциальности данных), будет являться выгодным и правильным решением, так как, в таком случае, государства остаются центральными регуляторами. Помимо этого необходимо сформировать техническое регулирование, на основе соответствующих международных стандартов, например, введение обязательной сертификации для платформ, которые собирают биометрические данные (осуществляемой национальными органами по сертификации), но оставить разработку различных сервисов и VR/AR пространств за частными компаниями на основе гражданско-правовых договоров (это будет способствовать развитию конкурентных рыночных отношений).

⁸ Признана экстремистской организацией в Российской Федерации.

Тем не менее, остается нерешенной проблема определения юрисдикции, и, соответственно, – обязанности соблюдения национального законодательства. Сложность цифрового пространства в том, что оно охватывает пользователей различных юрисдикций, и оно никак не ограничено территориальными границами. Существует два основных принципа для определения юрисдикции: принцип территории (закон того государства, на территории которого находится человек, организация, имущество); принцип гражданства (государство властвует над своими гражданами вне зависимости от территории) [10]. Однако при использовании этих принципов возникают коллизии между национальными законодательствами разных стран (различная квалификация одного и того же действия). Предлагается следующий вариант решения проблемы определения юрисдикции – использование принципа местонахождения сервера [17]. То есть, будет применяться законодательство той страны, на территории которой расположены серверы, на основе которых функционирует метавселенная (или созданная внутри нее виртуальная среда). Данный подход будет обоснованным, так как он явно упростит практику правоприменения национальных норм. Однако несмотря на кажущуюся простоту, такой принцип не учитывает в полном объеме многогранную архитектуру технологий метавселенных. Прежде всего возникает проблема использования множества серверов (серверы хранения данных пользователей, серверы CDN и маршрутизации трафика), находящихся в разных странах, для функционирования метавселенных, что усложняет определение юрисдикции. Кроме того, данный принцип вступает в противоречие с концепцией суверенитета хранения и обработки данных граждан исключительно на территории определенного государства. Также, некоторые ученые-юристы ведут речь о таком подходе определения юрисдикции как ограничение компетенции государства национальными доменными именами [20], однако и такой вариант имеет ряд трудностей (не все домены (такие как .com, .org) привязаны к территории определенного государства, также регистрация доменного имени и хостинг сайта могут быть в разных юрисдикциях). Таким образом, ни один из указанных подходов не обеспечивает возможность решения трансграничных споров в регулировании метавселенных. Тогда решением проблемы может являться сочетание принципа местонахождения пользователя, который будет гарантировать соблюдение его прав законодательством той страны, где он фактически находится, с принципом «наибольшей связи», заключающемся в анализе релевантных факторов необходимых для выбора подходящей юрисдикции. Вероятно, такой подход позволит создать гибкую и устойчивую модель правового регулирования метавселенных.

Еще один вызов для государства – это появление новых видов преступлений. Раньше мы и подумать не могли о том, что цифровое насилие возможно, однако в Великобритании был зафиксирован случай сексуального надругательства над цифровой личностью подростка [11]. Это ставит новый вызов перед законодателем о квалификации таких преступлений, переосмыслении уже привычных нам составов преступлений, предусмотренных уголовными кодексами как РФ, так и других стран. В настоящее время «цифровая личность», «аватар» не признаются субъектами права, а также нет такого понятия как «цифровое те-

ло», непонятно что считать «нанесением вреда» аватару или как определить «согласие», например, на действия сексуального характера, в виртуальном мире.

Закключение. Подводя итог, следует подчеркнуть, что метавселенные создают серьезные вызовы и требует новых подходов к правовому регулированию для обеспечения безопасного и стабильного «существования» пользователя в сети. Будущее правовое регулирования должно быть адаптивным, международным и гибридным не только для того, чтобы добиться успешной интеграции метавселенных в жизнь общества, но и для возможности граждан защитить свои права и свободы в новой цифровой реальности.

Список литературы

1. Bloomberg. Metaverse may be \$800 billion market, next tech platform. URL: <https://www.bloomberg.com/professional/insights/trading/metaverse-may-be-800-billion-market-next-tech-platform/> (дата обращения: 12.08.2025).
2. Gameoll. Roblox Decentralized Autonomous Organizations. URL: <https://gameoll.com/roblox-decentralized-autonomous-organizations/> (дата обращения 14.08.2025)
3. GeekBrains. Метавселенная: технологии и принципы. URL: <https://gb.ru/blog/metavselennaya/?ysclid=me8vabmxz4449810336> (дата обращения: 12.08.2025).
4. itWeek. Gartner: три фазы развития метавселенной. URL: <https://www.itweek.ru/digitalization/article/detail.php?ID=223585> (дата обращения: 13.08.2025).
5. ReLife. Централизованные и децентрализованные системы: Что выбрать в цифровую эру? URL: <https://relife.global/feed/48323-centralizovannye-i-decentralizovannye-sistemy-cto-vybrat-v-cifrovuiu-eru> (дата обращения: 13.08.2025).
6. The metaverse: what is it and why should you care? URL: https://translated.turbopages.org/proxy_u/en-ru.ru.51d590b4-689cc62c-57ddde42-74722d776562/https/www.techradar.com/features/the-metaverse-what-is-it-and-why-should-you-care (дата обращения: 12.08.2025).
7. Арутюнов А.С. О некоторых проблемных вопросах, связанных с правовым регулированием метавселенных // Общество и право. 2024. №1 (87). URL: <https://cyberleninka.ru/article/n/o-nekotoryh-problemnyh-voprosah-svyazannyh-s-pravovym-regulirovaniem-metavselennyh> (дата обращения: 16.08.2025).
8. Бегишев И. Р., Денисович В. В., Сабитов Р. А., Пасс А. А., Скоробогатов А. В. Уголовно-правовое значение метавселенных: коллизии в праве // Правопорядок: история, теория, практика. 2023. № 4 (39). URL: <https://cyberleninka.ru/article/n/ugolovno-pravovoe-znachenie-metavselennyh-kollizii-v-prave> (дата обращения: 15.08.2025).
9. Евсиков К. С. Метавселенные как новый объект регулирования для информационного права // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. № 1 (44). С. 47–57.
10. Зенин И.А. Основы права. Московский международный институт эконометрики, информатики, финансов и права. М.: 2003. 184 с.

11. Известия. Аватары под подозрением: эксперты предупредили о риске преступлений в метавселенных. URL: <https://iz.ru/1632428/dmitrii-bulgakov/avtary-pod-podozreniem-eksperty-predupredili-o-riske-prestuplenii-v-metavselennykh> (дата обращения :13.08.2025).
12. Интерфакс. Roblox после обращения Роскомнадзора удалила контент с ЛГБТ-пропагандой. URL: <https://www.interfax.ru/russia/1035479> (дата обращения: 13.08.2025).
13. Ковалева Н. Н., Изотова В. Ф., Чайковский Д. С., Шахновская И. В., Соловьев П. В. Метавселенные: проблемы правового регулирования // Вестник Полоцкого государственного университета. Серия Д. Экономические и юридические науки. 2024. №4. URL: <https://cyberleninka.ru/article/n/metavselennye-problemy-pravovogo-regulirovaniya-1> (дата обращения: 12.08.2025).
14. Ковалева Н.Н. Правовые аспекты цифрового совершенствования метавселенных // Право.by. 2022. № 5 (79). С. 81–84.
15. Минбалеев А. В. Цифровые двойники и цифровые аватары как новое явление в праве // Юридический мир. 2022. № 2. С. 27–32.
16. Танющева Н.Ю., Дюдикова Е. И. Централизованный и децентрализованный подходы к организации систем электронных денег: настоящее и будущее // Финансы и кредит. 2016. № 29 (701). URL: <https://cyberleninka.ru/article/n/tsentralizovannyy-i-detsentralizovannyy-podhody-k-organizatsii-sistem-elektronnyh-deneg-nastoyashee-i-budushee> (дата обращения: 13.08.2025).
17. Терентьева Л.В. Принципы установления территориальной юрисдикции государства в киберпространстве // Lex Russica. 2019. №7 (152). URL: <https://cyberleninka.ru/article/n/printsipy-ustanovleniya-territorialnoy-yurisdiksii-gosudarstva-v-kiberprostranstve> (дата обращения: 13.08.2025).
18. Филипова И.А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. №1. URL: <https://cyberleninka.ru/article/n/sozдание-metavselennoy-posledstviya-dlya-ekonomiki-sotsiuma-i-prava> (дата обращения: 16.08.2025).
19. Холодная Е.В. О правовой концепции метавселенных // Lex Russica. 2024. №3 (208). URL: <https://cyberleninka.ru/article/n/o-pravovoy-kontseptsii-metavselennyh> (дата обращения: 13.08.2025).
20. Якунина А.В. Определение юрисдикции государства в цифровом пространстве // Юридические исследования. 2024. №5. URL: <https://cyberleninka.ru/article/n/opredelenie-yurisdiksii-gosudarstva-v-tsifrovom-prostranstve> (дата обращения: 13.08.2025).

Ю. А. Трасковская,

студент,

Белорусский государственный университет транспорта

**Электронное правосудие в республике Беларусь:
современное состояние и перспективы развития**

Аннотация. Целью исследования является комплексный анализ развития системы электронного правосудия в Республике Беларусь. В статье рассматриваются ключевые элементы данной системы, такие как сервис «Электронный суд», система электронного судебного документооборота и подачи исковых заявлений. Особое внимание уделяется правовым основам их функционирования, выявлению практических проблем внедрения и использования цифровых технологий участниками процесса. На основе проведенного анализа определяются перспективные направления и формулируются рекомендации по дальнейшей оптимизации системы электронного правосудия для повышения ее доступности и эффективности.

Ключевые слова: право, цифровые технологии, электронное правосудие, электронный суд, судебная система, Республика Беларусь, электронный документооборот, цифровизация

Y. A. Traskovskaya,

Student,

Belarusian State University of Transport

**Electronic justice in the republic of Belarus:
current state and development prospects**

Abstract. The aim of this research is to provide a comprehensive analysis of the development of the e-justice system in the Republic of Belarus. The article examines key elements of this system, such as the "E-Sud" (Electronic Court) service, the system of electronic court document management, and the filing of claims online. Particular attention is paid to the legal framework for their operation, identifying practical problems of implementation and use of digital technologies by process participants. Based on the analysis, promising directions are identified and recommendations are formulated for the further optimization of the e-justice system to improve its accessibility and efficiency.

Keywords: law, digital technologies, e-justice, electronic court, judicial system, Republic of Belarus, electronic document management, digitalization

Введение. Цифровая трансформация судебной системы представляет собой один из наиболее значимых трендов современного правового развития. Глобализация и технологический прогресс обусловили необходимость модерниза-

ции традиционных форм правосудия, что нашло отражение в концепции электронного правосудия (e-justice). Республика Беларусь активно включилась в этот процесс, реализуя комплекс мер по внедрению цифровых технологий в судебную деятельность.

Актуальность исследования обусловлена необходимостью научного осмысления процессов цифровизации белорусской судебной системы, оценки эффективности implemented мер и выработки научно обоснованных рекомендаций по дальнейшему развитию электронного правосудия. Значимость темы определяется также потребностью в комплексном подходе к решению проблем, возникающих на пути цифровой трансформации правосудия.

Цель исследования заключается в комплексном анализе развития системы электронного правосудия в Республике Беларусь, выявлении существующих проблем и формулировании перспективных направлений совершенствования. Для достижения поставленной цели определены следующие **задачи**:

- исследовать исторические этапы развития электронного правосудия в Беларуси;
- проанализировать современное состояние нормативно-правовой базы;
- оценить практику применения цифровых технологий в судопроизводстве;
- выявить организационные и технические проблемы внедрения;
- разработать предложения по совершенствованию системы электронного правосудия.

Методологическую основу исследования составили общенаучные методы (анализ, синтез, сравнение) и частнонаучные методы (сравнительно-правовой, формально-юридический, историко-правовой). Эмпирическую базу исследования образуют нормативные правовые акты Республики Беларусь, статистические данные, материалы судебной практики.

Электронное правосудие как правовой феномен представляет собой комплексную систему организации и осуществления судебной деятельности с использованием цифровых технологий. В научной литературе выделяются различные подходы к пониманию сущности электронного правосудия. По мнению российского исследователя С. В. Петрова, электронное правосудие следует рассматривать как "совокупность организационных и технических мер, обеспечивающих возможность осуществления правосудия с использованием информационно-коммуникационных технологий" [1. С. 45].

В белорусской правовой доктрине электронное правосудие понимается как форма организации судебной деятельности, основанная на использовании цифровых технологий для обеспечения доступа к правосудию, повышения эффективности судебного процесса и качества отправления правосудия. Особенностью белорусского подхода является поэтапность внедрения цифровых технологий, сочетание традиционных и электронных форм судопроизводства.

Теоретической основой развития электронного правосудия в Беларуси стали работы таких ученых, как А. В. Барков, Л. А. Абрамчик, Н. В. Сидоренко, которые исследовали различные аспекты цифровизации судебной деятельности.

В своих работах они подчеркивают необходимость сохранения фундаментальных принципов правосудия при внедрении цифровых технологий [2. С. 78–79].

Международный опыт показывает, что эффективное функционирование электронного правосудия требует создания адекватной нормативно-правовой базы, развития цифровой инфраструктуры, обеспечения кибербезопасности и подготовки квалифицированных кадров. Европейская комиссия в своем докладе "Цифровое правосудие в Европе" отмечает, что успешная цифровая трансформация судебной системы возможна только при комплексном подходе, включающем технологические, правовые и организационные аспекты [3. Р. 15].

Историю развития электронного правосудия в Республике Беларусь можно разделить на три основных этапа. Первый этап (2000–2010 гг.) характеризовался созданием предпосылок для цифровизации судебной системы. В этот период были приняты основополагающие нормативные акты, такие как Закон "Об электронном документе и электронной цифровой подписи" (2009 г.), который заложил правовые основы для использования электронных документов в судопроизводстве [4].

На этом этапе началось создание автоматизированных систем в судах, прежде всего в хозяйственных судах, которые традиционно были более восприимчивы к технологическим инновациям. Основное внимание уделялось внутренней автоматизации судебной деятельности, а не взаимодействию с внешними пользователями.

Второй этап (2011–2018 гг.) ознаменовался активным развитием цифровой инфраструктуры судебной системы. В 2011 году начал функционировать официальный сайт судов общей юрисдикции, что стало важным шагом в обеспечении открытости судебной системы. В 2014 году была launched система "Электронное обращение" в хозяйственных судах, позволившая осуществлять подачу документов в электронном виде [5. С. 112].

Ключевым событием этого этапа стало принятие в 2016 году Концепции развития цифровой экономики, которая определила стратегические направления цифровизации всех сфер общественной жизни, включая правосудие. В рамках этой концепции началась работа по созданию комплексной системы электронного правосудия.

Третий этап (2019 г. – настоящее время) характеризуется комплексной цифровой трансформацией судебной системы. В 2019 году была launched система "Электронный суд", которая стала единой платформой для электронного взаимодействия участников судебного процесса с судами всех уровней. В этот период также началось активное использование видеоконференц-связи для проведения судебных заседаний, что особенно актуально в условиях пандемии COVID-19 [6. С. 34].

Особенностью современного этапа является ориентация на создание целостной экосистемы электронного правосудия, интегрированной с другими государственными информационными системами. Это позволяет обеспечить сквозное взаимодействие между различными органами государственной власти и участниками судебного процесса.

Правовую основу электронного правосудия в Республике Беларусь составляют нормативные правовые акты различного уровня. Конституционный уровень представлен Конституцией Республики Беларусь, которая гарантирует право на судебную защиту (статья 60) и доступ к правосудию (статья 62). Эти конституционные положения создают основу для развития электронного правосудия как средства обеспечения доступности правосудия.

Законодательный уровень включает codes и законы, регулирующие различные аспекты электронного правосудия. Гражданский процессуальный кодекс (статья 111¹) и Хозяйственный процессуальный кодекс (статья 107) закрепляют возможность подачи процессуальных документов в электронном виде [7; 8]. Закон "Об электронном документе и электронной цифровой подписи" устанавливает правовые условия использования электронных документов в судопроизводстве.

Важную роль играют подзаконные нормативные правовые акты. Постановление Совета Министров от 29 июня 2018 г. № 504 утвердило Положение о порядке подачи в суд процессуальных документов в электронном виде, которое детально регулирует процедуру электронного документооборота [9]. Инструкции и приказы Председателя Верховного Суда регулируют технические аспекты использования цифровых технологий в судебной деятельности.

Особого внимания заслуживает Декрет № 8 "О развитии цифровой экономики" (2017 г.), который создал благоприятные условия для развития цифровых технологий, включая blockchain и smart contracts, что имеет потенциальное значение для дальнейшего развития электронного правосудия [10].

Сравнительный анализ белорусского законодательства с нормами Европейского союза показывает, что Беларусь в целом следует общеевропейским тенденциям в регулировании электронного правосудия. Однако отмечается более осторожный подход к внедрению таких технологий, как искусственный интеллект в судебной деятельности.

Современная система электронного правосудия в Республике Беларусь представляет собой многоуровневую структуру, основанную на платформе "Электронный суд". Анализ статистики использования системы показывает устойчивый рост числа пользователей и подаваемых документов. По данным Верховного Суда, в 2022 году через систему было подано более 150 тысяч процессуальных документов, что на 25% больше, чем в предыдущем году [11].

Функциональные возможности системы включают:

- Подачу исковых заявлений, жалоб, ходатайств.
- Оплату государственной пошлины.
- Направление документов в рамках досудебного сотрудничества.
- Получение информации о движении дела.
- Участие в судебных заседаниях посредством видеоконференц-связи

Практика применения показывает, что наиболее востребованными являются функции подачи процессуальных документов и получения информации о движении дела. Использование видеоконференц-связи первоначально было ограниченным, но значительно увеличилось в период пандемии COVID-19.

Отраслевые особенности применения электронного правосудия проявляются в различной интенсивности использования цифровых технологий в разных видах судопроизводства. Хозяйственные суды демонстрируют наибольшую активность в использовании электронных сервисов, что объясняется более высоким уровнем цифровой грамотности участников хозяйственного процесса и наличием экономических стимулов для использования электронных форм взаимодействия.

В уголовном судопроизводстве использование электронных технологий ограничено соображениями безопасности и защиты прав участников процесса. Тем не менее, и здесь отмечается постепенное внедрение цифровых solutions, особенно в аспекте электронного документооборота между судами и правоохранительными органами.

Анализ судебной практики показывает, что суды в целом положительно относятся к использованию электронных документов, однако отмечаются случаи излишнего формализма при оценке соответствия электронных документов установленным требованиям.

Сравнительный анализ развития электронного правосудия в Беларуси и других странах позволяет выявить как общие тенденции, так и национальные особенности. Европейский опыт характеризуется высоким уровнем гармонизации законодательства благодаря Директиве 2016/2102/EU о доступности веб-сайтов и мобильных приложений государственных органов, которая устанавливает единые стандарты доступности электронных судебных сервисов [12].

В Германии система электронного правосудия (EGVP – Elektronisches Gerichts- und Verwaltungspostfach) отличается высоким уровнем безопасности и интеграции с другими государственными системами. Немецкий опыт интересен тем, что система изначально разрабатывалась как общегосударственная платформа для электронного взаимодействия с государственными органами, а не только с судами [13. Р. 89].

Эстонская модель признается одной из наиболее продвинутых в мире. Эстония реализовала сквозную цифровизацию судебного процесса, включая возможность полностью электронного судопроизводства. Особенностью эстонской системы является использование blockchain технологии для обеспечения безопасности и неизменности судебных документов [14. Р. 67].

Российская Федерация демонстрирует опыт, наиболее близкий к белорусскому. Система "Электронное правосудие" в России включает функционал, аналогичный белорусской системе, но отличается более широким использованием искусственного интеллекта для анализа судебной практики и прогнозирования судебных решений [15. С. 56].

Сравнительный анализ показывает, что Беларусь находится на среднем уровне развития электронного правосудия по сравнению с европейскими странами. Основными направлениями для совершенствования являются повышение удобства пользования системой, расширение функциональности и усиление интеграции с другими государственными информационными системами.

Анализ современного состояния электронного правосудия в Республике Беларусь позволяет выявить ряд **системных проблем**:

1. Технологические проблемы: Недостаточная пропускная способность каналов связи в регионах, устаревшее компьютерное оборудование в некоторых судах, проблемы совместимости с различными операционными системами и браузерами.

2. Организационные проблемы: Сложность процедуры регистрации и авторизации в системе, необходимость получения электронной цифровой подписи, недостаточная координация между различными государственными органами.

3. Правовые проблемы: Неопределенность правового статуса некоторых электронных документов, пробелы в регулировании cross-border электронного правосудия, отсутствие четких процедур использования искусственного интеллекта в судебной деятельности.

4. Кадровые проблемы: Недостаточная цифровая грамотность части судебного корпуса и участников процесса, сопротивление изменениям со стороны некоторых представителей юридического сообщества.

5. Финансовые проблемы: Ограниченное финансирование разработки и внедрения новых digital solutions, особенно в условиях экономических санкций.

Перспективные направления развития электронного правосудия в Республике Беларусь включают:

1. Развитие искусственного интеллекта: Внедрение AI-систем для анализа судебной практики, прогнозирования судебных решений, проверки процессуальных документов на соответствие формальным требованиям. Мировой опыт показывает, что использование AI может significantly повысить эффективность судебной системы [16. Р. 123].

2. Внедрение blockchain технологий: Использование distributed ledger technology для обеспечения неизменности и прозрачности судебных решений, создания системы электронного исполнительного производства.

3. Развитие мобильных решений: Создание мобильных приложений для участников судебного процесса, что особенно актуально в условиях роста мобильного интернет-трафика.

4. Международное сотрудничество: Участие в международных проектах по развитию электронного правосудия, harmonization законодательства с нормами Евразийского экономического союза.

5. Совершенствование пользовательского опыта: Упрощение процедур регистрации и работы с системой, создание многоязычного интерфейса, разработка системы онлайн-поддержки пользователей.

Реализация этих направлений требует разработки комплексной программы развития электронного правосудия на 2024–2030 годы, включающей technological, legal, organizational и educational аспекты.

Проведенное исследование позволяет сделать вывод о значительном прогрессе в развитии электронного правосудия в Республике Беларусь. Создана современная digital платформа, сформирована необходимая нормативно-правовая база, накоплен substantial опыт использования цифровых технологий в судопроизводстве.

Однако сохраняются серьезные challenges, связанные с technological, organizational и legal аспектами функционирования системы электронного правосудия. Для дальнейшего успешного развития необходимо реализовать комплекс мер, включающий:

- Модернизацию IT-инфраструктуры судов.
- Упрощение процедур доступа к системе.
- Развитие цифровой грамотности участников судебного процесса.
- Совершенствование законодательства.
- Развитие международного сотрудничества.

Особое внимание следует уделить внедрению перспективных технологий, таких как искусственный интеллект и blockchain, при обеспечении соблюдения фундаментальных принципов правосудия и защиты прав участников процесса.

Перспективы развития электронного правосудия в Республике Беларусь связаны с созданием целостной экосистемы цифрового правосудия, интегрированной в общегосударственную digital платформу и соответствующей международным стандартам в этой области.

Список литературы

1. Петров С. В. Электронное правосудие: теория и практика. М.: Норма, 2021. 256 с.
2. Барков А. В., Абрамчик Л. А. Цифровая трансформация правосудия: вызовы и возможности // Вестник Верховного Суда. 2022. № 3. С. 75–82.
3. Digital Justice in Europe: Challenges and Opportunities // European Commission. 2022. 45 p.
4. Об электронном документе и электронной цифровой подписи: Закон Респ. Беларусь от 28 дек. 2009 г. № 113–З // Нац. реестр правовых актов Респ. Беларусь. 2010. № 15. 2/1661.
5. Сидоренко Н. В. Развитие электронного правосудия в Республике Беларусь: этапы и перспективы // Юстиция Беларуси. 2021. № 4. С. 110–115.
6. Гражданский процессуальный кодекс Республики Беларусь: принят Палатой представителей 11 дек. 1998 г.: одобр. Советом Респ. 18 дек. 1998 г. // Нац. реестр правовых актов Респ. Беларусь. 1999. № 18–19. 2/13.
7. Хозяйственный процессуальный кодекс Республики Беларусь: принят Палатой представителей 11 нояб. 1998 г.: одобр. Советом Респ. 26 нояб. 1998 г. // Нац. реестр правовых актов Респ. Беларусь. 1999. № 7–9. 2/5.
8. Об утверждении Положения о порядке подачи в суд процессуальных документов в электронном виде: постановление Совета Министров Респ. Беларусь от 29 июня 2018 г. № 504 // Нац. правовой Интернет-портал Респ. Беларусь. 2018. 5/45601.
9. О развитии цифровой экономики: Декрет Президента Респ. Беларусь от 21 дек. 2017 г. № 8 // Нац. правовой Интернет-портал Респ. Беларусь. 2017. 1/17590.
10. Статистический отчет о деятельности судов общей юрисдикции за 2022 год // Верховный Суд Республики Беларусь. 2023. 35 с.

11. Directive (EU) 2016/2102 of the European Parliament and of the Council on the accessibility of the websites and mobile applications of public sector bodies // Official Journal of the European Union. 2016. L 327/1.
12. Müller, K. Digital Justice: German Experience and Perspectives / K. Müller // European Journal of Legal Reform. 2021. Vol. 23. No. 2. P. 85–102.
13. Laas K. E-Justice in Estonia: From Concept to Reality // Baltic Journal of Digital Governance. 2022. No. 1. P. 64–78.
14. Иванов А. А. Искусственный интеллект в правосудии: российский опыт // Закон. 2023. № 2. С. 54–67.
15. Smith, J. Artificial Intelligence in Judicial Systems: Global Perspectives / J. Smith, R. Johnson // Stanford Journal of Computational Law. 2022. Vol. 5. No. 1. P. 115–140.

В. В. Савкина,

студент,

Белорусский государственный университет транспорта,

Е. В. Тужикова,

студент,

Белорусский государственный университет транспорта

Цифровой контроль и родительский надзор

Аннотация. В условиях стремительной цифровизации общества особую актуальность приобретает вопрос обеспечения информационной безопасности несовершеннолетних. Статья посвящена анализу рисков, с которыми сталкиваются дети в онлайн-среде, включая кибербуллинг, утечку персональных данных и вовлечение в противоправную деятельность через интернет-каналы. Особое внимание уделено проблеме наркопреступлений, совершаемых с использованием цифровых платформ, а также механизмам вербовки несовершеннолетних через социальные сети и мессенджеры. Рассматриваются возможности родительского контроля как инструмента цифрового воспитания, направленного на формирование безопасной и поддерживающей среды. Описаны ключевые функции систем контроля: фильтрация контента, ограничение экранного времени, мониторинг активности и геолокация. Приведен обзор популярных программных решений, таких как Google Family Link, Kaspersky Safe Kids, Kids Security и Microsoft Family Safety, с указанием их функциональных особенностей и применимости в семейной практике.

Ключевые слова: цифровая безопасность детей; родительский контроль; киберугрозы; наркопреступления в интернете; геолокация; фильтрация контента; цифровое воспитание; Kaspersky Safe Kids; Google Family Link; Kids Security; Microsoft Family Safety; цифровая среда; несовершеннолетние; интернет-риски; Telegram; Darknet; VPN; цифровая социализация

V. V. Savkina,

student,

Belarusian State University of Transport,

E. V. Tuzhikova,

student,

Belarusian State University of Transport

Digital control and parental supervision

Abstract. In the context of rapid digitalization of society, the issue of ensuring information security for minors has become increasingly urgent. This article analyzes the risks children face in the online environment, including cyberbullying, personal data leaks, and involvement in illegal activities through internet channels. Special at-

tention is given to drug-related crimes committed via digital platforms, as well as recruitment mechanisms targeting minors through social networks and messaging apps. The article explores the potential of parental control as a tool of digital upbringing aimed at creating a safe and supportive environment. Key functions of control systems are described, such as content filtering, screen time limitation, activity monitoring, and geolocation tracking. An overview of popular software solutions is provided, including Google Family Link, Kaspersky Safe Kids, Kids Security, and Microsoft Family Safety, with details on their features and applicability in family settings.

Keywords: child digital safety; parental control; cyber threats; online drug crimes; geolocation; content filtering; digital upbringing; Kaspersky Safe Kids; Google Family Link; Kids Security; Microsoft Family Safety; digital environment; minors; internet risks; Telegram; Darknet; VPN; digital socialization

Введение. В современном обществе Интернет стал неотъемлемой частью повседневной жизни, охватывая все возрастные группы. Особенно это заметно среди детей: для них доступ к сети зачастую воспринимается как базовая потребность. Лишение мобильного устройства с выходом в Интернет воспринимается как серьезное ограничение. Согласно актуальным данным, более половины детей в возрасте от 3 до 6 лет регулярно используют смартфоны. Цифровые устройства – смартфоны, планшеты, компьютеры и смарт-телевизоры – активно применяются в образовательных целях, для общения и досуга [4. С. 15].

Однако наряду с очевидными преимуществами цифровой среды, такими как доступ к информации, расширение коммуникационных возможностей и разнообразие контента, существует и обратная сторона. Цифровое пространство несет в себе серьезные риски, особенно для несовершеннолетних пользователей. Среди наиболее актуальных угроз – кибербуллинг, доступ к нежелательной информации, а также утечка персональных данных. Статистика свидетельствует о ежегодном росте числа инцидентов, связанных с цифровой безопасностью детей [3, С. 48; 5].

Интернет, с одной стороны, предоставляет уникальные возможности для саморазвития и обучения, но с другой – становится каналом распространения киберпреступлений. Особую тревогу вызывают противоправные действия, связанные с незаконным оборотом наркотических средств, которые все чаще перемещаются в онлайн-пространство.

Современное цифровое пространство, охватывающее безграничные возможности Интернета, все чаще становится не только средой для общения и получения информации, но и платформой для противоправной деятельности, включая распространение наркотических средств. Интернет активно используется не только для совершения наркопреступлений, но и как инструмент вовлечения граждан в незаконный и опасный бизнес.

Рекламные предложения от наркомаркетов зачастую оформлены крайне привлекательно: обещания высокой оплаты простой работы, отсутствие физических усилий, гарантии безопасности и легальности, а также система бонусов – например, денежное вознаграждение за привлечение новых участников. Все это создает иллюзию доступного и безнаказанного заработка.

Особую тревогу вызывает тот факт, что на подобные предложения чаще всего откликаются несовершеннолетние. Осознавая характер предлагаемых действий и возможные последствия, они все же идут на осознанный риск ради быстрой и легкой прибыли. В результате подростки становятся так называемыми «закладчиками» – участниками организованных групп, занимающихся распространением наркотиков через интернет-магазины. Такие действия квалифицируются по части 4 статьи 328 Уголовного кодекса Республики Беларусь и влекут за собой серьезное наказание – от 10 до 20 лет лишения свободы [7; 13. С. 50].

Причина вовлечения проста: каждый считает, что его не поймают. Однако реальность показывает обратное. Некоторые действительно успевают получить оплату и даже вовлечь друзей, но многие задерживаются уже в первый день «работы».

Наиболее распространенные каналы вербовки – социальные сети («ВКонтакте», «Одноклассники») и массовые рассылки в мессенджерах. После проявления интереса общение переводится в Telegram – мессенджер, популярный за счет своей анонимности и слабой модерации [6. С. 115; 14. С. 5].

В связи с этим родителям следует проявлять повышенное внимание к цифровой активности своих детей: отслеживать круг общения, интересы в поисковых системах и установленные приложения. Программное обеспечение, используемое наркосбытчиками, как правило, имеет специфические функции и не применяется обычными пользователями.

Особую настороженность должны вызывать:

- доступ к Даркнету – скрытому сегменту Интернета, недоступному для поисковых систем и случайных пользователей;
- использование VPN-сервисов (например, MyVPN.Host, ExpressVPN, NordVPN), позволяющих обходить блокировки и скрывать цифровой след;
- установка приложений, накладывающих GPS-координаты на фотографии (например, NoteCam), что характерно для схем распространения наркотиков;
- попытки регистрации на криптовалютных биржах, использование электронных кошельков, неизвестных сим-карт и банковских карт.

Появление подобных признаков может свидетельствовать о вовлечении ребенка в противоправную деятельность. Важно своевременно реагировать, вести открытый диалог и предпринимать меры по обеспечению цифровой безопасности несовершеннолетних.

Родительский контроль в цифровой среде – это не просто технический инструмент, а ключевой элемент воспитания в условиях стремительного развития технологий. Его цель заключается не в ограничении свободы ребенка, а в создании защищенного и поддерживающего цифрового пространства, способствующего формированию навыков осознанного и безопасного взаимодействия с информационными ресурсами.

В условиях, когда дети начинают пользоваться цифровыми устройствами с раннего возраста, все больше родителей осознают необходимость регулирования их активности в сети. Отсутствие контроля может привести к ряду негативных последствий: нарушению режима сна, снижению концентрации внимания,

развитию зависимости от гаджетов. Кроме того, существует риск столкновения с нежелательным контентом, попытками доступа к запрещенным веществам, услугам или программному обеспечению.

Согласно данным исследования, проведенного «Лабораторией Касперского», 65% родителей ограничивают время, проводимое детьми за экранами, и вводят правила использования цифровых устройств [5].

Комплекс мер родительского контроля позволяет решать сразу несколько важных задач:

- обеспечение цифровой безопасности ребенка;
- регулирование времени взаимодействия с гаджетами;
- развитие навыков ответственного поведения в сети;
- поддержание доверительных отношений между родителями и детьми в условиях цифровизации повседневной жизни.

Основные функции систем родительского контроля:

1. Контентная фильтрация. Позволяет ограничить доступ к онлайн-ресурсам, содержащим нежелательные материалы, включая сцены жестокости, порнографию, пропаганду наркотических веществ, алкоголь и табак, азартные игры, а также экстремистский или манипулятивный контент.

2. Регулирование времени использования устройств. Обеспечивает контроль над продолжительностью взаимодействия ребенка с цифровыми технологиями. Родители могут устанавливать дневные лимиты, задавать расписание активности (например, запрет на игры в ночное время), а также ограничивать доступ к отдельным приложениям – к примеру, ограничить использование TikTok до 30 минут в сутки.

3. Анализ цифровой активности. Функция мониторинга позволяет отслеживать посещаемые веб-сайты, список установленных и используемых программ, поисковые запросы в популярных сервисах (Google, YouTube), а также – в рамках допустимого – переписку в мессенджерах.

4. Определение местоположения. Система геолокации отображает текущее положение устройства ребенка на карте, позволяет задать «безопасные зоны» (например, школа или дом) и получать уведомления при выходе за их пределы.

На рынке представлены как встроенные, так и сторонние решения. Выбор зависит от целей и используемых платформ. Если необходимо контролировать устройства на разных операционных системах (Windows, Android, iOS), целесообразно использовать универсальные приложения, такие как Kaspersky Safe Kids. В случаях, когда контроль требуется только на одной платформе, можно воспользоваться встроенными средствами – например, Google Family Link для Android или Apple Screen Time для iOS.

В рамках обеспечения цифровой безопасности детей существует ряд программных решений, позволяющих родителям контролировать активность ребенка в сети, управлять временем использования устройств и отслеживать местоположение. Ниже представлены наиболее востребованные приложения, отличающиеся функциональностью и доступностью.

– Google Family Link Официальное приложение от Google, предназначенное для контроля устройств на базе Android. Родители могут отслеживать, сколько времени ребенок проводит за экраном, какие приложения используются и какие файлы загружаются из Google Play. Управление осуществляется как с мобильного устройства, так и через веб-интерфейс. Среди функций – установка временных лимитов, блокировка отдельных приложений, настройка фильтрации контента в браузере Chrome и активация безопасного поиска. Также доступна геолокация, отображение заряда устройства и возможность подачи звукового сигнала. Для детей младше 13 лет автоматически ограничивается доступ к взрослым сервисам. Приложение полностью бесплатное и не содержит рекламы [8. С. 45–60].

– Kaspersky Safe Kids Многофункциональное решение от «Лаборатории Касперского», ориентированное на обеспечение баланса между контролем и комфортом. Поддерживает широкий спектр платформ: Android, iOS, Windows и macOS. Приложение позволяет отслеживать поисковые запросы, посещенные сайты, экранное время, а также блокировать нежелательные программы. Реализована фильтрация контента, контроль YouTube, настройка расписания сна и учебы, а также уведомления о нарушениях. Геолокация работает с настройкой безопасных зон и оповещениями. Базовые функции доступны бесплатно. Расширенные возможности – включая мониторинг YouTube и гибкие настройки – предоставляются по подписке.

– Kids Security Простое и интуитивно понятное приложение, ориентированное на отслеживание местоположения и активности ребенка в реальном времени. Поддерживает Android и iOS. Сервис отображает перемещения на карте, позволяет задать «геозабор» и получать уведомления о выходе за его пределы. В статистике отражается активность по категориям: игры, соцсети, браузеры. Родители могут блокировать приложения и устанавливать периоды «тишины» – например, во время занятий. Дополнительные функции включают тревожную кнопку, прослушивание окружения (на Android) и возможность подачи громкого сигнала. Бесплатная версия включает базовые функции, а премиум-подписка открывает расширенные отчеты и историю GPS [10. С.120–145].

– Microsoft Family Safety Решение от Microsoft, интегрированное в экосистему Windows и Xbox. Предназначено для управления цифровыми привычками всей семьи. Приложение позволяет задавать лимиты экранного времени, ограничивать доступ к приложениям и играм, устанавливать возрастные рейтинги и включать фильтрацию сайтов. Родители получают уведомления о запросах ребенка и могут оперативно реагировать. На платформах Windows и Xbox доступны расширенные настройки, включая контроль чата и списка друзей. На iOS функциональность ограничена – фильтрация работает только в браузере Microsoft Edge. Большинство функций доступны бесплатно. С ноября 2024 года геолокация и оповещения, ранее входившие в пакет Office 365, больше не поддерживаются, что снижает актуальность платной подписки.

Родительский контроль – это не столько про технологии, сколько про осознанное участие в воспитании ребенка в цифровом мире. Его задача – не заме-

нить живое общение, а стать его продолжением, помогая формировать у детей устойчивые ориентиры и навыки безопасного поведения в сети.

В условиях стремительного развития цифровой среды важно не ограничивать, а сопровождать ребенка, обучать его разумному использованию технологий. Эффективный контроль строится не на запретах, а на доверии, уважении и личном примере – именно это создает основу для успешной адаптации ребенка к цифровой реальности.

Обеспечение онлайн-безопасности детей – это совместная ответственность родителей, педагогов и разработчиков образовательных платформ. Важно вести открытые разговоры о рисках, с которыми ребенок может столкнуться в интернете, включая современные схемы обмана и манипуляции.

Проявляйте интерес к цифровым привычкам ребенка – узнавайте, какими приложениями он пользуется, какие сайты посещает. Но не превращайте это в тотальный контроль. Главная цель – не запугать, а научить ребенка критически оценивать информацию, принимать взвешенные решения и вести себя в сети осознанно и безопасно.

Список литературы

1. Об утверждении Правил определения детей, находящихся в социально опасном положении: постановление Министерства образования Респ. Беларусь от 25 июля 2022 г. № 259 // Нац. центр правовой информ. Респ. Беларусь. URL: <http://pravo.by/document/?guid=12551&p0=W22223059> (дата обращения: 03.09.2024).

2. О мерах по противодействию незаконному обороту наркотиков: Указ Президента Респ. Беларусь от 28 декабря 2021 г. № 517 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. Минск, 2024. URL: <http://pravo.by/document/?guid=12551&p0=P32100517> (дата обращения: 03.09.2024).

3. Гиренко Ю. В. Кибербуллинг в подростковой среде: особенности и меры профилактики // Психология и школа. 2021. № 2. С. 45–58.

4. Дети в цифровом мире: статистика и тенденции. Аналитический отчет по результатам исследования / ЮНИСЕФ, 2022. URL: <https://www.unicef.org/esa/ru/reports/дети-в-цифровом-мире> (дата обращения: 02.09.2024).

5. Касперский Е. И. Тренды цифровой безопасности 2023: угрозы для частных пользователей / Е. И. Касперский // Лаборатория Касперского. 2023. 15 февр. URL: <https://www.kaspersky.ru/blog/top-cyberthreats-2023-private-users/48815/> (дата обращения: 01.09.2024).

6. Ковалева О. А. Наркопреступность в интернет-пространстве: новые вызовы и стратегии противодействия // Вестник Академии МВД Республики Беларусь. 2022. № 1 (47). С. 112–119.

7. Отчет о наркоситуации в Республике Беларусь по итогам 2023 года [Электронный ресурс] / МВД Респ. Беларусь, ГУНиПТЛК. Минск, 2024. URL: <https://mvd.gov.by/ru/main.aspx?guid=10381> (дата обращения: 01.09.2024).

8. Родительский контроль в цифровую эпоху: как защитить ребенка онлайн. Исследование [Электронный ресурс] / РОЦИТ, 2022. URL: <https://rocit.ru/research/digital-parenting-2022> (дата обращения: 01.09.2024).

9. Смирнова А. А., Иванов П. В. Психологические аспекты вовлечения несовершеннолетних в наркопреступность через социальные сети // Вопросы психологии. 2023. № 4. С. 78–90.

10. Соколова Е. В. Цифровая гигиена: руководство для родителей по обеспечению безопасности детей в сети / Е. В. Соколова. Минск: Новое знание, 2022. 186 с.

Д. В. Усиков,

курсант,

Московская академия Следственного комитета Российской Федерации
имени А.Я. Сухарева

Виртуальная личность как слеодообразующий объект в системе цифровой криминалистики

Аннотация. Настоящая работа имеет своей целью сформулировать категорию виртуальной личности в цифровой криминалистике, описать ее природу, выявить сущность. На основе исследования природы цифровых следов и практики их применения выдвинута теоретическая концепция виртуальной личности, раскрыты ее составляющие, аспекты реального применения и значение в процессе образования цифровых следов. Акцент сделан на конкретных примерах проявления виртуальной личности. Продемонстрирована актуальность практического применения данной категории в целях раскрытия и расследования преступлений, правильной интерпретации цифровых следов и их использования при доказывании. На основе сделанных выводов предложена новая классификация цифровых следов.

Ключевые слова: виртуальная личность, цифровые следы, цифровая криминалистика, атрибуция, идентификация, учетная запись, пользователь

D. V. Usikov,

Cadet,

Moscow Academy of the Investigative Committee of the Russian Federation
named after A.Y. Sukharev

Virtual persona as evidence-leaving object in digital forensics

Abstract. The present article sets its goal to formulate a concept of virtual persona in application to digital forensics, portray ones nature, reveal the essence of it. On the basis of analysis of digital evidence and its implementation on practice a theoretical concept of virtual persona is proposed. Constituents of this concept, aspects of real use and significance in the process of forming digital evidence was demonstrated, the accent put on particular examples of expression of virtual persona. The paper demonstrates importance of practical implementation of this concept in everyday criminal investigations, proper interpretation of digital evidence and its use for argument. The new classification of digital evidence proposed based on present research.

Keywords: virtual persona, digital evidence, digital forensics, attribution, identification, account, user

Введение. Категория следа является одной из центральных в криминалистике. Под следом в широком смысле понимаются любые материальные последствия преступления, изменения объекта или вещной обстановки. След, согласно прочно устоявшейся в отечественной криминалистике «теории отраже-

ния», является отражением действий – необходимым изменением в окружающей среде, вызванным неким преступным актом [6. С. 195]. Значение следов для криминалистики в целом и, что очень важно, для настоящей работы, состоит главным образом в том, что они предоставляют возможность путем индуктивных умозаключений от знания о последствиях преступления перейти к знанию о событии преступления, его обстоятельствах и лицах, его совершивших [5. С. 29]. Следы принято делить на две большие группы: материальные – следы, запечатленные в объектах материального мира, доступные к непосредственному восприятию (следы-отображения, следы-предметы, следы-вещества); идеальные – следы, запечатленные в памяти человека, и доступные восприятию через психику этого человека (посредством проведения допроса, предъявления для опознания и т. д.).

Основная часть. С развитием информационных технологий и их ускоренным повсеместным включением в жизнь человека, криминальная активность распространилась на новую сферу, появились следы, которые сильно отличались от уже известных и привычных видов следов – цифровые следы. В настоящее время под цифровыми (или электронными, виртуальными) следами в криминалистике принято понимать любую криминалистически значимую компьютерную информацию, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [17. С. 103]. Цифровые следы относят к материальным невидимым следам в силу их соответствующих качеств. К свойствам цифровых следов принято относить их опосредованность через электронный носитель информации, возможность дистанционного и одновременного доступа к этой информации, возможность неограниченного копирования информации без ущерба для ее содержания [12 с. 13]. Предполагается, что цифровые следы служат источником информации об обстоятельствах подготовки, совершения и сокрытия преступлений, связанных с использованием компьютеров. Цифровая (или электронная) криминалистика в настоящее время активно развивается как самостоятельная теория, включающая в себя различные разделы [19].

Следует заметить, что за рубежом, в отрасли криминалистики, занимающейся исследованием компьютерной информации в целях раскрытия и расследования преступлений, закрепившейся там под названием *digital forensics*, отдельно оговаривается, что доступные исследованию цифровые следы (*digital evidence*) позволяют формулировать лишь ограниченный круг гипотез о цифровых событиях и состояниях [20]. Установление лица, совершившего некоторые действия, повлекшие образование цифровых следов, его «привязка» к этим событиям, выделяются и изучаются как отдельный процесс в цифровой криминалистике – атрибуция (*attribution*). Так, отдельно, в качестве примера, оговаривается, что запись (*log*) о совершении учетной записью (*account*) определенных действий сама по себе не говорит о совершении этих действий владельцем этой учетной записи, то есть каким-либо человеком [21. С. 365].

Действительно, если следовоспринимающий объект для цифровых следов определить можно точно – это компьютерная информация на материальном носителе в каком-либо из множества существующих или могущих существовать

видов; то сказать с уверенностью, что слеодообразующим объектом является непосредственно само лицо, пользователь этой информации (*user*) нельзя. Компьютерная информация, которая исследуется как цифровой след, на практике как правило не содержат никаких сведений о самом человеке, лишь о различных идентификаторах, которые взаимодействовали в рамках информационных систем: учетных записях на устройстве и в сети «Интернет», IP-адресах, MAC-адресах, абонентских номерах, IMEI и прочем. Вообще сам термин «пользователь» в информатике описывает человека очень ограниченно, лишь в той его части, в какой он доступен для информационной системы – а доступен он посредством учетной записи. Пользователь существует до тех пор и в такой степени, в какой существует его воплощение в информационной системе и интересен он лишь в той части, в какой является носителем этого самого воплощения.

Недавнее бурное развитие и скорый упадок метавселенных – постоянно действующих виртуальных пространств, в котором люди могут взаимодействовать с окружающей средой и другими пользователями через свои аватары (подробные цифровые воплощения) – ввело в обиход понятие, которым обозначалось воплощение человека в метавселенных, через которое он действовал в них как действовал бы в реальном мире – виртуальная личность [7]. Еще ранее понятие виртуальной личности или интернет-идентичности (*internet identity*) использовалось для обозначения создаваемой человеком в целях самопрезентации в сети «Интернет» сущности, обладающей совокупностью реально присущих или желаемых качеств, свойственных человеку. При этом такая сущность создавалась с расчетом на возможность восприятия ее другими пользователями. Виртуальная личность в различных исследованиях воспринималась как правило в части производимых различными ее проявлениями эффектов на психику человека и его личность. [8, 22].

Слово «виртуальный», произошедшее от латинского *virtualis* (возможный, воображаемый), в современном применении обозначает нечто относящееся к реальности компьютерной информации в противовес обычной, «живой» реальности. Личностью психология называет конкретного человека, взятого в системе его устойчивых социально обусловленных психологических характеристик, которые проявляются в общественных связях и отношениях, определяют его нравственные поступки и имеют существенное значение для него самого и окружающих. Личность определяется именно в своей способности взаимодействовать с окружающим миром, оказывая на него воздействие и воспринимая это воздействие извне, то есть ее конституируют внешние, действующие свойства, их многогранная совокупность [9. С. 401]. В категории «личность» в первую очередь важна внешняя составляющая, проявляемое вовне и воспринимаемое окружающими поведение, своего рода «личина», а не сам человек, который здесь лишь носитель этой личности.

Понятие «виртуальная личность», толкуемое не в строгих рамках контекста метавселенных, а в общем смысле, исходя из его природы, представляющей собой некоторую внешнюю сущность, действующую, то есть создающую последствия, в информационной системе от лица человека (проявляющуюся вовне – в информационную систему – и воспринимаемую этой системой как таковой),

по сути своей охватывает собой учетные записи. Именно посредством них человек взаимодействует с компьютерной информацией: действует от некоторого уникального имени (идентификатора), пройдя процесс аутентификации, и получает или не получает доступ к некоторой части информации, пройдя авторизацию. Учетная запись определяется государственным стандартом в области защиты информации как логический объект (т. е. объект, рассматриваемый в аспекте определения алгоритмом или программой безотносительно к реализации с помощью технических средств [2]), существующий в пределах одной или нескольких информационных систем и представляющий субъект доступа в ее (их) пределах [3]. В данном определении отражается два ключевых свойства учетной записи: ее принадлежность к *виртуальному*, то есть к миру компьютерной информации; и ее *субъектность*.

Причем субъектность здесь, безусловно, вторична – человек действует с компьютерной информацией через учетную запись, действует самостоятельно и в своих целях, но вот последствия этих действий, помимо тех, что человек намеревался получить для себя, остаются в информационной системе и являются последствиями, принадлежащими именно учетной записи. Это записи во всевозможных журналах событий (от лог-файлов до истории браузера), изменение состояния и содержания учетной записи (обновление страницы в социальной сети) и прочее. Учетные записи используются для доступа к информационным системам как на самих компьютерах, находящихся в распоряжении человека – учетные записи «гостя» и «администратора» на персональном компьютере; так и на компьютерах, доступ к информации на которых осуществляется удаленно, посредством сети «Интернет», проще – на различных сайтах, цифровых платформах, в социальных сетях и прочем. Учетная запись обязательно имеет некоторое индивидуальное, как правило цифровое обозначение, а доступ к ней самого человека защищен различными способами, самым распространенным из них является пароль. Это необходимо для защиты процесса доступа самого человека к информации посредством учетной записи, подразумевается, что лицо, использующее учетную запись достоверно определено, поскольку подтвердило свои права на использование этой учетной записи и, соответственно, доступ к информации введя пароль. Однако описанное является должным, а не сущим, и не обязательно соответствует действительности.

Сама учетная запись как правило также закрепляется за некоторой виртуальной сущностью. Это может быть еще одна учетная запись, в случаях, когда вход в информационную систему может осуществляться через одну стороннюю учетную запись – так происходит авторизация посредством сервисов экосистемы «Google» и «Яндекс». Также для создания учетной записи может использоваться абонентский номер или адрес электронной почты, которые также имеют виртуальную природу. Кроме того, взаимодействие с учетной записью в информационной системе в сети «Интернет», осуществляемое посредством телематической связи, происходит также через определенный идентификатор – IP-адрес. IP-адрес ведет с одной стороны к лицу, с которым был заключен договор на оказание таких услуг связи и который был при этом идентифицирован провайдером, а с другой к самому устройству, которым осуществлялось подключение –

это устройство идентифицируется по MAC-адресу. Стационарный MAC-адрес является уникальным и указывает на конкретное устройство, однако существующая в настоящее время в устройствах, имеющих выход в сеть «Интернет» функция рандомизации MAC-адреса позволяет автоматически изменять этот идентификатор на любой случайный, не принадлежащий этому устройству.

Именно по этой причине в пунктах коллективного доступа услуг телематической связи (публичные сети Wi-Fi) нормативными актами предписано осуществлять идентификацию пользователя и используемого им оконченного обслуживания (персонального компьютера или другого устройства), для чего провайдер запрашивает авторизацию через абонентский номер, или ЕСИА (Единая система идентификации и авторизации – портал государственных услуг), а подключение к сети возможно лишь через стационарный MAC-адрес [11]. Причем несмотря на строгость нормативных предписаний, такая идентификация является весьма условной и позволяет установить человека лишь с определенной степенью точности – ровно настолько, насколько пользуются доверием учетные записи ЕСИА и абонентский номер. Кроме того, расплывчато само понятие «пункт коллективного доступа». Например, в силу того, что обычным является возможность доступа к сетям Wi-Fi, располагающимся в жилище всех проживающих в нем лиц, при том, что стороной в договоре оказания услуг является только одно лицо, или даже лиц, находящихся вне этого жилища, но устройства которых способны уловить сигнал маршрутизатора. Юридическая фикция идентификации сторон договора оказания услуг связи не отвечает потребностям криминалистики и доказывания, не позволяет по умолчанию «привязать» человека к действиям в информационной системе. В целом, ни одно, даже самое строгое нормативное требование к идентификации пользователя в сети не гарантирует достоверности этой идентификации, в связи с чем, всегда существует потребность в установлении и доказывании причастности человека к действиям в информационной системе.

Каждый из описанных идентификаторов представляет собой так или иначе единую и индивидуальную сущность – уникальный набор символов, по предъявлении которого устройству дается возможность осуществлять действия с информацией – такие идентификаторы созданы именно с этой целью. Обособленно от них стоит цифровой отпечаток (*digital fingerprint*). Он представляет из себя «совокупность различных параметров устройства и установленного на нем программного обеспечения, считываемых информационной системой при осуществлении доступа в сети "Интернет", и вместе формирующих уникальный «портрет» устройства, позволяющий надежно его идентифицировать» [14]. Несмотря на два радикальных отличия от учетной записи: отпечаток представляет собой не единый идентификатор, а совокупность параметров; эта совокупность существует самостоятельно и заведомо не предназначена для предоставления информационной системе – «отпечаток» обладает важнейшими для цифровой криминалистики свойствами – он уникален и указывает на конкретное устройство. В силу таких причин, особенности конкретного полученного отпечатка будут зависеть от технологии, по которой сайт собирает информацию и считываемых так называемыми «счетчиками» параметров. Для получения цифровых

отпечатков сайты и их владельцы используют популярные сервисы «Google Analytics» и «Яндекс Метрика» [4]. Аналогичную функцию выполняют файлы "куки" (*cookie*), представляющие собой своеобразную метку – загружаемый на устройство пользователя файл, содержащий некоторую информацию и уникальный идентификатор, которые позволяют сайту в сети "Интернет" определить, осуществлялось ли некоторым устройством посещение данного сайта ранее и какие действия совершались, то есть идентифицировать его [10].

Описанные способы определить и зафиксировать некоторый уникальный случай доступа к компьютерной информации, путем авторизации или считывания набора параметров, представляют собой проявление виртуальной личности. Получается, что *виртуальная личность – это уникальный идентификатор в информационной системе, за которым закрепляется действие с компьютерной информацией*. Виртуальная личность по природе своей является цифровым (электронным) объектом, существующим и проявляющимся в пределах информационных систем. Причем виртуальная личность определяется здесь не в степени возможности ее восприятия человеком, а в возможности «восприятия» информационной системой, считывания ею и, соответственно, образования в этой информационной системе следов своей активности.

Виртуальная личность не обладает ни в какой степени субъектностью, самостоятельностью. Она не действует отдельно от человека и вне его намерений, но она является проводником его действий и источником изменений в информационных системах, с которыми человек взаимодействует через виртуальную личность. Кроме того, за такой виртуальной личностью нельзя усмотреть проявлений репрезентации личности человека вообще, в том смысле, в каком мы привыкли ее понимать в обыденной жизни. Это не полное воплощение, оно не содержит информацию о психике конкретного человека, его биологических и социально-психологических качествах. Это воплощение частичное, проявляющееся в определенной стороне и для определенной цели – действию с информацией. Отметим, что важнейшим для криминалистики свойством виртуальной личности является ее отчужденность от личности человека. Любым из существующих идентификаторов, созданных с целью определить конкретного пользователя в информационной системе может воспользоваться человек, для которого этот идентификатор изначально предназначен не был: войти в аккаунт в социальной сети или на устройстве (учетную запись), воспользоваться абонентским номером или мобильным телефоном (IMEI), компьютером (MAC-адрес), подключиться к сети "Интернет" через чужой Wi-Fi (IP-адрес) или же осуществить подмену такого идентификатора или его параметров намеренно (так называемые "виртуальные машины" – программное обеспечение предназначенное для предоставления информационным системам подложных данных об устройстве с целью сокрытия реального "отпечатка" устройства) или автоматически (упомянутая функция рандомизированного MAC-адреса используемая ныне по умолчанию на большинстве устройств, выходящих в сеть). При этом такие действия могут сами по себе носить криминальный характер, например, при взломе, т. е. несанкционированном входе в учетную запись, или же быть обыденностью, нормой – например, когда лица в одном жилище используют

общий Wi-Fi или когда различные лица пользуются одной учетной записью на устройстве с ведома ее создателя. Вообще понятие владельца учетной записи, идентификатора в таком случае значительно размывается – между реальным человеком и его виртуальной личностью всегда находится пропасть, которую в целях криминалистики необходимо преодолевать.

Становится ясной необходимость при исследовании цифровых следов и при использовании полученной из них информации в ходе доказывания помнить о необходимости осуществлять так называемую «привязку», то есть устанавливать и доказывать причастность, не только цифрового следа к его источнику, то есть в данном случае, виртуальной личности, но и, что очень важно, виртуальной личности как источника цифрового следа к человеку, ответственного за взаимодействие с информацией. Доказывание строится по логической цепочке: цифровой след – виртуальная личность – человек.

Заметим, что виртуальная личность в различных своих проявлениях не является единственным источником цифровых следов. Определение следа как цифрового отсылает к природе его носителя, следовоспринимающего объекта, но не к природе следообразующего объекта. Цифровой след сводится по сути своей к изменениям компьютерной информации, электромагнитным взаимодействиям, но это не значит, что он порождается исключительно такими же электромагнитными взаимодействиями. Вызвать эти изменения может как такой же цифровой, виртуальный, объект, действующий в той или иной степени самостоятельно, так и не цифровой объект, в том числе и сам человек. Безусловно, и в том, и в этом случае действует человек, именно его активность порождает изменения в окружающей обстановке, следы. Однако в одном случае эти следы несут в себе информацию о самом человеке – по ним можно восстановить информацию о человеке как о следообразующем объекте, а в другом след несет в себе информацию лишь о цифровом объекте – в том числе, виртуальной личности. Так, цифровые следы по степени участия человека в следообразовании можно разделить на две группы: *прямые* – вызванные воздействием непосредственно человека, и содержащие информацию о нем самом; *опосредованные* – вызванные воздействием человека через другой цифровой объект, содержащие информацию лишь об этом цифровом объекте. Существующая классификация цифровых следов по механизму их следообразования (на первичные и вторичные), хоть и имеет другое основание и является логически непротиворечивой, но содержательно не соответствует действительности, точнее не схватывает ее в полном объеме – цифровые следы, которые она относит к первичным далеко не всегда вызываются непосредственным воздействием пользователя, как уже было описано выше они могут отражать информацию либо о самом человеке, либо о цифровом объекте, через который он действовал, виртуальной личности. К прямым следам в описанной классификации можно отнести, например, запись голоса человека, его видеоизображение, созданный им текст. Причем следы из этих двух групп могут на практике соседствовать друг с другом. Так, в журнале событий о входе в учетную запись сведения об IP-адресе и технические данные устройства относятся к опосредованным цифровым следам, а дата и время входа – к прямым, поскольку эта информация отражает поведение са-

мого человека, время, когда он взаимодействовал с информационной системой, а совокупности его поведенческие привычки. Такая классификация имеет большое значение для использования цифровых следов в ходе раскрытия и расследования преступления, их правильной интерпретации при доказывании.

Заключение. Современная криминалистика, и в частности, формирующаяся цифровая криминалистика, занимающаяся изучением цифровых следов в целях раскрытия и расследования преступлений, нуждается во введении и дальнейшем развитии новой категории – виртуальная личность. Его наличие в системе цифровой криминалистике является крайне важным для адекватного объяснения изучаемых процессов и явлений, а также эффективного использования имеющихся знаний и собираемой информации в целях установления и доказывания причастности лица к действиям в информационной системе. Без категории виртуальной личности в этой области образуется критический пробел, белое пятно. Виртуальная личность, находящая воплощение в учетных записях и прочих идентификаторах, является как правило той самой сущностью, вызывающей последствия в компьютерной информации, которые наблюдаются как цифровые следы – предложенный теоретический концепт окажется очень полезным в практической деятельности.

Список литературы

1. Вехов В. Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики. 2017. С. 40–46.
2. Государственный стандарт Союза ССР ГОСТ 28397–89 Языки программирования. Термины и определения (утв. постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 21 декабря 1989 г. № 3961) URL: <https://files.stroyinf.ru/Data/111/11150.pdf> (дата обращения: 03.09.2025).
3. ГОСТ Р 71753–2024. Национальный стандарт Российской Федерации. Защита информации. Системы автоматизированного управления учетными записями и правами доступа. Общие требования. М.: ФГБУ "Институт стандартизации", 2024 URL: <https://docs.cntd.ru/document/1310068328> (дата обращения: 03.09.2025).
4. Данные, которые собирает счетчик Яндекс Метрики. Текст: электронный // Яндекс Метрика: [сайт]. URL: <https://yandex.ru/support/metrika/ru/code/data-collected> (дата обращения: 03.09.2025).
5. Криминалистика: учебник / Н.П. Яблоков. 2-е изд., перераб. и доп. М.: Норма, 2012. 400 с.
6. Криминалистика: учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. 3-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2012. 944 с.
7. Лутова Д. В. Виртуальная личность: доктринальные и практические проблемы идентификации субъектов // Уральский журнал правовых исследований. 2022. № 2 (19). С. 68–73.
8. Лучинкина А. И., Расина Э. О. Виртуальная личность как реализация адаптационного потенциала интернет-пользователя // Ученые записки Крымско-

го федерального университета имени ВИ Вернадского. Социология. Педагогика. Психология. 2024. Т. 10. № 4 (76). С. 132–144.

9. Маклаков А. Г. Общая психология. М.: Питер, 2008. 582 с.

10. Политика использования файлов cookie. Текст: электронный // Яндекс Правовые документы: [сайт]. URL: https://yandex.ru/legal/cookies_policy/ru/ (дата обращения: 03.09.2025).

11. Постановление Правительства Российской Федерации «Об утверждении правил оказания телематических услуг связи» от 31.12.2021 № 2607 (ред. от 30.09.2023). URL: <https://normativ.kontur.ru/document?moduleId=1&documentId=477462#h103> (дата обращения: 03.09.2025).

12. Работа следователя с «цифровыми следами»: учебно-методическое пособие / Бычков В.В., Скобелин С.Ю. М.: Московская академия СК России, 2021. 117 с.

13. Расследование преступлений, совершенных с использованием Интернета и мобильной телефонии: курс лекций / В.В. Бычков, А.А. Лебедева, С.Ю. Скобелин. М.: Московская академия СК России, 2021. 161 с.

14. Стандарт Банка России СТО БР БФБО–1.7–2023 “Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств” (принят приказом Банка России от 1 марта 2023 г. N ОД–335) [Электронный ресурс]. URL: <https://cbr.ru/Crosscut/LawActs/File/6177> (дата обращения: 03.09.2025).

15. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (ред. от 24.06.2025). URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 03.09.2025).

16. Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» от 29.12.2022 № 572-ФЗ (ред. от 28.12.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 03.09.2025).

17. Цифровая криминалистика: учебник для вузов / под редакцией В. Б. Вехова, С. В. Зуева. 2-е изд., перераб. и доп. Москва: Юрайт, 2025. 490 с. (Высшее образование). ISBN 978–5–534–17464–9. Текст: электронный // Образовательная платформа Юрайт [сайт]. С. 319 URL: <https://urait.ru/bcode/568013/p.319> (дата обращения: 03.09.2025).

18. Электронные доказательства в уголовном судопроизводстве: учебник для вузов / отв. ред. С. В. Зуев. Москва: Юрайт, 2025. 193 с. (Высшее образование). ISBN 978–5–534–13286–1. Текст: электронный // Образовательная платформа Юрайт [сайт]. С. 38 URL: <https://urait.ru/bcode/567334/p.38> (дата обращения: 03.09.2025).

19. Кушнарев А.С. Цифровые следы в криминалистике, их использование при расследовании преступлений // Вопросы российской юстиции. 2024. № 32. С. 338–351.

20. Carrier B. D. Basic digital forensic investigation concepts //Digital investigation and Digital Forensic Basics. 2006. URL: https://web.archive.org/web/20100226184652/http://www.digital-evidence.org/di_basics.html (дата обращения: 03.09.2025).
21. Casey E. Handbook of digital forensics and investigation. Academic Press, 2009. URL: <https://books.google.ru/books?id=xNjsDprqtUYC&printsec=frontcover&hl=ru#v=onepage&q=attribution&f=false> (дата обращения: 03.09.2025).
22. Suler J. The online disinhibition effect //Cyberpsychology & behavior. 2004. T. 7. №. 3. С. 321–326.

В. В. Федорова,

магистрант,

Российская академия народного хозяйства

и государственной службы

при Президенте Российской Федерации

**Автор VS нейросеть: как соблюсти баланс интересов
в современном авторском праве**

Аннотация. В данной статье рассмотрены основные вопросы, связанные с соблюдением режима авторско-правовой охраны на результаты интеллектуальной деятельности, которые могут быть задействованы в ходе обучения нейросетей. Изучен отечественный подход к свободному использованию объектов авторского права, зарубежная практика применения к отношениям, подразумевающим участие в них искусственного интеллекта, доктрины «fair use», а также основные способы легализации использования произведений науки и искусства для обучения генеративного ИИ. Сделаны выводы о возможном правовом урегулировании конфликта интересов авторов и разработчиков нейросетей.

Ключевые слова: авторское право, искусственный интеллект, обучение нейросетей, свободное использование, результаты интеллектуальной деятельности, нарушение авторских прав, сгенерированные объекты

V. V. Fedorova,

magistrate,

Russian Academy of National Economy and Public Administration

**Author VS neural network: how to maintain a balance of interests
in modern copyright law**

Abstract. This article discusses the main issues related to compliance with the copyright protection regime for the results of intellectual activity, which can be involved in the training of neural networks. The article examines the Russian approach to the free use of copyright objects, foreign practice of applying to relationships involving the participation of artificial intelligence, the doctrine of "fair use", as well as the main ways to legalize the use of scientific and artistic works for teaching generative AI. Conclusions are drawn about the possible legal settlement of the conflict of interests of the authors and developers of neural networks.

Keywords: copyright, artificial intelligence, neural network training, free use, intellectual property results, copyright infringement, generated objects

Введение. Цифровые технологии – это важный фактор настоящего и ключевая компонента будущего. Сегодня уместно говорить не просто об экспери-

ментах по внедрению искусственного интеллекта и алгоритмов обработки больших данных, а о консенсусе по вопросу о необходимости подобных инноваций [6. С. 910]. Повсеместное использование искусственного интеллекта, за счет его проникновения во все сферы жизни общества, коренным образом влияет на совокупность прав, принадлежащих человеку. Генеративный ИИ уже проявил себя в качестве одной из наиболее существенных угроз традиционным институтам авторского права, которые плохо подготовлены к тому, чтобы одновременно обеспечивать защиту права на творчество и самореализацию и охрану авторских прав создателей результатов интеллектуальной деятельности (далее – РИД) в условиях практически неконтролируемого использования произведений науки и искусства для обучения нейросетей. Таким образом, в современном авторском праве сформировалась ситуация, в которой в зоне правового риска находятся права не только лиц, заимствующих РИД для своих нужд, но и самих авторов, которые не давали согласия на предоставление своих произведений для обучения ГИИ.

Целью данного исследования стало выяснить, каким образом использование объектов, защищенных авторским правом, для обучения нейросетей, соотносится с защитой основных прав авторов произведений науки и искусства. Для достижения данной цели были выполнены следующие задачи: определить, какие способы свободного использования РИД не противоречат современному Российскому законодательству; изучить, каким образом зарубежная правоприменительная практика подходит к определению пределов допустимого свободного использования РИД, предположить, как будет развиваться правовое регулирование основ организации обучения нейросетей, для которого необходимы объекты авторского и смежного права, созданные третьими лицами, сделать выводы.

Основная часть. Гражданское законодательство четко очерчивает круг РИД, использование которых должно осуществляться в соответствии с нормами права. К этим объектам относятся все произведения искусства, науки и культуры, вне зависимости от художественной или научной ценности, формы и носителя. В рамках существующего правового регулирования права авторов подлежат приоритетной защите, что должно побуждать субъектов авторского права к творчеству. Однако, абсолютная охрана авторских прав никогда не существовала, поскольку такой правовой режим заблокировал бы возможности для какого-либо переосмысления или переработки созданных кем-либо произведений.

Отечественное гражданское законодательство оставляет достаточно свободы для использования произведений науки, культуры и искусства без производства выплат и отчислений. В статье 1274 ГК РФ содержится перечень видов такого использования, в который входят, в частности, цитирование, иллюстрирование, воспроизведение в периодических изданиях статей, речей и докладов по текущим вопросам, сурдоперевод и тифлокомментирование, создание пародий и карикатур [3]. Использование объектов, защищенных авторским правом, в качестве источника вдохновения для самостоятельного творчества также никак не ограничивается (кроме случаев плагиата) [2].

Очевидно, что все способы свободного использования, в т.ч. те, которые позволяют перерабатывать произведение, предусматривают наличие человека, который имеет представление о том, что и в каких количествах можно заимствовать из существующего результата интеллектуальной деятельности. Ситуация становится гораздо менее определенной, когда в ней появляется еще один квазиучастник – искусственный интеллект, который не имеет границ, определяющих недопустимость заимствования, и на данный момент не может нести какую-либо ответственность за несанкционированное использование РИД. В перечне, предлагаемом ГК РФ, отсутствуют положения, каким-либо образом упоминающие искусственный интеллект, в связи с чем в случае возникновения спорных ситуаций возникает необходимость разработки механизма, позволяющего оценивать нестандартные способы свободного использования РИД на предмет их допустимости [4].

Поскольку отечественная практика пока не выработала универсального способа определения допустимости свободного использования объектов, защищенных авторским правом, представляется целесообразным обратить внимание на зарубежные методы решения данного вопроса. Знаковым делом по данному направлению можно считать дело *Bartz v. Anthropic*, которое было рассмотрено 24 июня 2025 года судом Северного округа Калифорнии [5; С. 82]. Суть дела заключается в том, что авторы коллективно подали иск на компанию, осуществившую обучение своего ГИИ на текстах их книг. Революционность принятого в рамках дела решения заключается в том, что судья впервые провел аналогию между ИИ и читателем, который не воспроизводит текст, а воспринимает его и выдает вовне результат своего понимания и переосмысления. Таким образом, использование экземпляров книг, приобретенных на законных основаниях, было признано допустимым свободным использованием в соответствии с доктриной *fair use*, которая характерна для американского авторского права. Примечательно, что доктрина «преобразовательного использования», с которой также необходимо согласовываться при определении допустимости свободного использования, подразумевает, что воздействие такого использования на рынок не снижает заинтересованность покупателей к приобретению лицензионных экземпляров РИД. Уже сейчас с помощью ГИИ обычный пользователь может бесплатно сгенерировать книгу, изображение или музыку, исходя из своих предпочтений. В связи с этим возникают обоснованные сомнения относительно того, что обучение нейросетей действительно не влияет продажи официальных экземпляров.

Возможно ли перенесение основных принципов применения доктрины *fair use* на отечественную правовую почву? На данный момент такой исход представляется маловероятным, учитывая ориентированность российской цивилистики на конкретный перечень допустимых видов свободного использования. Однако, частичное заимствование многоступенчатого механизма определения допустимости свободно использования в конкретном случае (на основе установления справедливости цели использования, низкого творческого характера РИД и незначительности объемов заимствования), кажется целесообраз-

ным для тех случаев, которые выходят за стандартные рамки (которые не могут соответствовать темпам технического прогресса).

Заключение. Подводя итоги, можно сделать вывод о том, что сегодня авторы постепенно оказываются в уязвимом положении за счет того, что практика правоприменения демонстрирует лояльное или безразличное отношение к использованию результатов их творчества для обучения нейросетей, либо не имеет реальной возможности защитить их от незаконного использования РИД для машинного обучения. В связи с этим, необходимо внести в отечественное гражданское законодательство ряд изменений, определяющих условия, на которых владельцы нейросетей смогут приобретать произведения науки, культуры и искусства для обучения ИИ. В противном случае дисбаланс между интересами авторов и необходимостью получения новых данных для ГИИ может стать критическим [5], что негативно скажется на всем авторском праве в целом.

Список литературы

Васильева А.С. Использование объектов авторских прав для обучения искусственного интеллекта // Журнал Суда по интеллектуальным правам. 2024. Декабрь. N 4 (46). С. 80–84.

Демьяненко Е.В., Шпак А.В. К вопросу о свободном использовании произведений как объектов авторского права // ЮП. 2023. №1 (104). URL: <https://cyberleninka.ru/article/n/k-voprosu-o-svobodnom-ispolzovanii-proizvedeniy-kak-obektov-avtorskogo-prava> (дата обращения: 28.08.2025).

Кочубей Т.А. Понятие пародии как объекта авторского права // Legal Concept. 2018. №1. URL: <https://cyberleninka.ru/article/n/ponyatie-parodii-kak-obekta-avtorskogo-prava> (дата обращения: 28.08.2025).

Лукашова А.В. Авторское право и произведения, сгенерированные нейросетью // Вопросы российской юстиции. 2023. №28. URL: <https://cyberleninka.ru/article/n/avtorskoe-pravo-i-proizvedeniya-sgenerirovannye-neyrosetyu> (дата обращения: 28.08.2025).

«Impossible» to create AI tools like ChatGPT without copyrighted material, OpenAI says // The Guardian. URL: <https://www.theguardian.com/technology/2024/jan/08/ai-tools-chatgpt-copyrighted-material-openai> (дата обращения: 19.08.2025).

Казанцев Д.А. Авторские права на результаты деятельности искусственного интеллекта и способы их защиты // Journal of Digital Technologies and Law. 2023. Т. 1, № 4. С. 909–931. URL: <https://doi.org/10.21202/jdtl.2023.39>. EDN: phbnki

**Особенности использования отдельных видов
электронных и цифровых доказательств в судебной практике**

Аннотация. В статье рассмотрены подходы к определению понятия «электронные доказательства», выявлены основные признаки данного процессуального института. Приведены международно-правовые акты, с помощью которых были предприняты попытки установления порядка применения электронных доказательств в судах. Также в статье уделено внимание роли нотариусов и других специалистов в заверении материалов, полученных электронным путем. В приведенной судебной практике в основном затронуты вопросы применения скриншотов, спутниковых снимков, электронных переписок, номеров ID в гражданском и административном процессах.

Ключевые слова: электронные доказательства, электронный документ, информационные технологии, скриншот, фальсификация, спутниковый снимок, социальные сети

А.А. Khazieva,

student,

Kazan Federal University

**Features of using certain types of electronic and digital evidence
in judicial practice**

Abstract. The article examines approaches to defining the concept of "electronic evidence" and identifies the main features of this procedural institution. It also provides an overview of international legal acts that have been used to establish the procedure for using electronic evidence in courts. The article also focuses on the role of notaries and other professionals in certifying materials obtained electronically. The article discusses the use of screenshots, satellite images, electronic correspondence, and ID numbers in civil and administrative proceedings.

Keywords: electronic evidence, electronic document, information technology, screenshot, falsification, satellite image, social networks

Введение. Современные реалии, с одной стороны, упрощают многие процессы в судебной системе, а с другой, преподносят большие вызовы. Упрощение выражается в том, что становятся более доступными способы взаимодействия между судами и лицами, которые участвуют в судебных процессах, ведь на сегодняшний день благодаря отечественным платформам ГАС "Правосудие", "Мой арбитр" и др. появилась возможность подачи большинства документов в электронном виде, участия в судебных заседаниях с использованием

веб-конференций, электронного ознакомления и т.д. С другой стороны, развитие современных технологий предвосхищает появление новых процессуальных институтов. На сегодняшний наибольший интерес вызывает вопрос о применении цифровых (электронных) доказательств.

Основная часть. В российском законодательстве не дается определения понятиям «цифровые» или «электронные» доказательства. Более того, нет четкого разграничения между этими двумя прилагательными.

Согласно пункту 1 статьи 55 Гражданского процессуального кодекса Российской Федерации (далее – ГПК РФ) доказательствами по делу являются полученные в предусмотренном законом порядке сведения о фактах, на основе которых суд устанавливает наличие или отсутствие обстоятельств, обосновывающих требования и возражения сторон, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела [1].

В определении, данном законодателем, отражены следующие существенные признаки доказательств:

1) относимость – означает, что сведения имеют непосредственную связь с обстоятельствами по данному делу;

2) допустимость, то есть в соответствии со ст. 60 ГПК обстоятельства дела, которые в соответствии с законом должны быть подтверждены определенными средствами доказывания, не могут подтверждаться никакими другими доказательствами. Кроме того, судом принимаются только доказательства, полученные из предусмотренных законом источников;

3) достоверность, то есть сведения должны соответствовать действительности.

Следовательно, любые материалы, приложенные в качестве доказательств, должны соответствовать этим требованиям, в том числе цифровые.

Стоит отметить, что, по мнению большинства исследователей, понятия электронных и цифровых доказательств тождественны [2. С.110].

Несмотря на наличие общих черт, смешение этих двух понятий не совсем корректно. Цифровые материалы, это прежде всего, сведения, представленные в формате двоичного кода, и они не всегда могут передаваться и восприниматься на материальном носителе, например, в бумажной копии. Электронные доказательства могут иметь две формы: материальную – в виде физического документа, распечатанной фотографии и т. д., и в виде “неосязаемой” компьютерной информации. В контексте соотношения этих двух понятий, некоторые исследователи предлагают признать электронный документ подвидом цифрового документа, который перенесен на материальный носитель. В современном законодательстве, очевидно, превалирует понятие «электронных документов», так как именно этот термин был внедрен еще при создании первых электронно-вычислительных машин в СССР.

В настоящее время не существует легального определения понятия “электронное доказательство”, однако в Федеральном законе от 23.06.2016 № 220-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» [3] используется только понятие электронного документа,

в форме которых могут подаваться ходатайства, а также материалы, приложенные к ним. Все они должны иметь электронную подпись в соответствии с требованиями законодательства Российской Федерации.

Согласно процессуальным кодексам, а именно положениям ч. 3 ст. 75 АПК РФ [4], ч. 1 ст. 71 ГПК РФ [1], ч. 1 ст. 70 КАС РФ [5], документы и материалы, выполненные в форме цифровой, графической записи, включая полученные по факсу, электронной почте, из Интернета, подписанные электронной подписью, в порядке, установленном законодательством Российской Федерации, к письменным доказательствам по делу.

Значит с юридической точки зрения электронные документы, у которых можно установить достоверность, занимают место среди письменных доказательств. Ведь они являются материальным воплощением чьей-то мысли, зафиксированном в цифровом виде. Но что делать с более «неосязаемыми» цифровыми свидетельствами? Речь идет про фотоснимки, полученные со спутников, скриншоты веб-страниц, мессенджеров и другие материалы, полученные посредством Интернета. Одни авторы настаивают на отнесении их к письменным доказательствам. Другие склоняются к тому, что такие доказательства ближе к вещественным, так как они представляют собой некий объект, который можно исследовать, анализировать. Третья группа исследователей выделяет их в самостоятельную группу средств доказывания из-за специфических свойств, требующих особых методов проверки и оценки.

По мнению М.В. Горелова, «электронные доказательства – это сведения об обстоятельствах, имеющих значение для дела, выполненные в форме цифровой, звуковой и видеозаписи. К электронным доказательствам относятся также зафиксированные с помощью электронно-вычислительных средств протоколы судебных заседаний, протоколы совершения отдельных процессуальных действий» [6. С.24].

И.Н. Лукьянова утверждает, что в современных российских судах намечено использование трех видов электронных доказательств: «доказательства, созданные и сохраняемые в электронном виде, представляемые в суд в распечатанном виде и исследуемые как обычные традиционные доказательства»; «доказательства, созданные и сохраняемые в электронном виде, которые могут быть исследованы только в электронном виде»; «электронный образ документа, созданного и охраняемого в печатном виде, но поданного в суд в виде сканированного изображения» [7. С.132].

В 2014 году приказом Федерального агентства по техническому регулированию и метрологии был утвержден Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология. Методы и средства обеспечения безопасности» [8] (далее – стандарт), который идентичен международному стандарту ИСО/МЭК 27037:2012* "Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме" [9]. Пункт 3.5 стандарта содержит определение понятию «свидетельства, представленные в цифровой форме (digital evidence)»: это информация или данные, хранящиеся или передаваемые в виде двоичного кода. Интересно,

что по мнению создателей стандарта, не каждый человек может заниматься сбором и анализом цифровых доказательств. Так, согласно п. 3.7 и 3.8 лицами, которые обладают специальными знаниями в этой сфере, являются специалист "оперативного реагирования" по свидетельствам и специалист по свидетельствам, представленным в цифровой форме. В стандарте приведена детальная регламентация обработки цифровых свидетельств. Это связано с тем, что такая информация уязвима, то есть она могут быть сфальсифицирована.

Указанный стандарт больше относится к применению доказательств в уголовно-процессуальной сфере, поэтому интерес вызывает еще один документ международного уровня, а именно «Руководящие принципы, касающиеся использования электронных доказательств в гражданском и административном судопроизводстве» [10], принятые в 2019 году Комитетом министров Совета Европы.

В «Руководящих принципах» электронное доказательство означает «любое доказательство, полученное на основе данных, содержащихся на каком-либо устройстве или созданных им». Также здесь отдельно упоминаются «удостоверяющие центры», которые предоставляют услуги, связанные с удостоверением электронных подписей, печатей, меток времени и созданием сертификатов для аутентификации на веб-сайтах.

Лидером цифровизации судебной системы является Китай. В этой стране воплощен в жизнь проект Интернет-суда, в котором преимущественно рассматриваются споры о неправомерных действиях в сети Интернет. Закономерно то, что в гражданско-процессуальном законодательстве вопрос применения электронных материалов урегулирован более четко. 1 мая 2020 года вступили в силу изменения в «Несколько положений Верховного народного суда о доказательствах в гражданском судопроизводстве» (最高人民法院关于民事诉讼证据的若干规定) [23]. В этом документе примечательна статья 14, в которой перечисляется, что именно относится к электронным данным, применяемым в качестве доказательств: в частности, это информация на веб-платформах (например, в блогах), регистрационная информация пользователя, коммуникационная информация сетевых прикладных служб и др. В части 2 статьи 94 закреплена презумпция подлинности электронных данных: если содержание электронных данных было заверено нотариальным органом, народный суд подтверждает их подлинность, за исключением случаев, когда имеются доказательства обратного, достаточного для их отмены.

Действительно, если законодатель примет решение о внедрении в процессуальные кодексы понятия «электронных доказательств», то следует руководствоваться международными стандартами и опытом других стран. В упомянутых международно-правовых актах большое внимание уделяется роли специалистов и экспертов, которые на профессиональном уровне занимаются оценкой, сбором и удостоверением доказательств. В настоящее время заверением документов и др. занимаются нотариусы, но при внедрении электронных доказательств необходимо учитывать, что нотариусы не могут обладать достаточной компетенцией для заверения материалов в цифровом или электронном виде.

Следовательно, необходимо привлекать специалистов из соответствующей сферы. Так, уже сейчас в России существуют специализированные экспертные центры, которые предлагают услуги по экспертизе подлинности электронных файлов, например, проверка электронной переписки, заверение подлинности электронных сообщений и писем. Разумеется, исполнители таких услуг должны понимать, что в этой сфере важна беспристрастность, поэтому законодателю следует выработать определенный механизм, который обеспечит взаимодействие таких специалистов со сторонами разбирательства, судом или нотариусом. Если их деятельность будет регулироваться так же, как, к примеру, деятельность оценщиков при приобщении их заключений в дела, то может расшириться применение электронных доказательств в суде.

К настоящему времени субъектами законодательной инициативы не предпринимались попытки по внесению в Государственную Думу законопроектов по вопросу внедрения и применения электронных доказательств в судах. Чтобы приступить к данному шагу, нужно, в первую очередь разграничить два понятия: «электронные» и «цифровые» доказательства. Второй шаг – необходимо определиться, в чью компетенцию входит заверение подлинности таких материалов. Стоит отметить, что в 2021 году в Государственную Думу был внесен проект Федерального закона «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации»[22], который регламентирует конвертацию и хранение электронных документов, а также процесс создания дубликатов электронных и материальных документов. Главная цель законопроекта – уменьшить затраты на архивное хранение документов в бумажном виде и расширение сферы электронного документооборота. Указанный законопроект предусматривает перечень лиц, которые могут заниматься конвертацией, созданием и хранением электронных документов: в частности, это обладатель документа и субъекты предпринимательской деятельности, имеющие лицензию в соответствии со статьями 11.6 и 11.7 Законопроекта. Хотя предложенные изменения не нашли отражения в действующем законодательстве, положения этого законопроекта актуальны в сфере применения электронных доказательств. Так, если будет принят закон о регулировании и определении места электронных доказательств, также снизится объем бумажной документации в судах, так как участники судебного разбирательства будут чаще обращаться к электронному формату. Кроме того, подтверждением подлинности электронных материалов и сведений для приобщения в суд могут заниматься профессиональные участники – эксперты, имеющие лицензию для такой деятельности. Такие нововведения помогут сторонам и их представителям в судебном процессе преодолеть неопределенность при использовании доказательств, полученных электронным путем.

Таким образом, проанализировав разные определения понятия «электронные доказательства», можем отметить их основные признаки:

1) Электронные (цифровые) доказательства базируются на цифровой информации, которая представляет собой сведения, хранящиеся в памяти компью-

тера (в цифровой форме) или телекоммуникационной сети "Интернет", а также локальной сети.

2) Такие сведения хранятся, передаются и отображаются и либо в серверах телекоммуникационной сети "Интернет" (например, существуют облачные хранилища), либо на материальных носителях. Следовательно, для восприятия такой информации необходимы специальные технические средства.

Что касается тождества «электронных» и «цифровых» доказательств, несмотря на наличие общих черт, смешение этих двух понятий не совсем корректно. Цифровые материалы, это прежде всего, сведения, представленные в формате двоичного кода, и они не всегда могут передаваться и восприниматься на материальном носителе, например, в бумажной копии. Электронные доказательства могут иметь и материальную форму в виде физического документа, распечатанной фотографии и т.д., и представляться в форме компьютерной информации. В современном законодательстве, очевидно, превалирует понятие «электронных документов», так как именно этот термин был внедрен еще при создании первых электронно-вычислительных машин в СССР.

В судебной практике не выработано единообразие по многим аспектам применения электронных доказательств, но тем не менее, наблюдается тенденция к восприятию судом такого рода доказательств в качестве достоверных и допустимых.

Обратимся к использованию скриншотов в российской судебной практике.

Использование снимков экрана регулируется статьей 71 ГПК РФ: «К письменным доказательствам, в частности, относятся документы и материалы, полученные посредством электронной или другой связи, с использованием информационно-телекоммуникационной сети «Интернет». В действующем законодательстве не дается понятия «скриншота», однако данный пробел в законодательстве восполняется судами. Например, Федеральный арбитражный суд Волго-Вятского округа в постановлении от 27 апреля 2011 г. N Ф01-1661/11 по делу N А82-12456/2010[12] дал свое определение понятию «скриншот»: «...это страницы в сети Интернет (снимок экрана, показывающий то, что видит пользователь на экране монитора), подтверждающие размещение информации, подлежащей раскрытию».

В постановлении Федерального арбитражного суда Северо-Западного округа от 6 декабря 2010 г. по делу N° А56-11028/2010[13] суд дает схожее определение рассматриваемому понятию, а также определяет критерии, на основании которых суд удовлетворяет ходатайство о приобщении к делу скриншотов.

Так, исполнитель и заказчик заключили договор оказания услуг по обслуживанию Интернет-проекта в сети Интернет, предметом которого является продвижение интернет сайта заказчика, то есть выведение сайта в ТОП 10 по запросам в поисковой системе www.yandex.ru. В приложении к договору были указаны ключевые слова, которые должны быть выведены на первые 10 позиций в поисковой системе www.yandex.ru.

Истец сделал «скриншоты» сайта – изображения, полученные компьютером и показывающие в точности то, что видит пользователь на экране монитора. В ТОП 10 имелись не все ключевые слова, указанные в приложении к договору.

Истец обратился в суд и представил в качестве доказательств сделанные им скриншоты. Однако суд отклонил их, обосновав следующим образом: «скриншоты» не свидетельствуют о ненадлежащем исполнении Обществом [ответчик] своих обязательств по продвижению сайта, поскольку отсутствуют доказательства относительности данных «скриншотов» к сайту, названному в спорном договоре; отсутствует указание на дату и точное время их составления, а также на лицо, которое произвело их выведение на экран и дальнейшую распечатку; отсутствуют данные о программном обеспечении и использованной компьютерной технике. При этом существенным обстоятельством является то, что положение в поисковых системах меняется ежесекундно, то есть для объективной оценки положения сайта в Интернете необходимо предоставление сведений в динамике за весь период действия спорного договора».

Суд встал на сторону ответчика, так как истец не предоставил скриншоты только за определенный промежуток, а не за весь необходимый период.

В абз. 2 п. 55 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 "О применении части четвертой Гражданского кодекса Российской Федерации"[14] указано, что допустимыми доказательствами являются в том числе сделанные и заверенные лицами, участвующими в деле, распечатки материалов, размещенных в информационно-телекоммуникационной сети (скриншот), с указанием адреса интернет-страницы, с которой сделана распечатка, а также точного времени ее получения.

В 2023 году Судебной коллегией по гражданским делам Верховного Суда Российской Федерации в Определении от 07.02.2023 № 5–КГ22–144–К2 была сформулирована позиция, согласно которой суд, отказывая в принятии незаверенных скриншотов переписок, препятствует истцу в осуществлении своих прав[15].

Согласно материалам дела, истец при подаче искового заявления о нарушении ответчиком исключительных прав приложил скриншоты переписки электронной почты. Суд первой инстанции решил: доказательства продажи спорных произведений ответчиком третьему лицу в предоставленной суду форме переписки не могут быть приняты, поскольку не отвечают требованиям допустимости и относимости. Из незаверенной переписки невозможно установить причастность именно ответчика к участию согласования условий сделки, оплаты третьим лицом и получения ответчиком денежных средств, отправке (получению) спорных произведений в печатном, электронном, либо аудио исполнении.

Апелляционная и кассационная инстанции поддержали решение первой инстанции.

Однако Верховный суд, отменяя судебные акты нижестоящих инстанций, отметил, что ответчиком не было сделано заявлений о фальсификации, что в совокупности с другими фактами подтверждает достоверность доказательства. Верховный суд указал на ошибку апелляционной инстанции, так как суд сослался на отсутствие экспертного заключения достоверности электронной пе-

реписки, при этом на обсуждение этот вопрос не поставил. Верховный суд пришел к следующему выводу о том, что суды не создали необходимые условия для всестороннего и объективного выяснения действительных обстоятельств дела, не оказали лицу, участвующему в деле, содействие в осуществлении его прав».

Из этого Определения можно прийти к выводу, что если противоположная сторона не заявляет о фальсификации, то суд вполне может принять скриншоты переписок в качестве доказательств без нотариального заверения.

Современные технологии позволяют использовать в процессе доказывания еще один вид скриншотов – это снимки экранов, полученных из геоинформационных систем. В частности, при спорах, связанных с правом собственности на земельные участки, а также защитой экологических прав, обращаются к фотоснимкам и панорамам из сервисов Google Maps и «Яндекс.Карты».

В рамках дела о банкротстве по делу № А70–6990/2018 Восьмой арбитражный апелляционный суд в Постановлении от 22.02.2019 признал такие снимки в качестве допустимых доказательств [16].

Первая инстанция удовлетворила заявление финансового управляющего о признании недействительной сделки купли-продажи земельного участка между Митьковым (должник) и Чебоксаровым. Чебоксаров обратился в суд апелляционной инстанции для отмены определения суда первой инстанции в части о признании вышеуказанной сделки недействительной. Его аргументы основывались на следующем: «...выводы суда о том, что на момент продажи земельного участка на нем находился жилой дом, несостоятельны, поскольку основаны на снимках Google Планета Земля, которые не отвечают принципам достоверности и не подтверждены иными доказательствами».

Согласно материалам дела, договор купли-продажи был заключен 09.12.2016, согласно которому Митьковым было совершено отчуждение только земельного участка, хотя на нем находился и объект недвижимости, а именно жилой дом. Тем самым при совершении сделки цена объекта купли-продажи была сильно занижена.

Суд, принимая доказательства, представленные финансовым управляющим, отмечает: «Согласно спутниковым снимкам земной поверхности, размещенным в программе Google Планета Земля, по координатам спорного земельного участка на дату совершения оспариваемой сделки (09.12.2016) находился объект недвижимости».

Суд проанализировал снимки, сделанные в разные даты: 15.05.2014, 09.08.2014, 03.06.2015, 17.06.2015, 23.07.2016. На всех изображениях зафиксирован незарегистрированный объект недвижимости. На снимках 15.05.2014 и 09.08.2014 был виден построенный на земельном участке объект без крыши, а на снимках от 03.06.2015, 17.06.2015, 23.07.2016, построенный на земельном участке объект, увеличенный в размерах по ширине и имеющий крышу.

«Признавая указанные снимки в качестве допустимого доказательства суд апелляционной инстанции учитывает, что Google Планета Земля (англ. Google Earth) – проект компании Google, в рамках которого в сети Интернет были размещены спутниковые (или в некоторых точках аэрофото) изображения земной

поверхности. Проект является открытым источником информации, а используемые снимки размещены на серверах компании, а не на устройстве информация доступна для предметной проверки...».

Таким образом, апелляционная инстанция для установления достоверности представленных доказательств сравнила несколько снимков, сделанных в разные года, а также отметила открытость источника получения доказательств, что позволяет сторонам судебного разбирательства проверить их подлинность.

В деле о привлечении к административной ответственности за нарушение правил дорожного движения Тагилстроевский районный суд г. Нижнего Тагила в решении № 12-77/202112-82/2021 от 1 июня 2021 г. по делу № 12-77/2021 не признал спутниковые снимки, размещенные в сервисах «Яндекс.Карты» и Google.Maps, надлежащим доказательством из-за отсутствия на снимках времени, однако отметил[17]:

"Представленные защитником спутниковые снимки 183 километра автодороги Екатеринбург – Серов сами по себе не могут быть признаны надлежащим доказательством ввиду наличия того же порока, что и представленная должностными лицами схема расположения технических средств – отсутствуют данные о времени выполнения снимков. В то же время спутниковые снимки в совокупности с исследованной видеозаписью косвенно подтверждают отсутствие на участке дороги разметки 1.1".

В данном деле суд признал снимки из спутника в качестве косвенного доказательства в совокупности с другим доказательством (видеозаписью).

В судебной практике других государств применение снимков из спутника также не является редкостью. К примеру, в 2015 году Коллегия судей Девятого окружного апелляционного суда в деле Пасиано Лизаррага–Тирада постановила, что «поскольку спутниковый снимок Google Earth, как и фотография, не содержит утверждений, он не является слухами. Коллегия также постановила, что метка, нанесенная на спутниковый снимок программой Google Earth и автоматически помеченная GPS–координатами без какого-либо вмешательства человека, не является слухами»[18].

Хотя комиссия признала, что «машинные записи могут вызывать сомнения в качестве доказательств, в том числе из-за сбоев в работе или фальсификации», она написала в судебном документе, что эти сомнения могут быть «устранены с помощью правил аутентификации».

Информация, размещенная в социальных сетях, также может стать существенным доказательством или предметом спора.

Обратимся к Постановлению Арбитражного суда Московского округа от 16.10.2019 по делу № А40-139272/2017[19]. В рамках дела о банкротстве банка арбитражный управляющий подал заявление о признании сделок по купле-продаже недвижимого имущества недействительными.

Судами установлено, что между ПАО «Банк Премьер Кредит» (далее – Банк) и ООО «Альянс» был заключен договор об открытии кредитной линии. Обеспечением своевременного исполнения обязательств заемщика по кредитному договору являлся залог в пользу банка недвижимого имущества, приобретае-

мого ООО «Альянс» на выданные банком денежные средства. В установленный договором срок заемщик не исполнил свои обязательства по возврату кредита.

Банк обратился в суд с заявлением о взыскании задолженности по кредитному договору и обращении взыскания на заложенные объекты недвижимости. В этот период ООО «Альянс» продало имущество другому лицу – Каримовой Р.Р., которая в свою очередь, совершила сделку по купле-продаже данного имущества Раевскому И.С. Суд первой инстанции счел последнего покупателя добросовестным приобретателем, поэтому не признал сделку недействительной. Однако апелляционная инстанция пришла к выводу о недобросовестности покупателей. В частности, удовлетворяя заявление о признании сделки недействительной, суд указывает на следующее: «Согласно данным, размещенным в сети Интернет, на сайте социальной сети «В контакте» Надюков И.Р. [единоличный исполнительный орган ООО «Альянс»] является родным племянником Каримовой Р.Р.».

Таким образом, информация, размещенная в социальных сетях, может стать важным доказательством.

Данная позиция прослеживается и в Определении Верховного суда Российской Федерации от 16.12.2016 по делу № 309-ЭС16-10730: Унитарное предприятие, занимающееся развитием телерадиовещания на территории Республики Башкортостан (далее – Истец), обратилось в арбитражный суд с иском к Воробьевой С.Л. (далее – ответчик) о признании сведений, распространенных ответчиком в социальной сети «В Контакте», порочащими деловую репутацию истца и применением соответствующих санкций в отношении ответчика [20].

Первая, апелляционная инстанция и кассационная инстанции не удовлетворили иск ввиду того, что публикация информации в социальной сети представляет собой высказанные ответчиком суждения и субъективное мнение, следовательно, ее нельзя признать порочащей деловую репутацию.

Однако Верховный суд не согласился с данной позицией. Удовлетворяя иск, высшая инстанция отметила: «Под распространением сведений, порочащих деловую репутацию юридических лиц, следует понимать, среди прочего, ... распространение таких сведений в сети Интернет».

В этом деле также особого внимания заслуживает то, каким образом Истец определил Ответчика, поскольку публикация была выложена в сообществе, в котором работали 5 администраторов, обладающие правом публиковать сообщения. В связи с этим Воробьева С.Л., привлеченная в качестве ответчика, в отзыве на исковое заявление утверждала, что неясно, кем именно опубликована данная информация, следовательно, она не является надлежащим ответчиком. Однако в социальной сети «В Контакте» каждому пользователю присваивается ID, который представляет собой определенный набор цифр. Истец определил ID лица, опубликовавшего сообщение, и пришел к выводу, что надлежащим ответчиком является Воробьева С.Л. Суды приняли доводы Истца.

Можно сделать вывод, что в настоящее время «посты» в социальных сетях, часто носящие субъективный характер, могут стать предметом спора касательной деловой репутации, ведь имидж участников гражданского оборота в современности формируется в том числе через социальные сети. Хотя номера

ID или названия аккаунтов, которые представляют собой цифровую информацию и имеются у каждого пользователя, созданы лишь для удобства идентификации и не носят формально-официальный характер, они все равно принимаются судами во внимание. Кроме того, номера ID и адреса страницы в социальных сетях можно отнести к персональным данным в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных"[21], так как они тоже являются информацией, относящейся к физическому лицу. Исходя из легального определения персональных данных, номера ID наряду с именем, адресом, абонентским номером и другими сведениями вполне могут относиться к персональным данным, а значит, служить в качестве специфических доказательств в суде.

Заключение. Таким образом, в современности цифровизация охватывает большинство процессуальных институтов. В российской судебной практике электронные сведения принимаются в качестве средств доказывания, но к ним предъявляются повышенные требования: такие доказательства должны содержать указание на время или другие конкретные данные, либо должны заверяться нотариусом. Что касается сущности электронного доказательства, то многие авторы рассматривают его через призму электронного документа. Законодатель же рассматривает электронные доказательства в качестве разновидности письменных доказательств. Разумеется, чтобы внести единообразие в использование таких специфичных материалов в судебных процессах, нужно установить правовые рамки их использования, руководствуясь в том числе международно-правовым опытом.

Список литературы

1. Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. №138-ФЗ (ред. от 01.07.2021) // Собрание законодательства РФ. 2002. №46. Ст. 4532; 2021. №27 (часть I). Ст. 5071.
2. Черецких А.В. Цифровые (электронные) доказательства в уголовном судопроизводстве // Правопорядок: история, теория, практика. 2023. № 4 (39). С. 110–117. DOI: 10.47475/2311-696X-2023-39-4-110-117.
3. Федеральный закон № 220-ФЗ от 23.06.2016 «О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти» // Собрание законодательства Российской Федерации от 2016 г. , N 26 , ст. 3889 (*Часть I*).
4. Арбитражный процессуальный кодекс Российской Федерации (АПК РФ) от 24.07.2002 №95-ФЗ // Собрание законодательства Российской Федерации от 2002 г., N 30. Ст. 3012.
5. Кодекс административного судопроизводства Российской Федерации от 08.03.2015 N 21-ФЗ // Собрание законодательства Российской Федерации от 2015 г., N 10. Ст. 1391.
6. Горелов М.В. Электронные доказательства в гражданском судопроизводстве России: Вопросы теории и практики: дисс. ... канд. юрид. наук. Екатеринбург, 2005. С.24.

7. Лукьянова И.Н. Доказательства в гражданских делах в эпоху электронного правосудия // Вестник Воронежского государственного университета. Серия: Право. 2018. № 4. С. 132.

8. ГОСТ Р ИСО/МЭК 27037–2014: Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 09 сентября 2014 г. № 1028–ст). URL: <https://base.garant.ru/71163010/> (дата обращения: 22.07.2025).

9. Международный стандарт ИСО/МЭК 27037:2012* "Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме" (ISO/IEC 27037:2012 "Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence"). URL: <https://docs.cntd.ru/document/1200112857> (дата обращения: 22.07.2025).

10. Руководящие принципы Комитета министров Совета Европы от 30 января 2019 года и пояснительный меморандум «Электронные доказательства в гражданском и административном судопроизводстве. URL: <https://rm.coe.int/prems-147419-rus-2019-sm-2018-169-lignes-> (дата обращения: 24.07.2025).

11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448 (Часть I).

12. Постановление Федерального арбитражного суда Волго-Вятского округа от 27 апреля 2011 г. № Ф01–1661/11 по делу № А82–12456/2010. URL: <https://sudrf.cntd.ru/document/770452572> (дата обращения: 17.07.2025).

13. Постановление Федерального арбитражного суда Северо-Западного округа от 6 декабря 2010 г. N Ф07–13497/2009 по делу № А56–7735/2009. URL: <https://www.garant.ru/products/ipo/prime/doc/36224067/> (дата обращения: 17.07.2025).

14. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 "О применении части четвертой Гражданского кодекса Российской Федерации". URL: https://www.consultant.ru/document/cons_doc_LAW_323470/ (дДата обращения: 20.07.2025).

15. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 07.02.2023 N 5–КГ22–144–К2 (УИД 77RS0011–02–2021–006027–07). URL: <https://legalacts.ru/sud/opredelenie-sudebnoi-kollegii-po-grazhdanskim-delam-verkhovnogo-suda-rossiiskoi-federatsii-ot-07022023-n-5-kg22-144-k2/> (дата обращения: 01.08.2025).

16. Постановление от 22 февраля 2019 г. по делу № А70–6990/2018. URL: <https://sudact.ru/arbitral/doc/fe5V4O63bvoW/> (дата обращения: 3.08.2025).

17. Решение Тагилстроевского районного суда г. Нижнего Тагила по делу № 12–77/202112–82/2021 от 01.06.2021 г. URL: <https://судебныерешения.рф/60233877> (дата обращения: 6.08.2025).

18. Дело «Соединенные Штаты против Лисарраги-Тирадо», № 13-10530 (9-й округ, 2015 г.) / United States v. Lizarraga-Tirado, No. 13-10530 (9th Cir. 2015). [Электронный ресурс]. URL: <https://law.justia.com/cases/federal/appellate-courts/ca9/13-10530/13-10530-2015-06-18.html> (дата обращения: 18.08.2025).

19. Постановление Арбитражного суда Московского округа от 16.10.2019 по делу № А40-139272/2017. URL: <https://base.garant.ru/42035198/> (дата обращения: 19.08.2025).

20. Определение Судебной коллегии по экономическим спорам Верховного Суда РФ от 16.12.2016 N 309-ЭС16-10730 по делу № А07-12906/2015. URL: <https://legalacts.ru/sud/opredelenie-verkhovnogo-suda-rf-ot-16122016-n-309-es16-10730-po-delu-n-a07-129062015/> (дата обращения: 19.08.2025).

21. Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ // Собрание законодательства Российской Федерации от 2006 г., № 31, ст. 3451 (Часть I) (дата обращения: 19.08.2025).

22. Законопроект № 1173189-7 «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации». URL: <https://sozd.duma.gov.ru/bill/1173189-7> (дата обращения: 05.09.2025).

23. «Несколько положений Верховного народного суда о доказательствах в гражданском судопроизводстве» (вступил в силу 01.05.2020). URL: http://www.law-lib.com/law/law_view.asp?id=674942&page=3 (дата обращения: 05.09.2025).

А. М. Шамсутдинова,
студент,
Набережночелнинский филиал
Казанского инновационного университета
имени В. Г. Тимирязова

**Проблемы привлечения к административной ответственности
за оскорбление в мессенджерах с помощью голосовых сообщений:
вопросы квалификации и анализ практики**

Аннотация. В статье рассматриваются актуальные вопросы привлечения к административной ответственности за оскорбления, совершаемые посредством голосовых сообщений. Автор рассматривает проблемы квалификации оскорбительных высказываний. Проведен анализ правоприменительной практики и выявлены недостатки существующих норм законодательства. Автор указывает на необходимость разработки единой методики и стандартов для определения квалифицирующего состава по статье 5.61. Кодекса об административных правонарушениях.

Ключевые слова: административная ответственность, оскорбление, мессенджер, голосовое сообщение, проблемы квалификации, честь, достоинство, цифровое пространство, лингвистическая экспертиза

A. M. Shamsutdinova,
student,
Naberezhnochelny branch
Kazan Innovative University. V. G. Timiryasova

**Problems of bringing to administrative responsibility for insulting messengers
using voice messages: qualification issues and analysis of law practice**

Abstract. The article discusses current issues of bringing to administrative responsibility for insults committed through voice messages. The author considers the problems of qualification of offensive statements. An analysis of law enforcement practice has been carried out and the shortcomings of existing legislation have been identified. The author points out the need to develop a unified methodology and standards for determining the qualifying staff under Article 5.61 of the Code of Administrative Offences.

Keywords: administrative responsibility, insult, messenger, voice message, qualification problems, honor, dignity, digital space, linguistic expertise

Введение. Вербальная коммуникация между людьми использует широкий спектр демонстративных механизмов, в связи с чем, социальные сети и мессенджеры стали основными источниками общения. В условиях их стремительного

развития возникают новые вызовы для правовой системы государства. Указанные вызовы касаются в первую очередь защиты прав и свобод населения. Средства массовой информации стали распространенной платформой для коммуникации, используемой в качестве инструмента оскорбления. Оскорбления, совершаемые в том числе голосовыми сообщениями в мессенджерах, указывают на необходимость правильной классификации правонарушения.

Резкое увеличение количества пользователей мессенджеров создает пространство для минимизации социального контроля. Именно этот фактор приводит к частым случаям кибербуллинга, который проявляется в оскорблениях и унижениях. Нормативно-правовая база, регулирующая защиту прав личности в цифровом пространстве, нуждается в детальном изучении и актуализации. Данная необходимость связана с тем, что действующие нормы были приняты до широкого распространения сети Интернет и мобильных приложений. Весьма серьезными могут быть и социальные последствия оскорблений в мессенджерах.

В связи с вышеизложенным, появляется необходимость в исследовании правовых аспектов оскорблений, происходящих через голосовые сообщения. Такого рода исследования должны быть направлены на формирование более эффективной правовой защиты граждан и на разработку рекомендаций для совершенствования национального законодательства.

Основная часть. Необходимо ознакомиться с понятием «оскорбление». В соответствии со статьей 5.61. Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ) под данным термином понимается «унижение чести и достоинства другого лица, выраженное в неприличной или иной противоречащей общепринятым нормам морали и нравственности форме» [1]. С точки зрения законодателя оскорбление затрагивает личностные и социальные ценности каждого индивида, в частности. Основываясь на данном определении, защита чести и достоинства получает особую актуальность в современном цифровом пространстве. Важно отметить, что в данном определении учитываются как культурный, так и социальный контекст значения оскорбления. Законодательное закрепление такого понятия подчеркивает, что необходимо учитывать не только правовую, но и моральную составляющую. Как указывает В.С. Конюхова, «оскорбление по данной статье не будет считаться таковым, если высказано не в адрес конкретного лица либо лиц» [2. С. 669] Важно понимать, что не все высказывания, даже если они могут быть восприняты как оскорбительные, подлежат правовой оценке.

В закреплённом определении имеется широкое поле для субъективной оценки оскорбления, причем как с точки зрения инициатора оскорбления, так и его жертвы. Это означает, что один человек может считать определенное высказывание оскорбительным, в то время как другой – нет. Среди ключевых факторов, влияющих на восприятие выражений и высказываний, можно выделить:

- психологические факторы жертвы;
- ситуационные факторы;
- социальные факторы;
- территориальные и культурные факторы.

К первой группе факторов относятся, прежде всего, личностные характеристики жертвы, такие как самооценка, уровень чувствительности и эмоциональная восприимчивость. К этой группе можно также отнести прожитый жизненный опыт человека, эмоциональное состояние на момент получения голосового сообщения и психическое здоровье.

К факторам, характеризующим ситуацию, можно отнести контекст общения в конкретный момент и отношения между собеседниками в общем.

Социальные факторы представлены в первую очередь социальным статусом собеседников, их принадлежностью к определенной социальной группе, гендерными и возрастными различиями.

Разные культуры могут иметь различные представления о том, что считается оскорблением, именно поэтому необходимо выделять данный фактор. Географическое положение может влиять на восприятие оскорблений, например, диалекты, используемые в одном регионе, могут быть поняты иначе в другом.

Голосовые сообщения, в отличие от текстовых, несут в себе эмоциональную окраску. Необходимо учитывать, что восприятие оскорблений в голосовых сообщениях во многом зависит от интонации, тембра и эмоционального фона. В отличие от текстового контента, который можно легко зафиксировать, голосовые сообщения требуют внимательного анализа для установления контекста и эмоционального состояния сторон.

Такой субъективный подход приводит к проблемам в правоприменении. Правоохранительные органы могут испытывать трудности в оценке ситуации, поскольку для каждого конкретного случая необходимо учитывать обстоятельства и мнение обеих сторон.

Мировым судьей судебного участка № 2 г. Новотроицка было рассмотрено дело об административном правонарушении, предусмотренном ст. 5.61. ч. 1 КоАП РФ. Судом установлено, что гражданка оскорбила сестру своего супруга, отправив ей голосовое сообщение в мессенджере «WhatsApp». Данное сообщение содержало нецензурную брань и уничижительные высказывания, что явилось нарушением норм морали и унижением достоинства потерпевшей.

Женщина свою вину признала. Согласно материалам дела, она отправляла эти сообщения в состоянии сильного эмоционального волнения из-за конфликта. Потерпевшая настаивала на привлечении к ответственности обидчицы.

С учетом всех обстоятельств дела мировой судья постановил назначить женщине административный штраф в размере 3 000 рублей [3].

Как мы выяснили, за оскорбления, содержащихся в голосовых сообщениях, предусмотрена административная ответственность [4]. Однако действующие нормы не учитывают специфику такого общения. В отличие от письменных оскорблений, в голосовых сообщениях интонация, паузы и эмоции могут иметь иное значение. В связи с этим интерпретировать голосовые сообщения намного сложнее.

Важным инструментом в данной сфере выступает лингвистическая экспертиза. Она позволяет подробно проанализировать речевые единицы, которые используются в сообщении. Задачей лингвистической экспертизы является определить истинные намерения голосовых сообщений. Эксперты-лингвисты

проводят детальный анализ содержания голосовых сообщений. Цель их деятельности – выявить неприличные формы высказываний.

Для экспертов необходимо рассматривать все детали общения, в том числе контекст произнесенных оскорблений. Однако на практике лингвисты не обладают необходимым объемом информации, а получают только копию протокола судебного заседания. Они не имеют возможности оценить интонацию, тембр голоса, манеру речи – все самые необходимые элементы.

Важно отметить тот факт, что определенной методики выявления признаков оскорблений нет. С точки зрения права, использование неприличных форм высказываний рассматривается как нарушение норм коммуникации, а в дальнейшем и как основание для привлечения к административной ответственности.

Заключение. Таким образом, мы выявили особенности квалификации оскорблений в мессенджерах, содержащихся в голосовых сообщениях. В контексте голосовых сообщений правоприменителям необходимо учитывать не только лексическое содержание слов, но и контекст разговора, а также интонацию и эмоциональное состояние собеседников. Анализ правоприменительной практики показал, что суды сталкиваются с трудностями при квалификации оскорблений, происходящих в цифровой среде. Главной проблемой в этом плане является отсутствие единого подхода и методики оценки голосовых сообщений. В условиях разнообразия коммуникационных платформ недостаток четких критериев затрудняет процесс доказывания. В следствие это приводит к несоответствиям в судебной практике, поскольку одни и те же обстоятельства могут оцениваться по-разному в зависимости от субъективного восприятия судей. Итак, перед законодателем встает явная необходимость разработки стандартов отнесения голосовых сообщений к оскорблениям.

Список литературы

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 31.07.2025) (с изм. и доп., вступ. в силу с 06.09.2025) // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.
2. Конюхова В. С. Оскорбление как деструктивный тип поведения в социальных сетях // Молодежь, наука и цивилизация: материалы международной студенческой научной конференции, Красноярск, 18 мая 2023 года. Красноярск: Сибирский юридический институт МВД РФ, 2023. С. 668–672.
3. Архив Судебного участка № 2 мирового судьи города Новотроицка. URL: <https://nwtr2.kodms.ru>, свободный (дата обращения: 05.09.2025).
4. Обзор судебной практики Верховного Суда Российской Федерации № 2 (2021) (утв. Президиумом Верховного Суда РФ 30.06.2021) // Бюллетень Верховного Суда РФ. № 10. 2021.

А.Е. Шмелев,

студент,

Российский университет дружбы народов
имени Патриса Лумумбы**Интеграция цифровых платформ online dispute resolution (ODR)
в модель «суда с множеством дверей»: опыт зарубежных стран**

Аннотация. Статья анализирует интеграцию платформ онлайн-разрешения споров (ODR) в модель «суда с множеством дверей» на основе опыта Канады, ЕС, Сингапура, Бразилии и Великобритании. Рассмотрены правовые рамки, технологические решения и принципы внедрения: поэтапность, многоканальность, интеграция с существующими системами. Выявлены преимущества ODR для разгрузки судов и ускорения процедур, а также вызовы, связанные с использованием ИИ. Делается вывод о фундаментальной трансформации систем разрешения споров.

Ключевые слова: альтернативное разрешение споров, электронное правосудие, онлайн-разрешение споров, зарубежный опыт, цифровизация, суд со множеством дверей, доступ к правосудию

A.E. Shmelev,

Student,

RUDN University after Patrice Lumumba

**Integration of online dispute resolution (ODR) digital platforms
into the «multi-door courthouse» model: experience of foreign countries**

Abstract. The article analyzes the integration of Online Dispute Resolution (ODR) platforms into the multi-door courthouse model based on the experience of Canada, the EU, Singapore, Brazil, and the UK. The legal frameworks, technological solutions, and implementation principles such as a phased approach, multi-channel access, and integration with existing systems are examined. The advantages of ODR for reducing court workload and expediting procedures are identified, along with challenges associated with the use of artificial intelligence. The study concludes that a fundamental transformation of dispute resolution systems is underway.

Keywords: alternative dispute resolution, e-justice, online dispute resolution, international experience, digitalization, multi-door courthouse, access to justice

Введение. Концепция «суда с множеством дверей» (Multi-Door Courthouse), впервые предложенная американским юристом Фрэнком Сандерсом в 1976 году, представляет революционный подход к разрешению споров, при котором судебная система предоставляет различные альтернативные методы урегулирования споров под одной крышей. В современных условиях цифро-

вой трансформации правосудия интеграция платформ онлайн-разрешения споров (Online Dispute Resolution, ODR) в эту модель становится ключевым элементом обеспечения доступа к правосудию. Анализ зарубежного опыта показывает, что наиболее успешные примеры внедрения ODR демонстрируют Канада, Европейский Союз, Сингапур, Бразилия и Великобритания, каждый из которых представляет собой уникальные подходы к интеграции цифровых технологий в судебную систему [1].

Основная часть. Организация экономического сотрудничества и развития (ОЭСР) в своей Рамочной программе по ODR 2024 года определяет онлайн-разрешение споров как использование цифровых технологий и данных для поддержки урегулирования споров как в рамках, так и вне судебной системы [2]. Данная программа ОЭСР основывается на трех основных столпах: управление (governance), политические рычаги (policy levers) и этика и гарантии (ethics and safeguards). В контексте интеграции в модель множественных дверей особое значение приобретает первый столп, который подчеркивает необходимость стратегического подхода к разрешению споров для создания более экономически эффективной, оперативной системы, которая является гибкой и отвечает на развивающиеся потребности людей и организаций.

Канадская провинция Британская Колумбия стала пионером в области интеграции ODR в официальную судебную систему с созданием Трибунала гражданского разрешения (Civil Resolution Tribunal, CRT) в 2016 году. CRT представляет собой первый в Канаде онлайн-трибунал, созданный в соответствии с Законом о Трибунале разрешения гражданско-правовых споров (Civil Resolution Tribunal Act). Законодательство четко определяет задачи трибунала как предоставление услуг по разрешению споров «доступным, быстрым, экономичным, неформальным и гибким способом» с использованием «электронных коммуникационных инструментов для облегчения разрешения споров». Система CRT демонстрирует классическую модель суда со множеством дверей, предоставляя несколько стадий разрешения споров: обязательное использование онлайн-услуг ODR перед подачей формального запроса, стадию подготовки дела к разбирательству, и стадию слушания в трибунале, если соглашение не достигнуто. Особенностью канадской модели является принцип «от простого к сложному», при котором стороны сначала пытаются разрешить спор самостоятельно через онлайн-инструменты, затем получают помощь посредников, и только в случае неудачи переходят к формальному рассмотрению дела [3].

Европейский Союз реализовал масштабную инициативу по интеграции ODR через Регламент (ЕС) № 524/2013 об онлайн-разрешении споров потребителей. Данный регламент установил общеевропейскую ODR-платформу как «единую точку входа для потребителей и торговцев, стремящихся к внесудебному разрешению споров». Платформа функционирует как интерактивный веб-сайт, доступный бесплатно на всех официальных языках ЕС [4]. Европейская модель демонстрирует подход, где ODR-платформа служит координирующим механизмом, направляющим споры к аккредитованным национальным учреждениям альтернативного разрешения споров (ADR). Директива 2013/11/ЕС об альтернативном разрешении потребительских споров дополняет эту систему,

требуя от государств-членов обеспечить полное покрытие ODR-услуг во всех секторах [5]. Важной особенностью европейской модели является интеграция с существующими национальными системами ADR, что обеспечивает уважение к правовым традициям государств-членов при создании единообразного европейского подхода.

Сингапур представляет интегрированный подход к ODR через множественные институциональные каналы. Государственные суды Сингапура внедряют ODR-процедуры через специализированные трибуналы: Трибунал по малым искам (Small Claims Tribunal), Трибунал по разрешению общественных споров (Community Dispute Resolution Tribunal) и Трибунал по трудовым искам (Employment Claims Tribunal), все из которых функционируют в рамках Системы общественного правосудия и трибуналов (Community Justice and Tribunals System) [6]. Сингапурская модель характеризуется высокой степенью технологической интеграции, включая систему eLitigation для гражданских дел и Интегрированную систему управления делами (ICMS) для уголовных дел. Особенностью сингапурской системы является то, что ODR-процессы внедрены как в государственном секторе (судебная власть, аппарат правительства), так и среди поставщиков ADR по всему Сингапуру.

Бразилия демонстрирует уникальную модель интеграции ODR, сочетающую государственные и частные инициативы. Национальный совет правосудия Бразилии (CNJ) активно поощряет внедрение ODR с 2017 года и даже реализовал проект «100% цифрового судопроизводства». Государственный портал «Consumidor.gov» представляет собой онлайн-платформу, которая позволяет прямое общение между поставщиками и потребителями в попытке разрешить споры о защите прав потребителей онлайн. Бразильская модель характеризуется сильной правительственной поддержкой согласительных процедур, медиации, ODR и переговоров в попытке избежать судебных разбирательств [7]. Закон о медиации (Law № 13.140) и Гражданско-процессуальный кодекс Бразилии предусматривают медиацию как добровольную и частную процедуру [8].

Великобритания разрабатывает комплексную систему онлайн-процедурных правил через Комитет по правилам онлайн-процедур (Online Procedure Rule Committee), установленный в соответствии с Законом о судебном пересмотре и судах 2022 года [9]. Практические директивы 51R по цифровым гражданским денежным искам (Online Civil Money Claims) демонстрируют поэтапный подход к внедрению ODR, включающий медиацию, переговоры и подачу исковых заявлений онлайн. Британская система характеризуется принципом «удобства для всех», обеспечивающим доступность платформ для уязвимых пользователей [10].

Анализ международного опыта выявляет несколько ключевых принципов успешной интеграции ODR в модель суда со множеством дверей. Во-первых, поэтапный подход к внедрению, начиная со споров с малой ценой иска и постепенно расширяя юрисдикцию. Во-вторых, обеспечение множественных каналов доступа (omnichannel approach), позволяющего пользователям выбирать предпочтительный канал разрешения споров. В-третьих, интеграция с существующими ODR-механизмами и судебными системами для обеспечения перехода

информации и дел между различными механизмами разрешения споров. В-четвертых, установление четких правовых рамок и регулятивных механизмов для управления ODR и его реализацией.

Особое внимание заслуживает принцип технологической нейтральности, при котором ODR-платформы разрабатываются с учетом конфиденциальности пользователей с этапа проектирования (*privacy by design*) и доступности для всех, включая уязвимых пользователей (*design for all*). Европейский опыт показывает важность создания сети платформ ODR для поддержки сторон в разрешении споров, особенно в трансграничных спорах. Канадская модель демонстрирует эффективность обязательного использования ODR-услуг перед обращением к формальным процедурам, что способствует разгрузке судебной системы и ускорению разрешения споров.

Интеграция искусственного интеллекта и автоматизации в ODR-системы представляет следующий этап развития цифрового правосудия. Сингапурский опыт показывает потенциал использования ИИ-систем для анализа документов и оценки исходов споров. Однако это также поднимает вопросы о прозрачности, справедливости и равенстве в применении автоматизированных решений.

Заключение. Зарубежный опыт демонстрирует, что успешная интеграция ODR в модель множественных дверей требует комплексного подхода, включающего законодательные изменения, технологическую инфраструктуру, подготовку кадров и культурные трансформации в правовом сообществе. Наиболее эффективные системы характеризуются гибкостью, адаптивностью и постоянным совершенствованием на основе обратной связи пользователей и анализа эффективности. Интеграция цифровых платформ ODR в модель «суда со множеством дверей» представляет не просто технологическое обновление, а трансформацию подходов к разрешению споров, направленную на обеспечение более доступного, эффективного и ориентированного на пользователя правосудия.

Список литературы

1. Cashman P., Ginnivan E. Digital justice: online resolution of minor civil disputes and the use of digital technology in complex litigation and class actions // *Macquarie Law Journal* №4, 2019.
2. OECD Online Dispute Resolution Framework // OECD, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/oecd-online-dispute-resolution-framework_e88b6c6a/325e6edc-en.pdf (дата обращения: 05.09.2025).
3. “Civil Resolution Tribunal Act”, SBC 2012, с. 25 // King's Printer, Victoria, British Columbia, Canada. URL: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/12025_01 (дата обращения: 05.09.2025).
4. Регламент (ЕС) №524/2013 Европейского Парламента и Совета от 21 мая 2013 года относительно онлайн разрешения споров в сфере потребления, вносящая поправку в Регламент (ЕС) №2006/2004 и Директиву 2009/22/ЕС (Директива по ОПС в сфере потребления). URL: <https://base.garant.ru/70500878/?ysclid=mf9qtou99s622904301> (дата обращения: 05.09.2025).

5. Директива 2013/11/EU Европейского Парламента и Совета от 21 мая 2013 года относительно альтернативного разрешения споров в сфере потребления, вносящая поправку в Регламент (ЕС №2006/2004 и Директиву 2009/22/ЕС (Директива по APC в сфере потребления). URL: <https://base.garant.ru/70500878/?ysclid=mf9qtou99s622904301> (дата обращения: 05.09.2025).

6. Alexander N., Leu A. APEC's ODR Collaborative Framework, 2022. URL: https://www.academia.edu/95671171/APECs_ODR_Collaborative_Framework (дата обращения: 05.09.2025)

7. Sansone P., Rudzit A. Online dispute resolution and means of negotiation // Official cite of International Bar Association. URL: <https://iacajournal.org/articles/255/files/submission/proof/255-1-933-1-10-20180724.pdf> (дата обращения: 05.09.2025).

8. «Brazilian Mediation Act», Law № 13140, of june 26, 2015. URL: https://imimediation.org/wp-content/uploads/2017/09/Brazilian_Mediation_Act_English_Version_posted_on_IMI_Portal_10.8.15_.pdf?ysclid=mf9rolvtvg812751883 (дата обращения: 05.09.2025).

9. Judicial Review and Courts Act, 2022, с. 35. URL: <https://www.legislation.gov.uk/ukpga/2022/35/contents> (дата обращения: 05.09.2025)

10. Online Civil Money Claims pilot (PD 51R). URL: <https://www.justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-51r-online-court-pilot> (дата обращения: 05.09.2025).

Н. С. Яковлева,
магистрант,
Московский финансово-юридический университет

**Смарт-контракты в договоре поставки:
особенности правового регулирования и проблемы применения**

Аннотация. В статье исследуется юридическая природа применения смарт-контрактов в сфере договорных отношений, касаемых поставки товаров. Проводится анализ существующих доктринальных подходов к определению смарт-контракта, его соотношения с нормами гражданского законодательства о договоре поставки. Автором выявляются проблемы, связанные с имплементацией рассматриваемой технологии в коммерческий оборот, включая вопросы верификации качества поставляемого товара и определения оснований ответственности сторон договорных отношений. Формулируются выводы о необходимости детального правового регулирования инновационного института.

Ключевые слова: смарт-контракт, договор поставки, блокчейн, цифровизация, автоматизированное исполнение, смарт-договор, электронный документооборот

N.S. Yakovleva,
Master's student,
Moscow Finance and Law University

**Smart contracts in the supply contract:
features of legal regulation and application issues**

Abstract: The article explores the legal nature of the application of smart contracts in the field of contractual relations related to the supply of goods. It analyzes existing doctrinal approaches to the definition of a smart contract and its relationship with the norms of civil law on the supply contract. The author identifies the challenges associated with the implementation of this technology in commercial transactions, including the verification of the quality of the supplied goods and the determination of the grounds and limits of liability for the parties to the contractual relations. The article concludes that there is a need for detailed legal regulation of this innovative institution.

Keywords: smart contract, supply agreement, digitalization, blockchain, automated execution, smart contract, electronic document management

Введение. Цифровизация экономики, определенная в качестве одного из стратегических векторов развития Российской Федерации, ставит перед правовой системой задачу адаптации традиционных регуляторных механизмов к новым технологическим реалиям [5]. Особый интерес в этом контексте представ-

ляет договор поставки, который в силу своей логистической сложности и многоэтапности исполнения сопряжен со значительными транзакционными издержками. Технологии распределенных реестров (далее по тексту – блокчейн) и функционирующие на их основе смарт-контракты открывают новые возможности для оптимизации договорных правоотношений.

Основная часть. Ключевые преимущества использования таких контрактов заключаются в снижении издержек за счет автоматизации рутинных операций, устранении посредников и повышении прозрачности всего процесса поставки [8. С. 78]. Гарантированное исполнение программного кода минимизирует риски недобросовестного поведения контрагентов, что, в свою очередь, делает внедрение смарт-контрактов закономерным и перспективным направлением повышения эффективности коммерческого оборота.

При этом, несмотря на активное обсуждение, легальное определение смарт-контракта в российском праве до сих пор отсутствует. Тем не менее, действующее законодательство создает предпосылки для его имплементации. Так, исходя из ст. 160 Гражданского кодекса Российской Федерации (далее – ГК РФ), допускается совершение сделок с помощью технических средств. В ст. 309 ГК РФ презюмируется право сторон договорных отношений автоматизировать исполнение обязательств. Кроме того, в ч. 2 данной статьи законодатель указывает, что возможно и автоматическое исполнение обязательств без необходимости выражать каждый раз волю на исполнение, если это будет предусмотрено договором.

В современной цивилистической доктрине отсутствует единая концепция к определению правовой природы смарт-контракта.

Так, согласно технократическому подходу, смарт-контракт должен определяться прежде всего техническими характеристиками. В частности, Н. Сабо охарактеризовал его как «компьютеризированный протокол транзакций, который выполняет условия договора» [3. С. 57]. В рамках данного подхода смарт-контракт рассматривается как электронный алгоритм, запрограммированный на совершение определенных действий при наступлении заданных условий [4. С. 164]. Посредством такого толкования авторы акцентируют внимание на автоматизации процесса, однако подобная интерпретация полностью игнорирует волевой аспект, присущий любому договору как соглашению сторон.

Юридический подход более многогранен. Одни исследователи, как, например, А.И. Савельев, рассматривают смарт-контракт как полноценный договор, существующий в особой электронной форме [6]. Другие, в частности Д.С. Дядькин, Ю.М. Усольцев и Н.А. Усольцева, предлагают квалифицировать его как форму договора или способ обеспечения исполнения обязательств, поскольку он гарантирует неотвратимость расчетов [1. С. 2].

Наиболее взвешенной представляется позиция, рассматривающая смарт-контракт не как обособленный вид договора, а как особую договорную конструкцию, сочетающую в себе элементы различных правовых институтов. Так, Е.В. Зайнутдинова определяет его как «договор, заключаемый в децентрализованной распределенной информационной системе, предусматривающий автоматизированное исполнение обязательств и опосредующий оборот цифровых прав

и цифровой валюты» [7. С. 18]. Данный подход позволяет учесть как волевою (соглашение сторон), так и техническую (программный код) составляющие смарт-контракта, в связи с чем такая концепция представляется наиболее обоснованной.

Использование смарт-контрактов при осуществлении договора поставки имеет ряд существенных преимуществ. Как справедливо отмечает Е.М. Шапкина, автоматическое исполнение обязательств при достижении предусмотренных договором условий и обеспечение конфиденциальности взаимодействующих сторон являются значимыми достоинствами рассматриваемых соглашений [8. С. 42]. В правовой доктрине обоснованно акцентируется внимание на тот факт, что при анализе вопроса легитимации смарт-контрактов необходимо учитывать фактор сокращения транзакционных издержек посредством исключения институтов-посредников (например, банков) [1. С. 3].

Однако при практической реализации смарт-контрактов в правоотношениях по поставке товаров наличествует ряд системных проблем, требующих правового решения.

Во-первых, нередко возникает проблема верификации физических характеристик товара. Смарт-контракт как программа не способен самостоятельно оценить качество, количество и ассортимент поставляемых материальных объектов. Для связи между физическим миром и цифровым кодом необходимы «оракулы» – доверенные внешние источники данных. В контексте поставок в их роли могут выступать автоматизированные системы (сканеры на складе), независимые экспертные организации (сюрвейерские компании) или государственные органы (таможня).

Оракул поставляет в блокчейн данные (например, «товар соответствует спецификации»), которые, при условии соответствия договору, служат отправной точкой для исполнения смарт-контракта. Так, оракул может внести данные о текущем курсе валют для автоматического исполнения условий договора [9. С. 85].

Правовая проблема заключается в отсутствии законодательного регулирования деятельности и ответственности оракулов. Зависимость реализации смарт-договора от действий оракулов вводит в автоматизированную систему элемент риска, связанный как с человеческим фактором, так и техническим сбоем. Так, ошибка, допущенная в коде договора, может являться как результатом деятельности человека, так и негативным влиянием скачков напряжения, однако в любом случае такая ошибка потенциально влияет на все операции, осуществляемые посредством контракта, а не на отдельные транзакции, то есть масштаб ущерба в таком случае значительно возрастает [10. С. 12].

Во-вторых, остро стоит проблема неизменности (ригидности) смарт-контракта. Классическая форма договора поставки традиционно предполагает его гибкость: стороны могут согласовать отсрочку, изменить график поставок или приостановить исполнение обязательств из-за наступления обстоятельств непреодолимой силы. Однако адаптировать условия, предусмотренные смарт-контрактом, под обстоятельства будет невозможно.

Невозможность одностороннего изменения кода после его запуска в блокчейн делает затруднительным учет непредвиденных обстоятельств. Как справедливо отмечают исследователи, данная проблема ярко проявляется, например, при уступке права требования (цессии): смарт-контракт, следуя исходному алгоритму, продолжит исполнение в пользу первоначального кредитора, что приведет к его неосновательному обогащению [2. С. 95].

Кроме того, возникают сложности при возникновении обстоятельств непреодолимой силы, связанные с тем, что смарт-договор является автоматизированной системой и санкции будут применяться к другой стороне отношений автоматически при наступлении формальных условий (например, просрочки). Указанная программная детерминированность вступает в противоречие с п. 3 ст. 401 ГК РФ, устанавливающим, что сторона, доказавшая, что не исполнила или ненадлежаще исполнила обязательства вследствие наступления обстоятельств непреодолимой силы, освобождается от ответственности.

Таким образом, механизм автоматизированного исполнения пока не способен в полной мере учитывать форс-мажорные обстоятельства, что требует совершенствования его адаптационных функций.

Заключение. Следует признать, что смарт-контракты являются инновационным и перспективным инструментом для оптимизации договорных отношений в сфере поставки. Их внедрение способно существенно снизить трансакционные издержки, минимизировать риски неисполнения и повысить прозрачность коммерческого оборота.

Однако для полномасштабной и безопасной реализации этого потенциала необходимо создание комплексной нормативно-правовой базы. Ключевыми направлениями законодательной работы должны стать:

1) разработка системы регулирования деятельности «оракулов» с установлением четких критериев к их лицензированию и введением механизмов ответственности за предоставление недостоверных данных, повлекших неправомерное исполнение (или неисполнение) договора;

2) создание правовых механизмов гибкости смарт-контрактов, позволяющих приостанавливать или изменять их исполнение при наступлении экстраординарных обстоятельств (форс-мажор, существенное изменение обстоятельств), а также по взаимному соглашению сторон, подтвержденному электронными цифровыми подписями.

Список литературы

1. Дядькин Д.С., Усольцев Ю.М., Усольцева Н.А. Смарт-контракты в России: перспективы законодательного регулирования // *Universum: Экономика и юриспруденция*. 2018. № 5(50). С. 1–4.

2. Ефимова Л.Г., Михеева И.В., Чуб Д.В. Сравнительный анализ доктринальных концепций правового регулирования смарт-контрактов в России и в зарубежных странах // *Право. Журнал Высшей школы экономики*. 2020. № 4. С. 78–105.

3. Лукоянов Н.В. Legal tech: смарт-контракты сквозь призму современного частного права // Юридические исследования. 2018. № 7. С. 56–62.
4. Новиков Р.В. К вопросу о понятии и сфере применения смарт-контрактов // Новиков Р. В. К вопросу о понятии и сфере применения смарт-контрактов // Пермский юридический альманах. 2019. № 2. С. 431–440.
5. Об утверждении программы «Цифровая экономика Российской Федерации»: Распоряжение Правительства РФ от 28.07.2017 № 1632-р // Собрание законодательства РФ. 2017. № 32. Ст. 5138.
6. Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.
7. Зайнутдинова Е.В. Смарт-контракт в гражданском праве: автореф. дис. ... канд. юрид. наук. Красноярск, 2022. 25 с.
8. Шапкина Е.М. Смарт-контракты: возможны в современной России и надежны ли? // Актуальные вопросы права, экономики и управления: XX Международная научная конференция. 2018. С. 41–43.
9. De Filippi P., Wright A. Blockchain and the Law: The Rule of Code // Harvard University Press. 2018. 310 p.
10. Papantoniou A. Smart contracts in the new era of contract law // Digital Law Journal. 2020. Vol. 1. № 4. P. 8–24. <https://doi.org/10.38044/2686-9136-2020-1-4-8-2>

Ю. В. Пантазий,
курсант,
Санкт-Петербургский университет ГПС МЧС России

Криптовалюта: правовое положение и перспективы распространения

Аннотация. В данной статье рассмотрено правовое положение криптовалюты, как в России, так и за рубежом. Дано определение криптовалюте в рамках законодательства, а также рассмотрены основные проблемы, связанные с цифровыми деньгами и предложены пути решения для окончательного внедрения данного феномена в России.

Ключевые слова: криптовалюта, цифровой обмен, частные деньги, правовое регулирование

J. V. Pantazy,
3rd year student of the Faculty of Economics and Law,
St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia

Cryptocurrency: legal status and prospects for distribution

Abstract. This article examines the basic provisions of cryptocurrency, both in Russia and abroad. It provides a definition of cryptocurrency within the framework of legislation, and also examines the main problems associated with digital money and proposes solutions for the final implementation of this phenomenon in Russia.

Keywords: cryptocurrency, digital exchange, private money, legal regulation

Введение. В современном мире криптовалюта незаметно вошла в нашу жизнь и стала неотъемлемой частью жизни современных людей. За последние несколько лет рынок криптовалют в мире вырос в десятки раз, так с 1 января 2024 года по 1 января 2025 года общая рыночная капитализация выросла с \$1,65 трлн до \$3,28 трлн. И в связи с этим актуальным становится вопрос о правовом регулировании отношений, которые возникают с ее использованием и квалификации в качестве объекта гражданских правоотношений. Следовательно, необходим пересмотр классических подходов к финансовому регулированию, а также нормативному закреплению криптовалюты и операций, связанных с ней.

Главной целью исследования – является сравнение подходов по определению термина «криптовалюта», рассмотрению методов к правовому регулированию данного феномена за рубежом, а также выдвинуть предложение основных способов к закреплению защиты прав участников сделок, связанных с незаконным отмыванием денег или оплатой цифровой валюты преступных сделок и установить налоги для держателей криптобирж.

Основная часть. Как указывается в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»: цифровая валюта – это совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе [1].

Криптовалюта по своему определению является видом электронных финансов, которые используются в качестве альтернативной меры платежа. По общему правилу принято разделять криптовалюты на два вида. Первый тип характеризуется привязкой к официальным государственным валютам или к драгоценным металлам. Примером подобного понимания и реализации криптовалюты является WebMoneyTransfer. Он квалифицируется как электронная система расчетов, предполагающая процесс трансфера имущественных прав, а также их учета посредством специальных расчетных единиц. При этом, единицы учета номинируются в привязке к конкретным национальным валютам и к драгоценным металлам. Второй вид восприятия – криптоденьги. Он реализуется как цифровая валюта, связанная с учетом внутренних расчетных единиц. Что при определенных обстоятельствах обеспечивает создание и работу децентрализованных платежных систем [3].

Е. М. Андреева описывает криптовалюту как цифровой феномен современной экономики [4]. Целесообразность в разработке правовых механизмов обусловлена стремительным развитием и распространением криптовалют. Подобные правовые разработки должны быть направлены, в первую очередь, на гарантию защиты прав всех заинтересованных сторон и снижению рисков.

Из приведенных выше определений видно, что одно определение на законодательном уровне показывает нам криптовалюту как цифровые данные, а в другое определение относят к источнику денег. В связи с этим возникают трудности по правовому пониманию этого феномена: это деньги или просто данные?

Криптовалюта, в наш мир, вошла относительно недавно, но правовые споры вокруг нее только набирают обороты. Издание статьи С. Накамото под названием «Peer-to-PeerElectronicCashSystem» стало революционным для 2008 года. Мнение программиста о системах онлайн-обмена, предполагающей полноценное шифрование и осуществление процесса обмена индивидуальными расходами между сторонами, несло в себе ключевое значение для отрасли. Немаловажным фактором была и защита личной информации о себе и своих финансовых счетах.

Система Накамото была предназначена не только для банковских структур, но и для пользователей. Она уравнивала разных исполнителей платежей, позволяя им отправлять транзакции цифровых денег [11]. Также система оказывала большое влияние на неподвижность в банках или компаниях, по сути, она должна была исчезнуть при условии выпуска кредитных карт. Это также ограничивало участие сторонних платежных провайдеров или третьих сторон в биржах. Другими словами, так формировалась форма цифровой наличности.

Изначально, большинство стран с опаской относились к цифровому обмену, но с учетом большого роста транзакций и операций с криптовалютами возникла целесообразность в правовом закреплении этого феномена.

Так, многие авторы отмечают разнообразные подходы различных государств к вопросу правового положения криптовалюты [10]. Например, в Китае установлены ограничения на пользование криптовалютой, а вот Япония, наоборот, поддерживает новую тенденцию и создает все условия для развития криптоиндустрии [8]. В этой стране биткоин выступает носителем стоимости и приравнивается к активу.

Болгария еще в 2014 году легитимизировала биткоин и приравнила криптовалюту к финансовым активам, но условием пользования цифровой валютой является уплата налога в 10% от продаж. К примеру, в Германии криптовалюта приравнена к частным деньгам, но пользоваться разрешается на официальном уровне [6]. Как можно заметить из приведенных выше примеров большинство стран создали предпосылки к легитимизации использования криптовалюты.

Российская Федерация на современном этапе входит в этап принятия крипто индустрии, но есть ряд спорных моментов. В 2017 году возникли первые обсуждения об этом Центральный банк (далее – ЦБ) одновременно с другими государственными органами начали рассматривать вероятность установления ряда ограничений на все проводимые операции, связанные с криптовалютой [7].

Главным нормативно-правовым актом (далее – НПА), который закрепил правовой статус биткоина стал принятый в 2021 году Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах» [1]. Данный НПА ввел понятие «цифровые валюты». Также федеральным законом дополнительно утверждались правила выпуска и обращения цифровых активов, определялись требования к операторам информационных систем, отвечающих за выпуск и обращение цифровых финансовых активов (далее – ЦФА). Основным требованием было получение лицензии ЦБ и соблюдение ряда требований, обращенных на предотвращение незаконной деятельности.

Указания ЦБ, обращенные к физическим и юридическим лицам, имеют и свои особенности. Так, в одной из рекомендаций указываются требования по аккуратности использования криптовалюты в банковских операциях при обслуживании клиентов.

В дополнение, стоит упомянуть, Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [2], касающийся вопросов противодействия использованию криптовалют в незаконных целях.

Наличие широкого спектра возможностей криптовалюты не отменяет факта наличия и перечня недостатков. Все еще отсутствует четкое определение термина данного феномена как «криптовалюта». Терминологический словарь разных государственных органов имеет и разное определение биткоина, что в свою очередь приводит к затруднительному применению [5].

Также Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» устанавливает ограниченное использование криптовалюты в системе средств платежей. Кроме того, существует проблема недостаточной защиты прав потребителей, поскольку права участ-

ников сделок, которые связаны с криптовалютой, слабо защищены и зачастую криптовалюта выступает средством оплаты «преступных сделок».

В силу того, что операции с криптовалютой полны рисков и обманных схем и неконтролируемая реклама, связанная с ней, могут приводить к мошенническим сделкам 19 августа 2024 г. была внесена поправка о запрете криптовалюты неограниченному кругу лиц. Так, в статье говорится: «Теперь в России запрещена реклама цифровой валюты. Распространение информации о криптовалюте пресекалось и раньше. Однако осуществлялось это в судебном порядке по требованию прокуратуры о признании незаконным распространения в России информации об использовании цифровой валюты в качестве платежного средства» [14]. Но возможно, что полный запрет рекламы не будет особо эффективен, поскольку информационное пространство довольно сложно контролировать и реклама все же будет процветать, только в другом контексте и более завуалировано, а также рекламный запрет способен к ограниченному распространению и развитию узаконенного крипторынка.

Возвращаясь к проблеме криптовалюты как предмету «преступных сделок», приведем пример дела второго Западного окружного военного суда, где были осуждены бывшие следователи за вымогательство миллиона долларов в криптовалюте. Осужденные получили взятки в виде криптовалюты. При этом ст. 81 УПК РФ и ст. 104¹ УК РФ регламентируют конфискацию имущества, нажитого преступным путем [12]. Однако практическое применение конфискации криптовалюты сталкивается с трудностями, поскольку у государства отсутствует механизм прямого доступа к цифровым кошелькам.

Вопрос реализации изъятого имущества в таких случаях остается открытым. Одним из его решений является продажа носителя с кодом доступа на торгах, с последующим зачислением выручки в пользу государства. Иной способ сводится к передаче прав требования в пользу третьего лица с правом реализации на криптобирже.

Как следствие успешная конфискация криптовалюты остается связана с такими сложностями как дальнейшая законодательная проработка. При этом, законодателю будет необходимо учесть специфику уголовного и гражданского судопроизводства.

Заключение. Таким образом, из вышеизложенного видно, что регулирование криптовалюты правовыми методами в России на современном этапе остановилось на этапе формирования. Наличие сформированной нормативной базы пока еще не решает все спорные вопросы.

Полномасштабное внедрение криптовалюты в экономику России возможно лишь при развитии законодательства. Исключительно после закрепления криптовалюты в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» в качестве цифровых денег, а не цифровых данных позволит рассматривать экономическое развитие страны. Также, для совершенствования экономических процессов необходимо принять во внимание зарубежный опыт по официальному закреплению «феномена крипто-

валюта». Особенности российского рынка разительно отличаются, что также может усложнить процесс.

Помимо указанного, большое внимание должно быть уделено ответственности за нарушения, связанные с криптовалютой. Дополнительным рычагом воздействия и урегулирования станет выработка мер по борьбе с незаконным отмыванием денег [8]. Механизм введения уголовной или административной ответственности за применение криптовалюты в «преступных сделках» в дополнение ко всему станет подспорьем для развития финансово-правовой базы. Указанные методы станут базой для безопасного и эффективного внедрения и использования цифровых активов.

Список литературы

1. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/
2. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации от 15 мая 2017 г. № 20. Ст. 2901.
3. Официальный сайт Международной системы расчетов и среда для ведения бизнеса в сети «WebMoneyTransfer». Текст: электронный. URL: <https://www.webmoney.ru/>
4. Андреева Е.М. Модель правового регулирования криптовалют в Российской Федерации // Ленинградский юридический журнал. 2022. №2 (68). С. 61–74.
5. Гизатулин И.Ю. Правовое регулирование криптовалют // Юридические науки. International Journal of Humanities and Natural Sciences. 2025. Т. 2–1 (101). С.258–261.
6. Гордеева О. Регулирование криптовалют в разных странах. URL: <https://vc.ru/crypto/32207-regulirovanie-kriptovalyut-v-raznyh-stranah>.
7. Доклад для общественных консультаций «Криптовалюты: тренды, риски, меры». Официальный сайт Центрального Банка – Банка России. URL: http://www.cbr.ru/content/document/file/132241/consultation_paper_20012022.pdf
8. Зыкова Т.А. Практика применения криптовалют зарубежных стран // Юридические науки // International Journal of Humanities and Natural Sciences. 2020. №. 4–2 (43). С.162–168.
9. Камышанова А.Е., Брилева А.Д. Правовое регулирование криптовалюты в России: проблемы и перспективы // Гражданское право; предпринимательское право; семейное право; международное частное право. 2022. № 4 (208). С.121–123.
10. Ляшенко М.С., Андреева О.А. Теоретические методы правового регулирования цифровых финансовых валют (криптовалюты) в Российской Федерации // Вестник науки. 2024. №1 (70). С. 294–304.

11. Меликов У.А. Криптовалюта в системе объектов гражданских прав // Вестник ЮУрГУ. Серия: Право. 2019. №1. С. 60–66.

12. Планов А.С. Криптовалюты: проблемы и возможности / СКИФ: вопросы студенческой науки. 2023. №1 (77). С. 209–213.

13. Постановление Девятого арбитражного апелляционного суда от 15.05.2020 № 09АП-16416/2020 по делу № А40-124668/2020. URL: https://storage.consultant.ru/ondb/attachments/201805/u/usukgz7wdco3d_sa/Postanovlenie_suda_JWj.pdf (дата обращения 24.08.2025).

14. Скан О. Криптовалюта выходит из тени. Как меняется правовое регулирование цифровых денег (от 09.10.2024) // Информационно-правовой канал Гарант.ру. URL: <https://w.garant.ru/article/1759006/> (дата обращения: 24.08.2025).