Как цитировать: Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 424 с. EDN: YKIPUU. DOI: http://dx.doi.org/10.21202/978-5-8399-0816-1_3_424

For citation: Digital Technologies and Law: collection of scientific articles of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 424 p. EDN: YKIPUU. DOI: http://dx.doi.org/10.21202/978-5-8399-0816-1_3_424

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 3

Казань ■ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2023

DIGITAL TECHNOLOGIES AND LAW

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

2023, September 22
Kazan

In 6 volumes
Volume 3

Kazan ■ KIU "POZNANIYE" PUBLISHERS ■ 2023

УДК 004:34(063)
ББК 67с51я43
Ц75

Печатается по решению редакционно-издательского совета
Казанского инновационного университета имени В. Г. Тимирясова

Ц75 **Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции** (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 424 с. EDN: YKIPUU. DOI: http://dx.doi.org/10.21202/978-5-8399-0816-1_424.
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0816-1 (Том 3)

Вошедшие в сборник научные труды приурочены к II Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 22 сентября в Казани в рамках Международного форума Kazan Digital Week 2023, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

Широкий круг рассмотренных на конференции теоретико-методологических и практико-ориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, нормативным регулированием цифровой среды, перспективами правового воздействия на формирующиеся и новые общественные отношения, когнитивно-поведенческие паттерны в условиях цифровизации и алгоритмизации социального программирования, автоматизированного принятия правовых решений операционно-интеллектуальными системами, доминирования цифровых платформ на цифровом рынке, технологических инноваций и многое другое.

Научные труды представленного тома отражают взгляды и подходы, формируемые в молодежной – преимущественно студенческой – среде, в которой заметно возрастает исследовательский интерес к современным вопросам развития цифровых технологий в системе правовых отношений.

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 достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0816-1 (Том 3)

UDC 004:34(063)
LBC 67с51я43

Published by the decision of the Editorial-Publishing Board
of Kazan Innovative University named after V. G. Timiryasov

Digital Technologies and Law: collection of scientific papers of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 3. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 424 p. EDN: YKIPUU. DOI: http://dx.doi.org/10.21202/978-5-8399-0816-1_424
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0816-1 (Vol. 3)

The scientific works included in the collection are timed to coincide with the II International Scientific and Practical Conference "Digital Technologies and Law", held on September 22 in Kazan as part of the International Forum "Kazan Digital Week 2023", organized by the Government of the Russian Federation jointly with the Cabinet of Ministers of the Republic of Tatarstan.

A wide range of theoretical, methodological and practice-oriented, interdisciplinary and sectoral issues discussed at the conference are related to the priorities of the legal development of digital technologies, regulatory regulation of the digital environment, prospects for legal influence on emerging and new social relations, cognitive-behavioral patterns in the context of digitalization and algorithmization of social programming, automated legal decision-making by operational-intelligent systems, the dominance of digital platforms in the digital market, technological innovation and much more.

The research works included in this volume reflect the attitudes and approaches forming among the youth, mainly students, under the significantly increasing academic interest in the modern issues of the development of digital technologies within the legal relations system.

The ideas and proposals reflected in the multi-volume publication in their entirety 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, representatives of law-making and law enforcement bodies, government officials and participants in the real sector of the economy, including developers and manufacturers of products of digital technology achievements, young student researchers, undergraduates and graduate students, everyone interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67с51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0816-1 (Vol. 3)

А. Ю. Абабкова,
студент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ МЕДИЦИНСКИХ РАБОТНИКОВ: КОНКУРЕНЦИЯ НОРМ И СУДЕБНАЯ ПРАКТИКА

Аннотация. В статье анализируется актуальная в судебной практике проблема защиты персональных данных медицинских работников, которые распространяются в отзывах пациентов в сети Интернет. Сложность данного вопроса обусловлена конкуренцией норм, регламентирующих право средств массовой информации на получение и распространение информации и право граждан на неприкосновенность частной жизни. Предлагаются критерии допустимости вмешательства средств массовой информации в частную жизнь граждан, которыми нужно руководствоваться при рассмотрении такой категории споров.

Ключевые слова: персональные данные, защита персональных данных, субъект персональных данных, общественный интерес, обработка персональных данных, общедоступные персональные данные

PROTECTION OF PERSONAL DATA OF MEDICAL WORKERS: COMPETITION OF STANDARDS AND JUDICIAL PRACTICE

Abstract. This article analyzes the actual problem in judicial practice of protecting the personal information of medical workers, which are distributed in patient reviews on the Internet. The complexity of this issue is due to the competition of norms regulating the right of the media to receive and disseminate information and the right of citizens to protect their privacy. The article proposes criteria of the permissibility of media interference in the private life of people, which should be guided when considering such a category of disputes.

Keywords: personal information, protection of personal information, subject of personal information, public interest, processing of personal information, publicly available personal information

В соответствии со ст. 152 ГК РФ лицо, в отношении которого в сети Интернет распространены порочащие сведения, вправе требовать их удаления и опровержения. Такими способами защиты чести и деловой репутации могут воспользоваться и медицинские работники в случае, когда на сайтах в сети Интернет, предназначенных для оставления пациентами отзывов об оказанных им медицинских услугах, о профессиональной деятельности врачей, пациенты размещают не соответствующую действительности информацию.

Право на защиту персональных данных медицинских работников как информации об их частной жизни гарантировано Конституцией РФ. Аналогичная ситуация складывается с биометрическими данными [6] и с распространением заведомо ложных сведений [7]. Однако сведения о качестве оказанных медицинских услуг имеют общественное значение, размещение отзывов о профессиональной деятельности врачей необходимо тем лицам, которые нуждаются в услугах высококвалифицированных врачей данной специальности, поэтому само по себе распространение данной информации на сайтах в сети Интернет не является нарушением прав субъекта персональных данных. Владелец сайта в сети Интернет вправе не удалять отрицательный отзыв пациента об оказанных последнему медицинских услугах, и при этом обрабатывать общедоступные персональные данные врача без согласия последнего [5].

Если данный сайт представляет собой средство массовой информации, его администратор может осуществлять обработку общедоступных персональных данных без согласия медицинских работников, при этом сохраняется право последних на опровержение данной информации, если она противоречит действительности. В противном случае удовлетворение исковых требований медицинских работников об удалении отзыва в сети Интернет приведет к нарушению права средств массовой информации (далее – СМИ) на доведение информации до заинтересованных лиц. Частью 3 ст. 9 Федерального закона «О персональных данных» предусмотрена обязанность оператора доказать факт получения согласия субъекта на обработку его персональных данных. Согласно ст. 7 данного закона, оператор не вправе распространять персональные данные лица без его согласия. Однако в соответствии со ст. 6 допускается обработка персональных данных лица в целях осуществления профессиональной деятельности СМИ, если это не нарушает права субъекта персональных данных. Данный вопрос разъясняется в Постановлении Пленума Верховного Суда РФ от 15.06.2010 № 16 «О практике применения судами Закона Российской Федерации “О средствах массовой информации”». В п. 5 ч. 1 ст. 49 данного закона запрещается обработка, распространение без согласия лица информации о его личной жизни, за исключением случая, если это необходимо для реализации общественных интересов.

Понятие «общественный интерес» разъясняется в п. 25 Постановления Пленума ВС РФ от 15.06.2010 № 16, исходя из которого можно полагать, что, поскольку медицинский работник осуществляет публичную деятельность, СМИ должно предоставлять гражданам информацию по вопросам осуществления медицинской деятельности. Поскольку вопрос качества оказываемой медицинской помощи затрагивает интересы неопределенного круга лиц, распространение

персональных данных врачей необходимо для удовлетворения потребности пациентов в получении информации о профессиональной компетентности медицинских работников. Жизнь и здоровье человека – ценности, охраняемые Конституцией РФ, поэтому информация о качестве оказываемой данным медицинским работником помощи представляет собой общественный интерес [3. С. 107–110].

Данный вопрос также регламентируется п. 7 ч. 1 ст. 79 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», в соответствии с которым граждане вправе получать информацию о медицинской деятельности, квалификации врачей. Поскольку данной нормой предусмотрена обязанность размещать сведения о медицинских работниках на сайтах медицинских учреждений, следовательно, они являются общедоступными, субъект персональных данных предоставляет персональные данные своему работодателю – медицинской организации. Пунктом 4 ч. 4 ст. 22 ФЗ «О персональных данных» регламентировано право оператора на обработку общедоступных персональных данных лица без согласия органа по защите прав субъекта персональных данных. Таким образом, в отзывах пациентов содержатся персональные данные медицинских работников, которые размещаются на сайтах медицинских организаций и являются общедоступными. Право граждан на получение информации о конкретном лице, оказывающем услугу, также предусмотрено п. 2 ст. 10 Закона РФ «О защите прав потребителей», сведения о медицинском работнике являются существенными для пациента. Следовательно, распространение медицинской организацией и в последующем пациентами в оставляемых на сайтах в сети Интернет отзывах персональных данных медицинских работников, являющихся общедоступными, не противоречит нормам российского законодательства [2].

Необходимо также рассмотреть вопрос о том, насколько законно размещение в сети Интернет отзывов пациентов о профессиональной деятельности медицинских работников. Поскольку право на распространение информации гарантировано ст. 29 Конституции РФ, пациент вправе выражать субъективное мнение о качестве оказываемой медицинской помощи и квалификации медицинских работников. При этом у врача есть право на опровержение данной информации.

Рассматриваемая в настоящей статье проблема, связанная с распространением в отзывах пациентов персональных данных медицинских работников, коррелирует с правом врача на неприкосновенность его частной жизни. Таким образом, в данных отношениях проявляется конкуренция норм, регламентирующих право СМИ на получение и распространение информации, содержащей персональные данные медицинских работников, право граждан на получение информации о медицинской деятельности, квалификации врачей и норм, которые закрепляют право граждан на охрану частной жизни. Согласно Определению КС РФ № 248-О от 9 июня 2005 г., право на неприкосновенность частной жизни означает в том числе гарантированную государством возможность осуществлять контроль над распространяемой о гражданине информации. Существует очень тонкая грань между данными конкурирующими нормами, и СМИ, реализуя свое право на получение и распространение общедоступных персональных данных медицинских работников, которые ранее были размещены медицинской организацией,

должны соблюдать право врачей на неприкосновенность и защиту частной жизни. Необходимо установить баланс между данными правами, в силу этого нужно выделить критерии, определяющие пределы права СМИ на вмешательство в жизнь медицинских работников. К таким критериям следует отнести определение, каково значение данных сведений при рассмотрении значимых для общества вопросов, степень известности лица, персональные данные которого распространяются на сайтах в сети Интернет, содержание, предмет и достоверность размещенной информации.

Обязанность государства по контролю качества медицинской помощи и доступности информации об этом, в том числе обязанность медицинских учреждений публиковать информацию о врачах, не исключают потребность общества в обсуждении в СМИ данных вопросов, в опубликовании отзывов о квалификации медицинских работников. Но необходимо соотносить объем, способ получения и размещения данных сведений с правом гражданина на защиту его частной жизни. Суды при рассмотрении исковых заявлений медицинских работников по данной категории споров должны обращать внимание на следующие вопросы: представляет ли обсуждение профессиональной деятельности конкретного медицинского работника общественный интерес, является ли врач «публичным лицом», т. е. лицом, которое играет важную роль в общественной жизни. Закон об основах охраны здоровья граждан РФ регламентирует обязанность размещать на сайте медицинского учреждения список врачей, которые работают в нем. Данное положение закона преследует цель, заключающуюся не в оценке профессионализма конкретного медицинского работника, а в оценке качества условий оказания медицинской помощи в целом данной организацией здравоохранения.

Это положение должно учитываться судами при рассмотрении такой категории дел. Баланс между правом пациентов на оставление отзывов, представляющих собой общественный интерес, и правом медицинского работника на защиту его частной жизни будет достигаться в том случае, если в отзывах будут обсуждаться условия оказания помощи медицинским учреждением, а не предлагаться персональная оценка конкретного медицинского работника.

Кроме того, суды должны обращать внимание на то, имелась ли у медицинского работника возможность защиты своего права. Зачастую оставляемые в сети Интернет отзывы пациентов являются анонимными, в связи с чем весьма проблемным является вопрос оценки их объективности. Также нужно учитывать то, что медицинский работник не вправе разглашать сведения, составляющие врачебную тайну, поэтому он ограничен в возможности ответа на выраженную в сети Интернет и адресованную ему критику, ведь, согласно ст. 13 Закона об основах охраны здоровья граждан в РФ, врач не вправе разглашать даже факт обращения конкретного лица к нему для оказания медицинских услуг [1. С. 78–84].

В случае установления факта распространения на сайте в сети Интернет сведений, порочащих деловую репутацию медицинских работников, последние вправе воспользоваться предусмотренным ст. 152 ГК РФ способом защиты нарушенного права. В обоснование исковых требований о защите чести, достоинства и деловой репутации медицинскому работнику необходимо предъявить доказательства того,

что указанная в отзывах, размещенных в сети Интернет, информация не соответствует действительности.

Как следует из разъяснений Верховного Суда РФ, при рассмотрении такой категории дел судье необходимо установить, носит ли размещенная в сети Интернет информация, касающаяся оказанных пациенту медицинских услуг, оценочный характер или она представляет собой соответствующие действительности факты о ненадлежащим образом проведенном лечении. Для оценки соответствия действительности сведений о данных фактах необходимо проведение лингвистической экспертизы.

Важным в судебной практике является вопрос о том, кого следует привлекать в качестве ответчика по данной категории дел. Так, в случае предъявления исковых требований об удалении из СМИ порочащих деловую репутацию сведений ответчиком по делу будет выступать владелец данного сайта в сети Интернет, лицо, которое обладает возможностью удалить информацию. В качестве соответчика будет выступать автор данного отзыва, в случае же невозможности установления его личности судом будет установлен лишь факт распространения ложной, унижающей честь, достоинство медицинского работника информации [4].

Из всего вышесказанного можно сделать вывод, что действующее российское законодательство регламентирует право СМИ на распространение общедоступных персональных данных лица без его согласия. Однако норма, закрепляющая право на свободное получение и распространение информации, конкурирует с нормой, провозглашающей право на неприкосновенность частной жизни лица, и для соблюдения баланса между свободой слова и правом на защиту частной жизни необходимо устанавливать, имелась ли у медицинского работника возможность удаления размещенных в сети Интернет и содержащих его персональные данные отзывов.

Кроме того, суды при рассмотрении такой категории дел должны руководствоваться следующими критериями, определяющими допустимость вмешательства СМИ в частную жизнь граждан: содержание размещенной в сети Интернет информации, способ ее получения, общественная значимость и достоверность данной информации, публичность данного лица.

Список литературы

1. Болик В. Н., Туркиашвили А. М. О правомерности законодательных ограничений конституционного права на неприкосновенность частной жизни // Законы России: опыт, анализ, практика. 2015. № 7. С. 78–84.

2. Гаврилов Е. В. О новейшей практике Верховного Суда РФ по делам о защите чести, достоинства и деловой репутации опороченных в сети Интернет // Пермский юридический альманах. Ежегодный научный журнал. 2019. № 1.

3. Трофимова И. А. Обработка и хранение персональных данных / И. А. Трофимова // Делопроизводство. 2015. № 3. С. 107–110.

4. Определение Верховного Суда РФ от 26.04.2022 № 5-КГ22–28-К2. КонсультантПлюс.

5. По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг»: постановление Конституционного Суда РФ от 25.05.2021 № 22-П // Собрание законодательства РФ. 2021. № 22.

6. Утеген Д., Рахметов Б. Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 825–844. EDN: DRGDDJ

7. Шутова А. А., Никифорова А. А. Уголовная ответственность за распространение заведомо ложных сведений в период пандемии: вопросы теории и практики // Вестник Удмуртского университета. Серия: Экономика и право. 2021. Т. 31, № 1. С. 81–89. EDN: ZYQLYQ

А. К. Архипова,
студент,
Российский университет дружбы народов
имени Патриса Лумумбы
Х. Л. Хасиева,
студент,
Российский университет дружбы народов
имени Патриса Лумумбы

ТЕНДЕНЦИЯ ЦИФРОВИЗАЦИИ ПРАВОСУДИЯ В КОНТЕКСТЕ ОПЫТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Цифровизация правосудия – это процесс, который преобразует традиционные методы юридической работы, внедряя современные цифровые технологии и системы. Судебная система, будучи одной из важнейших сфер общественной жизни, местом защиты основных гражданских прав и свобод, не стала исключением из общей тенденции цифровизации. Особенно четко внедрение научно-технических средств в процесс отправления правосудия прослеживается в период пандемии COVID-19, которая вызвала острую необходимость в применении средств связи, позволяющих людям осуществлять дистанционную коммуникацию. В этой связи ключевой формой цифровизации судебного процесса во многих правопорядках, в том числе и Российской Федерации, стало проведение судебных заседаний в режиме онлайн посредством видео-конференц-связи. В данной статье анализируются наиболее значимые тенденции, актуальные вызовы и перспективы развития цифровизации правосудия в России.

Ключевые слова: цифровизация, правосудие, электронный документооборот, электронные судебные заседания, цифровая идентификация, судопроизводство, процессуальные документы

THE TENDENCY OF DIGITALIZATION OF JUSTICE IN THE CONTEXT OF THE EXPERIENCE OF THE RUSSIAN FEDERATION

Abstract. Digitalization of justice is a process that transforms traditional methods of legal work by introducing modern digital technologies and systems. The judicial system, being one of the most important spheres of public life, a place of protection of basic civil rights and freedoms, has not become an exception to the general trend of digitalization. The introduction of scientific and technical means into the process of administration of justice is particularly clearly traced during the COVID-19 pandemic, which caused an urgent need for the use of communication tools that allow people to carry out remote communication. In this regard, the key form of digitalization of the judicial process in many legal systems, including the Russian Federation, has become the holding of court sessions on-line via web conferencing. In this article, the authors analyze the most significant trends in the digitalization of justice in Russia, considering examples, current challenges and development prospects.

Keywords: digitalization, justice, electronic document management, electronic court sessions, digital identification, legal proceedings, procedural documents

Цифровизация стала неотъемлемой частью современного общества и оказывает глубокое воздействие на множество аспектов нашей жизни, включая сферу правосудия. С развитием информационных технологий и цифровых решений необходимость адаптации правовой системы к новым вызовам и возможностям становится более чем явной. В связи с этим изучение тенденций цифровизации правосудия становится неизбежным явлением.

Суть цифровизации правосудия заключается в применении современных технологических решений для улучшения эффективности и доступности судебных услуг, что позволяет сократить временные и ресурсные затраты, увеличить прозрачность и справедливость судопроизводства, а также обеспечить более широкий доступ граждан к правосудию [1. С. 151–154].

Цифровая революция внесла существенные изменения в различные сферы общественной жизни, включая правосудие. В эпоху, когда информационные технологии стали неотъемлемой частью нашей повседневной жизни, цифровизация правосудия стала необходимым этапом современной юридической системы.

В Российской Федерации вопрос цифровизации судопроизводства приобрел особую актуальность, это было обусловленно вспышкой пандемии COVID-19 в 2020 г. [14], которая привела к введению ограничений на организацию событий, включая судебные заседания, в целях снижения риска распространения коронавирусной инфекции [8. С. 63–63].

В апреле 2020 г., президиумы Верховного Суда и Совета судей рекомендовали всем судам проводить судебные заседания в формате видео-конференц-связи с использованием собственных средств связи [6]. К 13 июля 2020 г. только в системе арбитражных судов состоялось 19 213 онлайн-процессов [2. С. 7]. Аналогичная ситуация прослеживается и в Австралии [13].

На современном этапе развития цифровое правосудие перестало быть временной мерой и стало неотъемлемой частью реальности [10], о чем свидетельствует высокая динамика законопроектной деятельности органов государственной власти по внесению изменений в процессуальное законодательство в контексте информатизации судопроизводства, когда субъекты права законодательной инициативы представляют возможным подачу искового заявления, заявления, жалобы, представления и иных документов в суд в электронном виде через информационную систему, определенную Верховным Судом РФ, либо через систему электронного документооборота участника процесса посредством единой системы межведомственного электронного взаимодействия, или представляют возможным участие в судебном заседании путем использования системы веб-конференции при условии заявления ими ходатайства об этом и при наличии в судах технической возможности осуществления веб-конференции.

Цифровизация правосудия позволит существенно улучшить качество и доступность судебных решений, оптимизировать судебные процессы и укрепить доверие к системе правосудия. Однако на пути к успешной реализации цифровых инноваций возникают ряд сложностей, которые требуют серьезного внимания и решения. Цифровизация правосудия представляет собой множество процессов и практик, охватывающих применение информационных и коммуникационных технологий для улучшения работы юридической системы. Цифровизация правосудия представляет собой «средство обеспечения перехода к системе электронной подачи обращений в суд и автоматизированного распределения дел между судьями; внедрения средств информатизации судебного разбирательства» [11. С. 135–139].

Под цифровизацией правосудия ученые понимают процесс использования информационных технологий для автоматизации и улучшения судебных процессов, включая управление документами, судопроизводство, доступ к информации и взаимодействие с участниками правовых процедур. Обратим внимание на то, как цифровизация способствует улучшению работы судебных учреждений: автоматизация судопроизводства и электронный документооборот уменьшают риск ошибок и позволяют судьям сосредотачиваться на анализе и принятии судебных решений.

Цифровизация правосудия также способствует увеличению прозрачности и доступности судебной информации. В Москве сейчас предоставляется уникальная возможность обращения в суды через многофункциональные центры. При обращении гражданина в МФЦ создается подтвержденная учетная запись на Портале gosuslugi.ru, а также личный кабинет на Портале судов общей юрисдикции города Москвы mos-gorsud.ru, предоставляющие такие функциональные возможности для реализации принадлежащих гражданам процессуальных прав в 35 районных судах столицы и в Московском городском суде, как:

«1) подача исковых заявлений и других документов в суды в электронном виде;

2) возможность ознакомления с аудиопротоколами судебных заседаний;

3) работа с материалами электронных дел;

4) получение сведений о движении по делу;

5) получение электронного исполнительного листа и направление в ФССП России на принудительное исполнение;

6) получение судебных решений, заверенных усиленной квалифицированной электронной подписью» [9].

Цифровизация сокращает временные и административные барьеры в судебном процессе, позволяя миновать бюрократические процедуры. К примеру, система «Мой Арбитр» в России способствует тому, чтобы стороны в арбитражных спорах обменивались документами и информацией онлайн, что ускоряет рассмотрение дел [5].

Исторический контекст цифровизации правосудия в России играет важную роль в понимании современных тенденций и изменений в юридической системе страны, а также подчеркивает, что цифровая модернизация юридической системы является не случайным событием, а результатом долгосрочных усилий по улучшению доступности, прозрачности и эффективности судебных процессов.

В России специализированными структурами внедряются современные информационные технологии для повышения эффективности и доступности правосудия, что позволяет выделить следующие основные направления информатизации судебного процесса:

1. **Электронное судопроизводство**: ГАС «Правосудие» предоставляет возможность электронной подачи заявлений, документов и жалоб, а также онлайн-доступ к материалам судебных дел, что существенно сокращает временные и административные затраты сторон и судов.

2. **Электронная архивация судебных дел**: цифровизация также включает в себя электронную архивацию судебных дел. Системы, такие как «Мой Арбитр», позволяют судам и сторонам архивировать судебные документы и предоставлять доступ к ним для последующего использования и анализа.

3. **Использование средств искусственного интеллекта**: в сферу цифровизации правосудия также активно внедряются средства искусственного интеллекта (ИИ), что включает в себя анализ судебных решений с целью выявления аномалий и предсказания исходов дел. ИИ также может использоваться для автоматической обработки больших объемов судебных данных.

4. **Усовершенствование системы учета и статистики**: современные информационные системы позволяют автоматизировать сбор и анализ данных о судебной деятельности, что помогает в принятии более обоснованных управленческих решений.

Основные направления цифровизации правосудия в России свидетельствуют о стремлении к более эффективным, прозрачным и доступным судебным процессам.

Тенденция цифровизации отечественного судопроизводства оказывает благоприятное воздействие на большинство сфер жизнедеятельности граждан, а также способствует модернизации судебной системы.

Посредством внедрения в процесс отправления правосудия цифровых технологий обеспечивается реализация принципов доступности правосудия, предписанного ст. 46 Конституции Российской Федерации [3], и гласности судопроизводства, установленного ст. 123 Конституции Российской Федерации [3].

Право подачи процессуального документа в электронной форме и возможность проведения судебного заседания с помощью института веб-конференц-связи обеспечивает доступ каждого гражданина к судебной форме защиты его права и устраняет необходимость физического присутствия в судах, а также делает информацию более транспарентной для всех участников процесса. Данное достоинство детерминируется сравнительно большой территорией Российской Федерации и отсутствием ресурсов для обеспечения даже самого удаленного уголка страны аппаратом суда.

Размещение текстов судебных актов в сети Интернет является одним из основных преимуществ процесса информатизации правосудия, так как способствует повышению гласности судебного разбирательства и предоставляет возможность каждому субъекту правоотношений ознакомиться с практикой релевантного для него суда. Вместе с тем важно отметить, что отечественная система публикации направлена на реализацию процессуальных прав граждан в том контексте, что является бесплатной и открытой, в сравнении с иностранными государствами, где подобные механизмы доступны только при оплате данных услуг.

Внедрение электронного судопроизводства и электронной архивации судебных дел позволяет ускорить судебные процессы. Судьи, адвокаты и стороны дела могут эффективно обмениваться документами и информацией онлайн, сокращая временные задержки, связанные с традиционными бумажными процедурами. Кроме того, цифровизация правосудия сокращает бюрократическую нагрузку для судей, адвокатов и судебных служителей. Онлайн-системы автоматизируют многие процессы, такие как регистрация документов и назначение заседаний, что позволяет сосредотачиваться на сущности дела.

Цифровизация правосудия способствует уменьшению человеческого вмешательства в судебный процесс и повышает надежность и объективность решений, что снижает возможности для коррупции и судебных ошибок. Кроме того, документы в бумажной форме, несмотря на свою надежность, часто подвержены потере или повреждению, в то время как электронные файлы и сообщения хранятся в компьютерной системе, благодаря чему не подвергаются временным изменениям. К примеру, справочная система «АМИРС», используемая в рамках деятельности мировых судей, позволяет сокращать затраты на поиск информации конкретного дела и упорядочивать элементы делопроизводства.

Несмотря на все вышеуказанные преимущества, следует отметить, что цифровизация судопроизводства в России также сопряжена с некоторыми недостатками. Нерешенными остаются вопросы, связанные с соответствием процессов судебных заседаний в режиме онлайн формальным и установленным законодательством правилам судопроизводства.

Среди основных трудностей можно выделить слудующие:

1. Протоколирование судебных заседаний: целесообразность ведения протокола секретарем судебного заседания;

2. Гарантирование свободы участников судебного процесса, которые подвергнуты допросу, от постороннего воздействия при применении технологии веб-конференц-связи;

3. Механизм предоставления суду вещественных доказательств, в том числе документов, при проведении судебного заседания в режиме «онлайн».

Преимущества цифровизации правосудия в России оказывают существенное воздействие на судебную систему, делая ее более эффективной, доступной и прозрачной. Данные изменения положительно влияют на всех участников судебного процесса, включая судей, адвокатов, граждан и юридических лиц, и способствуют справедливому и эффективному разрешению судебных споров. Одновременно с этим цифровизация правосудия содействует модернизации судебных институтов и поддерживает страну на пути к развитию информационного общества.

Несмотря на множество преимуществ, цифровизация правосудия в России сталкивается с рядом вызовов и проблем, которые необходимо учитывать при реализации этого процесса, среди них:

1) **кибербезопасность и защита данных**: с ростом использования информационных технологий в правосудии возрастает угроза кибератак и утечек конфиденциальной информации [1. С. 151–154]. Недостаточная защита судебных данных может привести к серьезным последствиям, включая утечку персональных данных. Эффективная кибербезопасность становится критически важной задачей [12. С. 621–627];

2) **доступность для всех групп населения**: цифровизация может создать барьеры для тех, кто не обладает должными навыками в области информационных технологий или доступом к интернету, что может вызвать неравенство в доступе к правосудию и снизить доступность судебных услуг для определенных групп населения, таких как пожилые люди или малообеспеченные слои общества;

3) **технические сбои и неполадки**: на практике системы электронного судопроизводства могут подвергаться техническим сбоям и неполадкам, что может вызвать задержки и неудобства для всех участников судебных процессов. Надежность и стабильность судебных информационных систем становятся приоритетными задачами;

4) **защита от злоупотреблений и мошенничества**: цифровизация правосудия также может сопровождаться новыми формами злоупотреблений и мошенничества, такими как фальсификация документов или хакерские атаки на системы судопроизводства [7. С. 292–294];

5) **легальные и этические вопросы**: цифровизация правосудия также вызывает легальные и этические вопросы, связанные с обработкой данных, автоматизацией процессов и использованием ИИ в судебных решениях и требующие разработки соответствующих нормативных и этических стандартов;

6) **финансирование и ресурсы**: развитие и поддержание современных судебных информационных систем требует значительных финансовых ресурсов. Недостаток финансирования может замедлить процесс цифровизации правосудия и ограничить доступность судебных услуг.

Успешная цифровизация правосудия требует комплексного подхода и многосекторального сотрудничества, чтобы обеспечить эффективное и справедливое правосудие для всех граждан России.

Тем не менее цифровизация правосудия в России имеет обширные перспективы, которые могут повысить качество судебных услуг, сделать судебные процессы более эффективными и справедливыми.

Отечественная цифровизация правосудия представляет собой важное направление, которое способствует повышению эффективности и доступности судебных услуг, улучшению качества судебных решений и обеспечению более прозрачных и справедливых судебных процессов [4].

В заключение нельзя не отметить, что цифровизация правосудия – неотъемлемая часть современной судебной системы. Внедрение цифровых технологий в процесс отправления правосудия помогает сократить бюрократические процедуры, ускорить рассмотрение дел и повысить прозрачность судопроизводства. Системы электронного судопроизводства и электронной архивации дел значительно упрощают процессы обмена документами и обеспечивают доступность судебных данных для всех участников процесса. Вместе с тем кибербезопасность и защита данных становятся приоритетными задачами при внедрении цифровых систем в судебной сфере. Сотрудничество с международным сообществом и заимствование эффективного опыта передовых стран может способствовать развитию судебных информационных систем в России.

Цифровизация правосудия в России продолжит развиваться и вносить инновации в судебную систему, что способствует созданию более справедливой, эффективной и доступной юстиции для граждан страны.

Список литературы

1. Грязнов С. А. Цифровое правосудие // Modern Science. 2021. № 2–2. С. 151–154.

2. Кашанин А. В. Информационные технологии в правосудии: состояние и перспективы. Россия и мир. Аналитический доклад // црсп.рф: электронный журнал. URL: http://црсп.рф/wp-content/uploads/2020/07/w-informacionnie-tehnologii-v-pravosudii.pdf

3. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_28399/

4. Концепция информационной политики судебной системы на 2020–2030 годы (одобрена Советом судей РФ 5 декабря 2019 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_339776

5. Мой Арбитр // Федеральные арбитражные суды. URL: https://my.arbitr.ru/#index

6. О приостановлении личного приема граждан в судах: Постановление Президиума Верховного Суда Российской Федерации Президиума Совета судей Российской Федерации от 08.04.2020 № 821 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_349751

7. Свищенкова К. А. Перспективы и проблемы цифровизации правосудия в Российской Федерации // Молодой ученый. 2022. № 15(410). С. 292–294.

8. Сергеева К. А. Правосудие и пандемия коронавируса: вынужденная цифровизация // International Law Journal. 2021. Т. 4, № 6. С. 63–68.

9. Состоялось совещание по вопросам расширения доступа граждан к правосудию с использованием цифровых технологий // Верховный Суд Российской Федерации. URL: https://vsrf.ru/press_center/news/32662

10. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

11. Шатковская Т. В., Гончаров Е. И. Электронный документооборот в судебной системе Российской Федерации: проблемы и перспективы // Северо-Кавказский юридический вестник. 2021. № 2. С. 135–139.

12. Razveykina N. A. Digitalization of legal proceedings as a way to ensure access to justice // Vestnik Permskogo Universiteta. Yuridicheskie Nauki. 2022. № 58.

13. Рэн Й. Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 712–724.

14. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

Т. С. Асташова,
магистрант,
Новосибирский государственный университет

ВИДЕОИГРЫ КАК ОБЪЕКТ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ

Аннотация. Статья отражает актуальные исследования российских и зарубежных ученых, нормативно-правовую базу, а также практику правоприменительных органов в сфере индустрии видеоигр. Цель исследования заключается в раскрытии подходов к пониманию сущности видеоигры как объекта интеллектуальных прав, ее основных черт, отличающих ее от других объектов интеллектуальных прав.

Ключевые слова: интеллектуальные права, цифровые технологии, видеоигра, компьютерная игра, мультимедийный продукт, программа для ЭВМ, интерактивность, виртуальность, цифровая среда

VIDEO GAME AS AN OBJECT OF INTELLECTUAL RIGHTS

Abstract. The article reflects current research by Russian and foreign scientists, the regulatory framework, as well as the practice of law enforcement agencies in the video game industry. The purpose of the study is to reveal approaches to understanding the essence of a video game as an object of intellectual rights, its main features that distinguish it from other objects of intellectual rights.

Keywords: intellectual rights, digital technologies, video game, computer game, multimedia product, computer program, interactivity, virtuality, digital environment

Темпы развития научно-технического прогресса во многом превосходят скорость развития и актуализации правовых норм. За последние пять лет рынок индустрии видеоигр составил 178 млрд долларов, что эквивалентно 20 % от глобального рынка развлечений. Видеоигра – универсальный продукт на рынке

развлечений, существует большое множество игр для пользователей любого возраста и пола. Безусловно видеоигра представляет интерес как крайне неординарный и сложный объект интеллектуальных прав.

Индустрия видеоигр начала зарождаться в 1970-е гг. Хотя годом создания первой видеоигры считается 1940 г. Американский физик-ядерщик Эдвард Кондон впервые показал на Всемирной выставке в Нью-Йорке компьютерную электронно-релейную машину для игры. Сейчас такие устройства называют аркадными автоматами. Первой же компьютерной игрой считается Tetris for two (с англ. – «тетрис для двоих»).

Законодательство РФ в сфере прав на объекты интеллектуальной собственности в настоящее время основывается на масштабной нормативно-правовой базе, имеет широкий опыт правоприменения, и в целом можно сказать, что законодательство об интеллектуальной собственности относительно современно и достаточно развито. Однако с появлением новых объектов, таких как видеоигры, VR-технологий и других новейших объектов интеллектуальных прав, возникает угроза стабильности правовой системы в сфере интеллектуальной собственности. Это связано с тем, что процесс актуализации нормативно-правовой базы происходит гораздо дольше, чем развитие технологий.

В векторе развития цифрового пространства неизбежно и развитие технологий, используемых в производстве видеоигр – создание новейших графических, звуковых и иных эффектов, совершенствование игровых алгоритмов. Игры становятся современней и реалистичнее из-за высокого уровня техники, интереснее благодаря огромному выбору жанров, поведения персонажей, их внешних обликов и игровых способностей. Интерес потребителя к игровой индустрии также возрос и в связи с пандемией. Будучи ограниченными в перемещении, граждане активно использовали всевозможные формы видеоигр для проведения досуга.

С другой стороны, возрастающий интерес потребителей влечет за собой высокую доходность видеоигр в секторе развлечений, что в свою очередь обуславливает появление большого числа новых разработчиков игр. Такое стремительное появление большого числа новых объектов интеллектуальных прав порождает потребность в их защите.

Темпы роста индустрии видеоигр значительно выросли за последние пять лет, особенно в 2020 г. Это обусловлено в большей степени вынужденными ограничениями в связи с распространением коронавирусной инфекции [16]. Так, в 2020 г. темп роста игрового рынка составил 19,7 %, тогда как в 2019 г. он составлял лишь 7,2 % [5]. Что касается мировой выручки разработчиков и правообладателей видеоигр, то в 2020 г. этот показатель достиг отметки в 178 млрд долларов, что составляет 20 % мирового рынка (в 2016 г. названный показатель находился на уровне около 12 %) [5]. К концу 2021 г. показатели популяризации видеоигр немного снизились: эксперты связывают это с отменой ковидных ограничений, возобновлением очного формата работы, учебы. Однако аналитики организации Newzoo ожидают постепенный рост рынка видеоигр – к 2024 г., по прогнозам экспертов, показатель выручки рыночного сегмента видеоигр достигнет 218 млрд долларов.

Стоит отметить, что рынок видеоигр в основном охватывает три платформы: мобильные телефоны (49 %), консоли (29 %) и персональные компьютеры (22 %). Специалисты отраслевой аналитической фирмы Newzoo отмечают, что основной движущей силой роста рынка видеоигр являются игры для мобильных устройств. Во всем мире число игроков вырастет с 2,9 млрд в 2020 г. до 3,6 млрд к 2025 г., что в среднем за пять лет составит 4,3 % роста. Глобальный рынок видеоигр в 2022 г. составил 184,4 млрд долларов. 2022 г. стал корректирующим годом для рынка игр после двух лет роста, вызванного карантином.

Учитывая вышесказанное, сложно не согласиться с крайне высокой популярностью и доходностью видеоигр. Очевидно, что развитие этой области деятельности не может быть оставлено без внимания правоведов и законодателей.

Обобщая попытки зарубежных ученых определить понятие «видеоигра», можно сказать, что видеоигра, по их мнению, – это способ взаимодействия игрока с другими игроками либо игрока с алгоритмами игры, посредством специальной платформы (персональный компьютер, консоль, смартфон, телефон, аркадный автомат), которая графически и аудиовизуально отображает зачастую вымышленный контекст и поддерживает эмоциональную привязанность между игроком и результатом его действий в этом вымышленном контексте [14].

При визуальном исследовании видеоигр можно заметить множество объектов авторских прав – персонажи, сюжет, текст, игровой фон, аудио-, и видео- и звуковые эффекты. Однако не стоит забывать о том, что технически любая видеоигра – это программный код. Программный код для ЭВМ называется объектом авторских прав в ст. 1259 ГК РФ [2]. Вместе тем также можно выделить как самостоятельные объекты интеллектуальных средства индивидуализации компаний-разработчиков, программное обеспечение игры и другие объекты патентных прав, а также объекты коммерческой тайны (списки пользователей – игроков и др.).

Видеоигра по своей структуре схожа с кинофильмом: оба объекта содержат сценарий, персонажи, текст, музыкальное сопровождение, спецэффекты, изображения и т. д. С другой стороны, видеоигры имеют и ряд общих черт с базами данных: совокупность множества элементов, структурирование, использование алгоритмов, программный код для использования базы данных.

В законодательстве РФ не содержится понятия «видеоигра». Суды же в своих судебных актах чаще всего используют формулировку «компьютерные игры». Учитывая тот факт, что компьютерные игры составляют меньше четверти объемов мирового рынка видеоигр, бóльшая часть объектов видеоигрового сектора остается вне правового поля судов РФ. Об этом писал и Д. В. Овчаров, подчеркивая отсутствие в России единого подхода к пониманию видеоигры [4]. Арбитражный суд города Москвы вместо термина «видеоигра», использует понятие «компьютерная игра», а саму игру определяет как услугу для целей налогообложения [10]. А в решении суда общей юрисдикции термины «видеоигра» и «компьютерная игра» вообще используются как равнозначные [11].

В свою очередь Правительство РФ обозначает эти два термина как самостоятельные понятия, относя видеоигры и компьютерные игры к творческой индустрии производства цифрового контента [9]. В постановлении Семнадцатого

арбитражного апелляционного суда от 22 сентября 2020 г. содержится уже более современный подход к пониманию видеоигр: суд рассматривает компьютерные игры как сложные объекты авторских прав [8]. В мировой доктрине сложилось три основных подхода к пониманию видеоигры как объекта интеллектуальных прав.

– видеоигра – аудиовизуальное произведение,
– видеоигра – программа для ЭВМ,
– видеоигра – мультимедийный продукт.

Суждение о том, что видеоигра является аудиовизуальным произведением, было популярно в период появления первых видеоигр в 70-х гг. XX в. в США. В силу вступления в 1976 г. Закона об авторском праве видеоигра была признана объектом авторских прав, а именно аудиовизуальным произведением [12]. Согласно этому закону, аудиовизуальное произведение состоит из совокупности связанных между собой изображений, изначально предназначенных для демонстрации с использованием специальных аппаратов или устройств. Однако такой подход не учитывает главную особенность видеоигр – непосредственное участие игрока. При просмотре фильма в кинотеатре от зрителя не требуется никаких действий для начала проигрывания фильма. Тогда как для хода видеоигры необходимо, чтобы игрок выбирал, как персонаж будет поступать в той или иной сюжетной ситуации.

Всеми известная видеоигра Tetris была создана в 1984 г. советским программистом Алексеем Пажитновым. Коммерческая версия была создана в компании The Tetris Company (далее – TTC). В 2009 г. TTC обратилась в суд с иском к разработчику Xio Interactive, который выпускал игры для iPhone, о нарушении авторских прав на Tetris [15].

Более ранние редакции Закона об авторском праве США предусматривали для авторов видеоигр право на защиту своих авторских прав в рамках видеоигры как аудиовизуального произведения. Согласно этому закону, считалось, что защите подлежат не идея, процедура, система, метод работы, концепция, принцип или открытие, а воплощение идеи. Таким образом, невозможно было защитить ни саму идею, которая лежит в основе Tetris (падение геометрических фигур с верхнего поля для заполнения пробелов по нижнему полю), ни программный код, благодаря которому игра приводилась в действие. В то же время суду удалось, помимо неохраняемых объектов интеллектуальных прав, выделить охраняемые объекты в игре: размер игрового поля, показ «заполненных» линий, появление теневых фигур, показ следующей фигуры и др.

Сейчас в США популярен подход, согласно которому видеоигра является сложным объектом авторского права и подлежит самостоятельной охране.

Статья 1261 ГК РФ так определяет программу для ЭВМ как объект авторских прав: программа для ЭВМ – представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Программа для ЭВМ при визуальном анализе представляет собой текст, состоящий из набора инструкций, порядка действий для исполнителя задачи, связанных между собой алгоритмическими выражениями, позволяющими идентифицировать объект как программу для ЭВМ. С другой стороны, программа для ЭВМ – это и подготовительные материалы, которые получены в ходе создания программы для ЭВМ, и аудиовизуальное отображение, которые приводятся в действие программой ЭВМ – ее алгоритмической частью.

Так как ЭВМ по своей сути представляет собой текст, составленный из символов, соединенных в алгоритмические выражения, программа для ЭВМ считается произведением и ее режим охраны приравнивается к режиму охраны литературного произведения.

Сторонники подхода «видеоигра – программа для ЭВМ» убеждены, что с учетом виртуальности и цифрового отображения аудиовизуальных элементов все элементы видеоигры выражены в цифровом коде и воспроизводятся специальным устройством. Поэтому все отображения изображения и звуков лишь приводятся в действие программным кодом игры. Такой упрощенный подход был популярен в судебной практике до 2018 г., когда суды без достаточных оснований приравнивали компьютерные игры к программе для ЭВМ. В этом случае акцентируется внимание на цифровом характере такого объекта исследования, как видеоигра, в котором основой функционирования, неким «двигателем» процессов является программный код. Такой подход до сих пор является ведущим в Аргентине, Китае, Канаде, Израиле и Италии [13].

Самым жизнеспособным подходом к пониманию видеоигр, на наш взгляд, является квалификация видеоигры как мультимедийного продукта – сложного объекта авторских прав. Видеоигра не является целостным произведением, она состоит из множества элементов: game engine (игровой механизм или базовое программное обеспечение игры), наборы звуковых рядов, графические и 3D-модели игрового фона, предметов, персонажей, которые в свою очередь являются составной частью сюжета игры. Все названные объекты, согласно теории авторского и смежного права, могут являться самостоятельными объектами защиты. Например, такой объект, как персонаж, может охраняться как самостоятельное произведение, с учетом его индивидуальности и узнаваемости, как отметил Пленум Верховного Суда РФ в постановлении от 23.04.2019 № 10 «О применении судами части четвертой ГК РФ», в п. 82 [7].

Основа любой видеоигры – программный код (программа для ЭВМ, программное обеспечение). Также важным элементом является сюжет. Однако объектом авторского права сюжет видеоигры быть не может, потому что представляет собой лишь общую идею, зачастую уже позаимствованную из литературных произведений или кинематографа [1]. Заимствование элементов сюжета правомерно. Однако можно привести сюжет к виду сценария – литературного произведения, которое в развернутой форме описывает от начала и до конца повествования конкретные действия, их последовательность, обозначает место, время, персонажей, содержит конкретные диалоги героев. Сценарий, являясь литературным произведением, охраняется как объект авторского права с момента создания. Личные

неимущественные права на сценарий принадлежат создателю – сценаристу, а исключительные права могут принадлежать (чаще всего) работодателю или заказчику в соответствии с договором между ним и сценаристом. Аналогично распределяются права и на программный код.

Игровые персонажи – вымышленные персонажи в видеоигре, особенность которых состоит в том, что их действия контролируются не правилами игры, а самим игроком. Персонажи, безусловно, являются частью произведения, видеоигры. Однако персонажа можно выделить как самостоятельный объект и использовать его, например, в других играх. Потому персонаж, конечно, охраняется нормами авторского права. Однако не любой персонаж может быть признан объектом авторского права и охраняться законом. Зачастую в видеоиграх можно встретить героев, которые выполняют роль игрового фона – заполняют местность для большей реалистичности. Зачастую текстура второстепенных персонажей и персонажей-фонов менее детализирована, чем облик главных героев игры. Для того чтобы персонаж стал объектом охраны, он должен быть самостоятельным результатом труда, должен иметь какую-либо ценность не только в конкретном произведении, игре, но и вне произведения. Кроме этого, обязательным условием считается выражение персонажа в объективной форме. На отдельно взятых персонажей в отличие от произведений науки, искусства или литературы не распространяется презумпция творческого характера.

Так называемый интерфейс видеоигры, так же, как и интерфейс интернет-сайта – графическое отображение, которое видит пользователь на экране своего устройства и с помощью которого взаимодействует с видеоигрой. Существует два варианта охраны этого объекта:

– обозначить интерфейс видеоигры как произведение дизайна, согласно ст. 1259 ГК РФ;

– зарегистрировать интерфейс в качестве промышленного образца, согласно ст. 1352 ГК РФ, однако в этом случае необходимо получить патент на основании государственной регистрации, а срок действия исключительных прав составит пять лет.

Но как произведение дизайна интерфейс видеоигры также рассматривать не совсем правильно. Он представляет собой составное произведение, состоящее из изображений, элементов дизайна, текста, «кнопок» (гиперссылок) и др.

Нельзя забывать, что почти любая видеоигра сопровождается как специальными музыкальными композициями, так и отдельными звуками (падения, удара, боли, звона монет), которые зачастую создаются специально для конкретной видеоигры. Для видеоигры The Elder Scrolls V: Skyrim была записана специальная музыкальная композиция, исполняемая целым хором. В этом случае, помимо авторских прав, могут возникать и смежные права на объекты музыкального творчества, например, право на исполнение и фонограмму песни [6]. Но также разработчики не исключают более простой и дешевый путь наполнения видеоигры звуками – покупка или использование существующих музыкальных произведений, посредством договора лицензии.

Приведенные выше элементы видеоигры, безусловно, являются ее неотъемлемой частью как единого целого, но в то же время некоторые из них могут позиционироваться как отдельные произведения – самостоятельные объекты авторских и смежных прав.

Важно понимать, что у названных отдельных объектов авторских прав могут быть разные авторы: геймдизайнеры, программисты, сценаристы, композиторы, художники, писатели и т. д. Но с другой стороны, не стоит забывать, что до конечного потребителя видеоигра доходит как единое целое, где отсутствие какого-либо из элементов делает невозможным или почти невозможным функционирование всей игры. Также важно, что игрок принимает непосредственное участие благодаря программного коду и внутренним алгоритмам, что отличает видеоигру от видеофильма.

Итак, самым состоятельным подходом к пониманию правовой сущности видеоигры является подход, согласно которому видеоигра – мультимедийный продукт. Внешняя (визуальная) составляющая видеоигры заключается во множестве элементов: сценарий (сюжет), аудиовизуальный компонент (музыка, звуки, графика и 3D-модели, игровой художественный фон), персонажи (главные, второстепенный, выполняющие роль игрового фона и т. д.), игра актеров (технологии захвата человеческого движения) и многое другое. Внутренняя часть видеоигры состоит в программном коде, программных алгоритмах, программном обеспечении и др.

Таким образом, видеоигры, будучи мультимедийным продуктом, обладают такими признаками, как виртуальность, интерактивность, сложность и цифровой характер среды. В создании видеоигр могут принимать участие множество авторов: сценаристы, геймдизайнеры, художники, композиторы, программисты и др. Многие элементы видеоигры могут выступать в качестве самостоятельных объектов авторских и смежных прав при определенных условиях.

Видеоигра как мультимедийный продукт не может одновременно охраняться и авторским, и патентным правом. Программа для ЭВМ не может выступать объектом патентных прав, что прямо предусмотрено ст. 1261 ГК РФ. Соответственно, и видеоигра, будучи сложным составным объектом интеллектуальных прав, не может охраняться патентным правом как цельный объект. Предоставление монополии на использование игровых механик поставило бы под угрозу развитие технического и общественного прогресса: при разработке видеоигры используется один из типовых игровых механизмов (game engine), а также уже существующие геймдизайнерские решения и подходы. По тем же причинам невозможно запатентовать операторские приемы для фильмов.

Тем не менее игровой интерфейс, как и интерфейс интернет-сайта, в некоторых случаях можно зарегистрировать в качестве произведения дизайна – промышленного образца (п. 1 ст. 1345 ГК РФ). В таком случае этот объект будет одновременно охраняться и авторским правом, и патентным. В случае патентования дизайна охраняется лишь внешний вид объекта без учета технической составляющей.

Патентование механик возможно в зарубежной юрисдикции, например, в США, благодаря DMCA (Digital Millennium Copyright Act – Закону об авторском праве в цифровую эпоху). В России патентование механик невозможно в силу

п. 1 ст. 1350 ГК РФ, который закрепляет, что в качестве изобретений охраняются технические решения в любой области, относящиеся к продукту или способу – процессу осуществления действий над материальным объектом с помощью материальных средств. Игровая механика не подходит под критерий материальности объекта. Она не существует в действительности, хотя содержит в себе некий набор правил, алгоритмов и инструкций, с помощью которых реализуется интерактивная составляющая игры.

Патентование ИТ-решения – в целом сложная и неоднозначная сфера. Оно возможно тремя способами:

1) патент на способ – описание последовательности действий, которая ведет в определенному результату (подходит для видеоигр);

2) патент на систему – ИТ-решение, которое помогает связать между собой несколько устройств (широко используется в военной промышленности);

3) патент на программно-аппаратный комплекс – ИТ-решение, которое помогает связать между собой программное обеспечение и устройство.

Патент для простого обывателя внушает уверенность в полной и безоговорочной защите, однако это не совсем так. К преимуществам патента на ИТ-решение можно отнести:

– монополия на решение в течение 10-20 лет,
– компенсация за нарушения прав на патент до 5 млн рублей,
– возможность передачи прав по договорам,
– увеличение капитализации компании,
– возможность правомерной рекламы, грантов и т. д.

Из недостатков следует отметить высокую сложность составления заявки и прохождения процедуры патентования, длительность процедуры (до 15 месяцев), сложность судебной защиты.

В зарубежной правоприменительной практике возможно запатентовать игровые механики видеоигры в качестве изобретения. В России прямое патентование программ для ЭВМ невозможно ввиду запрета п. 5 ст. 1350 ГК РФ, однако существует способ патентования алгоритма видеоигры – патентования его как способа.

Обобщая правоприменительную практику в связи с охраной видеоигры как объекта интеллектуальных прав, нельзя не учитывать опыт зарубежных правоприменительных органов, а также разнообразие областей правовой защиты видеоигр: сфера авторского права, патентного законодательства, а также товарных знаков и приравненных к ним средств индивидуализации организаций. Кроме того, в защите нуждаются не только создатели видеоигр, но и пользователи – в настоящее время распространены споры об одностороннем прекращении иностранных компаний лицензионных договоров с пользователями.

В настоящее время компания Epic Games получает в свой адрес колоссальное количество исков о нарушении авторских прав на танцы. Один из истцов – блоггер из США – не смог добиться защиты его авторского права на танец, используемый в игре от компании, потому что танец не был зарегистрирован в Библиотеке Конгресса США, ведь американская система авторского права требует обязательного депонирования произведений для подачи иска. Судебный прецедент создало

дело по иску одного из хореографов – Кайла Хаганами. Истец предоставил подтверждение регистрации танца в Библиотеке Конгресса США, а также видеоряд, который наглядно показывает абсолютное заимствование танца в игре. Однако суд иск отклонил, сославшись на незначительность нарушения. По мнению суда, использование отдельных общепринятых телодвижений из зарегистрированного танца не создает нарушение, а исключительное право на хореографическое произведение имеет своей целью защиту достаточно длительных танцевальных постановок, а не отдельных движений.

Что касается споров о «виртуальном имуществе» (условное имущество, приобретаемое в видеоиграх с помощью реальных или игровых денег внутри игры), то в вопросе классификации этих споров существует четыре основных подхода. Первый – невмешательство в игровое пространство и такого рода отношения и отнесение таковых к играм и пари. Этот подход подкрепляется ст. 1062 ГК РФ – требования граждан, связанные с организацией игри пари или участием в них, не подлежат судебной защите. Примером отражения этого подхода в судебной практике РФ является спор между игроком (истец) и ООО «Геймшок», ООО «Кверти», ООО «Новоплей» (ответчики). В Определении Московский городской суд от 16 ноября 2015 г. № 4г/611858/15 определяет сложившиеся отношения по поводу внутриигрового имущества в рамках ст. 1062 ГК РФ – отношения, сложившиеся в виртуальном пространстве, определяются согласно гл. 58 ГК РФ об играх и пари.

Второй подход заключается в том, что на виртуальную собственность должны распространяться нормы вещного права. Такого подхода придерживаются правоприменительные органы в Китае, Тайване и Нидерландах. В Китае возник спор между Ли Хогчен (истец) и Beijing Arctic Ice Technology Dev. Co Ltd (ответчик). Третье лицо украло у Ли виртуальную собственность. Истец заявил, что обменял виртуальный объект на свой труд, время, мудрость и деньги и поэтому он считает этот объект своей вещью в гражданско-правовом смысле. Китайский апелляционный суд обязал ответчика вернуть виртуальную собственность истца.

Такой же подход прослеживается в правоприменительной практике Тайваня. Постановление Министерства юстиции Тайваня в 2001 г. установило, что учетная запись и ценности онлайн-игр хранятся в виде электромагнитных записей на игровом сервере. Владелец учетной записи имеет право контролировать учетную запись и электромагнитную запись ценностей, свободно продавать или передавать ее. Министерство также подчеркивает, что, хотя указанные учетные записи и ценности существуют только в виртуальном пространстве, они представляют собой ценную собственность в реальном мире.

Третий подход заключается в признании отношений по виртуальной собственности в видеоиграх договорными. Отношения между игроком и разработчиком игры (правообладателем) оформляются в виде лицензионного соглашения.

Этот подход нашел отражение и в отечественной судебной практике. Так, в 2016 г. возник спор между игроком (истец) и ООО «Мэйл.ру» (ответчик). Гражданин подал иск в суд на ООО «Мэйл.ру» из-за того, что последний ограничил доступ истцу к его учетной записи на сайте, с помощью которой гражданин

пользовался услугами по предоставлению доступа к онлайн-игре. Московским городским судом отношения между игроком и разработчиком были квалифицированы как отношения из лицензионного соглашения, согласно которому разрешение всех споров данного соглашения должно происходить путем переговоров, переписки с использованием обязательного досудебного порядка.

Крайний подход основывается на том, что виртуальная собственность относится к «иному имуществу». К таким отношениям применяются нормы о соответствующих видах договоров, деликтах и неосновательном обогащении. Этот подход нашел применение в уголовном деле о разбое в Нидерландах. Важен даже не сам характер правонарушения (в данном случае – уголовное), а непосредственно позиции сторон о правовой природе виртуальной собственности. Суть дела: двое школьников заставили третьего посредством угроз и применения насилия войти в свою учетную запись в онлайн-игре и передать им виртуальные объекты, придающие персонажу новые навыки и умения, влияющие на игровое преимущество. Сторона защиты ссылалась на то, что виртуальный объект не существует на самом деле – это лишь представление битов и байтов и, следовательно, ценность этих объектов иллюзорна. Однако Верховный Суд, согласившись со стороной обвинения, подчеркнул, что данные виртуальные предметы имеют реальную ценность, которую можно оценить, – это результат усилий и затрат времени и потому они представляют реальную ценность для пользователя, так как приносят его персонажу «виртуальное богатство» и «виртуальную силу».

В заключение следует сказать, что видеоигры – по численности аудитории самая популярная сфера развлечений и универсальный продукт на рынке развлечений. Безусловно, видеоигра представляет интерес как крайне неординарный и сложный объект интеллектуальных прав.

Законодательство России в сфере прав на объекты интеллектуальной собственности основывается на масштабной нормативно-правовой базе, относительно современно и достаточно развито. Однако с появлением новых объектов интеллектуальных прав становится очевидно, что нормативно-правовая база развивается гораздо медленнее, чем технологии.

Видеоигра соединяет в себе множество объектов авторских прав – персонажей, сюжет, текст, игровой фон, аудио-, видео- и звуковые эффекты. В то же время любая видеоигра – это программный код для ЭВМ, который является объектом авторских прав согласно ст. 1259 ГК РФ.

В мировой доктрине сложилось три подхода к пониманию видеоигры как объекта интеллектуальных прав: как аудиовизуальное произведение, как программа для ЭВМ и как мультимедийный продукт.

Видеоигра как мультимедийный продукт – сложный объект авторских прав, который не является целостным произведением и состоит из множества элементов: game engine (игровой механизм или базовое программное обеспечение игры), наборы звуковых рядов, графические и 3D-модели игрового фона, предметов, персонажей. Все названные объекты, согласно теории авторского и смежного права, могут являться самостоятельными объектами защиты.

Квалифицируя видеоигру как мультимедийный продукт, можно выделить основополагающие признаки видеоигр: виртуальность среды (игрок совершает действия за персонажей в цифровом мире), сложность структуры (видеоигра состоит из множества элементов, некоторые из которых могут являться и самостоятельными объектами авторских и смежных прав), интерактивность (для хода игры необходимо взаимодействие игрока – нажатие определенных клавиш, комбинаций клавиш и др.), цифровая форма (цифровой программный код можно привести в действие лишь на специальном устройстве).

Недостаточность правового регулирования видеоигр, неоднозначность правовой природы видеоигр обуславливает возникновение споров и судебных тяжб в связи с нарушением прав на объекты интеллектуальной собственности.

Список литературы

1. Витко В. С. О признаках понятия «плагиат» в авторском праве / М.: Статут, 2017. С. 67.

2. Гражданский кодекс Российской Федерации. Часть четвертая: федеральный закон от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. 2006. № 52. Ст. 5496.

3. Индустрия видеоигр. Тинькофф Инвестиции. URL: https://www.tinkoff.ru

4. Овчаров Д. В. Сравнительно-правовой анализ терминов «видеоигра» и «компьютерная игра» // Юридическая наука, 2021. № 12. С. 44–48.

5. Отчет Newzoo о мировом рынке игр за 2022 г. URL: https://newzoo.com

6. Патрашкин Р. А. Видеоигры как объект интеллектуальной собственности в гражданском праве РФ // Государство и право. Юридические науки. № 9 (60). 2021. С. 413.

7. Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Российская газета. 2019. 6 мая.

8. Постановление Семнадцатого арбитражного апелляционного суда от 22 сентября 2020 г. № 17АП-8930/2020-ГКу по делу № А71-4683/2020. URL: https://kad.arbitr.ru

9. Распоряжение Правительства РФ от 20.09.2021 № 2613-р «Об утверждении Концепции развития творческих (креативных) индустрий и механизмов осуществления их государственной поддержки в крупных и крупнейших городских агломерациях до 2030 года» // СЗ РФ. 2021. № 40. Ст. 6877.

10. Решение Арбитражного суда города Москвы от 8 апреля 2015 г. по делу № А40-56211/14-90-70. URL: https://kad.arbitr.ru

11. Решение по гражданскому делу Московского городского суда по гражданскому делу № 3–866/2015 от 22.12.2015.

12. Рощенко С. В. Видеоигра как объект авторских прав в эпоху развития цифровых технологий // Вестник университета имени О. Е. Кутафина. № 4. 2022.

13. Чурилов А. Ю. Правовое регулирование интеллектуальной собственности и новых технологий: вызовы XXI века: монография. М.: Юстицинформ, 2020. 224 с.

14. Bergonse R. Fifty Years on. What exactly is a videogame? An essentialistic definitional approach // The Computer Games Journal. № 6 (4). 2017. P. 253.

15. TetrisHolding, LLC v. XioInteractive, Inc. URL: https://en.wikipedia.org
16. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

Г. М. Балахонцев,
студент,
Московский государственный университет
имени М. В. Ломоносова

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ РАСХОДОВ НА ИНФОРМАТИЗАЦИЮ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Аннотация. Статья посвящена проблеме правового регулирования бюджетных расходов на информатизацию государственного управления. Проводится анализ действующих нормативно-правовых актов. В статье описывается взаимосвязь норм, регулирующих расходы на государственные ИТ-проекты с принципами финансового и бюджетного права. Также в рамках статьи раскрываются положения действующих моделей жизненного цикла создания ГИС и их соотношение с принципом эффективности использования бюджетных средств. Обосновывается негативное влияние пробелов правового регулирования в данной сфере на достоверность мониторинга ИТ-расходов.

Ключевые слова: государственные информационные системы, модели жизненного цикла создания информационных систем, итерационная модель, каскадная модель, платформа «ГосТех», ведомственный план цифровой трансформации, национальный фонд алгоритмов и программ для электронных вычислительных машин

FEATURES OF LEGAL REGULATION OF EXPENSES FOR INFORMATIZATION OF STATE ADMINISTRATION

Abstract. The article is devoted to the problem of legal regulation of budget expenditures for informatization of state administration. An analysis of the existing legal and regulatory acts is being conducted. The article describes the relationship of the rules governing expenditures on state IT projects with the principles of financial and budget law. Also, the article reveals the provisions of the current life cycle models of GIS creation and their relationship with the principle of efficiency of the use of budget funds. The negative impact of legal regulatory gaps in this area on the reliability of IT monitoring is substantiated.

Keywords: state information systems, models of the life cycle of creation of information systems, iterative model, cascade model, platform «HosTech», departmental plan of digital transformation, national fund of algorithms and programs for electronic computers

В соответствии с документами стратегического планирования Российской Федерации для развития информационного общества необходимо повышение эффективности государственного управления, а также развитие экономической и социальной сферы жизни общества [9]. Во многом информатизация государственного управления и экономики связана с внедрением в управленческие и экономические процессы информационных систем. Сегодня государственные информационные системы (далее – ГИС) являются ключевым элементом цифровой трансформации государства, способствуя оптимизации функций, выполняемых органами государственной власти через свои алгоритмы формирования и анализа документов или организацию межведомственного взаимодействия. Граждане повсеместно сталкиваются с использованием ГИС, например, загружая документы на сайте «Госуслуги» или оплачивая налоги в мобильном приложении или личном кабинете ФНС. Реализуя стратегию по формированию информационного общества и цифровой экономики, государство тратит большие объемы бюджетных средств на ГИС. За 2022 г. сумма государственных расходов на информатизацию составила более 206 млрд руб. [12]. Как известно, каждый вид расхода государства обладает своими особенностями и должен соответствовать принципам финансового и бюджетного права, а также подчиняться общим нормам о бюджетных расходах, закрепленными в Бюджетном кодексе Российской Федерации. Однако каждый вид расхода государства также обладает собственной спецификой его исполнения, которая находит свое отражение в отдельных нормативно-правовых актах органов общей и специальной компетенции. Поэтому в рамках данной статьи мы постараемся проанализировать специфику нормативно-правового регулирования исполнения бюджета по расходам на информатизацию государственного управления.

Как известно, принципы являются основными началами отрасли права и задают векторы развития правового регулирования, поэтому вначале мы проанализируем, как принципы финансового и бюджетного права отражаются в правовом регулировании расходов на информатизацию. Одним из принципов, присущих отрасли финансового права, является принцип плановости, который проявляется в законодательно установленных требованиях для всех субъектов финансового права осуществлять финансовую деятельность на основе разработанных финансовых планов [4. С. 72]. Реализацию данного принципа мы можем увидеть в ст. 169 Бюджетного кодекса РФ, где указано, что проект федерального бюджета составляется и утверждается на три года – на очередной финансовый и на два года планового периода [2]. Подобное отражение принципа плановости в отношении расходов на информатизацию мы можем найти в Постановлении Правительства Российской Федерации от 10.10.2020 № 1646, где установлена обязанность федеральных органов исполнительной власти по формированию ведомственных планов цифровой трансформации (далее – ВПЦТ) на финансовый год и на два года планового периода [6].

В ВПЦТ включается перечень планируемых мероприятий по информатизации, а также показатели результативности цифровой трансформации. Следовательно, мы видим, что нормативное регулирование расходов на информатизацию

подчиняется принципу плановости и соотносится с регулированием деятельности по планированию проектов бюджетов. Принцип адресности и целевого характера бюджетных средств находит свое отражение в обособлении Министерством финансов расходов на информатизацию в отдельные коды бюджетной классификации. Согласно приказу Министерства финансов, расходы на информатизацию получают специальные коды видов расходов – 242 и 246 [8]. Подобное обособление позволяет органам финансового контроля, а также Министерству финансов и Министерству цифрового развития осуществлять контроль за объемом расходов на информатизацию и его целевым использованием.

Теперь мы разберем специальное регулирование бюджетных расходов на информатизацию государственного управления. Главным нормативно-правовым актом, который является основанием расходного обязательства в сфере информатизации, является Федеральный закон от 27.07.2006 «Об информации, информационных технологиях и защите информации». Данный закон дает определения понятий «информационная система», «оператор информационной системы», закрепляет цели создания ГИС и общие требования к ним [13]. В развитие данного Федерального закона принято Постановление Правительства Российской Федерации от 06.07.2015 № 676 (далее – Постановление № 676). Постановление определяет требования для органов государственной власти и органов управления государственными внебюджетными фондами по организации жизненного цикла ГИС. Постановление № 676 предусматривает ряд предварительных этапов до ввода системы в эксплуатацию, а также согласование технического задания на создаваемую систему с уполномоченными органами. Если размер затрат на создание ГИС, указанный в техническом задании, превышает 100 млн руб., то техническое задание на создание системы необходимо согласовать с Минцифры на предмет соответствия государственной политике в сфере информационных технологий и требованиям единой технической политики [10].

При данном согласовании Минцифры обязано проверять возможность реализации предусмотренных в техническом задании требований к программному обеспечению системы посредством использования программ для электронных вычислительных машин, размещенных в национальном фонде алгоритмов и программ для электронных вычислительных машин. Здесь необходимо раскрыть назначение национального фонда алгоритмов и программ для ЭВМ (далее – фонд алгоритмов). Фонд алгоритмов является федеральной государственной информационной системой, созданной в целях эффективного использования средств бюджетов бюджетной системы при решении задач цифровизации государственного и муниципального управления с помощью ряда способов:

1) учет и хранение алгоритмов и программного обеспечения, ранее приобретенных за счет средств бюджета;

2) обеспечение повторного использования на безвозмездной основе ранее приобретенных алгоритмов и ПО для нужд информатизации органов государственной власти [7].

Поскольку оплата труда разработчика за создание ГИС формируется исходя из сложности написания программ для ЭВМ и алгоритмов, где некоторые

алгоритмы заказчиком уже создавались, то гораздо целесообразней обязать разработчика использовать уже созданные алгоритмы, так как обязанность по использованию алгоритмов данного фонда направлена на исключение переплаты за создание алгоритмов, которые уже были использованы в иных ГИС. Это позволит снизить расходы на ее разработку, что также сочетается с принципом эффективности использования бюджетных средств. Одним из необходимых условий создания ГИС является правильный выбор организации жизненного цикла ее разработки. До 2022 г. Постановление № 676 предписывало федеральным органам исполнительной власти использовать каскадную модель жизненного цикла. Эта модель характеризуется поэтапной сменой циклов разработки ГИС без возможности вернуться на предыдущий цикл (рис. 1).

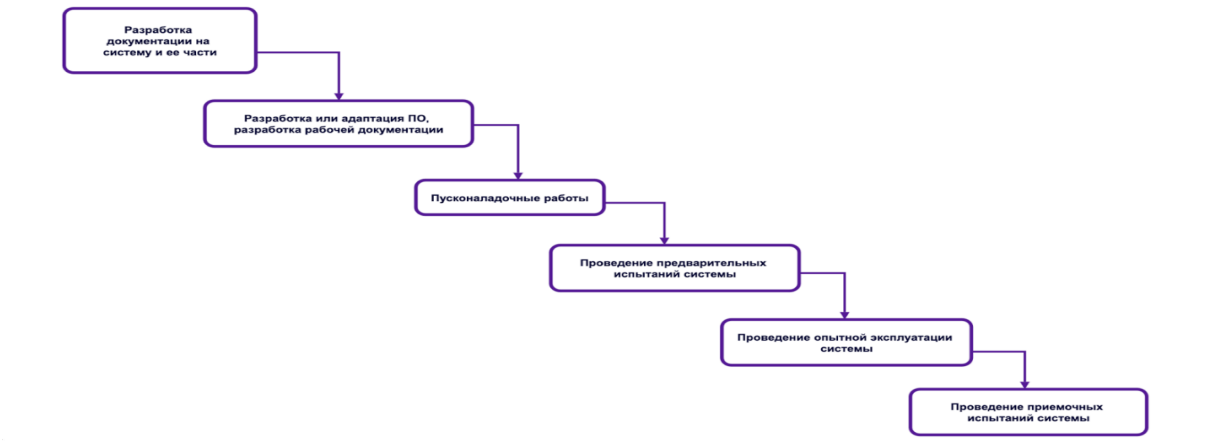

Рис. 1. Каскадная модель жизненного цикла

Данная модель жизненного цикла использовалась одной из первых при создании ПО. В ее основе лежит концентрация на каждом этапе разработки. Однако возможность использования такой методологии не позволяет вернуться на предыдущую стадию разработки в целях уточнения требований к создаваемой системе, из-за чего начальные этапы разработки документации и требований к системе отнимают много времени и денег, поскольку от них зависит дальнейшее движение циклов разработки, а следовательно, зачастую происходит удорожание конечного продукта [11. С. 1089].

В основном каскадная модель используется для систем с однотипной функцией с заранее определенными и неизменными требованиями, например, системы хранения данных. Однако с точки зрения планирования бюджетных расходов каскадная модель не подходит ввиду постоянного риска удорожания продукта и неопределенности срока ввода в эксплуатацию, что ведет к непредвиденным дополнительным расходам бюджета. Более выгодными и эффективными в современных условиях технологического развития признаются гибкие модели жизненного цикла, ярким представителем которых является итерационная или инкрементная модель, нашедшая свое отражение в Постановлении № 676 и обязательная к применению при создании ГИС на платформе «ГосТех». Учитывая недостатки

каскадной, итерационная модель направлена на создание системы очередями с возможностью возврата к предыдущей фазе работ для поиска наиболее оптимальных вариантов построения архитектуры системы или уточнения требований к системе после ее тестирования (рис. 2).

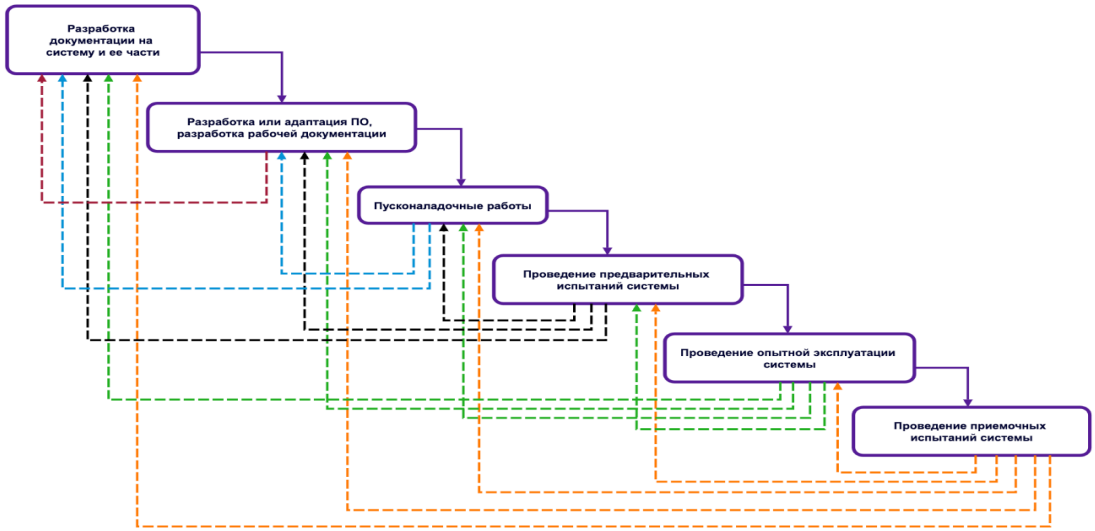

Рис. 2. Итерационная модель жизненного цикла

Стоит отметить, что крупные ИТ-компании наподобие Microsoft, а также действующие agile методологии, например, Scrum и Kanban, также берут за основу итерационную модель жизненного цикла [14. С. 67]. Очереди создания системы представляют собой временные промежутки разработки отдельных компонентов системы. Особенности данной модели позволяют планировать расходы на создание продукта на длительные временные промежутки, а следовательно, разбить их в рамках бюджетного планирования с исключением риска несения дополнительных бюджетных расходов, что сочетается с принципом плановости. В то же время возможность возврата к ранним стадиям цикла для уточнения требования или поиска наилучшей архитектуры системы повысит конечную результативность бюджетных расходов, а значит, удовлетворит одному из критериев эффективности бюджетных расходов, закрепленному в ст. 34 Бюджетного кодекса. Следовательно, нормативное закрепление применения итерационной модели в постановлениях Правительства РФ также является выражением действия принципа эффективности расходования бюджетных средств в отношении государственных расходов на информатизацию государственного управления. Однако, несмотря на реализацию принципа плановости, а также эффективности расходования бюджетных средств, Постановление № 676 обладает рядом недостатков, которые не позволяют осуществить достоверный мониторинг бюджетных расходов на информатизацию и провести достоверный учет действующих ГИС, на что обращает внимание Счетная Палата РФ. Поскольку Постановление № 676 обязательно для применения только федеральными органами исполнительной власти, а расходы на информатизацию

по КВР 242 применяются только ФОИВ, которые являются главными распорядителями бюджетных средств (далее – ГРБС) и должны проходить долгое согласование с Минцифры, то большинство ГРБС в обход согласования расходов на информатизацию передавало данные средства своим подведомственным организациям, которые не обязаны соблюдать Постановление № 676 и согласовывать расходы с координатором, тем самым уменьшая полноту мониторинга бюджетных расходов [1. С. 34]. Отсутствие четкого критерия отнесения информационной системы к ГИС как в ФЗ об информации, так и в Постановлении № 676 порождает неопределенность в вопросе реального учета ГИС, что затрудняет процессы планирования бюджетных ассигнований на их эксплуатацию [3. С. 15].

Новой вехой в развитии правового регулирования расходов на информатизацию государственного управления можно считать Постановление Правительства РФ «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех» (далее – Постановление № 2338), которое не только определяет функции и цели платформы, но и закрепляет лучшие концепции, выработанные в сфере управления государственными ИТ-проектами. В первую очередь Постановление № 2338 обязывает заказчиков ГИС применять исключительно итерационную модель жизненного цикла, не закрепляя возможности работы по каскадной модели. Постановление № 2338 функционирует на таких принципах, как повторное использование и эффективность использования бюджетных средств. Повторное использование, как принцип функционирования платформы «ГосТех», реализуется в обязанности оператора ГИС на «ГосТех» использовать при создании системы ранее созданные типовые программы и цифровые продукты в целях снижения конечной стоимости создания ГИС, что является аналогом использования ПО из фонда алгоритмов по Постановлению № 676.

Постановление № 2338 также раскрывает определение принципа эффективности использования бюджетных средств применительно к информатизации, как обеспечение создания, развития и эксплуатации ГИС на платформе «ГосТех», исходя из необходимости достижения целей реализации соответствующих мероприятий с использованием наименьшего объема средств (экономности) [5].

Подводя итог, мы можем сказать то, что действующее нормативно-правовое регулирование расходов на информатизацию государственного управления обладает рядом специальных норм, сформированных исходя из специфики отрасли разработки информационных систем и управления ИТ-проектами (через применение гибких моделей жизненного цикла и повторной адаптации ПО и алгоритмов). Данные нормы выработаны практикой управления и работы с программными продуктами ИТ-компаний, адаптированы под требования государственных ИТ-проектов и представляют собой «отраслевое преломление» принципов финансового и бюджетного права в области ИТ-расходов. Однако существующее регулирование на системном уровне до сих пор содержит пробелы, из-за которых усложняется процесс мониторинга ИТ-расходов бюджета и учета действующих ГИС.

Список литературы

1. Бертяков А. В. ИТ-бюджеты федеральных органов власти: знание явное и скрытое. М.: Счетная палата Российской Федерации, ФКУ «ЦЭАИТ СП», 2020. URL: https://ach.gov.ru/upload/pdf/Zapiska_IT_budgets.pdf

2. Бюджетный кодекс Российской Федерации от 31.07.1998 № 145-ФЗ // СПС «КонсультантПлюс». URL:https://www.consultant.ru/document/cons_doc_LAW_19702

3. Государственные информационные системы // Бюллетень Счетной палаты Российской Федерации. 2022. № 8. С. 117. URL: https://ach.gov.ru/statements/bulletin-sp-8-2022

4. Крохина Ю. А. Финансовое право России: учебник. 6-е изд., перераб. М.: Норма; Инфра-М., 2023.

5. Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех», о внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 и признании утратившим силу пункта 6 изменений, которые вносятся в требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных постановлением Правительства Российской Федерации от 11 мая 2017 г. № 555: Постановление Правительства РФ от 16.12.2022 № 2338 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_434913

6. О мерах по обеспечению эффективности мероприятий по использованию информационно-коммуникационных технологий в деятельности федеральных органов исполнительной власти и органов управления государственными внебюджетными фондами: Постановление Правительства РФ от 10.10.2020 № 1646 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_364874

7. О национальном фонде алгоритмов и программ для электронных вычислительных машин: Постановление Правительства РФ от 30.01.2013 № 62 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_141713/

8. О Порядке формирования и применения кодов бюджетной классификации Российской Федерации, их структуре и принципах назначения: Приказ Минфина России от 24.05.2022 № 82н (Зарегистрировано в Минюсте России 30.06.2022 № 69085) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_418512/

9. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_216363

10. О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации: Постановление Правительства РФ от 06.07.2015 № 676 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_182413

11. Поклонский А. Ю., Васильев М. М. Анализ методологий разработки программного обеспечения // Аллея Науки. 2018. № 6(22). С. 1084–1094.
12. Портал ФГИС КИ. URL: https://portal.eskigov.ru
13. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798
14. Шульга Т. Э., Храмов Д. Э. Онтология жизненного цикла разработки программного обеспечения. // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2023. № 2. С. 66–74.

Е. С. Балобанов,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

СОВРЕМЕННЫЕ ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВООТНОШЕНИЙ

Аннотация. Статья посвящена определению роли современных технологий сети Интернет и искусственного интеллекта в системе правоотношений как главных инструментов и помощников человека в различных ситуациях по разрешению правовых проблем, реализации труда, защите прав и интересов и др.

Ключевые слова: право, цифровые технологии, искусственный интеллект, трудовая функция

MODERN DIGITAL TECHNOLOGIES IN THE SYSTEM OF LEGAL RELATIONS

Abstract. This article is aimed at determining the role of modern Internet technologies in solving various situations in the field of legal relations, the possibility of their improvement, as well as the involvement of artificial intelligence in the labor function. The possibility of using artificial intelligence in the future as the main tool and assistant to a person not only in the field of law, but also in various other spheres of human activity, both in the implementation of labor and the protection of rights and interests in various legal spheres, for the convenience of using programs and saving time on finding the right answer to requests and specifics on resolution of legal problems.

Keywords: law, digital technologies, artificial intelligence, labor function

Цифровые технологии в системе правовых отношений в современном мире занимают важное место во всех сферах своего проявления. Развитие технологий влечет за собой развитие не только способностей достигнуть быстрого разрешения определенной ситуации, но и принятия новой нормативной правовой базы относительно урегулирования цифровых технологий.

Если вернуться в прошлое, где всевозможные вопросы необходимо было решать либо через справочную, либо придя на консультацию в какую-либо организацию, то с появлением Интернета все упростилось. При его возникновении было задумано, что это будет сеть, которая не будет контролироваться государством, по задумке это было место для общения, размещения определенной полезной информации, возможности общения на разных концах земного шара с различными людьми. Но с развитием Сети из-за отсутствия регулирования со стороны государства стали появляться различные негативные последствия, что и повлекло за собой возникновение нормативной правовой базы относительно регулирования и наказания.

В системе же правовых отношений технологии такого вида помогают в быстрые сроки, иногда моментально, узнать о верности их действий, получить быструю консультацию на расстоянии с опытными юристами, которые могут оказывать дистанционную помощь.

В 2019 г. с COVID-19 государство было вынуждено наладить возможность работы и обучение своего населения в определенные сроки, и это получилось [7]. Появились новейшие отечественные программы, благодаря которым и в настоящее время происходит процесс выполнения трудовой функции отдельными категориями людей, появились новые профессии и расширились возможности людей [6].

Происходят ситуации, при которых у лиц, желающих получить консультацию у юристов, отсутствуют денежные средства, на это тоже есть помощь. Так существуют различные чат-интернет-боты, которые благодаря технологиям могут в кратчайшие сроки найти необходимую информацию и дать конкретный ответ, конечно, это еще не является точным источником информации, поскольку законодательная база может обновляться несколько раз в год, и уже в зависимости от создателей загруженная в ботов база может обновляться или оставаться устаревшей.

В мире все больше становится интровертов – людей, не желающих контактировать с другими. Им на помощь также приходят цифровые технологии, помогающие связаться со специалистами организаций, которые могут оказывать дистанционное консультирование, составление документов и иных актов как платно, так и на бесплатной основе.

С развитием данных технологий происходит оптимизация кадров, помещений, уже становится не обязательным вкладываться в офисные помещения с большой квадратурой, ведь можно создавать специальные чаты, где группа юристов может реализовывать трудовую функцию, не выходя из дома, естественно, при обеспечении их специальным оборудованием – компьютерами [1. С. 13].

Также происходит развитие искусственного интеллекта (далее – ИИ), благодаря которому консультация и поиск определенных ошибок в составленных договорах становятся максимально оперативными, ведь ИИ может проанализировать загруженную информацию от клиента и проанализировать по всем правилам за считаные секунды и выдать развернутый ответ, ничем не отличающийся от ответа опытного юриста, что в результате своего развития есть опасения о потере такой профессии, как юрист.

ИИ может подстраиваться под каждого клиента индивидуально, вести свою базу данных по пользователям, быть личным ассистентом, что не дает сказать негативное о нем. ИИ может предлагать различные способы в разрешении конкретных проблем клиентов, и решения будут законные, потому что искусственный интеллект не обладает полноценным разумом человека, которому свойственно получение определенной выгоды, даже при не всегда законной своей деятельности и поступках. Благодаря ИИ можно будет сократить количество коррупционных схем по обману как самих клиентов, так и в других сферах жизнедеятельности [5. С. 202–204].

Но, учитывая позитивность такого развития, может произойти и самостоятельное развитие искусственного интеллекта и восстание против человечества. Данный факт отрицать никто не может и гарантировать безопасность тоже, ведь при создании любой новой технологии никто не может знать, как она повлияет на население, будущее государства и т. д.

Таким образом, с созданием информационных технологий население может наиболее быстро разрешить практически любые споры, конфликты.

При ДТП необязательно вызываться сотрудников ГИБДД, достаточно просто зафиксировать самостоятельно и передать снимки в ГИБДД и в страховую компанию, где уже по фотографиям выявят ущерб, при возникновении спорных ситуаций не нужно идти в справочную, можно обратиться к онлайн-операторам или чат-ботам для консультации и разрешения проблемы [3. С. 185–190].

Требуется меньше средств на содержание имущества, с каждым годом траты уменьшаются, сокращаются кадры, тем самым, главным направлением становится внесение средств в развитие технологии, поддержании актуальности информации, которая предоставляется клиентам [4. С. 147–148]. Но важно понимать, что даже при создании технологий, которые облегчают жизнь человека, юристов, нужны люди, ведь без силы мыслей человека нельзя будет создавать какие-либо инновации в мире.

Список литературы

1. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». URL: http://www.consultant.ru

2. Боровская Е. В., Давыдова Н. А. Основы искусственного интеллекта: учебное пособие. 4-е изд., электрон. М.: Лаборатория знаний, 2020. С. 13.

3. Кэти Уорр. Надежность нейронных сетей: укрепляем устойчивость ИИ к обману. С. 185–190.

4. Лука Массарон, Джон Пол Мюллер. Искусственный интеллект для чайников. СПб.: Питер, 2021. 272 с.

5. Яшин С. Н., Иванов А. А., Иванова Н. Д. Анализ зарубежного опыта использования технологических платформ // Цифровая экономика и индустрия 4.0: Форсайт Россия: материалы науч.-практ. конф. с зарубежным участием, Санкт-Петербург, 26–28 марта 2020 г. СПб.: Политех-Пресс, 2020. С. 202–204.

6. Рицу С. Концепция труда: от традиционных социально-трудовых представлений к современным эффектам цифровой трансформации / С. Рицу, Г. Мелипатаки, Д. А. Мате // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 175–190. EDN: ZENNZF

7. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

К. И. Башаратьян,
магистрант,
Санкт-Петербургский государственный университет

НАЦИОНАЛЬНО-ПРАВОВЫЕ И МЕЖДУНАРОДНО-ПРАВОВЫЕ АСПЕКТЫ РЕГУЛИРОВАНИЯ ОБОРОТА НЕВЗАИМОЗАМЕНЯЕМЫХ ТОКЕНОВ

Аннотация. Целью исследования является анализ доктрины относительно правовой сущности криптоактивов, невзаимозаменяемых токенов, в том числе для определения наиболее подходящего правового статуса, что позволит легализовать оборот цифровых активов и исключить злоупотребления со стороны участников оборота.

Ключевые слова: криптоактивы, невзаимозаменяемый токен, блокчейн, смарт-контракт, криптотокен, объект гражданских прав, цифровые права

NATIONAL LEGAL AND INTERNATIONAL LEGAL ASPECTS OF REGULATING THE TURNOVER OF NON-FUNGIBLE TOKENS (NFT)

Abstract. The purpose of the study is to compile all prevailing opinions regarding the legal essence of cryptoassets, non-fungible tokens in particular, in order to determine the most appropriate legal status, which will legalize the circulation of digital assets and exclude abuses by the participants of the circulation. The key features of the article are the structure of the article, taking into account the opinions of leading experts of the legal community of both the Russian Federation and foreign countries, Europe in particular.

Keywords: cryptoassets, non-fungible token, blockchain, smart-contract, cryptotoken, civil rights object, digital rights

С 2021 г. одной из самых обсуждаемых тем в юридическом сообществе являются криптоактивы, которые включают в себя криптомонеты и криптотокены [1. С. 74–115] – два инструмента, которые не являлись новинкой для цифрового пространства, но стали таковой для реального мира. Такая известность обусловлена наиогромнейшим оборотом денежных средств при совершении операций

с криптоактивами, который с каждым годом становится все больше и больше. По данным компании DappRadar, объем сделок с невзаимозаменяемыми токенами (далее – NFT) в первой половине 2021 г. достиг $2,5 млрд, а в 2022 г. торговый оборот NFT на базе Ethereum с начала года составил уже $23,7 млрд, отметили исследователи Nansen. Эта статистика свидетельствует о растущем спросе на криптоактивы.

Такой рост обусловлен не только преимуществами криптоактивов, но и громкими сделками, которые были заключены с целью привлечь внимание общественности к данным инструментам [17]. В качестве примера можно привести сделку, по условиям которой художник Beeple (Майк Винкельманн) продал свою картину в формате NFT за рекордную для рынка сумму – $69 млн через аукционный дом Christie's [14]. В 2021 г. впервые в мире материальное произведение искусства, а именно работа художника Бэнкси Morons (White) была воспроизведена путем создания NFT, а оригинальное произведение было уничтожено посредством сожжения. Сама же картина была куплена для этого перформанса за 80 тысяч долларов, а ее цифровая версия была перепродана за $400 тысяч. И это лишь самые громкие сделки, о которых известно прессе.

Само по себе название NFT – это акроним, произошедший от английских слов «non-fungible token», что переводится как «невзаимозаменяемый токен». Для понимания дальнейших рассуждений важно раскрыть понятия «блокчейн-технология», «токен» и «смарт-контракт».

Блокчейн представляет собой распределенный реестр, который преимущественно необходим для использования криптовалюты [18], наиболее известным представителем которой является биткоин, появившийся на свет в 2009 г. Ключевым преимуществом блокчейна является то, что у данной системы отсутствует центральный сервер, на котором хранятся сведения о всех произведенных и производимых операциях с криптоактивами. В ином случае существовал бы риск того, что если центральный сервер рухнет по причине массированной кибератаки или крупного внутреннего сбоя, то все хранящиеся там сведения будут утрачены либо подделаны, что подорвет доверие людей к такой системе. В ситуации с блокчейном такой риск исключается, поскольку сведения о всех транзакциях хранятся на компьютерах пользователей, являющихся частью системы. На каждом устройстве хранятся свои списки операций, которые регулярно обновляются, что исключает возможность подделки сведений в реестре либо «падения» целой системы. Продажа NFT также осуществляется с использованием технологии блокчейн, поскольку под криптотокеном понимается сама запись в этой системе, подтверждающая право ее обладателя на какое-то благо. То есть, по своей сути невзаимозаменяемый токен представляет собой «цифровую запись об обладании», которая может возникать при помощи использования технологии смарт-контракта.

Отечественный законодатель не истолковывает термин «смарт-контракт», однако некоторые зарубежные догматики попытались дать ему определение. Например, в соответствии с новым законом штата Аризона, под смарт-контрактом понимается программа для ЭВМ, существующая в блокчейне, которая может

контролировать передачу активов и обеспечивать запись о ней в реестре [6]. Эти программы закрепляются на отдельных счетах и могут активироваться посредством особого порядка действий, реализуемого владельцами счетов. Помимо прочего, такие программы могут использоваться для автоматизации заключения и исполнения договоров между пользователями системы, откуда и происходит название «смарт-контракт» [1. С. 74–115]. Он является эффективным инструментом для автоматизации исполнения сторонами своих обязательств.

Вследствие скорого роста популярности криптоактивов и технологии блокчейн, в частности NFT, российские и иностранные догматики дали ему свои определения, отличающиеся по своим формулировкам, но объединенные общей сутью. Например, по мнению Юрия Брисова, члена Комиссии по правовому обеспечению цифровой экономики Московского отделения Ассоциации юристов России, NFT есть видимая технологическая фиксация прав на объект интеллектуальных прав и на него следует распространить положения о цифровых правах, а именно ст. 128 и 141.1 Гражданского кодекса Российской Федерации (далее – ГК РФ) и положения, касающиеся регулирования защиты объектов интеллектуальных прав и товарооборота [15]. Что же касается зарубежной точки зрения, то в иностранной литературе чаще всех цитируется экономист Усман В. Чохан, который определяет NFT как единицу цифровой информации, содержащуюся в децентрализованном реестре и которую нельзя обменять на иные цифровые активы [12].

Центральный банк Российской Федерации также предложил определение токенов для публичного обсуждения в рамках своего доклада «Цифровой рубль». В докладе токены рассматриваются как расчетные единицы в сети блокчейн, которые используются для представления цифрового баланса конкретного актива или для учета гибкого цифрового актива. В отчете подчеркивается, что токены обычно используются для создания деривативов на основе распределенного реестра [4].

Указанные выше субъекты, а также иные догматики сходятся во мнении, что невзаимозаменяемым токенам свойственны следующие отличительные особенности: невзаимозаменяемость или уникальность, нематериальность, неделимость и существование при помощи технологии распределенных реестров. Стоит отметить, что поначалу может показаться, что критерий «уникальность» применим исключительно к объекту прав, на который невзаимозаменяемый токен удостоверяет права, а не к самому токену, поскольку NFT не имеет самостоятельной ценности, так как зависит от ценности закрепленного за ним цифрового объекта. Но автор с таким тезисом не может согласиться, поскольку каждый невзаимозаменяемый токен обладает уникальным идентификатором, а значит, критерий «уникальность» можно распространить и в отношении токена.

Перед российским законодательством поставлено целое множество вопросов: какова правовая природа NFT и цифровых объектов; можно ли рассматривать невзаимозаменяемые токены как объекты права интеллектуальной собственности или эта логика является ошибочной; возникает ли право авторства на произведения, преобразованные в NFT; каков объем приобретаемых прав на цифровое имущество и многие другие. Основополагающим и первостепенным все же является понимание правовой природы NFT, а также цифровых объектов, так как именно

это позволит разработать новые нормы или применить уже существующие методы защиты в отношении сделок с токенизированными объектами, закрепить права и обязанности сторон и упорядочить оборот цифровых активов, т. е. важно понять, потребуются ли «надстройки» в законодательстве для создания правовой определенности в обороте токенов или, руководствуясь принципом «Бритва Оккама», не стоит множить сущности в действующем законодательстве и в отношении токенов можно будет распространить нормы действующего законодательства. Важно отметить, что такой порядок рассуждений уместен в рамках как российского, так и международного законодательства.

Статья 128 ГК РФ закрепляет список объектов гражданского права, в который входят вещи и иное имущество. Из предыдущей градации следует дальнейшая классификация, а именно «иное имущество», которое, исходя из формулировки нормы, подразделяется на «имущественные права» и иные объекты (т. е. имущество, которое не является ни вещами, ни имущественными правами). Для того, чтобы признать NFT объектом гражданских прав, он должен входить в одну из указанных категорий.

Можно ли назвать NFT вещью? Так утверждать крайне проблематично, поскольку ключевой характеристикой вещи как объекта гражданского права является его материальность. Биткоин, NFT и иные криптоактивы не являются овеществленными объектами, они существуют лишь в цифровом пространстве и являются кодом в системе, а значит, и вещью являться не могут. Вследствие такой цепочки рассуждений NFT трудно признать вещью по смыслу ГК РФ. Из этого следует, что как в отношении самого токена, так и оцифрованного объекта интеллектуальной собственности не могут действовать вещно-правовые нормы, а значит и обладатель такого токена не может быть признан его собственником.

Вопреки указанному выше есть, и иное мнение, бытующее в профессиональном сообществе. Так, Сергей Будылин отмечает, что у криптотокенов и вещей есть схожесть, которая заключается в том, что обладатель криптоактивов, подобно владельцу вещи, имеет возможность самостоятельно защищать свои активы от посягательств других лиц, не обращаясь для этого к содействию правопорядка.

Самостоятельная защита криптоактива означает, что доступ к кошельку пользователя обеспечивается при помощи секретного ключа (определенного набора символов). Владелец кошелька хранит данный ключик в секрете и никому о нем не сообщает, никому не демонстрирует. Другие лица, не знающие ключа, не имеют доступа к кошельку. Передать криптоактивы другому пользователю может лишь их обладатель либо кто-то, получивший от него секретный ключ.

Следующая особенность сравнения криптографических токенов с вещами заключается в том, что владелец криптоактива может восприниматься как обладатель абсолютных прав на этот криптоактив (аналогично признанию в рамках правового государства права собственности за владельцем вещи). Важно отметить, что, как и в случае с реальными монетами, злоумышленники могут получить доступ к чужим криптоактивам путем кражи ключей, а также с использованием взлома и мошенничества. Нельзя не отметить, что суть признания криптоактивов «собственностью» заключается в том, что правопорядок оказывает владельцам

криптоактивов помощь в защите от посягательств со стороны других лиц, предоставляя им средства правовой защиты в дополнение к уже известным обществу техническим средствам защиты.

Право может защищать криптоактивы от посягательств со стороны неопределенного круга. Иными словами, правовое государство признает, что владелец криптоактивов обладает абсолютными правами на них. Если понятие собственности является своего рода юридической надстройкой, построенной на понятии физической близости с объектом, то абсолютные права на криптоактивы являются юридической надстройкой, основанной на понятии собственности на криптоактивы [1. С. 74–115].

Все указанное свидетельствует о том, что криптоактивы имеют определенные схожести с вещами. Нельзя не отметить, что квалификация NFT в качестве вещи заметно упростила бы регулирование оборота криптотокенов, позволила бы применять в отношении NFT такие инструменты защиты, как, например, виндикационный иск, поскольку невзаимозаменяемый токен по своим характеристикам мог бы быть сходен с индивидуально определенной вещью.

В международно-правовой практике есть примеры признания криптоактивов вещами, которые хотелось бы выделить. Статья 1122 Гражданского кодекса Китайской Народной Республики (далее – КНР) закрепила широкий перечень собственности, которая может быть передана по наследству, в том числе цифровая валюта, виртуальные игровые продукты и иная интернет-собственность. То есть, в КНР признается наличие абсолютного права, аналогичного праву собственности, на нематериальные объекты, что заметно упрощает действие гражданского законодательства в отношении цифровых объектов. Нематериальность данных объектов не мешает признанию криптоактивов и цифровых объектов вещами.

Если NFT не является вещью, то можно ли признать его имущественным правом по аналогии с бездокументарными ценными бумагами? Такая позиция имеет право на существование и даже предлагалась некоторыми представителями юридического сообщества, поскольку, как и NFT, имущественные права имеют нематериальный характер. Но иных схожестей с имущественными правами у NFT нет. Как верно отмечает М. И. Рожкова, на документарные ценные бумаги существовало «право на бумагу» как объект материального мира и «право из бумаги», т. е. то самое имущественное право, которое подтверждается соответствующим документом. При появлении бездокументарных ценных бумаг «право на бумагу» исчезло, поскольку в нем не было необходимости ведь самой материи не стало. Так как бездокументарная ценная бумага является записью в реестре, то «право на бумагу» и «право из бумаги» были заменены на «право на запись» и «право из записи». В отношении NFT действует именно эта логика. «Право на запись» в таком случае облечено в форму цифрового кода в информационной системе на основе распределенного реестра [11. С. 29–39]. А вот с «правом из записи» ситуация иная, поскольку бездокументарные бумаги и NFT удостоверяют разные вещи. Невзаимозаменяемый токен в юридическом сообществе признается средством инвестирования, однако NFT не может подпадать под эту категорию, ведь основной целью данного токена является исключительно подтверждение существующих

прав, а не инвестиция, в отличие от бездокументарных ценных бумаг. Из указанного следует, что NFT имеет череду отличий, не позволяющих приравнять имущественные права к невзаимозаменяемым токенам. Их нематериальность есть точка соприкосновения двух указанных институтов, однако этого недостаточно для однозначного, итогового вывода.

NFT может подпадать под категорию «иное имущество», не относящееся ни к вещам, ни к имущественным правам. Такая позиция также имеет поддержку в юридическом сообществе, которое полагает, что необходимо разработать отдельные нормы, регулирующие оборот криптоактивов, и включить их в Цифровой кодекс, который активно обсуждается в рамках тематических заседаний и форумов 2023 г. (Петербургский международный экономический и юридический форумы 2023 г.) [16].

Нельзя не отметить, что в Государственную Думу был внесен законопроект № 126586-8 [10] (далее – Законопроект), согласно которому в ст. 1225 ГК РФ предлагается внести поправку в части дополнения закрытого перечня объектов интеллектуальной собственности невзаимозаменяемым токеном. Данная статья устанавливает закрытый перечень результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации. Он был раскритикован юридическим сообществом, поскольку, как было указано ранее, NFT представляет собой запись в реестре блокчейн с информацией о правах на тот или иной объект (в том числе объект интеллектуальной собственности). Из определения прямо следует, что сам NFT нельзя признать результатом интеллектуальной деятельности, он лишь подтверждает права владельца токена на такой объект. По логике Законопроекта, сертификат, удостоверяющий право на объект интеллектуальной собственности, не будет оборотоспособным, т. е. отчуждаться будут имущественные права на такой токен, что технически осложняет их оборот, а значит, дезавуирует одно из главных преимуществ блокчейна как системы – простоту оборота активов. Нельзя не отметить, что NFT может представлять собой не просто запись в распределенном реестре со ссылкой на цифровой объект, хранящийся в репозитории, но и токены, в которые «вшиты» объекты интеллектуальной собственности (если вес таких объектов небольшой). Но от этого сама сущность NFT в качестве записи в реестре не меняется, она лишь осложняется еще одним элементом, а именно результатом творческой или интеллектуальной деятельности. Таким образом, идея о признании NFT в качестве объекта интеллектуальной собственности является неудачным решением инициаторов. Необходимо дальнейшее изучение данного инструмента для определения правовой сущности токенов.

К такому же выводу пришло Правительство Российской Федерации в Официальном отзыве на проект Федерального закона № 126586-8 «О внесении изменений в статью 1225 части четвертой Гражданского кодекса Российской Федерации (в части расширения перечня охраняемых результатов интеллектуальной деятельности в виде невзаимозаменяемых токенов)» (далее – Отзыв), подготовленный 30 августа 2022 г. Авторы Отзыва пришли к выводу, что законопроект не содержит четкого указания на категорию интеллектуальной собственности, к которой можно отнести невзаимозаменяемый токен, а с учетом еще и отсутствия

четкого правового определения NFT его включение в закрытый перечень объектов интеллектуальной собственности приведет к проблемам в правоприменении [9].

Из предыдущих пассажей видно, что встроить NFT в действующее законодательство крайне проблематично в силу его отличия от объектов, указанных в ст. 128 ГК РФ. Ранее была приведена цитата Юрия Брисова, где он причисляет NFT-токен к числу цифровых прав (ст. 141.1 ГК РФ). Но является ли токен таковым?

Согласно ст. 141.1 Гражданского кодекса РФ, цифровые права ограничиваются теми, которые прямо предусмотрены законом в качестве таких прав в специальных законах. На сегодняшний день законодатель предусмотрел два специальных закона, посвященных двум видам цифровых прав: цифровым финансовым активам (далее – ЦФА) и утилитарным цифровым правам (далее – УЦП). Согласно Федеральному закону от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах», к ЦФА относятся: «цифровые права, в том числе денежные требования, предусмотренные решением о выпуске цифровых финансовых активов, возможность осуществления прав, основанных на акциях, право требовать передачи долей участия в уставном капитале общества с ограниченной ответственностью» [7]. Если буквально читать норму этого Федерального закона, то NFT не может являться цифровым финансовым активом, поскольку для признания токена ЦФА он должен содержать цифровые права, которые предусмотрены специальным решением, а значит, всякий токен, находящийся в обороте без соответствующего решения, не является ЦФА по смыслу действующего законодательства. С другой стороны, целевое назначение ЦФА, по мнению автора, заключается в цифровом оформлении прав на соответствующий объект гражданского оборота. Именно такую функцию и выполняет NFT. Отличие заключается в том, что ЦФА не регистрируются в распределенных реестрах, существует централизованная база данных, в которой они фиксируются, хотя возможны и исключения, предусмотренные законом. Если учесть все вышеуказанные пассажи, можно прийти к выводу, что ЦФА и NFT имеют определенную схожесть, однако при буквальном толковании действующего законодательства становится ясно, что в один ряд их поставить не представляется возможным.

Федеральный закон от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ» [8] указывает, что УЦП включает в себя следующие цифровые права: «право требовать передачи вещи, право требовать передачи исключительных прав на РИД, и (или) прав использования РИД, право требовать выполнения работ, и (или) оказания услуг». Эта категория включена в закон для регулирования процесса краудфандинга, т. е. процесса привлечения инвестиций. УЦП представляет собой запись, подтверждающую право инвестора на получение определенных выгод от проекта, в который он вложил определенную сумму денег. По своей функции DRM схожи с «токенами полезности». Токены (utility tokens), представляющие собой право на передачу товаров, уступку исключительных прав, использование объектов интеллектуальной собственности или требование выполнения работ или услуг [1. С. 74–115].

В дополнение к вышеизложенному хотелось бы выделить практику зарубежных юрисдикций, которые имеют диаметрально противоположную точку

зрения касательно сущности NFT как объекта прав. Законодательство Федеративной Республики Германия (далее – ФРГ) в разделе 1 Закона ФРГ «Об инвестициях в активы» (Vermögensanlagegesetz) прямо указывает на то, что NFT могут классифицироваться как криптоактивы, с меньшей вероятностью, как расчетная единица, а в некоторых, скорее частных, случаях как электронные ценные бумаги или инвестиционные активы. Все они признаны законодателем ФРГ финансовыми инструментами. Следовательно, любая услуга, предоставляемая в отношении таких инструментов, будь то консультативная (инвестиционная консультация), купля-продажа, кредитование, могут быть предметом лицензионных требований в ФРГ [13].

В США также наличествует собственный подход к определению правовой сущности токена. Комиссия по ценным бумагам и биржам Соединенных Штатов Америки (далее – SEC) отстаивает позицию, что криптоактивы можно отнести к ценным бумагам, руководствуясь Тестом Хоуи (Howey Test). Тест Хоуи – это стандартная методология, введенная Верховным судом США для признания сделки операцией с ценными бумагами. В частности, криптоактивы и токены признаются ценной бумагой в том случае, если соответствуют следующим параметрам теста:

– инвестиционная деятельность;
– вклад в общее дело;
– инвестирующее лицо намерено извлечь прибыль;
– прибыль зависит от активности третьих лиц.

Однако некоторые американские юристы считают, что отнесение NFT к ценной бумаге является крайне спорным вопросом.

В настоящий момент единого подхода в законодательстве США нет. Для определения сущности каждого отдельного NFT смотрят на цель его создания и продажи. Важно понимать, что если NFT создается и в последующем продается с целью осуществления предпринимательской деятельности, то к возникшим правоотношениям применим Закон США «О ценных бумагах», а если NFT используется или отчуждается для некоммерческих целей, то этот закон неприменим, вследствие чего требуется разработка отдельного нормативно-правового акта с целью создания правовой определенности в отношении статуса такого токена.

Как итог, камнем преткновения для разрешения вопросов перераспределения прав при совершении сделок в отношении NFT-токенов является сама сущность NFT-токена. Обобщая все вышеуказанное, можно прийти к выводу, что NFT в рамках российского законодательства может быть:

1) вещью по смыслу ст. 128 ГК РФ. Применяя такую юридическую фикцию, следует закрыть глаза на нематериальность невзаимозаменяемого токена. Это означает, что в отношении NFT будет действовать большинство норм вещного права, а значит, им можно будет владеть и иметь его в собственности. Такой вывод является допустимым и заметно упрощает регулирование гражданского оборота криптоактивов, не создавая отдельное «Цифровое законодательство»;

2) имущественным правом, однако, автор не считает этот подход допустимым, поскольку нематериальность является единственной характеристикой, объединяющей два инструмента;

3) «иным имуществом», не относящимся ни к вещам, ни к имущественным правам. Этот подход логически безупречен, но тогда неясно какие нормы

гражданского права применимы к этому виду имущества. Поскольку NFT имеет определенные схожести с вещами, возможно применение норм о движимых вещах по аналогии. Но стоит заметить, что термины «владение» и «право собственности» уже не будут применимы к разбираемому инструменту. Возможна замена данных терминов на «обладание» и «абсолютное право».

Первый и третий варианты являются наиболее удобными для реализации. Однако если выбирать одну из возможностей, то автор бы предпочел первый вариант, поскольку такой подход заметно упростит оборот активов без возможного дублирования норм.

Понимание сущности NFT-токена повлечет за собой разрешение совокупности накопившихся вопросов регулирования данного инструмента, распространение схожей логики на иные криптоактивы (биткоин, стейблкоины, утилитарные токены и т. д.), а также урегулировать оборот столь неизвестной и прогрессивной сущности.

Список литературы

1. Будылин С. Л. Криптоактивы: роль в гражданском обороте и правовая природа // Вестник экономического правосудия Российской Федерации. 2023. № 5. С. 74–115.

2. Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Гражданский кодекс КНР от 28.05.2020. URL: http://www.ccdi.gov.cn/yaowen/20–2006/t20200601_219283.html

4. Доклад Банка России для общественных консультаций «Цифровой рубль». URL: https://www.cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf

5. Емельянов Д. С., Емельянов И. С. Невзаимозаменяемые токены (NFT) как самостоятельный объект правового регулирования // Имущественные отношения в Российской Федерации. 2021. № 10 (241). С. 71–76.

6. Закон штата Аризона. URL: https://law.justia.com/codes/arizona/2017/title-44/section-44–7061

7. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 года № 259-ФЗ // Собрание законодательства акты Российской Федерации. 2020. № 31 (часть I). Доступ из справ.-правовой системы «КонсультантПлюс».

8. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 2 августа 2019 года № 259-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

9. Официальный отзыв Правительства РФ на проект федерального закона № 126586–8. URL: https://sozd.duma.gov.ru/bill/126586–8#bh_histras

10. Проект поправок в Федеральный закон № 126586–8. URL: https://sozd.duma.gov.ru/bill/126586–8

11. Рожкова М. А. NFT и иные токены: право на запись и право из записи // Журнал Суда по интеллектуальным правам. 2022, декабрь. Вып. 4(38). С. 29–39.

12. Chohan Usman W. Non-Fungible Tokens: Blockchains, Scarcity, and Value. Critical Blockchain Research Initiative (CBRI) Working Papers, 2021. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822743

13. Di Bernardino Claudia NFT – Legal Token Classification / Di Bernardino, Claudia and Chomczyk Penedo, Andres and Ellul, Joshua and Ferreira, Agata and von Goldbeck, Axel and Herian, Robert and Siadat, Alireza and Siedler, Nina-Luisa // EU Blockchain Observatory and Forum NFT Reports. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891872

14. Michaela Moscufo, Digital artwork sells for record $69 million at Christie's first NFT auction (2021) NBC news, online. URL: https://clck.ru/agswC

15. Как правильно использовать NFT в России и не нарушить закон. URL: https://www.rbc.ru/crypto/news/60e2f4609a794732c30fc130

16. Эксперты ПМЮФ приветствуют разработку Цифрового кодекса и применение ИИ в судах. URL: https://rapsinews.ru/digital_law_publication/20230511/308896477.html

17. Бурдова В. Д. Правовая природа воспроизведения музейных предметов в цифровой форме NFT // Journal of Digital Technologies and Law. – 2023. Т. 1, № 1. С. 152–174. EDN: JMLRDF

18. Жарова А. К. Риски информационной безопасности и возможности правового регулирования криптовалюты в России // Информационное право. 2018. № 4. С. 11–16. EDN: YPNFET

К. В. Белоусов,
магистрант,
Московская высшая школа социальных и экономических наук

ИНТЕРНЕТ ВЕЩЕЙ: ПРОБЛЕМНЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РАМКАХ ПРАВООТНОШЕНИЙ

Аннотация. Статья посвящена анализу проблемных аспектов защиты персональных данных применительно к инфраструктуре интернета вещей. Компоненты инфраструктуры интернета вещей оказывают огромное влияние на жизни пользователей, начиная от фитнес-браслетов, заканчивая умными домами. Однако, согласно пользовательским соглашениям, ежедневно субъектам, занимающимся обработкой таких данных, передается огромный массив конфиденциальной информации (например, информация о здоровье и активности пользователей), накапливающийся с каждым годом, в связи с чем важно обеспечить надежную защиту указанного массива и снизить риск утечки персональных данных.

Ключевые слова: интернет вещей, цифровые технологии, персональные данные, сеть Интернет

INTERNET OF THINGS: PROBLEMATIC ASPECTS OF PERSONAL DATA PROTECTION WITHIN LEGAL RELATIONS

Abstract. The article is devoted to the analysis of problematic aspects of personal data protection in relation to the Internet of Things infrastructure. Internet of Things infrastructure components have a huge impact on the lives of users, from fitness bracelets to smart homes. However, according to user agreements, a huge array of confidential information (for example, information about the health and activity of users), which accumulates every year, is transferred every day to entities involved in the processing of such data, and therefore it is important to ensure reliable protection of this array and reduce the risk of leakage of personal information.

Keywords: IoT, digital technologies, personal data, Internet

Термин «интернет вещей» (далее – IoT) был предложен в 1999 г. Кевином Эштоном на презентации компании Procter & Gamble. Впрочем, общепринятого определения указанного термина не существует. Так, например Оксфордский словарь предлагает понимать под IoT своего рода соединение вычислительных устройств посредством сети Интернет, встроенных в повседневные предметы, что, в свою очередь, позволяет им отправлять и получать данные [9].

Достаточно лаконичное определение содержится в Internet of Things (IoT) Cybersecurity Improvement Act of 2020, где под IoT рассматриваются любые устройства, подключенные и использующие сеть Интернет [6].

Любопытное определение было предложено Е. П. Зараменских [3. С. 79]. Так, под IoT автор рассматривает концепцию мира, в рамках которой информационные системы встроены в традиционные объекты и интегрированы в единое информационное поле.

Определение терминов является важным элементом юридической техники, позволяющим избежать многозначительности и добиться точности толкования соответствующих нормативных актов.

Между тем ни одно из указанных определений в должной мере не раскрывает сущность IoT (да и едва ли возможно корректно изложить важнейшие элементы столь сложной концепции посредством одного короткого предложения, потому и упрекать авторов не слишком уместно).

На практике IoT превращает материальные объекты в своего рода информационную экосистему, позволяющую обмениваться данными между различными носимыми, портативными и имплантируемыми устройствами. Так, IoT объединяет материальный и виртуальный «мир», в рамках которого связь M2M (машина – машина) является связью базового уровня, необходимой для обеспечения взаимодействия между вещами и приложениями в облачных хранилищах.

В рамках термина «интернет вещей» «вещи» представляют из себя те устройства, что позволяют собирать и передавать данные по сети Интернет, притом в автоматическом порядке (без необходимого вмешательства пользователя) [8. P. 79].

Устройства, входящие в экосистему IoT, могут собирать, в частности, контекстные данные по заданным параметрам, шлюзовые устройства (gateway devices)

собирают данные, получаемые из совокупности различных сенсоров и датчиков, направляя данные в централизованное хранилище, где последние подвергаются аналитической обработке.

Вышеприведенные элементы инфраструктуры IoT (каждый из них, а равно и все в совокупности) представляют угрозу конфиденциальности персональных данных.

Так, в центре Политики в области информационных технологий Принстонского университета заметили, что различного рода IoT-устройства нередко передают незашифрованную информацию пользователей в облачное хранилище, притом, взаимодействуя между собой, данные устройства используют облачное хранилище в качестве посредника [5. P. 4].

Кроме того, имеют место и случаи отправки данных (например, информации о здоровье и активности пользователей, как в случае с фитнес-браслетами Fitbit) на неизвестные IP-адреса.

Вышеизложенное приводит к риску утечки конфиденциальной информации пользователей.

В целях реакции и средства противодействия подобного рода рискам был принят «Регламент Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС» (далее – GDPR) [2].

Под персональными данными, в соответствии со ст. 4 (1) GDPR, понимается любая информация, что относится к субъекту данных (лицо, которое подлежит прямой или косвенной идентификации) и может обрабатываться исключительно с его согласия (ст. 7).

Обработка персональных данных, в соответствии со ст. 5 GDPR, осуществляется на основе таких принципов, как: законность, справедливость и прозрачность; ограничение; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность; ответственность (подотчетность) [10].

Аналогичные принципы обработки персональных данных закреплены и в отечественном законодательстве.

Так, ст. 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных) [4] формализует следующие принципы: законная и справедливая основа обработки персональных данных (принцип законности), ограничение обработки персональных данных конкретными и законными целями, точности и достаточности персональных данных при их обработке, хранение персональных данных должно осуществляться таким образом, чтобы позволить определить субъект персональных данных, и не дольше цели такой обработки.

Как видно из приведенных выше положений, Закон о персональных данных практически дублирует положения GDPR. Указанное справедливо не только для ст. 5 данного закона.

Например, определение персональных данных, закрепленное в п. 1 ст. 3, в соответствии с которым под последними полагается понимать информацию, что прямо или косвенно относится к субъекту персональных данных.

Вышеприведенное определение (ввиду его тождественности), равно как и определение, данное в GDPR, указывает, что любая информация, что позволяет косвенно определить субъект последней, относится к персональным данным, а значит, и подпадает под регулирование указанных положений.

Излишняя «широта» является недостатком данного определения, впрочем, и «сужение» последнего – решение в известной степени опасное. Поиск столь необходимого баланса, что позволит избежать правовой неопределенности и обезопасить субъектов персональных данных от нарушения конфиденциальности, – задача, которую предстоит решить доктрине.

В США IoT регулируется, в частности, общими нормами, что не были разработаны с учетом специфики IoT, к указанным относится, например, Privacy Act 1974, что основывается на Руководстве по принципу справедливой информационной практики (Fair Information Practice Principles, FIPP) [11. P. 110].

FIPP включает в себя, кроме прочего, принцип уважения контекста, что непосредственно выражается в наличии у потребителей права требовать, чтобы сбор, хранение и использование персональных данных соответствовали цели их предоставления.

Кроме того, пользователи имеют право контролировать в индивидуальном порядке сбор и использование своих персональных данных компаниями.

В соответствии с указанными принципами Белым домом была выдвинута инициатива по определению необходимых рамок для защиты потребителя в условиях современных интернет-технологий [12].

Таким образом, принципы, закрепленные в GDPR, Законе о персональных данных и FIPP, в известной степени схожи.

Однако большинство пользователей, давая согласие на обработку персональных данных, не читают пользовательское соглашение.

Так, пользователи приложения, отслеживающего спортивную активность (посредством данных, передаваемых фитнес-браслетами, например, ранее упомянутым Fitbit), отправляли данные о своих передвижениях в компанию Starva, а та размещала их на карте The Global Heat Map. Примечательно, что среди пользователей были военнослужащие вооруженных сил США, чьи перемещения также были размещены на указанной карте.

Таким образом, широкий круг интернет-пользователей смог увидеть в The Global Heat Map расположение военных баз США в Ираке, Сирии, Афганистане и т. д. [7].

В указанном случае не имела место утечка данных вследствие непринятия компанией Starva необходимых мер безопасности, данные также не были переданы в незаконном порядке третьим лицам, пользователи сами дали согласие на использование их персональных данных для данной цели, что вполне соответствует принципу целевого ограничения. Данная ситуация стала следствием нежелания пользователей ознакомиться с положениями соглашения об обработке персональных данных.

Определенную опасность представляет и уязвимость баз данных, где хранятся персональные данные пользователей.

Так, в 2022 г. произошла массовая утечка данных пользователей «Яндекс еды». В сети Интернет были опубликованы данные о миллионах пользователей, включая их номера телефонов, адреса, Ф.И.О. и т. д.

Анализируя судебную практику [1], полагается сделать вывод, что суды, удовлетворяя требования истцов о возмещении морального ущерба, приходят к выводу о наличии причинно-следственной связи между утечкой персональных данных и недостаточностью мер безопасности, принятых ответчиком.

Следует заметить, что для повышения уровня защищенности персональных данных в рамках инфраструктуры IoT метаданные, непосредственно относящиеся к персональным данным субъекта, должны быть замаскированы и предоставляться только для авторизованного доступа.

Кроме того, поскольку информация, хранящаяся в формате cookies, используется для таргетирования индивидуальной (для каждого пользователя) рекламы в коммерческих целях, необходимо предоставлять доступ к последней исключительно через достаточно защищенные серверы с высоким уровнем шифрования передачи данных.

Таким образом, принципы, закрепленные в GDPR, Законе о персональных данных и FIPP, схожи, позволяют обрабатывать персональные данные лишь с согласия субъекта последних, предъявляются и требования к безопасности хранения указанных данных (при этом конкретные технические меры, которые необходимо принять для обеспечения безопасности персональных данных, не раскрываются).

Список литературы

1. Апелляционное определение Московского городского суда от 14.06.2023 по делу № 33-25182/2023. URL: https://www.consultant.ru/search/?q=33-25182 %2F2023

2. Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных. URL: https://base.garant.ru/71936226

3. Зараменских Е. П. Основы бизнес-информатики: учебник и практикум для вузов. 2-е изд. М.: Юрайт, 2023. 79 с.

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». URL: https://www.consultant.ru/document/cons_doc_LAW_61801

5. Chaudhuri, Abhik. «Internet of things data protection and privacy in the era of the General Data Protection Regulation» // Journal of Data Protection & Privacy, Henry Stewart Publications. 2016. Vol. 1(1). P. 4.

6. IoT Cybersecurity Improvement Act of 2020. Available online: https://www.cio.gov/handbook/it-laws/iot

7. Liz Sly. U.S. soldiers are revealing sensitive and dangerous information by jogging. URL: https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?hpid=hp_hp-top-table-main_strava-415pm%3Ahomepage%2Fstory

8. Mouha R. A. Internet of Things (IoT). Journal of Data Analysis and Information Processing. 2021. № 9. P. 79.

9. Oxford Dictionaries, Definition of “Internet of Things”. URL: https://www.lexico.com/en/definition/internet_of_things

10. Утеген Д. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования / Д. Утеген, Б. Ж. Рахметов // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 825-844. EDN: DRGDDJ

11. Tzafesta, S. G. Ethics and Law in the Internet of Things World. Smart Cities 2018, 1, 98-120.

12. White House. Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. 2012. URL: http://www.whitehouse.gov/ sites/default/files/privacy-final.pdf

М. П. Бессонов,
магистрант,
Среднерусский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

ФОРМИРОВАНИЕ ДОКУМЕНТОВ ДЛЯ ГОСУДАРСТВЕННОЙ РЕГИСТРАЦИИ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН ИЛИ БАЗЫ ДАННЫХ СРЕДСТВАМИ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматривается процесс регистрации программ для электронно-вычислительных машин и баз данных. Приводятся требования, которым должны соответствовать объекты патентования, а также рассматривается суть регистрации как способа защиты идеи, заложенные в программы для электронных вычислительных машин или базы данных, и суть технического решения. Кроме того, в статье описывается авторская программа, упрощающая заполнение документов, необходимых для регистрации.

Ключевые слова: право, цифровые технологии, государственная регистрация, программа для ЭВМ, база данных, патент

FORMATION OF DOCUMENTS FOR STATE REGISTRATION OF COMPUTER PROGRAMS AND DATABASES BY MEANS OF DIGITAL TECHNOLOGIES

Abstract. The article discusses the process of registering programs for electronic computers and databases. The requirements that the objects of patenting must meet are given, and the essence of registration as a way to protect ideas embedded in computer programs or databases and the essence of a technical solution are also considered. In addition, the article describes the author's program that simplifies filling out the documents required for registration.

Keywords: law, digital technologies, state registration, computer program, database, patent

В современном мире практически не осталось таких сфер жизни, которые не были бы так или иначе связаны с информационными технологиями. С появлением электронно-вычислительных машин (далее – ЭВМ) и, как следствие, возможности создания различных программ и информационных хранилищ остро возник вопрос создания такой системы регулирования правовых отношений, которая позволила бы при помощи различных правовых институтов создать все необходимые условия для охраны этих объектов.

Компьютерные программы, так же как и базы данных, на территории РФ относятся к объектам авторского права. При этом нужно сказать, что компьютерные программы принято относить к литературным произведениям [4]. Следовательно, законодательство РФ охраняет код компьютерных программ (т. е. текст, написанный на каком-либо языке программирования) так же, как и тексты книг (п. 1, ст. 1261 ГК РФ).

Но на практике часто возникает ситуация, при которой одно лицо, увидев результат работы программы для ЭВМ у другого лица, создает свою программу, которая может существенно отличаться от оригинальной по содержанию программного кода, но иметь функционал, идентичный оригиналу. А так как законами РФ не предусмотрено распространение охраны в авторском праве на содержание программы для ЭВМ (на ее структуру, функционал, алгоритмы и т. п.), необходим был особый режим правовой охраны: патентование [2].

Рассмотрим защиту программ для ЭВМ и баз данных (далее – БД) с точки зрения патентного законодательства Российской Федерации. Определения рассматриваемых в статье объектов патентования подробно приведены в ст. 1260, 1261 ГК РФ. Здесь только стоит отметить, что при патентовании программа будет рассматриваться как изобретение в случае наличия конкретных технических средств, предназначенных для решения конкретной технической задачи (п. 5 ст. 1350 ГК РФ). Также при регистрации баз данных стоит учитывать, что хранимые материалы необязательно должны быть оригинальными. Достаточно, чтобы они представляли собой ценную информацию.

Стоит оговориться, что для успешного патентования программы для ЭВМ/базы данных необходимо соблюдение трех условий патентоспособности [3]: новизна (разработанный объект не является известным на уровне техники), изобретательский уровень (создание объекта не является очевидным из текущего уровне техники) и промышленная применимость (программа или база данных может быть использована в какой-либо сфере жизни общества).

Закон Российской Федерации (ст. 1262 ГК РФ) позволяет владельцу зарегистрировать программу для ЭВМ или базу данных в Федеральной службе по интеллектуальной собственности (также известной как Роспатент).

Для регистрации программы для ЭВМ или БД необходимо представить определенные документы [1]: заявление о регистрации программы для ЭВМ или базы данных; материалы для однозначной идентификации (фрагменты исходного текста, структура базы данных и т. п.); реферат; согласие на обработку персональных данных и на указания сведений об авторе. Кроме того, нужно приложить документ об оплате государственной пошлины.

Так как перечень необходимой документации достаточно объемный, а также при оформлении некоторых документов нужно учитывать ряд установленных правил [6], для упрощения процесса формирования документации автор статьи (выпускник Орловского государственного университета им. И. С. Тургенева, бакалавр направления подготовки «Программная инженерия») создал программу на языке программирования Python, которая будет предоставлять пользователю определенные поля для заполнения, а затем на их основе сформирует необходимые документы.

Официальные шаблоны документов будут взяты с сайта Роспатента. Также оттуда будет взята информация для формирования дополнительных подсказок пользователю: реквизиты для оплаты и адреса (электронный и физический) для подачи комплекта документов.

Основной интерфейс будет включать в себя ряд полей, которые необходимо заполнить вручную, а также выборов некоторых необходимых параметров регистрации (рис. 1).

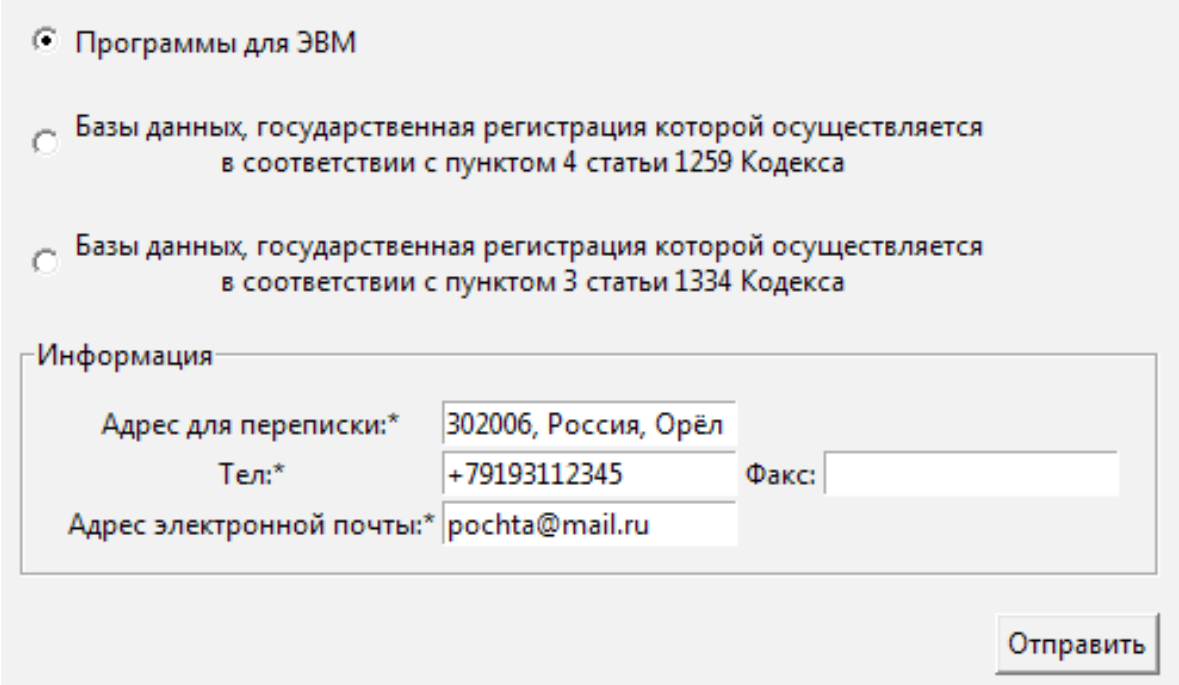

Рис. 1. Внешний вид программы для формирования документации для регистрации

Таким образом, государственная регистрация программ для ЭВМ/БД защищает суть технических решений, заложенную в них идею. Она позволяет избегать споров, касающихся прав на созданную программу, с другими авторами или третьими лицами. Но так как для регистрации программы для ЭВМ/базы данных необходимо предоставить в Роспатент определенные документы, каждый из которых имеет определенные правила заполнения, а также из-за того, что при регистрации невозможно подать одну заявку на программу и базу данных совместно

(или на несколько программ) [5], упрощение заполнения документов позволит снизить вероятность ошибки и увеличить качество обработки документа.

Список литературы

1. Государственная регистрация программы для электронных вычислительных машин или базы данных. URL: https://rospatent.gov.ru/ru/stateservices/gosudarstvennaya-registraciya-programmy-dlya-elektronnyh-vychislitelnyh-mashin-ili-bazy-dannyh-i-vydacha-svidetelstv-o-gosudarstvennoy-registracii-programmy-dlya-elektronnyh-vychislitelnyh-mashin-ili-bazy-dannyh-ih-dublikatov

2. Захарова А. В. Проблемы правовой охраны программ для электронно-вычислительных машин. 2021. URL: http://ui.tsu.ru/wp-content/uploads/2021/07/Захарова-Алена-Викторовна.pdf

3. Защита программ для ЭВМ в мире. 19.02.2019. URL: https://zakon.ru/blog/2019/02/19/zaschita_programm_dlya_evm_v_mire

4. Какие права имеет автор программы для ЭВМ и базы данных. – 26.05.2020. URL: https://zakon.ru/blog/2020/05/26/kakie_prava_imeet_avtor_programmy_dlya_evm_i_bazy_dannyh

5. Необходимость регистрации программы для ЭВМ и базы данных, а также тонкости и нюансы при их регистрации. 11.04.2019. URL: https://zakon.ru/blog/2019/04/11/neobhodimost_registracii_programmy_dlya_evm_i_bazy_dannyh_a_takzhe_tonkosti_i_nyuansy_pri_ih_registr

6. Приказ Минэкономразвития России от 05.04.2016 № 2. Роспатент. URL: https://rospatent.gov.ru/ru/documents/prikaz-minekonomrazvitiya-rossii-ot-05-04-2016-211

К. В. Блинова,
магистрант,
Южно-Уральский государственный университет
(национальный исследовательский университет)

ДОГОВОРНЫЕ ФОРМЫ ГОСУДАРСТВЕННО-ЧАСТНОГО ПАРТНЕРСТВА В СФЕРЕ ЦИФРОВЫХ ИННОВАЦИЙ И ТЕХНОЛОГИЙ

Аннотация. Статья посвящена исследованию государственно-частного партнерства в сфере цифровых инноваций и технологий. Анализируются нормативные акты, регулирующие развитие цифровых инноваций, практика применения данного института в целях развития конкурентоспособных цифровых инноваций и технологий, а также проблемы в реализации государственно-частного партнерства в сфере цифровых инноваций и технологий. Предложены способы совершенствования законодательства в данной сфере.

Ключевые слова: государственно-частное партнерство, муниципально-частное партнерство, концессионное соглашение, информационные технологии, цифровые технологии, цифровизация, искусственный интеллект, право

CONTRACTUAL FORMS OF PUBLIC PRIVATE PARTNERSHIP IN THE FIELD OF DIGITAL INNOVATION AND TECHNOLOGY

Abstract. The article is devoted to the study of public-private partnership in the field of digital innovations and technologies. The normative acts regulating the development of digital innovations, the legally established methods of implementation, as well as the current application of this institute in order to develop competitive conditions for digital innovations and technologies are being investigated. Problems in the implementation of public-private partnership with digital innovations and technologies and planned development trends in this area

Keywords: public-private partnership, municipal-private partnership, concession agreement, information technologies, digital technologies, digitalization, artificial intelligence, law

Одной из важных задач сегодня является создание отечественных конкурентоспособных цифровых технологий [1. С. 42]. Указанное объясняется тем, что на данном этапе развития ряд секторов национальной экономики и промышленного производства испытывают проблемы с отсутствием необходимых цифровых технологий, ранее импортируемых из-за рубежа. Это касается и квантовых технологий [2].

Государственно-частное партнерство (далее – ГЧП) в сфере цифровых технологий потенциально может стать одним из способов решения указанной проблемы. Дело в том, что реализация инновационных проектов в рамках ГЧП является выгодным как для публичной стороны, так и для частной стороны [4. С. 202]. Так, например, в Европейском союзе разработка технологий искусственного интеллекта успешно осуществляется на началах ГЧП [5. С. 17].

На сегодняшний день можно выделить две основных формы ГЧП в сфере цифровых инноваций и технологий. Так, в Федеральном законе «О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 13 июля 2015 г. № 224-ФЗ (далее – Закон о ГЧП) отмечается, что соглашение о ГЧП может заключаться по поводу создания: программ ЭВМ, баз данных, информационных систем и (или) сайтов в информационно-телекоммуникационной сети Интернет или других информационно-телекоммуникационных сетях, в состав которых входят такие программы для ЭВМ и (или) базы данных, либо совокупность указанных объектов (далее – объекты информационных технологий), либо объекты информационных технологий и имущество, технологически связанное с одним или несколькими такими объектами и предназначенное для обеспечения их функционирования или осуществления иной деятельности, предусмотренной соглашением (п. 19 ст. 7). Аналогичная норма содержится и в Федеральном законе «О концессионных соглашениях».

На сегодняшний день в России заключены всего лишь восемь соглашений о ГЧП и шесть концессионных соглашений. Одним из примеров такого партнерства выступает проект «PROПуск», направленный на создание технологической витрины региона, реализуемый в Челябинской области. Вкладываемые в него

частные инвестиции составляют 59,8 млн руб. Суть проекта заключается в создании выставочной площадки для профориентации и обмена техническими знаниями, где также возможно будет развернуться и бизнесу путем презентации и поиска как партнеров, так и товаров и закупочных материалов.

Думается, что столь малое число проектов в сфере инновационного ГЧП может быть обусловлено тем, что перечень объектов в сфере информационных технологий является достаточно ограниченным, а используемая терминология явно устарела. Так, следует согласиться с учеными, полагающими, что тот факт, что на основе ГЧП можно создать только лишь объекты информационных технологий, ограничивает возможность осуществления ГЧП в сфере инновационной деятельности. Избранный законодателем термин «объекты информационных технологий» существенно ограничивает потенциал ГЧП в сфере создания инноваций [3. С. 34].

В этой связи необходимо отметить, что законодательство о ГЧП все еще требует модернизации и адаптации к современным условиям развития.

Список литературы

1. Громова Е. А. Создание цифровых технологий в рамках государственно-частного партнерства: опыт БРИКС // Вестник ЮУрГУ. Серия: Право. 2019. Т. 19, № 1. С. 42–45.

2. Громова Е. А., Петренко С. А. Квантовое право: начало // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 62–88. EDN: FKAWRT.

3. Громова, Е. А. Государственно-частное партнерство в цифровую эру: поиск оптимальной правовой формы // Юрист. 2018. № 10. С. 34–40.

4. Севастьянова И. Г., Докшина М. А. О механизмах поддержки инновационной деятельности в условиях модернизации российской экономики // Фундаментальные исследования. 2016. № 2. С. 202–208.

5. Ferreira D. B., Gromova E. Tools to stimulate Blockchain: application of regulatory sandboxes, special economic zones, and public-private partnerships // International Journal of Law in Changing World. 2023. Vol. 2, № 1. Pp. 17–36.

Д. А. Бойковская,
студент,
Московский государственный юридический
университет имени О. Е. Кутафина (МГЮА)

МОЖНО ЛИ ПРИЗНАТЬ СЛУЖЕБНЫМ ПРОИЗВЕДЕНИЕМ РЕЗУЛЬТАТ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА?

Аннотация. Цель исследования настоящей статьи заключается в определении правового статуса продукта, созданного искусственным интеллектом. В частности, основания возникновения прав на такой продукт у работника, использующего искусственный интеллект, и у работодателя. Отдельно рассматривается

вопрос о роли искусственного интеллекта в процессе генерирования продукта и критерий творческого участия автора в создании результата интеллектуальной деятельности.

Ключевые слова: право, цифровые технологии, искусственный интеллект, нейросеть, работник, результат интеллектуальной деятельности, служебное произведение, исключительное право

WHETHER THE RESULT OF INTELLECTUAL ACTIVITY OF ARTIFICIAL INTELLIGENCE CAN BE RECOGNISED AS A WORK MADE FOR HIRE?

Abstract. The purpose of the research of this article is to determine the legal status of a product created by artificial intelligence. In particular, the grounds for the emergence of rights to such a product from the employee using artificial intelligence and from the employer. The issue of the role of artificial intelligence in the process of generation of the product and the criterion of creative participation of the author in the creation of the result of intellectual activity are considered separately.

Keywords: law, digital technologies, artificial intelligence, neural network, employee, results of intellectual activity, a work made for hire, intellectual property

Представим ситуацию, что издательское агентство поручило своему штатному сотруднику написать очередной детский рассказ для выпуска ежемесячного сборника детских рассказов. Сотрудник его написал, но с использованием технологии искусственного интеллекта (далее – ИИ). Можно ли считать находчивого работника автором, а полученное произведение – служебным? Возникнет ли у издательского агентства исключительное право на такой рассказ?

Для разрешения спорных вопросов необходимо в первую очередь определить правовой статус самого неоднозначного участника данной цепочки – искусственного интеллекта.

Искусственный интеллект определяется как 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 [5]. Результаты функционирования ИИ сопоставимы, но никак не приравнены к результатам интеллектуальной деятельности человека в понимании статьи 1225 Гражданского кодекса Российской Федерации [1] (далее – ГК РФ). Отсюда можем сделать вывод: сам законодатель не спешит ставить в один ряд продукты, создаваемые человеком, и продукты ИИ. Логика данного определения вполне разумна – распространение на результаты функционирования ИИ правового режима результатов интеллектуальной деятельности означало бы наделение ИИ, как носителя прав на результат интеллектуальной деятельности и, соответственно, как субъекта правоотношений, всеми сопутствующими правами и обязанностями, в том числе исключительным правом на созданные результаты. Однако на данный момент придание ИИ правосубъектности противоречит основным положениям законодательства Российской Федерации, а также законодательству зарубежных стран [2].

Помимо прочего, сам ИИ также является результатом чьей-то интеллектуальной деятельности. В правилах использования сервисов и платформ, функционирование которых основано на технологии ИИ, правообладатели зачастую не распространяют действие авторского права на продукты, сгенерированные нейросетью. К тому же разработчики и себе не присваивают исключительное право на результаты деятельности ИИ. Так, платформа DeepAI [6], основанная на технологии ИИ, прямо указывает на неприменение авторского права ко всему сгенерированному контенту. Соответственно, ни пользователь, ни сам искусственный интеллект не могут признаваться автором, а полученный с помощью нейросети объект – произведением.

Более того, ключевой критерий отнесения продуктов человеческого ума к результатам интеллектуальной деятельности – творческий характер деятельности. Об этом прямо свидетельствует позиция высших судов [3. абз. 2 п. 80]. Здесь важно отметить, что понятие интеллектуальной деятельности и творческой деятельности не тождественны. Функционирование ИИ способно только имитировать когнитивные функции человека, однако творческие способности человеческого разума ему не свойственны. Нейросеть создает продукты с помощью алгоритмов, на которых она обучена и с помощью той базы данных, на которой она была обучена. Исходя из указанного, можно предположить, что результату деятельности искусственного интеллекта если и присущ, то только интеллектуальный характер, имитирующий когнитивные функции, но никак не творческий характер деятельности. Также невозможно представить ситуацию, что ИИ вдохновился внешним миром или на основе пережитого жизненного опыта через призму внутреннего ощущения создал произведение, деятельность по созданию которого сопряжена с творческим вкладом.

Также еще одним аргументом в пользу неприменимости понятия «результат интеллектуальной деятельности» в отношении объектов, созданных ИИ, является философия И. Канта и Г. Гегеля и созданная на ее основе личная теория (personal theory), согласно которой в результате интеллектуальной деятельности отражена личность человека. На постулатах о произведении как «печати индивидуальности автора» строилась и цивилистическая доктрина [4. С. 42]. На сегодняшний день говорить о присущей ИИ личности преждевременно.

Исходя из вышеприведенных рассуждений, следует лишь один вывод: результаты деятельности искусственного интеллекта нельзя отнести к результатам интеллектуальной деятельности в понимании ст. 1225 ГК РФ [1]. Искусственный интеллект не может признаваться автором генерируемых продуктов, он всего лишь инструмент в руках работника.

Следовательно, возникает вопрос: авторство произведения, сгенерированного ИИ, принадлежит сотруднику и произведение является служебным?

Вернемся к творческому характеру деятельности как ключевому признаку результата интеллектуальной деятельности. В соответствии со ст. 1257 ГК РФ [1] автором произведения признается гражданин, творческим трудом которого оно создано. Точного определения, что понимается под творческим трудом, законодатель не дает.

При этом использование автором технических средств при создании произведения не исключает творческий характер деятельности его создателя [2. п. 80]. Соответственно, искусственный интеллект в его самом упрощенном виде можно обозначить как «техническое средство», и использование работником такового при создании произведения не исключает его творческий вклад. Но это не так: работник не может признаваться автором, если он не принимал творческого участия в создании произведения.

Все же вопрос о творческом характере деятельности остается открытым. Например, можно ли считать творческим характером деятельность работника детально сформулированный и продуманный для конкретной задачи промт – запрос для нейросети? Вопрос остается открытым.

Соответственно, разрешая вопрос о признании работника автором, а произведения – служебным, необходимо выяснить, был ли внесен творческий вклад работника в создание, доработку или переработку произведения, которое является продуктом функционирования искусственного интеллекта, и в каком количестве и качестве наличествовал данный вклад. Если рассматривать вклад сотрудника исключительно в формулировании промта, то, по мнению автора данной статьи, это недостаточный вклад в создание произведения. Запрос для нейросети не отражает личность автора, его творческие способности.

В то же время если работник, получив результат деятельности искусственного интеллекта, доработал его путем детализации персонажей, включения дополнительного сюжетного поворота, добавления средств выразительности и т. д. и если такой вклад отвечает требованию «творческой» деятельности, то произведение может быть признано служебным, а работник – автором.

Следовательно, признание произведения, сгенерированного ИИ и доработанного человеком, в качестве служебного влечет за собой все сопутствующие юридические последствия, в частности, возникновение у работодателя исключительного права на данное произведение, а у работника, например, права на выплату авторского вознаграждения.

Таким образом, можно сделать следующие выводы: результаты деятельности искусственного интеллекта действующим законодательством не охраняются в качестве объектов интеллектуальной собственности, авторами произведений могут выступать только физические лица, а произведение может считаться служебным только при существенном творческом вкладе работника по его созданию, даже при использовании технологии искусственного интеллекта.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_64629

2. Галлезе-Нобиле К. Регулирование умных роботов и искусственного интеллекта в Европейском союзе // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 33-61. EDN: UNSONV.

3. Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации». // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_323470

4. Спасович В. Права авторские и контрафакция. СПб.: Тип. М. О. Вольфа, 1865. С. 42.

5. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335184

6. Terms of Service. URL: https://deepai.org/terms-of-service/terms-of-service

М. А. Бурдакова,
магистрант,
Волгоградский государственный университет

НАЛОГ НА ПРОФЕССИОНАЛЬНЫЙ ДОХОД КАК ЭФФЕКТИВНОЕ ПРОЯВЛЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Аннотация. Данное исследование посвящено специальному налоговому режиму – налогу на профессиональный доход. В рамках исследования сформулирована цель по выявлению эффективных проявлений цифровых технологий в налоговых правоотношениях. Для достижения указанной цели рассмотрены некоторые аспекты налогообложения самозанятых через призму цифровых технологий. Обозначена существующая в настоящее время проблема отсутствия обязанности по уплате страховых взносов и сложности их уплаты в порядке волеизъявления.

Ключевые слова: налог на профессиональный доход, цифровые технологии, налоговые правоотношения, налогоплательщик, страховые взносы, специальный налоговый режим, налогообложение самозанятых

PROFESSIONAL INCOME TAX: EFFECTIVE MANIFESTATION OF DIGITAL TECHNOLOGIES

Abstract. This study is devoted to a special tax regime – the tax on professional income. Within the framework of this study, the author formulated a goal to identify effective manifestations of digital technologies in tax legal relations. To achieve this goal, the author considered some aspects of taxation of the self-employed through the prism of digital technologies. In addition, the current problem of the lack of obligation to pay insurance premiums and the difficulty of paying them by way of expression of will was identified.

Keywords: professional income tax, digital technologies, tax legal relations, taxpayer, insurance premiums, special tax regime, taxation of the self-employed

Каждое государство обладает естественным и неотъемлемым правом в получении налоговых платежей, поскольку без их получения представится невозможна реализация основных задач государства, в том числе и по вопросам суверенитета и безопасности государственных границ.

Пополнение бюджета государства является важной задачей, результаты которой позволяют не только осуществить функции государства по обеспечению безопасности населения, но и предоставить населению социальные блага, достойные демократического общества. Социально-экономические проблемы, стоящие перед государством, – это задачи, которые государство может решить посредством налогообложения с помощью установления соответствующих налоговых платежей. В результате верной налоговой политики государство обладает возможностью разрешить две основные задачи: пополнение государственного бюджета и решение социальных проблем.

В настоящее время решение указанных выше задач осложняется такими процессами, как глобализация, всеобщее взаимодействие различных государств с разным уровнем экономики в рамках гиг-экономики, а также цифровизация. Все перечисленные процессы влияют на цели, способы и варианты решения поставленных перед государством задач. При этом все трансформации, которые происходят, способствуют осуществлению государством активных действий, соответствующих тем или иным вызовам. Налоговая сфера не является исключением.

В настоящее время у российского законодателя присутствует успешный опыт разрешения важной социальной проблемы посредством налогообложения. До 2018 г. в Российской Федерации существовала проблема теневой деятельности самозанятых, по решению которой осуществлялись различные попытки без положительного результата.

В ноябре 2018 г. Российская Федерация представила уникальный эксперимент, результаты которого с точки зрения поставленной цели по выводу самозанятых из тени экономической деятельности превзошли любые ожидания. Налог на профессиональный доход был в режиме эксперимента на определенных территориях, среди которых Москва, Московская и Калужская области и Республика Татарстан. Показательным, на наш взгляд, является тот факт, что уже в 2020 г. эксперимент был распространен на всю территорию Российской Федерации, что уже свидетельствует о его успешности.

Следует отметить, что уникальность данного эксперимента заключается, во-первых, в том, что в Российской Федерации деятельность самозанятых урегулирована наиболее оптимальным способом, способствующим дальнейшему развитию современной экономики государства, по сравнению с многими другими государствами, которые каким-либо образом затрагивали вопрос налогообложения самозанятых.

Во-вторых, подобный эксперимент приобрел популярность среди самозанятых, о чем свидетельствует тот факт, что на 31.08.2023 количество самозанятых, являющихся налогоплательщиками НПД, достигло более 8 млн человек (а именно 8 283 519 человек) [6], тогда как на 30.12.2020 подобная цифра была чуть больше 1 млн человек. Подобная статистика свидетельствует об успешности эксперимента, поскольку количество самозанятых, вышедших из тени, больше, чем изначально предполагалось.

Следует отметить, что любые налоговые правоотношения строятся на обязанности налогоплательщика внести установленную сумму в качестве налога, поступающего в соответствующий бюджет.

Характеризуя тот или иной налоговый режим, следует отметить, что существенное значение имеет определение субъекта налоговых правоотношений.

В этой связи интересно обратить внимание и на мнение известного ученого-правоведа С. С. Алексеева, который в своих трудах отмечал, что в качестве содержания правового статуса субъекта следует понимать, прежде всего, правовое положение субъекта, которое способствует отражению его «фактического состояния во взаимоотношениях с обществом и государством» [1].

Субъектный состав налоговых правоотношений в рамках специального налогового режима НПД определен ФЗ о налоге на профессиональный доход. Законодателем достаточно четко сформулировано, кто является налогоплательщиком НПД.

В науке налогового права вопросу субъекта НПД уделено достаточное внимание, поскольку существуют различные дискуссии относительно определения, сформулированного законодателем.

Обращая внимание на точку зрения М. Д. Шапсуговой, отметим, что ФЗ о НПД «деятельность плательщика такого налога не относит к предпринимательской, выделяя в качестве ее признаков отсутствие работодателя при ее ведении, запрет на привлечение наемных работников по трудовым договорам, а также получаемый от использования имущества доход» [9].

По мнению автора данной статьи, следует определить два ключевых аспекта, которые достаточно удачно были определены законодателем. Во-первых, речь идет о субъектах, иначе говоря, налогоплательщиками НПД являются исключительно либо физические лица, либо индивидуальные предприниматели. Во-вторых, одной из основных особенностей является указание на вид деятельности. Налогоплательщики НПД осуществляют исключительно профессиональную деятельность, подразумевающую под собой соответствующий творческий, интеллектуальный результат, выраженный в различных формах. Думается, что это подчеркивает уникальность статуса самозанятого.

Из этого логичном вытекает вопрос о необходимости рассмотреть и такой аспект, как виды деятельности налогоплательщика НПД, так как речь идет об отдельной категории, которая обладает определенной спецификой. В этой связи законодатель ограничил виды деятельности для налогоплательщиков НПД, поскольку подразумевалось, что рассматриваемый налоговый режим направлен непосредственно на самозанятых.

Во-первых, налогоплательщики НПД не могут осуществлять реализацию подакцизных товаров и товаров, подлежащих обязательной маркировке.

Во-вторых, под запрет попадают такие виды деятельности, как перепродажа товаров, имущественных прав.

В-третьих, законодатель исключил такой вид деятельности как добыча и (или) реализация полезных ископаемых.

В-четвертых, с точки зрения законодателя, деятельность самозанятого не может включать в себя предпринимательскую деятельность в интересах другого лица на основе договоров поручения, договоров комиссии либо агентских договоров.

В-пятых, законодатель запретил осуществлять услуги по доставке товаров с приемом (передачей) платежей за указанные товары в интересах других лиц.

В сфере налогового права существуют различные точки зрения относительно сформулированных законодателем видов деятельности. Так, по мнению С. М. Мироновой и Е. Я. Стеценко, отдельные виды деятельности, которыми могут заниматься налогоплательщики НПД, могут вызвать сложности «с точки зрения соблюдения критериев для НПД» [5]. Думается, что подобная проблема действительно есть и требует соответствующего разрешения.

Однако в целом перечень видов деятельности, которые запрещены при применении налогоплательщиком НПД, позволяет в полной мере отразить особенность самозанятых как отдельную категорию налогоплательщиков. Характеризуя приведенный перечень запретов, следует отметить, что он является закрытым, а значит, налогоплательщики могут осуществлять любую деятельность, которая не связана с тем, что сформулировано законодателем. Из этого следует два важных вывода. Прежде всего, ФЗ о налоге на профессиональный доход не ограничивает, а позволяет самозанятым возможность творческого самовыражения при осуществлении своей деятельности. При этом следует отметить, что подобный подход законодателя позволяет разграничить профессиональную деятельность и предпринимательскую.

Помимо перечисленного, важным является вопрос о ставке налогообложения, которая является достаточно привлекательной для налогоплательщиков НПД.

Налоговая ставка является дифференцированной. Разграничение связано с тем, кому была оказана услуга: юридическому или физическому лицу. Так, при реализации товаров, работ или услуг в рамках применения НПД налогоплательщик платит 6 % с поступлений от юридических лиц и индивидуальных предпринимателей и 4 % – от физических лиц, не зарегистрированных в качестве индивидуальных предпринимателей [8].

Среди различных точек зрения относительно НПД как специального налогового режима интересным представляется мнение Н. Г. Апресовой. По ее мнению, специальный налоговый режим НПД «позволяет гражданам вести профессиональную деятельность без регистрации в качестве индивидуального предпринимателя, а также без представления отчетности и без применения кассовой техники» [2].

Все вышеперечисленные аспекты налогообложения налогоплательщиков НПД находят свое отражение в уникальной цифровой технологии, посредством которой в том числе и объясняется успех данного специального налогового режима. Речь идет об особенности НПД, которая выделяет данный специальный налоговый режим в рамках налогового права.

В рамках экспериментального налогового режима НПД была разработана новаторская по своей сути система регистрации самозанятого в налоговом органе и отчетности в тот же налоговый орган посредством цифровых технологий.

Подобная точка зрения находит свое отражение в трудах деятелей науки финансового права. Так, О. С. Соболь, рассматривая в своих исследованиях такой специальный налоговый режим, как НПД, отмечала, что если говорить о постановке на учет лица в качестве плательщика НПД, то законодателем «в полной мере реализован концептуальный подход к цифровизации экономики в РФ» [6].

Новацией, безусловно, является техническая сторона вопроса, что достаточно важно не только в рамках достижения целей эксперимента со стороны законодателя, но и в целом для государства, которое стремится к модернизации системы налогообложения и упрощению регистрации и отчетности для налогоплательщиков. Именно поэтому НПД следует рассматривать как пример, в рамках которого государством была создана удобная процедура для всех сторон процесса осуществления налогообложения.

Следует отметить, что опыт Российской Федерации является достаточно уникальным и успешным по своей сути, о чем свидетельствуют статистические данные, указанные выше в данной статье. В сфере налогообложения была придумана такая площадка, при которой распространение НПД по территории государства стремительно увеличивается. Эффективным применением цифровых технологий в области налоговых правоотношений является мобильное приложение «Мой налог», через которое осуществляются как процесс регистрации налогоплательщика, так и осуществление отчетности.

Так, ни в одном государстве подобной системы не существует [3]. В качестве примера следует обратить внимание на опыт зарубежных стран в данном вопросе. В налоговом законодательстве США процедура регистрации является достаточно длительной. Налогоплательщик должен получить идентификационный номер, который является аналогом российского ИНН посредством почтовых услуг, факса или через сайт налоговой службы. Несмотря на тот факт, что заявление писать не требуется, налогоплательщик налога на самозанятых обязан самостоятельно подать в налоговую службу декларацию, которая будет заполнена по форме 1040 [9].

Проводя сравнение в вопросе применения цифровых технологий при регулировании аналогичных налоговых правоотношений, следует отметить преимущество российского опыта, поскольку применение мобильного приложения в качестве коммуникации налогоплательщика и налогового органа отвечает современным тенденциям. Применение подобной цифровой технологии представляет собой достаточно простой, удобный и экономный вариант с точки зрения временных трудозатрат для налогоплательщика. Думается, что российский опыт в данном случае представляет собой эффективный пример, который могут учесть зарубежные страны для осуществления умпешного правового регулирования деятельности самозанятых.

Несмотря на успешность НПД, следует задуматься о необходимости внесения корректировок, поскольку к моменту окончания эксперимента в правовом регулировании данного вопроса должны быть учтены существующие недостатки.

Необходимо отметить, что в ФЗ о НПД существуют различные пробелы, решить которые надо к моменту выхода из эксперимента. Так, в настоящее время одной из проблем является вопрос взносов на социальное и медицинское страхование самозанятых.

Следует отметить, что оформление и оплата самозанятыми взносов за социальное и медицинское страхование является их правом, т. е. добровольным волеизъявлением самозанятого. При этом в настоящее время реализация права самозанятого на внесении взносов на пенсионное и медицинское страхование

осуществляется посредством заключения договора о добровольном пенсионном страховании. Для заключения такого договора самозанятому необходимо написать заявление в территориальный орган ПФР, после подачи которого начнется расчетный период.

Автор настоящего исследования видит две основные проблемы.

Первая заключается в том, что налогоплательщик НПД, основываясь на своем желании, не уплачивает страховые взносы и претендовать на социальные гарантии не предполагается возможным. А поскольку по ст. 7 Конституции РФ Российская Федерация – социальное государство, гарантирующее создание таких условий, которые обеспечивали достойную жизнь человека, то государство должно способствовать обеспечению самозанятым таких условий, которые не нарушали бы их конституционного права на подобные социальные гарантии.

Вторая проблема сводится к неудобству подачи подобного заявления, связанному с необходимостью посетить территориальный ПФР или заполнить заявление через личный кабинет. При этом, с учетом позитивного опыта по взаимодействию налогоплательщика НПД и налогового органа посредством цифровой площадки – мобильного приложения, подобная ситуация является затруднительной.

Говоря о разрешении данных проблем, необходимо отметить, что государство в свою очередь достаточно сильно обеспокоено первой проблемой, касающейся неуплатой налогоплательщиками НПД страховых взносов в добровольном порядке. При этом государство предполагает попытки для ее разрешения. Так, об этом свидетельствует проект Федерального закона «О внесении изменений в Федеральный закон «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством», который подготовлен Минтрудом России, но в настоящее время не внесен в ГД ФС РФ. Однако данный проект не разрешает поставленную проблему, поскольку также построен на принципе добровольности. При этом безусловным плюсом является тот факт, что, согласно данному законопроекту, самозанятые будут включены в программы добровольного страхования на случай болезни. Так, им будет предоставлено право получать пособие по нетрудоспособности.

Думается, что подобный вариант не является правильным, поскольку построен на принципе добровольности, который не решает вопрос, ставший существенным и для российского законодательства в области налогообложения самозанятых.

В свете сказанного выше необходимо внести изменения в ФЗ о НПД, в рамках которых установить обязательную уплату налогоплательщиком НПД фиксированного процента уплаты страховых взносов в размере 3,84 % (в части размера выплаты учтены положения законопроекта Минтруда).

Такой вывод объясняется рядом аргументов. Во-первых, у граждан появляются соответствующие гарантии от государства получить доступ к медицинским услугам. Во-вторых, самозанятые становятся участниками накопительной пенсионной системы и, соответственно, будут получать пенсионную выплату в зависимости от стажа участия в системе.

При этом в данном предложении видится интересным и продуктивным применение цифровых технологий. Поскольку в настоящее время платежи

на пенсионное, медицинское и социальное страхование формируют бюджет фондов, из которых оплачиваются пенсии, пособия и медицинские услуги, а учетом страховых взносов занимается ФНС, то в приложении «Мой налог» представляется логичным добавить функцию «уплата страховых взносов».

Таким образом, в настоящее время налог на профессиональный доход действительно является уникальным налоговым режимом не только в силу успешности основных положений, но и в силу их цифровизации посредством использования мобильного приложения «Мой налог».

Однако до конца проведения эксперимента следует максимально усовершенствовать положения ФЗ о НПД посредством внесения соответствующих изменений.

Таким изменением является установление обязательного страхового взноса для самозанятых, уплата которого будет возможна через специально разработанную функцию «уплата страховых взносов» в приложении «Мой налог».

Подобное изменение представляется достаточно интересным, поскольку в результате его воплощения в действительности налог на профессиональный доход будет представлять собой специальный налоговый режим, в рамках которого цифровые технологии проявятся максимально эффективно.

Список литературы

1. Алексеев С. С. Право. Азбука. Теория. Философия. Опыт комплексного исследования. М., 1998. С. 49.

2. Апресова Н. Г. Правовой статус самозанятых как налогоплательщиков // Вестник Университета имени О. Е. Кутафина. 2020. №7(71). URL: https://cyberleninka.ru/article/n/pravovoy-status-samozanyatyh-kak-nalogoplatelschikov

3. Бурдакова М. А. Правовое регулирование деятельности самозанятых в РФ и зарубежных странах // Фундаментальные проблемы и перспективы развития предпринимательского права, конкурентного права и арбитражного процесса в современных экономических условиях санкционной политики: сборник научных трудов по материалам II Международной научно-практической конференции 22–23 апреля 2022 года. С. 366.

4. Миронова С. М., Стеценко Е. Я. Налогообложение самозанятых лиц (некоторые вопросы применения налога на профессиональный доход // Право и экономика. 2019. № 9. С. 74-79

5. Соболь О. С. Налог на профессиональный доход в системе специальных налоговых режимов: эксперимент правового обеспечения // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 7. С. 104–111.

6. Статистика для национального проекта «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы». URL: https://ofd.nalog.ru/statistics2.html?ysclid=le4ornkj9o994838209

7. Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» // СПС «Гарант».

8. Шапсугова М. Д. О влиянии неопределенности материально-правового статуса самозанятого на неопределенность его процессуального статуса // Право и экономика. 2021. № 3. С. 5–9.

9. U.S. Bureau of labor statistics. URL: https://www.bls.gov/spotlight/2016/self-employment-in-the-united-states

Д. С. Вебер,
студент,
Томский государственный университет
систем управления и радиоэлектроники
Я. О. Никоненко,
студент,
Томский государственный университет
систем управления и радиоэлектроники

РЕЗУЛЬТАТЫ ТВОРЧЕСТВА НЕЙРОСЕТИ КАК ОБЪЕКТ АВТОРСКОГО ПРАВА

Аннотация. В статье на основе анализа правовой доктрины и правоприменительной практики устанавливается ряд правовых проблем, связанных с возникновением распределения авторских прав на результаты творчества нейросети.

Ключевые слова: право, цифровые технологи, искусственный интеллект, нейросеть, авторское право, субъекты интеллектуального права, интеллектуальное право

THE RESULTS OF NEURAL NETWORK CREATIVITY AS AN OBJECT OF COPYRIGHT

Abstract. The article, based on an analysis of the justification of the doctrine and law enforcement practice, examines a number of legal problems associated with differences in copyright in relation to the results of the creativity of neural networks.

Keywords: law, digital technologies, artificial intelligence, neural network, copyright, subjects of intellectual property rights, intellectual property rights

Введение. Что общего между беспилотными автомобилями, виртуальными помощниками с голосовым управлением и «роботами-журналистами», которые могут автоматически писать и публиковать новостные статьи? Развитие в этих технологических областях осуществляется компаниями разных стран непрерывно. Яркими примерами могут служить Tesla, Amazon (с помощником Alexa) или «Яндекс» (с помощником Алисой). Automated Insights, поставщик текстового генератора, который с 2014 г. используется, в частности, Associated Press для создания простых новостных статей.

Однако во всех этих случаях одним из общих факторов является искусственный интеллект (далее – ИИ). Точнее, в каждом из этих примеров используются

алгоритмы самообучения на основе искусственных нейронных сетей. Конечно, искусственные нейронные сети составляют лишь небольшую часть искусственного интеллекта. Тем не менее нетрудно заметить, что они станут одной из ключевых технологий 21 века, имея при этом огромный потенциал для применения в различных отраслях.

Одной из компаний, которая провела исследование рынка использования нейронных сетей, является международное аналитическое агентство Gartner. В 2019 г. оно опубликовало отчет, в котором отмечало рост интереса к нейронным сетям и машинному обучению в целом, а также прогнозировало дальнейший рост этого рынка [12]. Оно также провело опрос среди представителей компаний, чтобы определить, как часто и какие виды нейронных сетей используются в бизнесе. Результаты опроса показали, что нейронные сети находят применение в различных областях, таких как финансы, здравоохранение, производство и транспорт.

Также New York Times в одной из своих статей отмечает универсальность и мультифункциональность нейросетей, описывая возможности их применения в обыденной жизни. Нейросети смогут всецело заменить различные поисковые системы, такие как Google, Yandex, Yahoo и т. д. Нейросети предоставляют информацию в максимально простой для усвоения форме, учитывая при этом содержание и особенность предоставляемой информации. На основе этой информации нейросети способны генерировать новые концепты в различных отраслях, таких как, например, экономика или бизнес [11].

Основная часть. Нейросетью можно назвать совокупность математических алгоритмов, функционирующих по схожей с живимыми организмами модели. Главной особенностью нейросетей являются их адаптивность и самосовершенствование, что позволяет им не только самообучаться и подстраиваться под конкретного пользователя, но и делать уникальные логические выводы на основе полученных ранее результатов, заданных человеком параметров или требований. Можно сказать, что нейросеть функционирует по принципам человеческого мозга, что делает ее универсальным инструментом для выполнения множества задач, которые ранее приходилось совершать непосредственно пользователю [3].

В российском законодательстве отсутствует понятие «нейросеть», что значительно усложняет правовое развитие в данной области. Однако нельзя говорить о том, что сфера развития искусственного интеллекта и нейросетей совсем не имеет правового обоснования. Так, Указ Президента Российской Федерации от 10 октября 2019 г. № 490 [7] сформулировал основные задачи и направления развития искусственного интеллекта, обозначив при этом необходимость в создании правовой системы, которая бы регулировала правовые отношения, связанные с использованием искусственного интеллекта. Понятия «искусственный интеллект» и «нейросеть» являются весьма схожими, что может натолкнуть на мысль прямого применения существующего законодательства в отношении нейросети. Однако эти понятия, хоть и взаимосвязаны, все же требуют универсального подхода. То есть любая нейросеть является искусственным интеллектом, но не любой искусственный интеллект является нейросетью.

На данном этапе отечественное законодательство безусловно не признает нейросети субъектом авторского права. Согласно положениям Гражданского кодекса, автором произведения является лицо, творческим трудом которого оно создано. Однако в п. 80 Постановления Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» [6] содержится тезис, согласно которому произведения, созданные с помощью технических средств в отсутствие творческого характера деятельности человека, объектами авторского права не являются. Исходя из этого, закономерен вывод: автором может признаваться только то лицо, которое самостоятельно и непосредственно создало данное произведение.

Стоит сказать, что, несмотря на фактическое отсутствие нормативной базы для регулирования правоотношений, связанных с использованием нейросетей, продолжают появляться примеры судебных разбирательств о вопросах прав на результаты работ нейросетей. Несколько художников подали коллективный иск, направленный против разработчиков из компаний Stability AI и Midjourney, разработавших AI art generators Stable Diffusion и Midjourney. Коллектив художников придерживается позиции, что эти компании нарушают авторские права на художественные продукты, созданные человеком, так как работа их системы искусственного интеллекта основывается непосредственно на пяти миллиардах изображений, взятых из Интернета, на обработку и использование которых авторы не давали своего согласия [10]. На данный момент судебное разбирательство продолжается.

Неопределенной также остается роль разработчика нейросети. Так, например, в программе Adobe Photoshop существует функция автоматического улучшения изображения. Означает ли это, что создатель такого инструмента может получить права на снимки, которые она отредактировала? С одной стороны, разработчик не имеет отношения к конечному результату работ нейросети, так как всю работу выполняют непосредственно компьютерные алгоритмы, функционирующие практически без стороннего вмешательства. С другой – разработчик обладает авторским правом на саму нейросеть, а значит, может распоряжаться результатами ее работы.

В 2022 г. Бюро авторского права Соединенных Штатов Америки вынесло апелляционное решение [4], согласно которому авторство человека является необходимым условием для возникновения и защиты авторских прав. В данном решении подчеркивается тесная связь между человеческим разумом и творческим самовыражением, которое выступает основой для защиты авторских прав. Также, согласно мнению зарубежных ученых, признание авторских прав за искусственным интеллектом должно основываться в первую очередь на степени участия человека в создании объекта авторских прав.

Главным аргументом здесь выступает тот факт, что генерация нейросеть изображения, звука, текста и т. д. происходит с использованием определенных требований, которые задает непосредственно человек. Данные требования называются «промты» (PROMT). Промты представляют собой определенные слова или теги, в которых пользователь указывает то, какой конечный результат он хочет получить, они выступают своего рода подсказками для нейросети. Каждый добавленный промт сужает спектр поиска нейросетью информации, которую она

использует при выполнении задачи. Иными словами, для получения более точного желаемого результата необходимо участие человека.

Неопределенность в вопросе о правоспособности нейросетей порождает множество мнений, в том числе среди ученых и правоведов. Так, например, согласно мнению представителя Совета Федерации ФС РФ от законодательного органа государственной власти Республики Алтай Р. Р. Сафина и адвоката К. А. Маскина, возможность закрепления авторского права на результаты работ нейросети за пользователем или разработчиком не представляется возможной. По их мнению, возникновение и признание авторского права неотъемлемо связано с творческим процессом, который всегда сопряжен с определенным человеческим выбором [8. С. 155], который, в случае с искусственным интеллектом, делает непосредственно нейросеть, моделируя и имитируя человеческое поведение.

Данная позиция, несмотря на кажущуюся логичность, не лишена недостатков. Если считать, что в данном случае вообще нет права авторства, то что же, творчество нейросети автоматически попадает в разряд общественного достояния? К тому же если нет личных неимущественных прав, то, следовательно, и не должно быть исключительных прав. А нейросеть может быть вполне нацелена на коммерческое использование.

Другой аргументации, придерживается В. Н. Синельникова и О. В. Ревинский [9. С. 24], описывающие правовую взаимосвязь между непосредственно разработкой программы, способной создавать новые объекты авторского права, и конечным результатом ее работы.

Согласно данной позиции, деятельность разработчика по созданию нейросети порождает за ним право авторства на такие объекты хотя бы потому, что итогом работы искусственного интеллекта является результат интеллектуальной деятельности «человека-творца».

Данная позиция также не лишена недостатков. Несмотря на то, что нейросеть сама является продуктом творчества человека (программой для ЭВМ), непосредственно в создании результата разработчик творческого участия не принимает, а значит, тоже не может считаться автором. Эту ситуацию можно сравнить с авторством на различные модификации (моды) к компьютерным играм. Сам разработчик игры, безусловно, обладает правами на созданную им игру. Тем не менее отказывать стороннему лицу в авторстве на мод было бы нелогично – налицо творческий труд стороннего лица. В отношении нейросети данный процесс был бы просто более автоматизированным. Или же можно провести аналогию с программой Adobe Photoshop и создаваемым с его помощью изображением. Безусловно, права на программу принадлежат ее разработчикам, однако едва ли они могут претендовать на права на созданное изображение. Но говорить о тождестве приведенных ситуаций с творчеством нейросети не приходится из-за очень высокой степени автоматизации.

Стоит отметить, что многие правоведы, хоть и не придерживаются позиции о правоспособности искусственного интеллекта, однако вполне допускают подобное развитие законодательства в отношении компьютерных систем в будущем. Например, В. А. Лаптев указывает, что результаты работ нейросети будут рассматриваться как полноценные объекты права уже в ближайшем будущем

[2. С. 141], отмечая при этом бурное развитие индустрии искусственного интеллекта, что обуславливает потенциальную возможность приобретения нейросетями правовой самостоятельности, выступая при этом полноценным участником правоотношений, реализуемых в пределах цели его создания и разработки, т. е. служения на благо человечества [5. С. 82].

При этом весьма вероятно, что вопрос об использовании результатов творчества нейросетей будет отдан на откуп пользовательским соглашениям.

Существует мнение, что человечество пока не готово к полноценному внедрению нейросетей в правовую систему, так как в законодательстве стран не существует устойчивой нормативной базы для регулирования правового положения искусственного интеллекта. Например, глава американской корпорации OpenAI, разработавшей одну из самых передовых нейросетей – ChatGPT, Илон Маск призвал приостановить развитие нейросетей на определенный срок. Глава компании призвал мировые, IT-лаборатории, занимающиеся разработкой нейронных систем, как можно скорее приостановить активные разработки в сфере обучения и развития искусственного интеллекта, отметив при этом, что развитие компьютерных нейросистем с возможностями шире, чем у GPT-4, может негативно сказаться на будущем человечества. Он призвал государства поддержать данное ограничение в случае невозможности или затруднении в его исполнении [1].

Заключение. Можно сказать, что в настоящий момент законодательство России нуждается во внесении определенных дополнений, регулирующих положение искусственного интеллекта по отношению к разработчику. Более правильным, на наш взгляд, было бы определенным образом расщепить права между разработчиком нейросети и лицом, задавшим промты. Из-за того, что именно разработчик нейросети устанавливает условия и пределы пользования ею, вероятно, именно за ним имеет смысл закреплять возможность выбрать каким образом, какие права, в каком объеме и на каких условиях передаются пользователю нейросети на результаты ее творчества. Однако на любом продукте нейросети, на наш взгляд, необходимо делать специальную отметку, что он создан именно нейросетью. Примером может выступать ситуация, связанная с порядком использования сгенерированного нейросетью Midjourney изображения. Субъектами данных правоотношений в данном случае будут выступать пользователь и разработчик нейросети. Особенностью данных правоотношений является особый динамичный статус пользователя, а также его правового положения по отношению к разработчику нейросети, а также конечному результату ее работы. На данный момент универсального ответа на вопрос авторства не существует, поэтому в каждом случае приходится проводить анализ авторских прав и заключать соответствующие договоры.

Список литературы

1. Илон Маск, Возняк и более 1000 IT экспертов призвали прекратить обучение нейросетей // renderu.com. URL: https://render.ru/ru/news/post/24134

2. Ишутин А. В., Косаримов С. В., Чикирка Е. В. Нейронное искусство как объект авторского права // Социальные новации и социальные науки. 2021. № 1. С. 137–142.

3. 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. 854–874.

4. К вопросу о наличии авторских прав у искусственного интеллекта // ГАРАНТ.РУ. URL: https://www.garant.ru/article/1605912

5. Лаптев В. А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79–102.

6. О применении части четвертой Гражданского кодекса Российской Федерации: Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 // Бюллетень Верховного Суда Российской Федерации. 2019. № 7.

7. О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 № 490 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 г.) // Собрание законодательства Российской Федерации. 14.10.2019. № 41. Ст. 5700.

8. Сафин Р. Р., Маскин К. А. Правовое регулирование объектов авторского права, созданных с использованием «нейросети» // Правовое регулирование интеллектуальной собственности и инновационной деятельности: сборник статей научно-методологического семинара. 2018. № 6. С. 154–158.

9. Синельникова В. Н., Ревинский О. В. Права на результаты искусственного интеллекта // Копирайт. 2017. № 4. С. 17–27.

10. AI art tools Stable Diffusion and Midjourney targeted with copyright lawsuit // The Verge. URL: https://www.theverge.com/2023/1/16/23557098/generative-ai-art-copyright-legal-lawsuit-stable-diffusion-midjourney-deviantart

11. Cade Metz the New Chatbots Could Change the World. Can You Trust Them? // New York Times. URL: https://www.nytimes.com/2022/12/10/technology/ai-chat-bot-chatgpt.html

12. Gartner Hype Cycle // Habr. URL: https://habr.com/ru/post/475032

И. С. Вишняков,
студент магистратуры,
Институт законодательства и сравнительного правоведения при
Правительстве Российской Федерации

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВИЗАЦИИ ОПУБЛИКОВАНИЯ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В СТРАНАХ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ И В СТРАНАХ ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. В статье рассматривается опыт электронного опубликования нормативных правовых актов. Дается обзор зарубежного законодательства ряда стран Содружества Независимых Государств и Европейского союза об официальном опубликовании актов.

Ключевые слова: опубликование, нормативный правовой акт, цифровизация законодательства, информатизация правотворчества

LEGAL REGULATION OF DIGITALIZATION OF PUBLICATION OF REGULATIVE LEGAL ACTS IN THE COUNTRIES OF THE COMMONWEALTH OF INDEPENDENT STATES AND IN THE COUNTRIES OF THE EUROPEAN UNION

Abstract. This article examines the experience of electronic publication of legal acts. A review of foreign legislation in a number of countries of the Commonwealth of Independent States and the European Union on the official publication of acts is given.

Keywords: publication, normative legal act, digitalization of legislation, informatization of law-making

Одним из основных факторов развития современного права является цифровизация. Цифровые технологии находят активное применение в правотворческом процессе [23] и правоприменении [24]. Отдельного внимания, с нашей точки зрения, заслуживают преобразования, которые коснулись этапа опубликования нормативного правового акта, поскольку последнее является обязательным условием его вступления в силу, гарантией его законности и обеспечивает реальность презумпции знания закона.

Способы опубликования актов как процесса распространения правовой информации и ее доведения до сведения субъектов права изменялись вместе с развитием средств хранения и передачи информации.

Авторы монографии «Официальное электронное опубликование» выделяют три эпохи развития официального опубликования решений власти: добумажную (до I века н. э.), бумажную (с I века н. э. по настоящее время) и электронную [19. С. 13]. Последняя, в свою очередь, подразделяется на два этапа: бумажно-электронный и собственно электронный.

Бумажно-электронный период, берущий начало в 1906 году, характеризуется законодательным признанием возможности передачи правовой информации с использованием сначала телеграфа, а затем и радио- и телевещания, но при этом официальное значение сохраняется исключительно за первой печатной публикацией. Электронный период, который авторы отсчитывают с 1994 года, характеризуется признанием официального характера актов, распространяемых в машиночитаемом виде. Современная российская система официального опубликования имеет комбинированный характер: опубликование производится и на бумажных, и на электронных носителях [20. С. 245].

Наблюдается тенденция расширения применения современных информационных технологий при опубликовании нормативных правовых актов – от введения государственных информационных систем для обеспечения возможности более широкого распространения правовой информации до перехода на исключительно электронную форму опубликования нормативных правовых актов.

Армения. Согласно ст. 25 Закона Республики Армения от 28 марта 2018 г. № ЗР-180 «О нормативных правовых актах» [1] официальное опубликование нормативного правового акта осуществляется посредством его публикации на едином интернет-сайте опубликования нормативных правовых актов, который ведется министерством, разрабатывающим и осуществляющим политику Правительства в сфере юстиции. Днем официального опубликования является день первого опубликования на едином интернет-сайте полного текста принятого или подписанного в окончательной редакции акта, подлежащего опубликованию.

Приказом министра юстиции Республики Армения от 7 мая 2018 г. № 180-Н [14] установлено, что официальное опубликование нормативных правовых актов в электронной форме осуществляется путем публикации на едином сайте ARLIS (http://www.arlis.am).

Беларусь. Процедура официального опубликования нормативных актов урегулирована Законом Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах» [2]. Согласно ст. 60 Закона, официальным опубликованием нормативных правовых актов, включаемых в Национальный реестр правовых актов, является доведение этих актов до всеобщего сведения путем размещения их текстов в полном соответствии с подписанными подлинниками на Национальном правовом интернет-портале Республики Беларусь.

7 апреля 2023 г. Законом № 261-З перечень принципов нормотворческой деятельности, указанных в ст. 6, был дополнен принципом цифровизации, который обеспечивается широким применением информационных технологий на всех стадиях нормотворческого процесса, в том числе за счет развития электронного документооборота, максимального использования цифровых инструментов в процессе нормотворческой деятельности.

Казахстан. Статьи 37–39 Закона Республики Казахстан от 6 апреля 2016 г. № 480-V «О правовых актах» [3] регулируют официальное опубликование принятых актов в Эталонном контрольном банке нормативных правовых актов в электронном виде. Статьей 1 Закона Эталонный контрольный банк определен как «совокупность нормативных правовых актов на бумажном носителе и электронная система нормативных правовых актов в форме электронного документа, сведения о которых внесены в государственный реестр нормативных правовых актов Республики Казахстан». Кроме того, предусмотрено в качестве официального опубликование актов официального разъяснения нормативных правовых актов на интернет-ресурсе уполномоченного органа (должностного лица), давшего разъяснение (ст. 62).

Молдова. В соответствии со ст. 56 Закона Республики Молдова от 22 декабря 2017 г. № 100 «О нормативных актах» нормативные акты опубликовываются в Государственном регистре юридических актов и в Официальном мониторе Республики Молдова или, в зависимости от обстоятельств, в официальных мониторах районов, муниципиев и автономных территориальных образований с особым правовым статусом или в Регистре местных актов. Нормативные акты также могут быть обнародованы посредством размещения на официальных веб-страницах органов публичной власти или вывешивания в предназначенных для этого местах [5].

Порядок опубликования нормативных актов регулируется Законом от 6 июля 1994 г. № 173 «О порядке опубликования и вступления в силу официальных актов». Согласно ему, законы и иные нормативные акты Республики Молдова публикуются в Официальном мониторе Республики Молдова, издаваемом Национальным агентством печати «Молдпрес» (ст. 1). Официальные акты публикуются в Официальном мониторе в семидневный срок со дня получения их Национальным агентством печати «Молдпрес», а в Государственном регистре юридических актов Республики Молдова – в трехдневный срок со дня их опубликования в Официальном мониторе (ст. 2) [4]. В электронном виде доступ к Официальному монитору представляется посредством сайта https://monitorul.gov.md.

Нормативной основой функционирования Государственного регистра юридических актов является Постановление Правительства Республики Молдова № 165 от 16 марта 2022 г. «Об Информационной системе «Государственный регистр юридических актов». ИС ГРЮА представляет собой совокупность автоматизированных информационных технических средств, предназначенных для хранения, обработки и предоставления правовой информации, необходимой для процесса систематизации законодательства Республики Молдова. ИС ГРЮА предоставляет всем физическим и юридическим лицам публичного и частного права механизм доступа онлайн, бесплатно, с любой платформы, через сеть Интернет ко всем содержащимся в ней данным. Доступ к информационной системе осуществляется посредством веб-страницы www.legis.md.

Узбекистан. Согласно ст. 38 Закона Республики Узбекистан от 20 апреля 2021 г. № ЗРУ-682 «О нормативных правовых актах», электронные версии текстов нормативно-правовых актов министерств, государственных комитетов, ведомств и органов государственной власти на местах подлежат обязательному опубликованию на официальных веб-сайтах принявших их органов в течение одного дня после официального опубликования нормативно-правового акта. Порядок опубликования электронных версий текстов нормативно-правовых актов министерств, государственных комитетов, ведомств и органов государственной власти на местах определяется законодательством [7].

Перечень официальных источников опубликования законов установлен ст. 39 Закона – это «Ведомости палат Олий Мажлиса Республики Узбекистан», «Собрание законодательства Республики Узбекистан», газеты «Халқ сўзи» и «Народное слово», «Национальная база данных законодательства Республики Узбекистан».

Информационно-поисковая система Национальной базы данных законодательства Республики Узбекистан осуществляет деятельность в соответствии с Законом Республики Узбекистан от 7 сентября 2017 г. № ЗРУ-443 «О распространении правовой информации и обеспечении доступа к ней» и постановлением Президента Республики Узбекистан от 8 февраля 2017 года № ПП-2761 «О мерах по коренному совершенствованию системы распространения актов законодательства». Согласно ст. 17 Закона «О распространении правовой информации и обеспечении доступа к ней», официальное опубликование нормативно-правовых актов в Национальной базе данных законодательства Республики Узбекистан осуществляется в течение одного дня с момента их поступления в Министерство

юстиции Республики Узбекистан в разделе «Официальное опубликование нормативно-правовых актов». Доступ пользователей к Национальной базе данных законодательства Республики Узбекистан осуществляется бесплатно [6].

Доступ к Информационно-поисковой системе Национальной базы данных осуществляется посредством веб-страницы https://lex.uz.

Германия. В конце 2022 г. в Германии была проведена реформа, направленная на модернизацию системы опубликования законов. 20 декабря 2022 г. Бундестагом были приняты два закона – закон об изменении статьи 82 Конституции ФРГ [15] и Закон «Об обнародовании законов и иных нормативных актов» [8] (Gesetz über die Verkündung von Gesetzen und Rechtsverordnungen und über Bekanntmachungen).

Предыдущая редакция абзаца 1 ст. 82 Конституции ФРГ устанавливала: «Законы, принятые на основании предписаний настоящего Основного закона, после их контрассигнации Федеральным президентом к официальной публикации в Федеральном вестнике законов. Постановления готовятся к официальной публикации издавшими их ведомствами и, если иное не установлено законом, публикуются в Федеральном вестнике законов» [16. С. 606–607]. В новой редакции статьи к упомянутому добавилось следующее положение: «Федеральный вестник законов может вестись в электронной форме».

Во исполнение этого положения вместе с поправкой к конституции был принят Закон об опубликовании законов и постановлений, устанавливающий исключительно электронное опубликование федеральных нормативных актов. Согласно параграфу 2 Закона об обнародовании, Федеральный вестник законов публикуется на сайте www.recht.bund.de и доступ к нему и размещенным на нем материалам предоставляется постоянно и в полном объеме. В случае невозможности опубликования актов на официальном сайте предусмотрена возможность опубликования на альтернативных ресурсах – сайте Федеральной газеты (официальный печатный орган Федерального правительства ФРГ), посредством радио- и телевещания, в печатных и цифровых ежедневных газетах, путем опубликования в местах, предусмотренных для опубликования актов муниципальных органов, а также в аккаунтах Управления печати и информации Федерального правительства в социальных сетях.

Польша. Часть 2 ст. 122 Конституции Польши предусматривает обязанность Президента подписать закон в течение 21 дня со дня представления принятого закона и издать приказ о его опубликовании в «Дзенник Устав Жечипосполитей Польскей» (Dziennik Ustaw Rzeczypospolitej Polskiej) [17. С. 706].

Согласно ст. 2а Закона от 20 июля 2000 г. «Об опубликовании нормативных актов и некоторых других правовых актов» нормативные акты и другие правовые акты, подлежащие обнародованию, объявляются в форме электронного документа по смыслу Закона от 17 февраля 2005 г. «Об информатизации деятельности субъектов, выполняющих публичные задачи».

Официальные журналы издаются в электронной форме. Для каждого официального журнала, издаваемого в электронной форме, издающий орган ведет отдельный веб-сайт.

Согласно ст. 26 Закона органы местной администрации и органы местного самоуправления обязаны обеспечить бесплатный доступ к изданиям «Dziennik

Ustaw» и «Monitor Polski» или содержащимся в них нормативным и иным правовым актам, а также к судебным решениям:

1) для просмотра и скачивания в форме электронного документа;

2) в электронной форме для публичного ознакомления в рабочее время офисов, обслуживающих эти органы, в месте, предназначенном для этой цели и доступном для публичного ознакомления.

Франция. Согласно ст. 10 Конституции Франции, Президент Республики промульгирует законы в течение 15 дней, следующих после передачи Правительству окончательно принятого закона [18. С. 414].

22 декабря 2015 г. были приняты ряд законов и подзаконных актов о цифровизации процесса опубликования нормативных актов. Органическим законом № 2015-1712 «О дематериализации Официального журнала Французской Республики» [9] и обычным законом № 2015-1713 [10] были внесены изменения в ряд законов, в том числе в Кодекс об взаимоотношениях общественности и администрации (Code des relations entre le public et l'administration).

Статья L. 221-9 Кодекса устанавливает, что законы и ордонансы подлежат опубликованию в Официальном журнале Французской Республики. Ключевые изменения коснулись статьи L. 221-10 – теперь официальное опубликование упомянутых в статье L. 221-9 допускалось только в электронной форме.

Декретом от 22 декабря 2015 г. № 2015-1717 [12] были внесены изменения в Декрет № 2002-1064 от 7 августа 2002 г. «О государственной службе по распространению права через Интернет». Декрет предусматривал создание публичной службы по распространению права через Интернет и опубликование в Интернете нормативных правовых актов, международных договоров Франции, актов Европейского союза и официальных изданий Французской Республики (в том числе «Официального журнала»), а также сайта Légifrance (http://www.legifrance.gouv.fr), предназначенного для предоставления доступа к законодательным актам, международным договорам Франции, судебной практике Франции и актам Европейского союза.

Швейцария. Вопросы опубликования актов в Швейцарии урегулированы Федеральным законом «О сборниках федерального законодательства и Федеральной газете» [11].

В 2014 г. Закон был дополнен статьей 1а «Онлайн-опубликование», установившей, что публикация актов в соответствии с Законом осуществляется на общедоступной онлайн-платформе. Публикация осуществляется в машиночитаемой форме, в которой доступны текущая и все предыдущие версии.

Такой платформой для публикации актов Конфедерации, соглашений между Конфедерацией и кантонами и соглашений между кантонами является FedLex (https://www.fedlex.admin.ch).

Статьей 15 Закона предусмотрено, что авторитетной является версия закона, опубликованная на платформе.

Ордонансом от 7 октября 2015 г. «О сборниках федеральных законов и Федеральной газете» установлено, что тексты на платформе должны быть опубликованы в формате PDF [13].

Как следует из приведенного обзора иностранного законодательства об опубликовании нормативных правовых актов, ряд стран уже перешли на исключительно электронную форму опубликования – Армения, Беларусь, Германия, Польша, Франция. Другие государства предусматривают наряду с опубликованием в печатных изданиях размещение текстов актов на специально предусмотренных для этого информационных платформах, официальных веб-сайтах органов государственной власти.

Электронная форма опубликования имеет ряд преимуществ, обуславливающих перспективность полноценного перехода на данную форму: высокая скорость передачи информации; относительная дешевизна; удобство хранения документов в электронном виде; простота и легкость доступа к информационным ресурсам; удобство поиска информации; возможность неограниченного копирования и тиражирования правовой информации и т. д.

Исходя из этого, полагаем неизбежным скорый переход на исключительно электронную форму опубликования нормативных актов и в России. Преимущества электронной формы, обширный зарубежный опыт в данной сфере, высокий уровень цифровизации [21], а также собственный опыт электронного опубликования посредством Официального интернет-портала правовой информации создают предпосылки для реформирования законодательства об опубликовании и модернизации системы официального опубликования в сторону признания электронной формы опубликования в качестве основной.

Список литературы

1. Закон Республики Армения от 28 марта 2018 г. № ЗР-180 «О нормативных правовых актах» // Система правовой информации Армении ARLIS. URL: https://www.arlis.am/DocumentView.aspx?DocID=129477

2. Закон Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах» // Национальный правовой интернет-портал Республики Беларусь. URL: https://pravo.by/document/?guid=3871&p0=H11800130

3. Закон Республики Казахстан от 6 апреля 2016 г. № 480-V «О правовых актах» // ИС «Параграф». URL: https://online.zakon.kz/Document/?doc_id=37312788&pos=965;-51#pos=965;-51

4. Закон Республики Молдова от 6 июля 1994 г. № 173 «О порядке опубликования и вступления в силу официальных актов» // Государственный реестр правовых актов Республики Молдова. URL: https://www.legis.md/cautare/getResults?doc_id=129566&lang=ru

5. Закон Республики Молдова от 22 декабря 2017 г. № 100 «О нормативных актах» // Государственный реестр правовых актов Республики Молдова. URL: https://www.legis.md/cautare/getResults?doc_id=135295&lang=ru

6. Закон Республики Узбекистан от 07.09.2017 № ЗРУ-443 «О распространении правовой информации и обеспечении доступа к ней» // Информационно-поисковая система Национальной базы данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/3329329#3333589

7. Закон Республики Узбекистан от 20 апреля 2021 г. № ЗРУ-682 «О нормативно-правовых актах» // Информационно-поисковая система Национальной базы данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/5378968

8. Закон Федеративной Республики Германия от 20 декабря 2022 г. «Об обнародовании законов и иных нормативных актов» // База данных действующих законов и правовых постановлений Gesetze im Internet. URL: https://www.gesetze-im-internet.de/vkbkmg/VkBkmG.pdf

9. Органический закон Французской Республики от 22 декабря 2015 г. № 2015-1712 «О дематериализации Официального журнала Французской Республики» // Государственный сервис распространения права через Интернет Légifrance. URL: https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031305046

10. Закон Французской Республики от 22 декабря 2015 г. № 2015-1713 «О дематериализации Официального журнала Французской Республики» // Государственный сервис распространения права через Интернет Légifrance. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031672289

11. Закон Швейцарской Конфедерации от 18 июня 2004 г. «О сборниках федерального законодательства и Федеральной газете» // Платформа публикации федерального законодательства Швейцарии FedLex. URL: https://www.fedlex.admin.ch/eli/cc/2004/745

12. Декрет Премьер-министра Французской Республики от 7 августа 2002 г. № 2002-1064 «О государственном сервисе распространения права через Интернет» // Государственный сервис распространения права через Интернет Légifrance. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000413818?page=1&pageSize=10&query=décret+n°+2002-1064+du+7+août+2002+relatif+au+service+public+de+la+diffusion+du+droit+par+l%27internet&searchField=ALL&searchType=ALL&tab_selection=all&typePagination=DEFAULT

13. Декрет Премьер-министра Французской Республики от 22 декабря 2015 г. № 2015-1717 «О дематериализации Официального журнала Французской Республики» // Государственный сервис распространения права через Интернет Légifrance. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031672333?init=true&page=1&query=Journal+officiel+de+la+République+française&searchField=ALL&tab_selection=all

14. Ордонанс Федерального совета Швейцарской Конфедерации от 7 октября 2015 г. «О сборниках федерального законодательства и Федеральной газете» // Платформа публикации федерального законодательства Швейцарии FedLex. URL: https://www.fedlex.admin.ch/eli/cc/2015/670/fr

15. Приказ министра юстиции Республики Армения от 7 мая 2018 г. № 180-Н // Система правовой информации Армении ARLIS. URL: https://www.arlis.am/DocumentView.aspx?DocID=145009

16. Законопроект о внесении изменений в статью 82 Основного закона Федеративной Республики Германия // Официальный сайт Бундестага ФРГ. URL: https://dserver.bundestag.de/btd/20/027/2002729.pdf

17. Конституции государств Европы: В 3 т. Т. 1 / под общей редакцией и со вступительной статьей директора Института законодательства и сравнительного правоведения при Правительстве Российской Федерации Л. А. Окунькова. М.: Норма, 2001. 824 с.

18. Конституции государств Европы: В 3 т. Т. 2 / под общей редакцией и со вступительной статьей директора Института законодательства и сравнительного правоведения при Правительстве Российской Федерации Л. А. Окунькова. М.: Норма, 2001. 840 с.

19. Конституции государств Европы: В 3 т. Т. 3 / под общей редакцией и со вступительной статьей директора Института законодательства и сравнительного правоведения при Правительстве Российской Федерации Л. А. Окунькова. М.: Норма, 2001. 792 с.

20. Официальное электронное опубликование: История, подходы, перспективы / под ред. проф. В. Б. Исакова. М.: Формула права, 2012. 320 с.

21. Юридическая техника: учебное пособие / Н. А. Власенко, А. И. Абрамова, Г. Т. Чернобель [и др.]; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М.: ЮСТИЦИЯ, 2016. 320 с.

22. Россия вошла в топ-10 стран по цифровизации госуправления // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/ru/events/42223/?utm_referrer=https%3a%2f%2fyandex.ru%2f&utm_referrer=https%3a%2f%2fdigital.gov.ru%2fru%2fevents%2f42223%2f%3futm_referrer%3dhttps%253a%252f%252fyandex.ru%252f

23. Цифровизация правотворчества: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2019.

24. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

В. В. Воронин,
студент,
Оренбургский государственный университет

ЦИФРОВИЗАЦИЯ ВЫБОРНОЙ СИСТЕМЫ КАК ВЕДУЩИЙ ФАКТОР РЕАЛИЗАЦИИ ПРИНЦИПА РАВНОГО ИЗБИРАТЕЛЬНОГО ПРАВА

Аннотация. В статье проводится анализ правовой природы информатизации избирательного права. Особое внимание уделяется текущему уровню цифровизации и информатизации избирательной системы Российской Федерации, возможных форм влияния инновационного способа голосования на принципы избирательного процесса и права. Выделяются основные направления развития и функционирования избирательной системы Российской Федерации. Отмечаются достоинства применения электронного дистанционного голосования. Делается акцент на практике применения новых процедур избирательного процесса.

Ключевые слова: выборы, голосование, право, цифровизация, информатизация, прогресс, цифровые технологии

DIGITALIZATION OF THE ELECTORAL SYSTEM AS A LEADING FACTOR IN THE IMPLEMENTATION OF THE PRINCIPLE OF EQUAL SUFFRAGE

Abstract. The article analyzes the legal nature of informatization of electoral law. Particular attention is paid to the current level of digitalization and informatization of the electoral system of the Russian Federation, possible forms of influence of an innovative method of voting on the principles of the electoral process and law. The main directions of development and functioning of the electoral system of the Russian Federation are highlighted. The advantages of using electronic remote voting are noted. Emphasis is placed on the practice of applying new procedures in the electoral process.

Keywords: elections, voting, law, digitalization, informatization, progress, digital technologies

Цифровизация выборной системы является неотъемлемой частью становления государства в современных условиях, т. е. в условиях повсеместного колоссального развития цифровых технологий. В наше время абсолютно все сферы жизни так или иначе начинают затрагивать стремительно развивающиеся технологии [2]. Отказаться от научно-технологического прогресса становится просто нереально, ведь возможность столь серьезного повышения уровня систематизации, структурирования и оптимизации всех процессов, которое достигается благодаря таким технологиям, нельзя недооценивать.

Согласно Конституции Российской Федерации, Россия есть федеративное, демократическое правовое государство с республиканской формой правления, высшую ценность в котором представляет человек. Единственный источник власти представляет многонациональный народ, осуществляющий власть непосредственно, в том числе через органы государственной власти, местного самоуправления. Главным выражением власти народа являются свободные выборы, референдум, а граждане России имеют право избирать и быть избранными в органы государственной власти и местного самоуправления, а также принимать участие в референдуме [3].

Все гарантии, обязательные для реализации гражданами Российской Федерации принципа равного избирательного права, а также конституционного права на участие в референдумах и выборах, проводимых на территории Российской Федерации в соответствии с Конституцией, находят свое отражение в Федеральном законе от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации».

Основываясь на устоявшихся в законодательстве принципах, становится ясно, что обеспечение равенства выборов, обеспечение возможности всем, независимо от каких-либо факторов, избирать и быть избранными является ведущей задачей государственного обеспечения функционирования избирательной системы, а также равенства выборов и их участников.

Принимая во внимание все эти факты, становится очевидным преимущество введения цифровизации избирательных процессов как гарантий обеспечения равенства участников выборов.

Дистанционное голосование по определению – это голосование, но без применения напечатанного на бумажном носителе бюллетеня, а также при помощи использования совокупности программ, разработанных для создания специализированной системы портала государственных и муниципальных услуг.

Так, если проанализировать электронное голосование, становится понятно, что его внедрение и использование позволит, несмотря на местоположение, что касается жителей отдаленных деревень, сел, несмотря на ограниченные возможности людей с инвалидностью, обеспечить доступность избирательного процесса для абсолютно любого гражданина. В итоге достигается наивысший уровень равенства всех участников избирательного процесса, исключая зависимость от определенных нежелательных обстоятельств. И государство реализует одну из главных своих целей, возможность каждого желающего гражданина осуществлять свое избирательное право, участвовать в выборах, в жизни страны, принимать участие в определении последующей судьбы своего государства, что неоценимо важно для каждого гражданина, уважающего свою родину и думающего о своем будущем, будущем своей страны.

На данный момент, чтобы участвовать в дистанционном электронном голосовании, необходимо подать заявление на Госуслугах. При желании его можно отозвать. Подать заявление могут пользователи с подтвержденной учетной записью. Услуга будет доступна, если данные, указанные на портале Госуслуг, сопоставимы с данными, содержащимися в регистре избирателей. Дистанционное голосование проводится на специально разработанном портале – vybory.gov.ru. В свою очередь, на портале mos.ru дистанционное электронное голосование проходит для граждан с пропиской в Москве. Для доступа к порталу дистанционного электронного голосования используется логин и пароль от Госуслуг. В настоящее время дистанционное электронное голосование доступно совершеннолетним гражданам с пропиской в Москве или следующих субъектах: Калининградская, Калужская, Курская, Новгородская, Псковская, Томская и Ярославская области.

Если рассмотреть пример Белоруссии, то внедрение электронного голосования непосредственно в Республике Беларусь – это один из самых дискуссионных вопросов, если обращаться к нему в проекции доктринального и практического применения, особенно если сравнивать с зарубежными государствами, где для избирательных систем модернизация не является новизной и постоянно изучается как часть реализации избирательного процесса. В любом случае государство достигает нового уровня развития различных институтов с использованием информационных технологий, т. е. делает все возможное, чтобы стать цифровым [1. С. 4].

Так, Светлана Хамутовская, анализируя белорусский опыт внедрения инновационных технологий голосования, рассматривает преимущества уже сформированной, разработанной учеными и функционирующей системы дистанционного голосования «Гарант», а конкретно в предоставлении расположенным удаленно компаниям информационных услуг, которые связаны непосредственно с собиранием персональных данных, а конкретно сборам подписей, выборами, опросами общественного мнения, референдумами; высочайшей степени защиты данных;

отсутствии нетривиальных требований относительно участников определенных мероприятий, к примеру, терминалов специального назначения, специальных ID-карт у избирателей; техническом анализе процесса формирования результатов мероприятия; возможности просмотра голосующими личных результатов голосования [4. С. 31–32].

Ведение и развитие дистанционного голосования – это не просто замена урн и бюллетеней электронными машинами для голосования, этот процесс является по-настоящему трудоемким, многоэтапным и сложным [5. С. 152].

Подводя итог, следует отметить следующее:

Во-первых, цифровые выборы способствуют повышению количества голосующих, что впоследствии является фактором обеспечения честных выборов, приводящим своим результатом выбор, действительно важный и необходимый гражданам своей страны.

Во-вторых, благодаря электронному голосованию проголосовать сможет абсолютно каждый желающий гражданин, в том числе пенсионеры, а также люди с ограниченными возможностями. В таком случае повторение не таких давних событий, связанных с пандемией, никоим образом не сможет помешать проведению выборов и повлиять на их организацию, количество голосующих и впоследствии на результат выборов.

Введение электронной системы выборов способствует реализации принципа равного избирательного права, а также возможности реализовывать свое право избирать и быть избранным каждым гражданином Российской Федерации, вне зависимости от каких-либо обстоятельств.

Список литературы

1. Былинкина Е. В. Понятие и виды электронного голосования в России и за рубежом: сравнительно-правовой анализ // Рос. право: образование, практика, наука. 2021. № 5. С. 4–10.

2. Ерахтина О. С. Подходы к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта: особенности и практическая применимость // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 421–437. EDN: LBWSXW.

3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_28399

4. Хамутовская С. Новые технологии голосования: зарубежный опыт // Наука и инновации. 2019. № 5(195). С. 29–32.

5. Pran V., Merloe P. Observations des technologies electroniques utilisees dans le processus electoraux. Washington, D. C. 2007. URL:https://www.ndi.org/files/Observations_des_Technologies_Electroniques_0.pdf

Л. А. Гаер,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

ЦИФРОВЫЕ ТЕХНОЛОГИИ В АРБИТРАЖНОМ ПРОЦЕССЕ

Аннотация. Современная система судопроизводства стремительно развивается, и применение цифровых технологий не обходит ее стороной. В статье рассматриваются вопросы сохранения доступности арбитражного судебного процесса в эпоху цифровизации, а также изменения в законодательстве в отношении исполнения судебных актов в электронной форме.

Ключевые слова: право, цифровые технологии, арбитражный процесс, электронное судопроизводство, информация

DIGITAL TECHNOLOGIES IN THE ARBITRATION PROCESS

Abstract. The modern judicial system is rapidly developing and the use of digital technologies does not bypass it. In this article, the author examines the issues of maintaining the availability of arbitration proceedings in the era of digitalization, as well as changes in legislation regarding the execution of judicial acts in electronic form.

Keywords: law, digital technologies, arbitration process, electronic court proceedings, information

Согласно части 5 статьи 15 АПК РФ, судебный акт, за исключением акта, содержащего сведения, составляющие государственную или иную охраняемую законом тайну, если дело рассмотрено в закрытом судебном заседании, может быть выполнен в форме электронного документа, который подписывается судьей усиленной квалифицированной электронной подписью [1. С. 3012].

Данная норма создает перспективы для ускорения процесса исполнения судебных актов, а также в теории обеспечивает повышенную эффективность работы судебной системы в целом.

Норма также несет в себе спорный характер относительно доступности подобного типа судебного разбирательства. Как правило, судебная система и доступ к правосудию должны быть доступны для всех без исключения граждан и юридических лиц, вне зависимости от их просвещенности в системе цифровых технологий. Если выдвигать эту теорию как возможную проблему, то решением ее может послужить разработка необходимых механизмов, которые будут работать на создание тех самых благоприятных условий для общей доступности цифрового электронного судопроизводства.

Во-первых, стоит сказать о необходимости обеспечения всеобщего доступа к судебной информации и электронным ресурсам, таким как электронные базы данных судебных актов и специализированные онлайн-платформы для подачи и получения судебных документов. Во-вторых, автор говорит о немаловажности предоставления юридических консультаций и помощи в работе с системой

цифрового судопроизводства. Разработка специализированных онлайн-платформ и порталов, возможность проведения онлайн-консультаций для граждан и юридических лиц также необходимы в данном случае.

Соответственно, главной задачей выступает разработка специальной программы обучения для юристов, судей и в целом работников судебной системы по грамотной и корректной работе с цифровым судопроизводством.

С использованием инновационных технологий в судопроизводстве для нас открываются новые возможности для более эффективного и ускоренного процесса исполнения судебных актов.

В настоящее время электронная подпись играет важную роль в сфере цифрового правосудия. Определение понятия «электронная подпись» закреплено в Федеральном законе «Об электронной подписи» [7. С. 2036] и означает информацию в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Важно соблюдать принцип, закрепленный в части 1 статьи 118 Конституции Российской Федерации [2. С. 8], согласно которому правосудие (будь то цифровое или с использованием бумажных документов) осуществляется исключительно судом.

С 1 января 2017 г. вступил в силу Федеральный закон, расширяющий перечень действий, которые арбитражные суды могут совершать в электронном виде [8. С. 38–89].

Изначально цифровые технологии были применены для обращения граждан и юридических лиц в суды, а также для извещения участников судопроизводства.

Пленум Верховного Суда Российской Федерации провел детальный анализ терминологии, применяемой в сфере электронного документооборота, предоставляя важные пояснения по этому вопросу. Так, «электронный документ» означает документ, созданный в электронной форме без предварительного бумажного носителя [4. С. 1].

Внедрение электронного исполнения судебных актов в России имеет ряд преимуществ. Прежде всего, это значительно сокращает временные затраты на передачу и доставку документов, что способствует более быстрому и эффективному исполнению судебных решений. Электронное исполнение позволяет избежать потери и искажения информации, поскольку электронные документы могут быть сохранены и переданы без изменений. Это также способствует повышению прозрачности и надежности процесса исполнения судебных актов.

Необходимо обеспечить исполнение судебных актов в электронной форме только в том случае, если они не содержат сведений, составляющих государственную тайну или иную охраняемую законом тайну. Это гарантирует защиту конфиденциальной информации и обеспечивает соблюдение соответствующих правовых норм.

В Российской Федерации первым шагом к информатизации стало принятие Концепции информационной политики судебной системы на 2020–2030 гг. Советом судей Российской Федерации 5 декабря 2019 г. [3. С. 24].

Центральными стратегическими направлениями данной политики охватываются: гармонизация отношений судебной власти и общества, открытость и гласность судопроизводства, а также улучшение доступа к информации о деятельности судов. Для достижения этих целей суды стремятся увеличить количество информационных ресурсов, доступных гражданам и организациям. Они разрабатывают порталы, издания, мобильные приложения, используют социальные сети и информационно-образовательные проекты, а также видео.

Совет судей также отмечает, что развитие цифровых технологий открывает новые перспективы для работы с большим объемом информации.

Облачное хранение аудиопротоколов судебных заседаний расширяет принцип открытости судебного заседания. Это позволяет избежать копирования аудиопротоколов на электронные носители и предоставляет возможность участникам процесса ознакомиться с аудиозаписью независимо от их местонахождения.

Однако информационная политика судебной системы не ограничивается только техническими аспектами. Она также предусматривает проведение обучающих и разъяснительных мероприятий в образовательных учреждениях. Планируется участие судов в программах профессиональной ориентации школьников и студентов, а также организация дней открытых дверей в судах для студентов-выпускников. Более того, в планах есть создание нового образовательного модуля в системе ГАС «Правосудие». Открытость и доступность правосудия на территории регионов Российской Федерации будут обеспечиваться путем создания непрерывно действующих комиссий по мониторингу. Эти комиссии будут действовать при советах судей региональных субъектов, следя за тем, чтобы судопроизводство оставалось прозрачным.

Онлайн-заседания имеют некоторые преимущества. Во-первых, они обеспечивают безопасность здоровья участников процесса [10], судей и сотрудников аппаратов судов. Во-вторых, они предоставляют возможность участвовать в судебном заседании и реализовать свое право на выслушивание, находясь в офисе или дома.

Открытость судебных заседаний является важным аспектом судебной деятельности, который обеспечивает прозрачность и справедливость. Согласно части 1 статьи 59 Арбитражного процессуального кодекса Российской Федерации, граждане имеют право вести свои дела в арбитражном суде лично или через представителей.

Автор также отмечает необходимость в целях обеспечения справедливости и учета разнообразных обстоятельств судебным органам уделить особое внимание упрощению процедуры подачи ходатайств на участие в онлайн-заседаниях.

Цифровое правосудие стало неотъемлемой частью современной юриспруденции, и его роль продолжает расти наряду с развитием информационных технологий [9].

Арбитражные суды внедрили такие онлайн-сервисы, как «Мой арбитр» (предназначен для дистанционного взаимодействия граждан с арбитражным судом), автоматизированную информационную систему «Банк решений арбитражных судов» (содержит данные и реквизиты всех судебных дел), сервис «Картотека

арбитражных дел» (получение информации по делам) и сервис «Электронный страж» (предоставляет возможность получать уведомления по арбитражным делам) [5. С. 176–182].

Ключевым преимуществом правосудия является некая возможность ведения аудиопротоколов судебного заседания, а также участие сторон процесса через системы видео-конференц-связи. Это преимущество призвано упрощать доступ к правосудию, особенно для тех граждан и юридических лиц, кто имеет ограниченные возможности для непосредственного присутствия на заседании.

В целом электронное правосудие представляет собой относительно новую сферу общественных отношений, которая требует постоянного совершенствования и четкого нормативно-правового регулирования.

Таким образом, автор приходит к выводу, что судебная система в целом находится на активном рубеже цифровизации, что определенно улучшает и сам арбитражный процесс. Важную роль современные технологии играют в обеспечении открытости, прозрачности и полной отчетности в судебной системе. В качестве одного из главных достижений в области цифровизации выступает функционирование цифровых инструментов в системе, с помощью которых информация переводится в цифровой формат, что обеспечивает точность результатов деятельности.

Благодаря внедрению цифровых технологий судопроизводство с каждым днем становится все проще и удобнее для использования всеми участниками процесса [6].

Стоит отметить, что при внедрении цифровизации должна соблюдаться защита информационных ресурсов и конфиденциальность данных от преступных посягательств и других атак. Цифровой формат информации должен обеспечивать сохранность документов без потери и какого-либо повреждения.

Цифровизация инструментов арбитражного процесса призвана повышать эффективность и создавать дополнительные гарантии защиты прав граждан и юридических лиц. Автор говорит от необходимости систематического совершенствования цифровизации правосудия, а также мониторинга за соблюдением информационной безопасности [11], что в совокупности может обеспечить надежность цифрового арбитражного процесса.

Список литературы

1. Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ // Собрание законодательства РФ. 2002. № 30. Ст. 3012.

2. Конституция Российской Федерации: (Принята всенародным голосованием 12 декабря 1993 г.) // Собрание законодательства РФ. 1993. № 31. Ст. 8.

3. Концепция информационной политики судебной системы на 2020–2030 годы (одобрена Советом судей РФ 5 декабря 2019 г.) // СПС «Гарант». URL: https://base.garant.ru/73161586

4. Постановление Пленума Верховного Суда РФ от 26.12.2017 № 57 «О некоторых вопросах применения законодательства, регулирующего использование

документов в электронном виде в деятельности судов общей юрисдикции и арбитражных судов» // Бюллетень Верховного Суда РФ. № 4. Апрель. 2018.

5. Саввинова Т. В. Цифровизация в арбитражном процессе // Вопросы российского и международного права. 2021. Том 11, № 6А. С. 176–182.

6. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497. EDN: ACSQXH

7. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

8. Федеральный закон 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» // Собрание законодательства РФ. 2016. № 26. Ст. 3889.

9. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

10. Шутова А. А., Ефремова М. А., Никифорова А. А. Уголовная ответственность за распространение заведомо ложных сведений в период пандемии: вопросы теории и практики // Вестник Удмуртского университета. Серия: Экономика и право. 2021. Т. 31, № 1. С. 81–89. EDN: ZYQLYQ

11. Жарова А. К. Риски информационной безопасности и возможности правового регулирования криптовалюты в России // Информационное право. 2018. № 4. С. 11–16. EDN: YPNFET

А. А. Галлямова
студент,
Московский государственный университет
имени М. В. Ломоносова

ПРАВО ЧЕЛОВЕКА НА ЦИФРОВОЙ ОБРАЗ В КОНТЕКСТЕ РАЗВИТИЯ ТЕХНОЛОГИИ БИОПРИНТИНГА

Аннотация. Цифровая трансформация повлекла за собой масштабные перемены во всех сферах жизни общества. В результате развития технологии биопринтинга под угрозу попала защита нематериальных прав человека. Это связано с тем, что в процессе образ человека переходит в цифровую среду, в результате чего это трехмерное воплощение ставит его обладателя в определенную зависимость, особенно в процессе использования его прав на жизнь и здоровье. Одним из возможных решений данной проблемы является реализуемая на данный момент во многих правовых системах концепция права на персональный образ.

Ключевые слова: цифровая трансформация, информация, персональные данные, биопринтинг, биофабрикация, трехмерный образ, нематериальный ущерб

THE HUMAN RIGHT TO A DIGITAL IMAGE IN CONTEXT DEVELOPMENT OF BIOPRINTING TECHNOLOGY

Abstract. Digital transformation has led to large-scale changes in all spheres of society. As a result of the development of technologies, such as bioprinting technologies, the protection of intangible human rights is at risk. This is due to the fact that in the process the image of a person passes into the digital environment, as a result of which this three-dimensional incarnation puts its owner in a certain dependence, especially in the process of using his rights to life and health. One of the possible solutions to this problem is the concept of the right to a personal image that is currently being implemented in many legal systems.

Keywords: digital transformation, information, personal data, bioprinting, biofabrication, three-dimensional image, non-material damage

Трехмерная (3D) биопечать тканеинженерных конструкций и прототипов органов для регенеративной медицины является одним из наиболее перспективных направлений цифровой биотехнологии. Биопринтинг в специальной литературе определяется как высокоточная технология послойного (аддитивного) производства трехмерных тканевых и органных конструктов с внешней и внутренней архитектурой, заданной цифровой моделью и с использованием живых клеток в качестве печатного материала. Главной функцией таких конструкторов является частичная или полная замена необходимых человеку органов и тканей. В основе биопринтинга лежит известное науке явление самосборки. Данный процесс представляет собой межбелковое взаимодействие, которое регулируется силами поверхностного натяжения, благодаря чему, например, формируются органы эмбриона.

Технологии биопринтинга, помимо множества новых возможностей и преимуществ в разных сферах жизни общества, также стали причиной возникновения новых проблем правового регулирования этого процесса, определение пределов и способов защиты как имущественных, так и личных неимущественных прав человека. Решению правовых проблем при этом неизбежно должно предшествовать установление правил биоэтики, которые необходимо установить при регулировании искусственного воспроизведения органов, их пересадки, моделирования, хранения и т. д. Отследив рассмотренный выше процесс создания новых органов посредством использования технологий биопринтинга, можно убедиться, что он неизбежно затрагивает сферу нематериальных благ, которые принадлежат всем людям от рождения. В основе любых медицинских исследований должны лежать два основополагающих принципа: принцип конфиденциальности и принцип информированного согласия. Первый предполагает сохранение ученым, врачом информации о состоянии здоровья пациента и особенностях его лечения в тайне. Второй принцип является, помимо правовой, важной этической составляющей медицинских исследований. Особую значимость ему придает также закрепление на международном уровне: Конвенция о защите прав и достоинства человека в связи с применением достижений биологии и медицины: Конвенция о правах человека и биомедицине (СЕД № 164) [8].

Интересным также будет рассмотреть вопрос об ответственности за вред, причиненный нарушением права на цифровой образ. Если обратиться к опыту зарубежного законодательства, то в Общем регламенте защиты персональных данных (GDPR) в статье 82 [9] установлено, что любое лицо, которому был причинен материальный или нематериальный вред в результате нарушения настоящего Регламента, имеет право на получение от контролера или процессора (обработчика данных) компенсации за причиненный вред.

В России в связи с аналогичной проблемой отсутствия должного правового регулирования процесс биопечати и создания новых органов человека вызывает множество вопросов на практике. Действующая редакция Федерального закона от 23.06.2016 № 180-ФЗ «О биомедицинских клеточных продуктах» [10] пока не может регулировать использование биофабрикатов органов человека, так как этот закон не регулирует вопросы трансплантации органов. В то же время Закон РФ от 22.12.1992 № 4180-1 «О трансплантации органов и (или) тканей человека» [11] также не может регулировать использование 3D-печатных органов, так как 3D-биопечатные изделия являются искусственными. Трудность создания эффективного и централизованного правового регулирования усугубляется также и тем, что использование биопечати воздействует на нематериальную сферу прав человека. В связи с этим возникает потребность в поиске эффективных средств защиты в случае нарушения данных прав человека. Установление безвиновной ответственности за нарушение права на цифровой образ представляет собой возможный ответ на последствия цифровой трансформации.

Список литературы

1. European Commission. European Commission-DG Health and Food Safety and European Medicines Agency Action Plan on ATMPs. 2017. URL: https://www.ema.europa.eu/en/documents/other/european-commission-dg-health-food-safety-european-medicines-agency-action-plan-advanced-therapy_en.pdf

2. Article 82 (1) GDPR: «Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered». Available at: http://eur-lex.europa.eu/

3. Федеральный закон от 23.06.2016 № 180-ФЗ «О биомедицинских клеточных продуктах». Доступ из справ.-правовой системы «КонсультантПлюс».

4. Закон РФ от 22.12.1992 № 4180-1 «О трансплантации органов и (или) тканей человека». Доступ из справ.-правовой системы «КонсультантПлюс».

З. А. Дятлов,
студент,
Санкт-Петербургский филиал
Национального исследовательского университета
«Высшая школа экономики»

АВТОРСКОЕ ПРАВО НА ПРОИЗВЕДЕНИЯ, СОЗДАННЫЕ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ: НОВЫЙ СУБЪЕКТ АВТОРСКОГО ПРАВА?

Аннотация. Стремительное развитие технологий искусственного интеллекта ставит много вопросов, связанных с правовым регулированием. В статье рассматриваются подходы к возможности наделения искусственного интеллекта правоспособностью в контексте возможности признания его автором созданных им произведений искусства. Рассматриваются основные подходы к определению авторства таких произведений, а также опыт зарубежной правоприменительной практики по данному вопросу.

Ключевые слова: право, цифровые технологии, искусственный интеллект, автономный искусственный интеллект, авторское право, субъекты авторского права, охраняемые авторским правом произведения

COPYRIGHT FOR WORKS CREATED BY ARTIFICIAL INTELLIGENCE: A NEW SUBJECT OF COPYRIGHT?

Abstract. The rapid development of technologies, namely artificial intelligence systems, raises many questions related to legal regulation. The article considers approaches to the possibility of granting artificial intelligence legal capacity in the context of the possibility of recognizing AI as the author of works of art created by it. The main approaches to determining the authorship of such works are considered, as well as the experience of foreign law enforcers in the context of this issue.

Keywords: law, digital technologies, artificial intelligence, autonomous artificial intelligence, copyright, copyright subjects, copyrighted works

Развитие информационных технологий меняет не только повседневную жизнь человека, позволяя автоматизировать рутинные процессы жизнедеятельности, но и проникает в такие, казалось бы, присущие лишь человеческому восприятию сферы, как наука и искусство. Искусственный интеллект (далее – ИИ) помогает в решении научных задач, «рисует» картины, «пишет» музыку и литературные произведения. Но в таком случае встает закономерный вопрос, кого же мы должны считать автором произведений, созданных искусственным интеллектом.

Во второй половине XIX и начале XX вв. ученые размышляли над самой сутью авторского права как такового, его необходимостью и целями. Так, например, Г. Ф. Шершеневич указывал, среди прочего, на следующую причину необходимости существования авторского права как легального института: необходимость защиты интересов автора [9. С. 9]. Такая защита необходима, поскольку человек,

посвящающий свою жизнь искусству, своеобразному «служению обществу», чаще всего не имеет источника дохода, позволившего бы ему нормально существовать и работать только в сфере искусства.

Авторское право входит в число институтов частного права. Трудно спорить с тем, что главным мотивом вступления акторов в частноправовые отношения является чистый экономический интерес в получении прибыли. И сфера охраны объектов интеллектуальной собственности в этом плане не исключение. Для многих авторов на первое место выходит экономический интерес, а не созидательный, о чем уже в начале XX века писал Г. Ф. Шершеневич [9. С. 19].

С появлением искусственного интеллекта, которому, по крайней мере в настоящий момент, не важен экономический вопрос его деятельности, возникает новый вопрос как для права в целом, так и для отдельных его институтов: как же все-таки квалифицировать автора таких произведений?

Ученые в данный момент разделяют искусственный интеллект на сильный и слабый. Слабый ИИ используется в качестве механизма для автоматизации рутинных задач, которые раньше выполнял человек. Такой искусственный интеллект не имеет технической возможности имитировать мыслительную деятельность человека [5. С. 531–540]. Создание же сильного искусственного интеллекта в настоящий момент невозможно, однако некоторые считают таким ИИ нейросети [21].

Вопрос о правосубъектности искусственного интеллекта также уже рассматривался учеными. Главная проблема состоит в том, что ИИ в настоящий момент слабо развит как автономный субъект. Можно говорить о повышенной автономности некоторых систем – ChatGPT смог пройти тест Тьюринга, – но все равно в конечном счете искусственный интеллект еще не «самоосознал» себя. Поэтому предложения некоторых ученых наделить ИИ ограниченной правосубъектностью выглядят чересчур футуристичными. В настоящий момент искусственный интеллект не имеет экономического интереса к участию в экономическом обороте, его не волнует, будет ли он указан в качестве автора размещенного кем-либо произведения. Последний вопрос скорее волнует разработчиков и пользователей, которые работают с искусственным интеллектом, когда тот создает произведения искусства.

Вопрос о правосубъектности искусственного интеллекта лежит в основе всех рассуждений по поводу возможности охраны исключительных прав на произведения, созданные ИИ. С правосубъектностью физических и юридических лиц все предельно понятно как с точки зрения законодательства, так и с точки зрения положений доктрины, хотя при рассмотрении правосубъектности юридических лиц применяются различные теоретические подходы. Основополагающей теорией считается теория фикции, впрочем, ее возможно применить и к искусственному интеллекту. Предполагается ввести условность о том, что система искусственного интеллекта обладает специфической правосубъектностью по типу правосубъектности некоторых видов юридических лиц.

Но при таком подходе снова возникает экономический вопрос, а именно с какой целью мы наделяем искусственный интеллект правосубъектностью.

Ответом может служить необходимость в создании условий для возмещения вреда, который своими действиями может причинить искусственный интеллект. Наделив искусственный интеллект ограниченной правоспособностью, в частности, способностью иметь в собственности определенное имущество, а также деликтоспособностью, мы сможем упростить процесс получения возмещения ущерба лицами, пострадавшими от действий системы искусственного интеллекта. Только такая конструкция будет слишком громоздкой и потребует обновления как законодательства, так и теоретических подходов к пониманию лиц, участвующих в гражданском обороте. Как было отмечено ранее, искусственный интеллект еще не достиг того уровня развития, при котором он сможет понимать значение своих действий и осознавать свою ответственность за них. В такой ситуации наделение его правоспособностью кажется излишним, а проблему с ответственностью за вред можно решить с помощью механизмов, которые уже существуют в отечественном законодательстве. Например, можно рассматривать искусственный интеллект как работника, за которого несет ответственность работодатель (1068 ГК РФ). Либо лица, использующие ИИ в гражданском обороте, могут страховать его деятельность.

Также наделение искусственного интеллекта правосубъектностью поможет решить вопрос с авторством произведений, созданных ИИ. В таком случае можно наделить систему искусственного интеллекта правом на авторство. Однако как быть с распоряжением исключительным правом? Искусственному интеллекту на данном этапе его развития не требуются материальные ценности, если только ему не нужно будет за их счет возмещать вред. Кроме того, искусственный интеллект не понимает ценности исключительных прав и не сможет ими распоряжаться так, как это бы сделал человек.

Как уже было сказано выше, искусственный интеллект еще не развит настолько, чтобы можно было сказать о наличии у него мышления. А именно наличие мышления отличает человека от других существ. С помощью способности к мышлению человек осознает свои поступки и понимает, что за ними последует, благодаря этому можно говорить и о правоспособности человека. Кажется, в настоящий момент еще рано наделять искусственный интеллект правоспособностью. Это можно будет сделать тогда, когда он себя «самоосознает» и приобретет навык, похожий на человеческое мышление.

Главным параметром, определяющим возможность правовой охраны авторства произведения, является концепция «творчества». В законодательстве большинства государств мира именно наличие творческой составляющей упоминается как обязательный элемент для признания произведения подлежащим правовой защите. Однако ни правоприменительная практика, ни доктринальные исследования не содержат единого общепризнанного подхода к пониманию «творчества», а главное, тех его характеристик, которые бы отличали процесс, содержащий элементы творчества, от обычной технической работы.

Толковый словарь С. И. Ожегова и Н. Ю. Шведовой определяет понятие творчества как создание новых по замыслу культурных или материальных ценностей [6]. Суд по интеллектуальным правам РФ придерживается похожего определения

«творчества» [2]. Из этого определения можно выделить две характеристики творчества: «новизна результата» и «создание культурных или материальных ценностей». Можно ли говорить о наличии данных характеристик в произведениях, создаваемых искусственным интеллектом?

Рассмотрим такую характеристику, как новизна результата. Например, в 2022 г. группа исследователей с помощью искусственного интеллекта создала «новую» картину в стиле Рембрандта [10]. Портрет мужчины выполнен в технике, до точности схожей с техникой голландского художника. Можно ли говорить, что было создано новое по своему замыслу произведение? С одной стороны, нет, так как искусственный интеллект использовал уже существующую технику живописи. Но можно утверждать и обратное по нескольким причинам. Во-первых, такой картины у Рембрандта не существовало, а значит, возникло новое произведение. Во-вторых, исследователи, которые трудились над созданием картины с помощью искусственного интеллекта, сформировали запрос о том, какой портрет должен быть нарисован. Представляется логичным, что появился совершенно новый по своему замыслу портрет «белого мужчины с бородой, в возрасте от 30 до 40 лет, в темных одеждах с пышным воротником, в шляпе, смотрит он в правую сторону». Использование техники не может говорить о плагиате, так как конечный результат все-таки отличается от существующих работ Рембрандта. Если судить иначе, то нельзя признать оригинальными и некоторые произведения русских композиторов, например, П. И. Чайковского, Н. И. Римского-Корсакова, М. П. Мусоргского, которые использовали в своих произведениях фольклорные мотивы.

Также можно рассмотреть работы широко известной нейросети Midjourney. В начале текущего года в США был подан коллективный иск, одними из ответчиков по которому являются ее разработчики [24]. Истцы считают, что, обучая нейросеть на доступных в свободном доступе изображениях, они нарушили авторские права художников. Решения суда пока нет, поэтому можно спекулировать на тему того, могут ли их требования быть удовлетворены. С одной стороны, это может случиться, так как некоторые результаты работы нейросети очень похожи на работы некоторых деятелей искусства, однако они не совпадают на 100 %. Видится, что требования истцов должны остаться без удовлетворения. Можно снова обратиться к Г. Ф. Шершеневичу [9. С. 3–4], который считал, что деятель искусства в первую очередь создает свои произведения для пользы общества, им движет порыв привнести в этот мир что-то новое и поделиться этим со всеми, а уже после идет коммерческий интерес. К сожалению, в современном мире коммерческий интерес зачастую ставится превыше высоких побуждений.

Вторая характеристика творчества, вытекающая из его определения, – «создание культурных или материальных ценностей». Кажется, все согласятся, что как минимум материальные ценности искусственный интеллект создает точно. Многие признают, что искусственный интеллект создает и культурные ценности. Особенно в настоящее время, когда современное искусство является понятным не всем, границы культуры стали очень размытыми. Поэтому можно сказать, что искусственный интеллект создает культурные ценности.

Кроме того, некоторые авторы определяют творческую деятельность умственной или мыслительной [3, 8]. Следуя их логике, механизм действия искусственного интеллекта нельзя назвать мыслительным. Ученые уверены, что искусственный интеллект не сможет создать подлинно творческие объекты по той причине, что они обучены создавать объекты, только имеющие сходство с результатами творческой деятельности.

Калин Христов и К. Р. Дэвис считают иначе. Последний указывает на то, что результат деятельности автономного ИИ является результатом не технического процесса, а изучением необходимой информации, что является одной из черт мыслительной деятельности [18. С. 704]. Учитывая высокую степень автономности искусственного интеллекта, лицо, разработавшее ИИ или использующее его, также не может быть названо автором. Участие указанных лиц в создании результатов интеллектуальной деятельности нельзя назвать непосредственным. Зачастую разработчик или пользователь только «направляет» деятельность искусственного интеллекта в необходимое для него русло.

Результаты деятельности искусственного интеллекта и результаты интеллектуальной деятельности человека в некоторой степени схожи между собой. Отечественное законодательство, которое действует в данный момент, не позволяет осуществлять правовую охрану результатов деятельности ИИ. В будущем такая возможность должна появиться, если законодатель нацелен на развитие технологии искусственного интеллекта.

Признаки творчества все-таки содержатся в процессе создания произведений искусственным интеллектом. Поэтому считаем необходимым предоставление правовой защиты таким произведениям как объектам авторских прав. Однако появляется вопрос, кого считать автором такого произведения.

В науке существует несколько ответов на данный вопрос [4. С. 182–184].

Некоторые исследователи придерживаются так называемого концепта нулевого авторства. Популярность данная концепция получила в связи с тем, что нельзя определить точный вклад каждого участника процесса создания произведения: разработчика системы ИИ, его пользователя, а в некоторых случаях на авторство претендуют и те лица, которые осуществили заказ или оплатили создание искусственного интеллекта. В. Н. Синельникова придерживается мнения, согласно которому объекты интеллектуальной собственности, созданные ИИ, не имеют автора, но могут получать правовую защиту [7. С. 326]. Получение правовой защиты необходимо для защиты интересов компании – владельца системы искусственного интеллекта и ее разработчиков. Если не предоставлять правовую охрану таким произведениям, может замедлиться технический прогресс. Ю. Роберт [25. С. 1265–1266] и Петер Манолакев [26. С. 40-42] считают, что такие произведения должны переходить в общественное достояние по образу народного творчества и не иметь никакой правовой охраны. Такое решение позволит свободно использовать и произведения, созданные искусственным интеллектом. Можно сказать, что данного концепта придерживался Пекинский суд при вынесении решения по делу Beijing Film Law Firm v. Beijing Baidu Netcom Science & Technology Co., Ltd. Фабула дела [17] состоит в том, что ответчик использовал статью истца,

которая содержала графики, созданные нейросетью «Wolters Kluwer Database», принадлежащей истцу. Право авторства на текстовую часть статьи было признано за истцом, а часть, созданная ИИ, была признана не подлежащей правовой защите как объект, в процессе создания которого не усматривается творческая деятельность.

Такой концепт видится ошибочным, а его принятие приведет к снижению интереса к системам искусственного интеллекта, способного к созданию произведений искусства.

Машиноцентричный концепт авторства напрямую связан с уже рассмотренной выше проблемой наделения искусственного интеллекта правоспособностью. Как было сказано ранее, искусственный интеллект на данном этапе своего развития пока не должен быть наделен правоспособностью, что исключает применение данного концепта. Однако такой подход может быть принят в будущем. Сторонники данного концепта считают, что признать автором созданного произведения нужно лишь искусственный интеллект, и к тому же ИИ должен быть и владельцем исключительных прав на созданное произведение. Но, как уже рассмотрено ранее, способность ИИ к распоряжению исключительными правами и целесообразность наделения его правом получения дохода от использования произведения представляются сомнительными.

Другой крайностью является антропоцентричный концепт, который предполагает, что искусственный интеллект не может быть признан автором ни при каких условиях [11. С. 112]. При таком подходе искусственный интеллект рассматривается лишь в качестве инструмента в руках его пользователя-человека [20. С. 9–11]. Тогда кого же все-таки считать автором? Автором можно признать владельца системы искусственного интеллекта, ее разработчика или конечного пользователя.

Признание авторства за владельцем приведет к снижению интереса пользователей к нейросетям и системам искусственного интеллекта. Тем более существуют ситуации, когда владелец искусственного интеллекта распространяет доступ к нему на коммерческой основе.

Признать авторство за создателем ИИ также будет неправильным и несправедливым. Во-первых, тогда придется указывать не одного автора, а целый коллектив, так как над созданием ИИ обычно работают большие команды разработчиков. Однако чаще всего такие разработки финансируются сторонними компаниями, интересы которых тоже должны быть учтены.

Более справедливым кажется признание автором пользователя, использующего искусственный интеллект, ведь именно он задает вектор работы нейросети. В частности, это будет хорошим решением, если все нейросети будут распространяться по платной подписке. Но такой подход тоже приведет к снижению интереса пользователей к искусственному интеллекту, так как не каждый готов вкладывать деньги в стремительно развивающуюся, но все еще не до конца понятную широкому кругу лиц область.

Поддерживаемая некоторыми исследователями концепция гибридного авторства скорее расширяет проблему, нежели дает ее решение. Согласно рассматриваемой

теории, нужно защищать вклад всех, кто участвовал в процессе создания произведения, – от разработчика системы искусственного интеллекта до самого искусственного интеллекта. Такой подход создает дополнительные проблемы, ведь система искусственного интеллекта творит почти автономно, оставляя большие вопросы о вкладе остальных участников процесса в конечный результат. В этом случае в интересах людей будет полное отрицание вклада искусственного интеллекта в создание произведения.

Концепт служебного произведения предлагает переосмыслить само понятие такого произведения и отношения «работодатель – работник». Действительно, в отношениях между искусственным интеллектом и разработчиком/владельцем/пользователем и работодателем и работником есть много общего. Но снова возникает вопрос, кто будет «работодателем»? Если система искусственного интеллекта используется только владельцем, то он будет обладать исключительными правами на объект интеллектуальной собственности, а определенный искусственный интеллект будет значиться автором. Но что делать, если искусственный интеллект используется третьим лицом – пользователем, да еще и на безвозмездной основе? Кому будут принадлежать исключительные права на объекты интеллектуальной собственности?

Иностранные правоприменители по-разному решают вопрос, кто является автором произведений, созданных искусственным интеллектом. В уже упомянутом деле Beijing Film Law Firm v. Beijing Baidu Netcom Science & Technology Co., Ltd. суд признал продукт деятельности искусственного интеллекта не подлежащим правовой охране по причине отсутствия творческой составляющей. А в деле Tencent v. Yingxun Tech [17] суд признал авторское право на статью, написанную искусственным интеллектом, за компанией Tencent, которая владеет ИИ. В обоснование решения суд заявил, что искусственный интеллект был использован в качестве инструмента коллективом разработчиков. Поэтому в соответствии с Законом Китайской Народной Республики «Об авторском праве» [14] авторское право было признано за компанией-работодателем.

Суды Европейского союза достаточно консервативно подходят к решению вопроса. В деле Infopaq International v. Danske Dagblades Forening была сформулирована позиция, что правовая защита распространяется только на объекты, которые являются оригинальными в том смысле, что они представляют собой результат независимой интеллектуальной деятельности автора-человека. Этот подход был положен в основу последующих решений Европейского суда.

Из Закона Соединенного Королевства Великобритании «Об авторском праве, промышленных образцах и патентах» [13] следует, что для признания произведения, созданного искусственным интеллектом, подлежащим правовой охране требуется наличие достаточной доли участия человека в создании такого произведения (секция 3(9) Закона). Суды Великобритании не рассматривают вопрос об оригинальности произведений, они лишь стараются определить степень участия человека в создании произведения [19. С. 458].

Параграф 102(a) Закона США «Об авторском праве» устанавливает, что охране подлежат только «оригинальные авторские произведения» [15]. Компендиум

практики Бюро регистрации авторских прав США содержит положения, согласно которым авторское право в Соединенных Штатах охраняет только «плоды интеллектуального труда», созданные «творческими силами разума». Это позволяет сделать вывод о том, что в регистрации произведения, созданного искусственным интеллектом, будет отказано. Так, например, в феврале Бюро регистрации авторских прав США отказало в регистрации прав на комикс Кристины Каштановой, изображения для которого были созданы нейросетью Midjourney [23]. Каштанова была признана автором комикса как сложного объекта, но не автором изображений. Она настаивала на том, что внесла вклад в создание изображений через отправление команд для нейросети, однако Бюро не признало ее вклад творческим.

В заключение хотелось бы предложить следующий способ решения вопроса о том, кто должен быть признан автором произведения, созданного нейросетью. Думается, что нужно будет развести автора и владельца исключительных прав на объект интеллектуальной собственности.

Если нейросеть свободна для использования, то автором произведения нужно признавать искусственный интеллект, но во избежание споров не должно возникать исключительных прав на это произведение. С одной стороны на них претендовал бы пользователь, задающий команду, с другой – владелец системы искусственного интеллекта либо команда разработчиков.

Если нейросеть распространяется по платной подписке (например, нейросеть Midjourney может быть использована по подписке, которая увеличивает возможности пользователя по созданию изображений), то автором произведения также нужно признавать искусственный интеллект, а исключительные права должен получать пользователь, который оплатил указанную подписку.

Если же нейросеть недоступна для широкого круга лиц и используется исключительно компанией-владельцем либо разработчиками, то автором нужно считать нейросеть, а обладателем исключительных прав либо компанию владельца, либо команду разработчиков.

Список литературы

1. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_64629

2. Постановление Суда по интеллектуальным правам от 28.10.2022 № С01–1784/2022 по делу № А19–9269/2021 // СПС «КонсультантПлюс» Версия Проф.

3. Ионас В. Я. Критерий творчества в авторском праве и судебной практике. М.: Юридическая литература, 1963.

4. 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. 854–874.

5. Резаев А. В., Трегубова Н. Д. Возможность и необходимость человекоориентированного искусственного интеллекта в юридической теории и практике // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 564–580. EDN: SADRZW

6. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. 4-е изд. М., 1997. 944 с.

7. Синельникова В. Н. Правовой режим результатов интеллектуальной деятельности, созданных саморазвивающимися программами // Пермский юридический альманах. 2019. № 2.

8. Сушкова О. В. Критерии творчества и новизны в объектах интеллектуальной собственности в РФ // Вестник ОмГУ. Серия: Право. 2008. № 4.

9. Шершеневич Г. Ф. Экономическое обоснование авторского права / [Сочинение] Г. Ф. Шершеневича. Казань: Типография Императорского университета, 1890. 26 с.

10. Нейросеть нарисовала «новую» картину Рембрандта: попробуй отличи! // TechInsider, 12.08.2022. URL: https://www.techinsider.ru/gadgets/237490-kompyuter-sozdal-novuyu-kartinu-rembrandta

11. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.

12. Compendium of U. S. Copyright Office Practices. URL: https://www.copyright.gov/comp3/docs/compendium.pdf

13. Copyright, Designs and Patents Act 1988. URL: https://www.legislation.gov.uk/ukpga/1988/48/contents

14. Copyright Law of the People's Republic of China (promulgated by Decree No. 31 of September 7, 1990, of the President of People's Republic of China) // WIPO Portal. URL: https://www.wipo.int/wipolex/ru/text/336460

15. U.S. Copyright Act of 1976. URL: http://www.wipo.int/wipolex/en/text.jsp?file_id=338108

16. Beijing Internet Court (2018) Jing 0491 Min Chu No. 239 Civil Judgment. April 25, 2019. Beijing Film Law Firm v. Beijing Baidu Netcom Science & Technology Co., Ltd. // Law Info China Portal. URL: http://www.lawinfochina.com/display.aspx?lib=case&id=3836

17. Tencent v. Yingxun Tech // China Law Portal. URL: https://ru.chinajusticeobserver.com/law/x/2019-yue-0305-min-chu-14010/intro

18. Davies C. R. An Evolutionary Step in Intellectual Property Rights – Artificial Intelligence and Intellectual Property // Computer Law and Security Review. 2011. Vol. 27. № 6.

19. Dickenson J. Creative Machines: Ownership of Copyright in Content by Artificial Intelligence Applications // European Intellectual Property Review. 2017. Vol. 39, № 8.

20. Gürkaynak G., Yılmaz I., Doygun T., İnce E. Questions of Intellectual Property in the Artificial Intelligence Realm // Robotics Law Journal. September – October. 2017.

21. Hristov K. Artificial intelligence and the copyright dilemma // IDEA – The Journal of the Franklin Pierce Center for Intellectual Property. 2017. Vol. 57. № 3.

22. Kerns J. What's the Difference Between Weak and Strong AI? // MachineDesign. 2017. February 15. URL: https://www.machinedesign.com/robotics/what-s-difference-between-weak-and-strong-ai

23. Zarya of the Dawn Letter – U. S. Copyright Office. URL: https://www.copyright.gov/docs/zarya-of-the-dawn.pdf

24. We've filed a lawsuit challenging Stable Diffusion, a 21st-century collage tool that violates the rights of artists. Because AI needs to be fair & ethical for everyone // Stable Diffusion litigation. 13.01.2023. URL: https://stablediffusionlitigation.com

25. Yu R. The Machine Author: What Level of Copyright Protection is Appropriate for Fully Independent Computer Generated Works. // University of Pennsylvania Law Review. 2016. № 165.

26. Manolakev P. H. Works Generated by AI–How Artificial Intelligence Challenges Our Perceptions of Authorship. Master thesis. Tilburg, 2017.

М. С. Евстефеева,
магистрант,
Самарский национальный исследовательский университет
имени академика С. П. Королева

К ВОПРОСУ О ПОНЯТИИ И ПРАВОВОМ РЕГУЛИРОВАНИИ КРИПТОВАЛЮТНОЙ БИРЖИ

Аннотация. В статье исследуется понятие и феномен криптовалютной биржи. Определены основные признаки централизованных и децентрализованных криптовалютных бирж. Затрагивается вопрос правового регулирования криптобиржи с учетом анализа законодательства о цифровых финансовых активах, цифровой валюте Российской Федерации.

Ключевые слова: право, цифровые технологии, цифровые активы, криптовалюта, биржа, криптовалютная биржа, криптобиржа, инвестиции

LEGAL REGULATION OF THE CRYPTOCURRENCY EXCHANGE

Abstract. The article explores the concept and phenomenon of a cryptocurrency exchange. The main features of centralized and decentralized cryptocurrency exchanges are determined. The issue of the state and prospects of legal regulation of the crypto exchange is touched upon, taking into account the analysis of the legislation on digital financial assets and digital currency of the Russian Federation.

Keywords: law, digital technologies, digital assets, cryptocurrency, stock exchange, cryptocurrency exchange, crypto exchange, investments

В настоящее время набирает популярность тема цифровых финансовых активов [2, 3, 7, 8]. Цифровые финансовые активы, а также их использование находится в стадии активного развития во всем мире. Одним из преимуществ их использования является наличие системы специальной защиты – технологий блокчейн, а также особой криптографической схемы. Движение таких активов становится возможным благодаря существованию так называемых криптовалютных бирж. Однако в настоящее время отсутствуют общие тенденции и подходы к регулированию криптобирж.

Биржа в классическом понимании – это площадка, благодаря и посредством которой участники финансового рынка заключают сделки. Сделки могу

осуществляться посредством передачи и обмена деньгами, ценными бумагами, товарами или же контрактами.

Согласно статье 9 Федерального закона «Об организованных торгах» биржей является организатор торговли, имеющий лицензию биржи. Законодатель определяет организационно-правовую форму биржи. Так биржей может являться только акционерное общество [4].

Криптовалютная биржа представляет собой специальную площадку, на которой встречаются уже участники особенного финансового рынка – криптовалютного. В роли участников могут быть трейдеры, инвесторы, институциональные игроки, а также разработчики. В дальнейшем между такими участниками совершаются сделки. Иными словами, криптобиржа – это биржа, на которой можно покупать и продавать криптовалюту.

В настоящее время самой популярной криптобиржей является Binance. Также среди криптобирж можно выделить: Huobi, Bybit, MEXC, OKX, KuCoin, EXMO, Bynex, CoinEX, Phemex и другие.

Сегодня криптобиржи представляют собой некий транзит для обмена криптовалютой между различными блокчейн-сетями.

Одной из особенностей криптобиржи является тот факт, что в отличие от обычной биржи, в ней отсутствует брокерская «прослойка». То есть финансовые операции производятся напрямую без участия брокера.

Кроме этого, криптовалютные биржи, в отличие от обычных, работают всегда, непрерывно, без праздников и выходных.

Выделяют централизованные и децентрализованные биржи. Централизованные биржи – это биржи, которые имеют единый центр управления, а также такие биржи берут на себя кастодиальную ответственность за хранение закрытых ключей пользователей. Децентрализованные же биржи представляют собой электронную платформу, работающую на технологии распределенного реестра с помощью смарт-контрактов [5].

В настоящее время крупнейшей криптобиржей в мире является Binance. Ее посещают 61,5 млн активных пользователей в месяц, а объем торгов за сутки на ней превышает 6 млрд долларов [6]. В августе 2023 г. стало известно, что Binance ввела ограничения для россиян. Теперь клиенты из России не могут совершать операции с любой иностранной для россиян валютой через p2p-платформу в силу запрета, введенного крупнейшей криптобиржей. От операций с рублями также были отключены пользователи, которые прошли верификацию в качестве граждан других государств, отключила от операций с рублями [1].

На мой взгляд, центральной проблемой с точки зрения права в сфере криптовалютных бирж является неопределенность правового регулирования.

Правовой статус криптобиржи зависит от конкретного государства. В случае если в стране криптовалюта находится под запретом, то и криптобиржи являются нелегальными. Однако возникает вопрос: на основании чего в таком случае действуют биржи? В лояльных к криптовалюте государствах национальным законодательством определяются основные параметры их регулирования, основные требования, предъявляемые к биржам. Однако и в данной сфере распространено применение лицензий. Централизованные биржи могут действовать на основании

лицензии и применять специальные протоколы, такие как «Знай своего клиента» (так называется обязательная проверка персональных данных клиента, обычно со стороны финансового института). Данный протокол требует документального подтверждения личности, а также определяет процедуры по борьбе с отмыванием денежных средств.

В настоящее время в России действует Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Данный закон ввел новое понятие. Так появился новый участник российского криптовалютного рынка – оператор обмена цифровых финансовых активов. По сути, они являются криптобиржами, однако обмен может осуществляться только токенами, которые в свою очередь признаются по российскому законодательству цифровыми правами. При этом криптобиржи, которые торгуют криптовалютой, например известным биткоином, не подпадают под определение оператора обмена цифровых финансовых активов. Рассматриваемый закон допускает возможность организации на территории России площадки для обмена криптовалют, однако правовое регулирование криптовалютных бирж не является достаточным, требуются дальнейшая разработка и уточнение понятийного аппарата в сфере цифровых активов.

Список литературы

1. Binance ввела ограничения для россиян. Почему это произошло и что дальше // РБК. URL: https://www.rbc.ru/crypto/news/64ecab6e9a794716a68e6534?ysclid=lm7o4klpur127601479

2. Мурадян С. В. Цифровые активы: правовое регулирование и оценка рисков // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 123–151. DOI: 10.21202/jdtl.2023.5. EDN: RIZOKS

3. Перетолчин А. П. Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 752–774. DOI: 10.21202/jdtl.2023.33. EDN: HLHZBU

4. Федеральный закон Российской Федерации «Об организованных торгах» от 21.11.2011 № 325-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_121888/?ysclid=lm81fuabnt489900405

5. Централизованные и децентрализованные криптобиржи // Fin-plan. URL: https://fin-plan.org/blog/investitsii/tsentralizovannye-i-detsentralizovannye-kriptobirzhi/?ysclid=lm7p1dbi2v280305051

6. Что происходит с криптобиржей Binance // Тинькофф Журнал. URL: https://journal.tinkoff.ru/news/what-is-going-on-binance/?ysclid=lm7nu6n0gt753771571

7. Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 725–751. DOI: 10.21202/jdtl.2023.32. EDN: HGBQGL

8. Жарова А. К. Риски информационной безопасности и возможности правового регулирования криптовалюты в России // Информационное право. 2018. № 4. С. 11–16. EDN: YPNFET

К. П. Ермоченко,
магистрант,
Смоленский государственный университет

СМАРТ-КОНТРАКТ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. Актуальность проблемы правового регулирования смарт-контрактов обусловлена стремительным развитием информационных процессов, которые порождают новые способы и механизмы взаимодействия в обществе. Они нуждаются в обязательном правовом закреплении для возможного эффективного встраивания их в жизнь человека. Целью данного исследования является определение возможной степени включенности информационного феномена смарт-контракта в сферу правовых отношений. На основе анализа действующих законов делается вывод о правовой несостоятельности смарт-контракта в сравнении с традиционными бумажно-договорными конструкциями.

Ключевые слова: мир цифры и информации, цифровая трансформация, информационная система, смарт-контракт, блокчейн, правовые отношения

SMART CONTRACT IN THE CONTEXT OF DIGITAL TRANSFORMATION: PROBLEMS OF LEGAL REGULATION

Abstract. The urgency of this problem is due to the rapid information processes that generate new ways and mechanisms of interaction in society. They need mandatory legal consolidation for their possible effective integration into human life. The purpose of this study is to determine the possible degree of inclusion of the information phenomenon of a smart contract in the sphere of legal relations. In the article, based on the analysis of the current laws, a conclusion is made about the legal insolvency of a smart contract in comparison with traditional paper-contractual structures.

Keywords: the world of numbers and information, digital transformation, information system, smart contract, blockchain, legal relations

Развитие российского общества сегодня находится в условиях прямого действия цифровой трансформации, которая определяет вектор развития во всех сферах человеческой жизни. Человек оказывается включенным в этот процесс без права выхода из него, но он имеет возможность влиять на все проявления, которые свойственны сегодняшней цифровой реальности. Новый этап в развитии общества по пути цифровизации и цифровой трансформации связан с выработкой ею большого количества информационных агентов, механизмов и инструментов, являющихся технологиями информационно-коммуникационных процессов в российском обществе, позволяющих обеспечить наибольшую эффективность при социальном взаимодействии ее пользователей.

Последнее положение крайне важно, потому что современный российский человек все больше признает результаты цифровых изменений в трансформирующемся обществе и пытается постепенно встроить их в свою жизнь. Так, 16 июня

2023 г. в информационном агентстве ТАСС были опубликованы результаты опроса, согласно которому 94 % россиян считают, что развитие технологий будущего важно для человечества, а доверяют таким технологиям порядка 77 % опрошенных [5].

В связи с этим крайне важно выявить характер возникающих проблем при регулировании отношений между «агентом» «мира цифры и информации» и непосредственно, субъектом, на который распространяется его влияние, т. е человеком. Получается, что в фокусе этого регулирования «информационный зародыш» цифровой трансформации, продолжительность жизни которого напрямую коррелирует с социальной реакцией на него человека как субъекта распространения влияния первого, должен всегда находиться в зоне социальной реальности человека сегодня.

Это становится возможным при условии, что «цифровой агент» способен выработать новый продукт, или модернизировать старый, который однозначно должен для субъекта-человека быть понятным, простым и, самое важное, эффективным и способным облегчить его жизнедеятельность.

В информационных реалиях сегодняшнего дня в первую очередь правовая сфера призвана обеспечить эффективность таких отношений между «живым и цифровым» [2. С. 241]. Только она способна законодательно гармонизировать цифровые нововведения, встроив их в повседневную жизнь человека. Бесспорно, одной из таких «новелл мира цифры и информации» сегодня является смарт-контракт.

Целью данного исследования является определение возможной степени включенности информационного феномена смарт-контракта в сферу правовых отношений в современном российском обществе. Данной проблеме уже посвящены научные труды Н. В. Мамаевой [4], Д. В. Чуб [8] и др. Их научные статьи, которые определяют положение смарт-контракта в современном мире и его закрепление в правовой сфере, легли в основу нашего исследования.

Возможности смарт-контрактов. Сегодня смарт-контракт выступает той автономной децентрализованной информационной системой, которая способна обеспечить безопасное осуществление сделки. При этом для ее сторон она гарантирует проверку и контроль соблюдения всех условий, что позволяет минимизировать распространение возникающих спорных и конфликтных ситуаций межу участниками переговоров [4. С. 6].

По своей функциональной сути смарт-контракт можно сравнить со своего рода «необычным» торговым автоматом, где автономность и выполнение всех обязательств являются его «долгом». Помимо автономности, смарт-контракт полезен еще и тем, что не требует присутствия третьего лица, создавая доверительные отношения между участниками сделки, которые возможны благодаря самоисполняемости смарт-контракта и невозможности вмешиваться в его исполнение. При несоблюдении условий, которые предъявляет смарт-контракт, в автоматическом режиме может произойти наложение на нарушителя штрафа.

Следует сказать, что явление смарт-контракта возникло в далеком 1994 г. и своим возникновением обязано криптографу, ученому-информатику Нику Сабо, который нашел возможность с помощью совокупности математических

алгоритмов, примененных к специально установленному им компьютерному протоколу, таким «нетрадиционным» способом совершать сделки, обеспечив полный надзор за процессом их выполнения. Но для этого был необходим полный централизованный контроль, что на тот момент было невозможно. В связи с этим полностью реализовать идею данного способа совершения сделки стало возможно лишь в 2008 г. с использованием технологии блокчейн. Она представляет собой цифровую базу данных, записи в которой представлены в виде блоков и отражают все совершенные трансакции.

Многофункциональность смарт-контракта позволяет его широко применять при краудфандинге, с целью формирования нового продукта, для процедуры первичного размещения цифровых токенов (Initial Coin Offering), для контроля прав интеллектуальной собственности и т. д. Сегодня многие ведущие компании и организации, например, Eleks, HashCash, прибегают к применению смарт-контрактов в своей работе. В России тоже смарт-контракт постепенно встраивается в деятельность организаций. Так, с помощью блокчейн-платформы Hyperledger, в 2018 г. был заключен смарт-контракт между «Альфа-банком», российской авиакомпанией «S7 Airlines» и «Газпромнефть-Аэро». А уже во второй половине 2023 г., по заявлению депутата Государственной Думы Анатолия Аксакова, возможно появление первых смарт-контрактов с использованием цифрового рубля

Но полностью потенциал смарт-контракта не раскрыт. Они применяются не повсеместно, и это связано, в частности, с их слабым законодательным оформлением. Следует отметить, что большинство российских и зарубежных авторов считают необходимым законодательное регулирование в том объеме, который способен полностью обеспечить реализацию прав человека и их защиту. То есть, положение смарт-контракта в сфере права должно быть полностью подчинено интересам человека и никаким образом не нарушать их, соблюдая основополагающий принцип гуманизма и верховенства права.

Правовое регулирование смарт-контрактов. Насколько смарт-контракт сегодня эффективен в качестве гарантии исполнения обязательств, и не является ли он «орудием преступлений»? Этот вопрос остается открытым, несмотря на постоянно совершенствующееся законодательство. Обратимся к опыту разных стран в этом вопросе, которые вырабатывают свои собственные подходы к сущности механизма правового регулирования отношений, связанных с применением технологии блокчейна или основанных на нем [6].

Если говорить о российском законодательстве, которое должно определять порядок заключения смарт-контракта, регулировать отношения между участниками сделки и т. д., то считаем необходимым обратиться к Федеральному закону от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», который вносит некоторые изменения в отношении законодательного регулирования смарт-контрактов. Так, согласно статье 160 ГК РФ признается письменная форма при совершении сделки, если первая выполнена с помощью электронных или технических средств. Согласно этому закону, договор в письменной форме может быть заключен путем обмена электронными документами либо иными

данными (ст. 434 ГК РФ). Статья 309 ГК РФ была дополнена и теперь гласит, что исполнение обязательств при заключении контракта возможно с использованием информационных технологий, определенных условиями сделки [7]. Но, несмотря на значительные изменения в законодательстве, однозначно говорить, что они распространяются конкретно и на заключение смарт-контрактов нельзя. Так, не совсем ясная формулировка закона привела к отсутствию безоговорочного отнесения его положений к смарт-контрактам и породила ряд сложностей. Можно заметить, что для суда смарт-контракт считается непризнанным в правовом отношении до тех пор, пока для него не принято соответствующее законодательство, четко определяющее его положение в гражданском обороте. [2. С. 90].

Российское законодательство не имеет дословного понятия «смарт-контракт», возможно, это тоже является проблемой при правильном толковании новых законов, относящихся к данному виду и форме договоров. К слову, французское законодательство тоже не дает этого понятия, но и не препятствует его использованию [8. С. 155] при условии, что лицо имеет право заключить такой договор. Итальянское законодательство признает смарт-контракт как форму договора и как способ выполнения исполнения обязательств [3. С. 140]. Но есть государства, которые законодательно все же выделяют смарт-контракт от какой-либо другой формы договоров и прописывают его правовые основы.

Так, Декрет Президента Республики Беларусь № 8 от 21 декабря 2017 г. «О развитии цифровой экономики» определяет конкретные условия, которые будут способствовать внедрению в экономику страны технологии реестра блоков транзакций (блокчейн). Отдельно скажем, что Декрет поощряет участников отношений, связанных с применением современных технологий, предоставляя им преференции и льготы (п. 3), и готов оказать все необходимые меры, которые будут направлены на повышение правовой защищенности участников отношений, связанных с применением современных финансовых технологий [1].

Таким образом, смарт-контракт сегодня является актуальным явлением, которое имеет определенные перспективы. Но многочисленные трудности в его законодательном оформлении на сегодняшний день доказывают, что его можно справедливо считать не до конца состоявшимся «цифровым зародышем» информационного общества. Справедливо по отношению к устоявшимся бумажно-договорным конструкциям рассматривать смарт-контракт как его пока законодательно плохо закрепленную альтернативу, которая применима лишь в конкретных областях и имеет ряд преимуществ. Мы солидарны с мнением М. Мекки, который видел в смарт-контракте всего лишь компьютерную программу, модифицирующую конкретные условия (конструкция «если... то») [4]. До тех пор, пока смарт-контракт будет «спотыкаться» о законодательные неточности и незавершенные положения, прямо коррелирующие с его быстрым внедрением в жизнь, он останется в статусе не до конца реализованного проекта цифровой трансформации. Очень важно, чтобы российский опыт законодательного закрепления смарт-контрактов, ориентировался также и на правовые новеллы зарубежных стран в данном вопросе.

Список литературы

1. Декрет Президента Республики Беларусь № 8 от 21 декабря 2017 г. «О развитии цифровой экономики» // Национальный правовой интернет-портал Республики Беларусь. URL: https://economy.gov.by/uploads/files/sanacija-i-bankrotstvo/Dekret-Prezidenta-Respubliki-Belarus-ot-12.12.2017–8-O-razvitii-tsifrovoj-ekonomiki.pdf

2. Ермоченко К. П. Смарт-контракт сегодня: «умный договор» в системе правовых отношений или малоэффективный «цифровой зародыш» несамостоятельной договорной конструкции // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 томах, Казань, 23 сентября 2022 г. / под редакцией И. Р. Бегишева [и др.]. Т. 4. Казань: Познание, 2022. С. 240–244.

3. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–60.

4. Мамаева Н. В. Смарт контракты и их особенности // Наука и образование сегодня. 2018. № 2(25). С. 6–7.

5. Официальный сайт Всероссийского центра изучения общественного мнения (ВЦИОМ). URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/tekhnologii-budushchego

6. Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 725–751. DOI: 10.21202/jdtl.2023.32. EDN: HGBQGL

7. Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации». Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru

8. Чуб Д. В. Правовое регулирование смарт-контрактов во Франции // Актуальные проблемы российского права. 2019. № 8(105). С. 151–158.

А. В. Жилина,
магистрант,
Уральский государственный юридический
университет имени В. Ф. Яковлева

ВЫСОКОАВТОМАТИЗИРОВАННОЕ ТРАНСПОРТНОЕ СРЕДСТВО КАК ИСТОЧНИК ПОВЫШЕННОЙ ОПАСНОСТИ В РЕГУЛЯТИВНЫХ ПЕСОЧНИЦАХ

Аннотация. В статье рассматривается вопрос об отнесении высокоавтоматизированных транспортных средств (беспилотных автомобилей) в качестве источников повышенной опасности. Проанализированы различные доктринальные подходы к вопросу об отнесении искусственного интеллекта

и высокоавтоматизированного транспортного средства к источникам повышенной опасности. Рассмотрены варианты ответственности за вред, причиненный высокоавтоматизированным автомобилем в рамках экспериментального правового режима.

Ключевые слова: источник повышенной опасности, высокоавтоматизированное транспортное средство, беспилотный автомобиль, искусственный интеллект, безвиновная ответственность, экспериментальный правовой режим, регулятивная песочница

HIGHLY AUTOMATED VEHICLE AS A SOURCE OF INCREASED DANGER IN REGULATORY SANDBOXES

Abstract. The article considers the issue of attributing highly automated vehicles (unmanned vehicles) as sources of increased danger. Various doctrinal approaches to the question of attributing artificial intelligence and highly automated vehicles to sources of increased danger are analyzed. The variants of liability for damage caused by a highly automated car within the experimental legal regime are considered.

Keywords: source of increased danger, highly automated vehicle, unmanned vehicle artificial intelligence, innocent liability, experimental legal regime, regulatory sandbox

Роботы, автоматизированные транспортные средства, искусственный интеллект – явления, которые мало изучены с правовой точки зрения. Зачастую связано это в первую очередь с тем, что законодательство не изменяется так быстро по сравнению с развитием цифровых технологий. В связи с чем порой возникают ситуации, когда обществу, и в частности экономическому сегменту, необходимо применить определенные новшества цифровых технологий, но из-за отсутствия необходимого правового регулирования это невозможно сделать. Поскольку существует большая вероятность возникновения непредвиденных ситуаций, в результате которых может быть причинен вред жизни и здоровью граждан, имуществу других лиц. Поэтому рассмотрение вопроса гражданско-правовой ответственности при применении цифровых инноваций является одним из приоритетных в настоящее время.

До создания экспериментального правового режима разработчики, изобретатели, правообладатели в области цифровых инноваций для регулирования отношений между собой и всей отрасли в целом создали так называемое мягкое право, т. е. кодексы (практики) и стандарты, которые призваны устранять риски, связанные с бесконтрольным развитием цифровых технологий [12. С. 79]. С одной стороны, данные акты были признаны регуляторами общественных отношений в области цифровых инноваций. С другой – у данных актов отсутствуют одни из ключевых признаков нормативных правовых актов – это общеобязательность и привлечение к ответственности в случае нарушения со стороны государства. Для того чтобы все-таки не тормозить развитие цифровых инноваций, в ряде стран был разработан особый правовой режим, так называемые регулятивные или регуляторные

песочницы. Создание таких «регулятивных песочниц» направлено на недопущение стихийного развития цифровой экономики, осуществление контроля над новейшими технологиями, как «можно скорее их внедрение в гражданско-правовой оборот и придание им нормативно-правовое регулирование» [8. С. 137].

Первая регулятивная песочница появилась в Великобритании в 2016 г. В рамках данной модели ее участникам можно было проверить свои инновации в условиях, приближенных к реальным, но под надзором государственного органа. Позже такая модель регулирования успешно появилась в таких странах, как Австралия, США, Китай, Канада и др.

В России в 2020 г. был принят Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» (далее – Федеральный закон № 258-ФЗ) [1]. В рамках данного Федерального закона были установлены направления, в отношении которых может быть применим экспериментальный правовой режим. По состоянию на сентябрь 2023 г. такими направлениями являются:

– проектирование;

– производство и эксплуатация транспортных средств (далее – ТС), в том числе высокоавтоматизированных транспортных средств и беспилотных воздушных судов;

– строительство;

– медицинская деятельность.

В период действия экспериментального правового режима применяется специальное правового регулирование, которое распространяет свое действие в отношении всех участников регулятивной песочницы. Это в свою очередь способствует тому, что цифровые инновации обретают правовую определенность, которая благоприятно влияет на развитие экономики, социальной и духовной сферы, а именно способствует развитию промышленности, строительства, науки и образования, доступности медицины и возможности получения гражданами качественных продуктов, работ и услуг, обеспечению безопасности государства, при соблюдении баланса частных и публичных интересов [9. С. 48]. В частности, это можно проследить в отношении гражданско-правовой ответственности участников регулятивной песочницы. Согласно Федеральному закону № 258-ФЗ, в рамках проведения регулятивной песочницы установлено, что лицо, причинившее вред, будет нести ответственность в рамках гражданского законодательства. При этом программой экспериментального правового режима может предусматриваться требование к субъекту, участвующему в регулятивной песочнице, в виде страхования им своей гражданско-правовой ответственности [1].

Так, к примеру, в Программе экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств, утвержденной Постановлением Правительства РФ от 09.03.2022 № 309, установлено требование в отношении субъекта экспериментального правового режима по поводу страхования им риска ответственности по деликтным обязательствам на сумму 10 млн руб. в отношении каждого высокоавтоматизированного транспортного средства [4].

По состоянию на сентябрь 2023 г. в реестре экспериментальных правовых режимов в сфере цифровых инноваций наибольшую популярность имеет направление по созданию высокоавтоматизированных транспортных средств и беспилотных воздушных автомобилей [15]. Высокоавтоматизированное транспортное средство представляет собой обычное транспортное средство, которое оснащено автоматизированной системой вождения (искусственным интеллектом) и предназначено для перевозки пассажиров и грузов. При этом данное транспортное средство делится на два типа [3]. Высокоавтоматизированное транспортное средство I категории осуществляет свое движение при помощи искусственного интеллекта. Однако при этом в салоне беспилотного автомобиля на месте водителя должен находиться водитель-испытатель. Тогда как высокоавтоматизированное транспортное средство II категории осуществляет свое движение при удаленных маршрутизации и диспетчеризации со стороны оператора. При этом в салоне беспилотного автомобиля отсутствует водитель-испытатель. Учитывая, что данные транспортные средства оснащены автоматизированными системами вождения, управление такими транспортными средствами осуществляется посредством искусственного интеллекта.

В связи с чем возникает вопрос, можно ли считать высокоавтоматизированное транспортное средство источником повышенной опасности (далее – ИПО). Ведь само по себе использование транспортного средства указано в качестве ИПО в ст. 1079 ГК РФ. Однако управление транспортным средством, указанным в ст. 1079 ГК РФ, осуществляет непосредственно человек, тогда как ключевым моментом в последующих рассуждениях будет то, а может ли транспортное средство, находящее под управлением искусственного интеллекта, быть ИПО. Если да, то кто должен нести ответственности в рамках строгой ответственности по ст. 1079 ГК РФ в случае причинения вреда беспилотным транспортным средством.

Стоит учесть, что само отнесение искусственного интеллекта к источникам повышенной опасности является дискуссионным вопросом. В научных работах последних лет указывается, что искусственный интеллект обладает признаками ИПО, в силу чего отсутствует необходимость выделения специального деликта в российском законодательстве и в отношении беспилотных автомобилей [6. С. 8–9]. Однако в данных работах, как правило, отсутствует какая-либо конкретизация по поводу того, какие признаки берутся за основу в качестве признания искусственного интеллекта источником повышенной опасности.

Для начала необходимо разобраться, что понимается под искусственным интеллектом. Согласно Указу Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», под искусственным интеллектом следует понимать определенный комплекс технологических решений, который позволяет имитировать когнитивные функции человека (в том числе самообучение и решение задач без заранее установленного алгоритма действий) и получать при выполнении конкретных задач результаты, которые как минимум сопоставимы с результатами интеллектуальной деятельности человека [2].

Ю. С. Харитонова, В. С. Савина, Ф. Паньини выделяют четыре наиболее распространенных подхода в отношении ответственности искусственного интеллекта [10. С. 695]:

– действия систем искусственного интеллекта рассматривать аналогично как обстоятельства непреодолимой силы и, следовательно, освободить какое-либо лицо от ответственности в результате причинения вреда действиями искусственного интеллекта;

– создание определенных источников, за счет которых будет компенсироваться причиненный вред, и при этом отсутствие ответственности какого-либо лица;

– наступление ответственности при наличии виновных действий лиц. Такими лицами, к примеру, могут быть разработчик, изготовитель, оператор беспилотного автомобиля и т. д.;

– рассматривать действия искусственного интеллекта как ИПО и, следовательно, рассматривать причинение вреда в рамках безвиновной ответственности;

– наделение системы искусственного интеллекта правосубъектностью. В результате чего искусственный интеллект самостоятельно будет нести ответственность за причиненный им вред.

При этом указанные авторы считают, что систему искусственного интеллекта стоит рассматривать как источник повышенной опасности и рассматривать причинение вреда в рамках безвиновной ответственности [10. С. 703].

На данный момент можно выделить следующие признаки искусственного интеллекта как ИПО – это высокая автономность и высокая вероятность причинения вреда. Высокая автономность подразумевает под собой то, что за искусственным интеллектом невозможно до конца осуществлять контроль. Ведь порой даже сами разработчики не могут предугадать, как поведут себя в том или ином случае робот, транспортное средство под управлением искусственного интеллекта. В связи с чем и имеется высокая вероятность причинения вреда.

Учитывая этот факт, экспертная группа по вопросам ответственности и новым технологиям в своем отчете для Европейской комиссии предлагает новый подход в определении ответственности в отношении высокоавтоматизированных транспортных средств. Так, при использовании высокоавтоматизированного транспортного средства появляется новый субъект – оператор ТС, под которым понимается лицо, осуществляющее контроль за транспортным средством и получающее выгоду от использования ТС. Однако такой оператор может выполнять разные функции. К примеру, frontend-оператор активирует транспортное средство и определяет место назначения. В свою очередь, изготовитель или иное лицо (backend-оператор) контролирует транспортное средство на постоянной основе. В связи с чем, по мнению экспертов, строгая ответственность будет лежать на том операторе, кто в большей степени осуществляет контроль за транспортным средством [14. P. 41].

На этот отчет критическое замечание в своей статье сделали Андреа Бертолини и Франческа Епископо. Данные авторы подметили, что введение новых ответственных лиц в случае наступления деликтной ответственности за вред, причиненный высокоавтоматизированными транспортными средствами, не упрощает, а, наоборот,

еще более нагружает нормативную базу. Впоследствии это влечет за собой множество потенциальных ответчиков, сложность доказывания и увеличение судебных издержек. Следовательно, основной целью любой правовой реформы в области деликтной ответственности высокоавтоматизированных транспортных средств должно быть ее упрощение путем определения одного субъекта ответственности, который впоследствии и будет страховать свою ответственность, либо разработка новой правовой конструкции такой ответственности. В связи с чем авторы предлагают ввести солидарную ответственность производителя высокоавтоматизированного транспортного средства и его владельца [13].

В Германии, несмотря на логичность доводов экспертной группы, также не поддерживают идею реформирования института строгой ответственности владельцев транспортных средств. В силу чего ответственность, по мнению ряда юристов Германии, за вред причиненного высокоавтоматизированного транспортного средства несет его владелец. Так как безвиновная ответственность владельца транспортного средства – цена за использование ИПО, в частности за использование высокоавтоматизированного транспортного средства [11. С. 198].

Учитывая нормативное регулирование в странах Европейского союза, старший эксперт направления «Правовое развитие» Центра стратегических разработок Д. В. Федоров предложил два варианта привлечения лица к строгой ответственности при использовании беспилотного автомобиля. Это владелец беспилотного автомобиля либо изготовитель беспилотного автомобиля. В случае с владельцем, как отмечает Д. В. Федоров, не нужно будет вносить какие-либо изменения в действующее законодательство, так как это будет регулироваться в рамках ст. 1079 ГК РФ. В случае же с изготовителем необходимо будет внести изменения в законодательство, а также понимать, что изготовитель будет отражать в экономическом плане свои риски в конечной стоимости продукции [11. С. 207].

А. В. Незнамов указал, что, несмотря на то, что проблема ответственности искусственного интеллекта является дискуссионной, в настоящее время кардинальное изменение института юридической ответственности не требуется, кроме, например, использования технологий автоматического управления. В связи с чем, по мнению автора, представляется целесообразным направить усилия на развитие института безвиновной ответственности, законодательства о страховании, создание специальных резервных фондов [7. С. 177].

До принятия Федерального закона № 258-ФЗ Правительство РФ приняло распоряжение № 2129-р от 19.08.2020 «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 года», где указано, что при развитии системы искусственного интеллекта кардинальных изменений в институт гражданско-правовой ответственности не предполагалось. Проблему использования систем искусственного интеллекта предлагалось решить путем постепенной доработки института юридической ответственности [5]. Учитывая наличие определенных признаков искусственного интеллекта как ИПО, предполагается, что под доработками подразумевалось внесение изменений в механизмы безвиновной ответственности и способов возмещения причиненного вреда.

Аналогичная позиция, как ранее было указано, отражена и в Федеральном законе № 258-ФЗ. В данном федеральном законе закреплено, что в рамках регулятивной песочницы за причиненный вред лицо, причинившее вред, будет отвечать в рамках гражданского законодательства [1]. Таким образом, каких-либо новых конструкций гражданско-правовой ответственности в указанном федеральном законе не было закреплено. Также стоит учесть, что какие-либо изменения в обязательства вследствие причинения вреда также не были внесены. Следовательно, по логике законодателя регулирование обязательства вследствие причинения вреда в результате использования беспилотного автомобиля будет осуществляться в рамках имеющегося законодательства о гражданско-правовой ответственности.

В результате можно сделать вывод о том, что институт юридической ответственности в регулятивной песочнице не претерпел каких-либо кардинальных изменений. Таким образом, управление транспортным средством при помощи искусственного интеллекта имеет признаки ИПО, так как данная деятельность не может полностью контролироваться человеком. Если при причинении вреда в регулятивной песочнице высокоавтоматизированное транспортное средство будет признано ИПО, то, согласно ст. 1079 ГК РФ, гражданско-правовую ответственность будет нести владелец высокоавтоматизированного транспортного средства. При этом не стоит забывать, что если привлекать владельца высокоавтоматизированного транспортного средства к юридической ответственности, то в случае признания вины изготовителя или иного лица в причинении вреда возможно применение регрессного требования в рамках ст. 1081 ГК РФ. Учитывая волю законодателя не вносить кардинальных изменений в институт гражданско-правовой ответственности и способствовать развитию информационных технологий, может быть, стоит внести изменения в возможности применения регрессного требования. А именно указать лиц, в отношении которых оно может быть применено. Ведь не стоит забывать, что ответственность владельца транспортного средства – это цена за то, что он использует ИПО. Либо же направить усилия на развитие страхового законодательства, что, как можно заметить, на данный момент и происходит.

При этом в рамках проведения экспериментального правового режима Правительство Российской Федерации порой самостоятельно определяет случаи, когда то или иное лицо в случае причинения вреда будет привлечено к гражданско-правовой ответственности. Так, в п. 31 Постановления Правительства РФ от 29.12.2022 № 2495 установлено, что оператор будет нести ответственность за причинение вреда жизни и здоровью участников ДТП с участием беспилотного автомобиля II категории только в том случае, если ДТП произошло в результате недостатков при осуществлении маршрутизации и диспетчеризации беспилотного автомобиля. К примеру, это может быть тогда, когда оператор построил маршрут движения транспортного движения через пешеходную зону. Если же причинение вреда беспилотным автомобилем II категории произошло в результате неисправного технического состояния указанного автомобиля, то ответственность за причинение вреда будет нести единоличный исполнительный орган субъекта экспериментального правового режима и (или) лица, ответственные за техническое состояние беспилотного автомобиля [3].

Таким образом, можно сделать вывод и о том, что высокоавтоматизированное транспортное средство имеет признаки источника повышенной опасности. Учитывая этот факт, законодатель решил не производить кардинальных изменений в регулировании института юридической ответственности в регулятивной песочнице. Следовательно, если высокоавтоматизированное транспортное средство будет признано источником повышенной опасности, то ответственность за причиненный вред будет нести владелец этого транспортного средства. Однако если причинение вреда беспилотным автомобилем II категории произошло в результате недостатков при осуществлении маршрутизации и диспетчеризации, то ответственность за вред будет нести оператор. К примеру, это может быть тогда, когда оператор построил маршрут движения транспортного средства через пешеходную зону. Если же причинение вреда беспилотным автомобилем II категории произошло в результате неисправного технического состояния указанного автомобиля, то ответственность за причинение вреда будет нести единоличный исполнительный орган субъекта экспериментального правового режима или иные лица, ответственные за техническое состояние беспилотного автомобиля.

Список литературы

1. Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации: Федеральный закон от 31.07.2020 № 258-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=389188&dst=1000000001&cacheid=A79F4EC45748CD4C47B1E93FEB4FA08D&mode=splus&rnd=6555B9362F641139D949835A2651350B#Ag1ZApTuuglo0s3u3

2. О развитии искусственного интеллекта в Российской Федерации: Указ Президента РФ от 10.10.2019 № 490 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=335184&cacheid=CA18064166780780539B7288A9EE1689&mode=splus&rnd=ekx9A#pmzZApTfo6aRvsy1

3. Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации: Постановление Правительства РФ от 29.12.2022 № 2495 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=446430&cacheid=29680FA9ACA3F86157A376F876C56D26&mode=splus&rnd=ekx9A#aBKaApTUc8u6XjrH1

4. Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по эксплуатации высокоавтоматизированных транспортных средств: Постановление Правительства Российской Федерации от 09.03.2022 № 309 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=411811&cacheid=58C0CD8CA6D4413F08B59F9FD55461DA&mode=splus&rnd=ekx9A#bGCbApTGeOXXLEfK1

5. Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года: Распоряжение Правительства РФ от 19.08.2020 № 2129-р // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=411811&cacheid=58C0CD8CA6D4413F08B59F9FD55461DA&mode=splus&rnd=ekx9A#bGCbApTGeOXXLEfK1

6. Антонов А. А. Беспилотные транспортные средства как источники повышенной опасности // Транспортное право. 2021. № 4. С. 7–10. DOI: 10.18572/1812-3937-2021-4-7-10. EDN: DDBJLG.

7. Незнамов А. В. О концепции регулирования технологий искусственного интеллекта и робототехники в России // Закон. 2020. № 1. С. 171–185.

8. Носкова Ю. Б. Роль экспериментальных правовых режимов в сфере развития цифровых инноваций в Российской Федерации и республике Беларусь: соотношение социально-экономических, правовых и государственных интересов // Современное государственное управление: образование, наука, практика: сборник статей Международной научно-практической конференции, Минск, 26 января 2021 года. Минск: Академия управления при Президенте Республики Беларусь, 2021. С. 137-139. EDN: VXKSCB.

9. Носкова Ю. Б., Лупашко Н. М. Экспериментальные правовые режимы в сфере цифровых инноваций как способ интеграции национальной экономики российской федерации в мировое экономическое пространство // Herald of the Euro-Asian Law Congress. 2020. № 1. С. 43-50. DOI: 10.34076/2619-0672-2020-4-1-43-50. EDN: WJJYCE.

10. Харитонова Ю. С., Савина В. С. , Паньини Ф. Гражданско-правовая ответственность при разработке и применении систем искусственного интеллекта и робототехники: основные подходы // Вестник Пермского университета. Юридические науки. 2022. № 58. С. 683-708. DOI: 10.17072/1995-4190-2022-58-683-708. EDN: PPVMZR.

11. Федоров Д. В. Безвиновная ответственность за причинение вреда при эксплуатации высокоавтоматизированного и полностью автоматизированного транспортного средства как источника повышенной опасности // Вестник гражданского права. 2020. № 6. С. 191–211.

12. Шахназаров Б. А. Применение технологий искусственного интеллекта при создании вакцин и иных объектов интеллектуальной собственности (правовые аспекты) // Актуальные проблемы российского права. 2020. №7 (116).

13. A. Bertolini, F. Episcopo The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment // European Journal of Risk Regulation. 2021. Pp. 645–659. URL: https://www.researchgate.net/publication/353284336_The_Expert_Group's_Report_on_Liability_for_Artificial_Intelligence_and_Other_Emerging_Digital_Technologies_a_critical_assessment.

14. Expert Group on Liability and New Technologies. Liability for Artificial Intelligence and Other Emerging Digital Technologies. European Union, 2019. 70 p. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf

15. Реестр экспериментальных правовых режимов в сфере цифровых инноваций // Министерство экономического развития Российской Федерации. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/eksperimentalnye_pravovye_rezhimy/reestr_eksperimentalnyh_pravovyh_rezhimov

16. Как устроен беспилотный автомобиль? // канал компании «Яндекс» на видео-хостинге Youtube. URL: https://youtu.be/izoPwpPSGRc?si=HURqyNRf79TR1jqP

17. Дмитрий Полищук – про беспилотное такси, эволюцию роверов-курьеров и города будущего | YaC 2021 // канал компании «Яндекс» на видео-хостинге Youtube. URL: https://www.youtube.com/watch?v=wFWy8Lw-rL8

В. Э. Жуков,
студент,
Санкт-Петербургский государственный университет
А. А. Щукина,
студент,
Северо-Западный филиал
Российского государственного университета правосудия

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЛУТБОКСОВ И ИХ СООТНОШЕНИЕ С АЗАРТНЫМИ ИГРАМИ

Аннотация. Исследование направлено на изучение, сравнение и анализ многообразных взглядов на проблемы, которые возникают при постановке вопросов о необходимости отнесения «лутбоксов» к категории азартных игр. Актуальность выбранной темы обусловлена тем, что многие авторы, рассматривая смежные проблемы правового регулирования «лутбокосов» и предлагая пути их решения, акцентируют внимание на цели защиты нравственности, прав и законных интересов граждан. Тем самым они ограничиваются лишь публичными интересами. Бесспорно, такой выбор не представляется ошибочным, однако, руководствуясь тем, что одним из ключевых свойств общественных отношений, регулируемых нормами права, является конфликтный интерес, невозможно обойти стороной и факт того, что при определении сбалансированного выхода из сложившихся проблем нужно учитывать также интересы игровых компаний и потребителей контента. Соответственно, целью настоящего исследования является поиск наиболее объективных вариантов решения ряда актуальных проблем, связанных с отнесением «лутбоксов» к категории азартных игр. Также нами была разработана собственная классификация лутбоксов, отражающая их специфику и многообразие.

Ключевые слова: право, цифровые технологии, информационное право, азартные игры, законодательство об азартных играх, игровая индустрия, лутбоксы

PROBLEMS OF LEGAL REGULATION OF LOOTBOXES AND THEIR RELATION TO GAMBLING

Abstract. The article is aimed at studying, comparing and analyzing diverse views on the problems that arise when raising questions about the need to classify "loot boxes" as gambling. The relevance of the chosen topic is due to the fact that many authors, considering the related problems of legal regulation of "loot boxes" and suggesting ways to solve them, place emphasis on the protection of morality, rights and legitimate interests of citizens. Thus, they are guided only by public interests. Undoubtedly, such a choice does not seem to be erroneous, however, considering that one of the key properties of public relations regulated by the norms of law is a conflicting interest, it is impossible to ignore the fact that when determining a balanced way out of the existing problems, it is also necessary to take into account the interests of gaming companies and content consumers. Accordingly, the purpose of this study is to search for the most objective solutions to a number of urgent problems related to the classification of "loot boxes" as gambling. We have also developed our own classification of loot boxes, reflecting their specificity and diversity.

Keywords: law, digital technologies, information law, gambling, gambling legislation, gaming industry, loot boxes

Понятие и классификация лутбоксов. Термин «лутбокс» является транслитерацией английского слова «lootbox» (loot – «добыча», box – «коробка»). Следовательно, для описания их сути можно провести аналогию, например, с новогодним подарком. Благодаря креативности игровых индустрий, система «коробок с лутом» оформляется в самые разнообразные вариации: «кейсы» (от англ. cases), «паки» (от англ. pack), «сферы» (от англ. spheres) и т. д. С целью терминологического единообразия авторы предлагают именовать подобные разновидности общими обозначениями: «лутбоксы», «контейнеры» и пр., так как все иные названия существенным образом обосновываются косметической составляющей. Однако необходимо указать, что механики получения, открытия «сундучков», а также форма наград, содержащихся в них, не являются однородными и влияют на контекст понимания лутбоксов в проблематике регулирования сферы азартных игр (см. далее).

Для целей формирования у читателей более детального представления о характере «лутбоксов» ниже представлена их примерная классификация:

По источнику получения: с помощью микротранзакций (микротранзакцией принято считать получение какого-либо внутреннего игрового контента за реальную валюту, как правило, за небольшую фиксированную сумму) [1. С. 146] / за игровые ценности и прочие геймплейные (от англ. game – «игра», play – «играть») механики / по совокупности возможностей (и/или).

Однако суть микротранзакций не следует понимать буквально. Встречаются случаи, когда один контейнер может стоить значительную сумму. Например, на момент 26.08.2023 цена Raritiesof the Benefactor 2020 («сокровищница» в популярной MOBA Dota 2) на торговой площадке Steam составляет ≈ 63 тыс. рублей. Данный лутбокс

был взят в качестве примера, на самом деле на рынке можно обнаружить и более дорогостоящие экземпляры. Такая высокая ценность обусловлена чрезвычайной редкостью некоторых из них. Нельзя напрямую утверждать, что сами игровые компании устанавливают столь значительные цены, ведь чаще всего «раритетные лутбоксы» продаются самими же пользователями на внутренних игровых рынках или игровой платформе. Подобные «сундучки» с определенной условностью можно считать sui generis (лат. особого рода), они являются исключением из общего правила.

По особенностям «наград»: предметы, влияющие на игровой процесс и (или) имеющие исключительно косметический эффект.

По дальнейшей реализации «наград»: использование лишь по назначению без предусмотренной механики передачи предметов другим игрокам (напр. ношение на персонаже); с возможностью такой передачи (за игровую валюту или иные внутренние игровые ценности) и (или) реальные денежные средства (с системой прямого вывода/через неофициальные «схемы»).

Заметим, что вышеназванное деление является условным, ведь предприимчивые игроки в обход правилам, установленным лицензионным соглашением, могут продавать аккаунты, внутреннюю валюту игры (которую нельзя вывести напрямую) и пр. Оно лишь характеризует разновидность прямых возможностей некоторых механик игровых продуктов.

По необходимости приобретения дополнительных предметов для открытия существуют лутбоксы, которые пользователь может открыть после самого факта приобретения или получения контейнера иным способом, либо же только после покупки так называемых ключей, которые могут иметь самые различные вариации.

Так, в игре Counter-Strike: Global Offensive для открытия контейнера с косметическими скинами на оружие (англ. skin – «кожа, оболочка»), помимо получения самого «ящика» за реальную валюту или в ходе игрового процесса, требуется купить ключ, который данный лутбокс открывает (на момент 26.08.2023 цена ключа за 1 шт. составляет ≈ 240 рублей).

По степени цифровизации: виртуальные и реальные.

В настоящее время доминирует первая категория. Но можно привести пример и второй. Ныне популярная карточная игра Hearthstone (Blizzard Entertainment) раньше существовала в виде настольной коллекционной карточной игры World of Warcraft Trading Card Game. В каждой упаковке («бустере» – от англ. booster pack) содержалось 15 карт. В комплекте могла находиться карта с кодом, ввод в игре которого позволял игрокам получить in-game ценности в многопользовательской онлайн-игре «World of Warcraft». Степень редкости самых ценных «карт с наградой» составляла примерно 1 шт. на несколько сотен упаковок, а цена кода могла варьироваться в диапазоне 200–5000$ на торговых интернет-площадках (продажу данных кодов можно встретить и в настоящее время, более того, стоимость некоторых из них растет каждый год в кратном размере). Этот пример показателен тем, что концепцию лутбоксов можно встретить не только непосредственно в игре.

Авторы-коллеги, занимавшиеся исследованием смежной проблематики, предлагают многообразные вариации понятия лутбоксов. Например, Станислав Махортов считает, что «в мировой практике под "лутбоксом" принято понимать виртуальный предмет в компьютерных играх, при использовании которого игрок получает случайные виртуальные предметы различной ценности и назначения» [2]. А. А. Варчук в своей статье сформулировал аналогичное определение [3. С. 263]. Схожие толкования можно обнаружить и в иных работах.

Полагаем, что указанные дефиниции являются слишком широкими, не позволяющими установить, какие именно игровые предметы следует квалифицировать как лутбоксы. Случайные ценные предметы могут получаться пользователями и при выполнении заданий, «уничтожении» противника (после активации «упавшей» с него добычи), использования исключительно in-game механики. Возникает вопрос, а как тогда различать сугубо игровой контент от системы монетизации в виде продажи «коробок с наградой»? Не рискуем ли мы при подобном понимании столкнуться с проблемой, что любая игра (как продукт) будет пониматься в качестве азартной, вредоносной для общественной нравственности?

Именно поэтому предложим собственное определение. Так, лутбокс (как предполагаемый предмет регулирования законодательством об азартных играх) – это самостоятельный источник получения случайных внутриигровых наград, приобретаемый и (или) используемый за счет микротранзакций и (или) игровой валюты, покупка которой за реальные денежные средства прямо предусмотрена политикой компании («донатная валюта»).

Отметим, что под «донатной валютой» в настоящей работе понимается не только внутриигровая валюта, приобретаемая исключительно путем микротранзакций. Под указанный тип также подходит валюта, которую можно приобрести как с помощью игровых механик, так и путем вложения реальных средств.

Признак самостоятельности характеризует лутбокс-систему как автономную от остального игрового процесса механику. Случайность подчеркивает, что использование такой системы основано на риске. Пользователь, осознавая данный факт, тратит свои собственные средства на шанс получить дорогой или желаемый предмет (персонаж, способность и пр.).

Отдельно следует разъяснить выбор способа получения и (или) использования. Исследование проблемных вопросов в плоскости правового регулирования лутбоксов позволяет сделать вывод, что самым популярным является вопрос именно о возможности отнесения «коробок с наградами» к категории азартных игр. Вряд ли можно согласиться с логикой, согласно которой «если игра стоит денег и позволяет пользователю случайным образом получить награду с босса, то все это характеризуется понятием "лутбокса" и является азартной игрой». Или, например, что раз игрок может приобрести игровую валюту на сторонней бирже (хотя политика компании-разработчика не позволяет или прямо запрещает это) и открыть за счет ее использования «сундук», хоть даже и предусматривающий получение случайной награды, то и такой in-game-механизм является «лутбокс-системой», которую необходимо регулировать законодательством о деятельности, связанной с проведением азартных игр. При таком ходе рассуждений мы можем столкнуться

с ситуацией, что недобросовестность игроков в совокупности с совершенно стандартным элементом случайности в играх (особенно в MMORPG) будет создавать риск того, что игра будет заблокирована.

Вышесказанное подчеркивает, что лутбокс-система имеет множество форм своего проявления, однако действующая терминология, предложенная коллегами-исследователями, является слишком широкой, что создает значительный риск признания азартными, «зловредными» практически всех продуктов игровой индустрии (следовательно, их ограничения или полного запрета), так как почти в каждой из них встречаются элементы случайности и неожиданности. Полагаем, что для целей разрешения указанной проблемы в качестве лутбоксов следует понимать только такой предмет (в шир. смысле), который можно приобрести и (или) использовать (открыть) только с помощью микротранзакций и (или) внутриигровой валюты, покупка которой за реальные денежные средства прямо предусмотрена политикой компании. Ведь именно в таком случае мы можем проследить субъективную и объективную связь между созданием разработчиком игрового продукта определенного механизма случайности и желанием заработать на этом (монетизировать).

Схожие мнения можно встретить в некоторых отечественных научных работах. И. А. Родионов указывает, что «лутбоксы – это предметы всегда доступные за плату» [4. С. 311]. Д. Е. Дроздов, Е. В. Генералова, В. В. Николаев аналогично пришли к выводу, что «Так же, как и казино, “лутбоксы” основываются на денежных вложениях – микротранзакциях» [5. С. 478].

Таким образом, на наш взгляд, чтобы достичь единообразия в понимании предмета, целесообразно руководствоваться предложенной в настоящей работе терминологией.

Проблемы соотношения лутбоксов и азартных игр и тенденции их правового регулирования. В Российской Федерации основополагающим нормативно-правовым актом сферы регламентации деятельности по организации и проведению азартных игр выступает Федеральный закон от 29.12.2006 № 244-ФЗ [6]. Статья 4 указанного Закона содержит основные понятия: так, согласно п. 1 ст. 4, азартная игра – это «основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным организатором азартной игры».

Иные интересующие нас дефиниции:

ставка – «денежные средства, передаваемые участником азартной игры организатору азартной игры в наличной форме или с использованием платежных карт (за исключением денежных средств, передаваемых организатору азартных игр в соответствии с пунктом 3.1 настоящей статьи) и служащие условием участия в азартной игре в соответствии с правилами, установленными организатором азартной игры» (п. 3 ст. 4);

выигрыш – «денежные средства или иное имущество, в том числе имущественные права, подлежащие выплате или передаче участнику азартной игры при

наступлении результата азартной игры, предусмотренного правилами, установленными организатором азартной игры» (п. 4 ст. 4);

игорная зона – «часть территории Российской Федерации, которая предназначена для осуществления деятельности по организации и проведению азартных игр и границы которой установлены в соответствии с настоящим Федеральным законом» (п. 7 ст. 4);

участник азартной игры – «физическое лицо, достигшее возраста восемнадцати лет, принимающее участие в азартной игре и заключающее основанное на риске соглашение о выигрыше с организатором азартной игры или другим участником азартной игры» (п. 10 ст. 4).

Как подчеркивает С. Махортов, в судебной практике выражен подход, согласно которому игры в сети Интернет относятся к азартным. Такой выбор обусловлен следующими критериями: наличием соглашения о выигрыше и внесением денежных средств участником такой игры [2]. В частности, Чертановский районный суд в своем решении по делу № 02-4488/2018 отмечает, что для правоотношений между организатором (владельцем) компьютерной онлайн-игры (юридическим лицом) и непосредственно пользователем этой игры (физическим лицом) специальным будет законодательство о проведении игр, регулируемое соответственно главой 58 ГК РФ [7].

Однако нельзя согласиться, что вышеназванные критерии полноценно применимы непосредственно к лутбоксам. Скажем, что следует понимать под «внесением денежных средств»? Если занимать позицию, что под таким внесением понимается приобретение самих «контейнеров, сундуков и пр.» и (или) их использование за счет реальных денежных средств и (или) «донатной валюты» (см. предложенное определение лутбоксов выше), тогда указанный вопрос разрешается.

А. О. Бурханова и М. Э. Червяков руководствуются схожей логикой и соотносят понятия «ставка» и «донат», утверждая, что «донат, являясь реальными денежными средствами, выступает условием участия игрока в процессе, который в итоге приносит определенный выигрыш, получаемый рандомным (случайным) путем» [8. С. 186]. Во-вторых, лутбоксы интегрированы преимущественно в виртуальную сферу видеоигр. Как было сказано ранее, с учетом игровой специфики характер наград может иметь самый разнообразный характер. Полагаем, что понятие выигрыша из ФЗ № 244-ФЗ едва ли применимо к ним, потому что Закон связывает выигрыш исключительно с «денежными средствами или иным имуществом, в том числе с имущественными правами». Вопросы правовой квалификации «игрового имущества», всевозможных усилений и эффектов, в настоящее время остаются неразрешенными, что препятствует их отождествлению с классическими объектами гражданского права. Однако А. О. Бурханова и М. Э. Червяков не обратили внимание на данный факт, указав, что «система лутбоксинга полностью приравнена к азартным играм, так как имеет все соответствующие атрибуты» [8. С. 186]. Авторы пришли к выводу, что указанную систему необходимо либо регламентировать как онлайн-казино, либо запретить [8. С. 186].

Л. Ю. Киселева также полагает, что лутбоксы полностью подпадают под признаки азартных игр (по ФЗ № 244-ФЗ). Более того, она сделала акцент на

проблеме квалификации «игрового имущества». Автор статьи предположила, что выходом из нее будет признание виртуального имущества объектами гражданских прав [9. С. 39]. Впрочем, невозможно согласиться, что выбранный путь является простым решением, ведь вопрос о возможности такого признания является еще более глубоким и дискуссионным. Далее Лидия Юрьевна выдвинула тезис, что необходимо создать особую игорную зону (по ФЗ № 244-ФЗ) – «цифровое виртуальное пространство внутри видеоигр», чтобы «игра являлась игорным заведением» [9. С. 39]. Авторы настоящей работы возражают против данного предложения. Сами по себе продукты игровой индустрии не имеют ничего общего с азартными играми, поскольку основная цель их разработки заключается не в организации «цифрового казино», а в реализации идеи создания «уникальной возможности перенестись в мир фантазий» [10. С. 10]. Однако, несмотря на то, что лутбоксы и подобные им формы монетизации крайне популярны, они присутствуют далеко не во всех играх. Таким образом, отождествление компьютерных игр с азартными играми повлечет огромный массив несоразмерных и необоснованных негативных последствий для потребителей целого направления современной культуры – видеоигр.

Л. А. Брушкова и И. А. Владимиров делают вывод, что «в настоящее время рынок лутбоксов никак не регулируется». Исследователи рассуждают о возможном создании межведомственной комиссии, которая устанавливала бы возрастной ценз на видеоигры, следила бы за его соблюдением [11. С. 183]. Отметим, что вряд ли цензы могут гарантированно разграничить целевую аудиторию продукта. Кроме того, совершеннолетние игроки также являются активными пользователями лутбоксов. Считаем, что необходимо рассматривать проблему комплексно, не сосредотачиваясь исключительно на возрастном цензе.

Некоторые коллеги в качестве основного аргумента за необходимость ограничения свободной реализации лутбоксов обращают особое внимание на зависимость, вызываемую чрезмерным азартом. Действительно, существует даже болезнь, именуемая лудоманией (лат. ludo – «играю», + древ. греч. μανία – «безумие»). С правовой точки зрения под такого рода пристрастием к азартным играм следует понимать психологическую зависимость, которая, кроме труднопреодолимого влечения к игре характеризуется также расстройствами поведения, психического здоровья и самочувствия. При этом такого рода зависимость проявляется в патологическом влечении к азартным играм, потере игрового контроля, а также в продолжительном участии в азартных играх вопреки наступлению неблагоприятных последствий для материального благосостояния членов семьи человека [12].

Ю. В. Мамедов (со ссылкой на исследования) делает вывод, что указанное расстройство может развиваться и от лутбоксов, что, по мнению автора, представляет наибольшую опасность именно для несовершеннолетних (в силу их несформировавшейся психики). В связи с этой проблемой Ю. В. Мамедов предлагает два решения: полный запрет лутбоксов (в работе не пояснено, каким образом он должен осуществляться) или ограничение использования с введением возрастного ценза (см. ранее) и лицензий для игровых компаний на проведение «азартных игр» [13. С. 472].

Интересное мнение в отношении предмета исследования высказывает Николай Андреев: с его точки зрения, лутбоксы в Российской Федерации должны приравниваться к азартным играм только в случае наличия возможности «прямого вывода денежных средств на счета игроков» [14]. Позиция коллеги коррелирует с логикой поиска баланса, но против него также можно найти контрдоводы. Во-первых, ничем не отличается от «прямого вывода» сюжет, когда игровые компании, зная, что существуют рынки неофициального сбыта игровых предметов и т. п., не предпринимают мер по борьбе с этим. Во-вторых, как уже было упомянуто, мотивация у игроков бывает различная. Для кого-то быть «уважаемым в гильдии человеком из-за редкого меча» может быть важнее, чем иметь доступ к конвертации такого меча в реальную валюту.

Подводя итоги, надо сказать, что большинство отечественных исследователей уверены, что «лутбоксы» должны быть признаны азартными играми. Следовательно, необходимо либо запретить их, либо ограничить.

Зарубежный опыт исследования и правового регулирования лутбоксов. Для начала хотелось бы отметить, что контексте понимания сюжетов, связанных с регулированием азартных игр, нужно иметь в виду следующее. Как верно отметил В. В. Архипов в авторском курсе «Индустрия компьютерных игр: ключевые правовые проблемы», проанализировав признаки азартных игр в различных юрисдикциях, в некоторых правопорядках ключевым квалифицирующим элементом является именно случайность. Однако в российском правопорядке признак случайности в понятии азартной игры отсутствует: согласно понятийному аппарату по ФЗ № 244-ФЗ (см. выше), есть лишь элемент риска. Как было отмечено в вышеназванном курсе, в контексте азартных игр риск воспринимается отечественной судебной практикой как риск случайности утраты объекта имущественных прав (гражданско-правового характера) [15]. Следовательно, исходя из буквального толкования, если игрок рискует игровыми ценностями, то это не может признаваться азартной игрой по смыслу Закона № 244-ФЗ.

Переходя непосредственно к зарубежному опыту, интерес вызывает доклад IMCO committee (European Praliament, 2020) под названием «Loot boxes in online games and their effect on consumers, in particular young consumers». В целом логика работы аналогично построена вокруг анализа влияния лутбоксов на пользователей. На стр. 8 делается акцент на опыте стран, которые активно противодействуют лутбоксам, считая их азартными играми (например, Бельгия). На стр. 20 выделены способы получения лутбокса: покупка, ad-viewing (реклама), расширенная (покупка доп. контента) и battle pas. Авторы настоящей работы склонны не согласиться с последними двумя классификациями. Системы закрытого дополнительного контента и «пропуски» также являются видами монетизации, и их исследование вызывает неменьший интерес, но вряд ли их можно отождествлять с лутбоксами, ведь в их основе заложен совершенно иной принцип функционирования.

С. Махортов в своей статье составил сводную таблицу прецедентов по интересующему нас вопросу. Так, в 2018 г. Бельгия приравняла применение лутбоксов к азартным играм [2]. Как указано в источнике, бельгийская комиссия исходила из следующих элементов: ставка с возможной прибылью или убытками, случайность.

Почти сразу же после принятого решения «Valve» убрали для бельгийских пользователей возможность открывать контейнеры.

В Нидерландах в 2018, 2019 и 2020 годах происходил ряд разбирательств, по итогам которых лутбоксы сначала признали азартными играми, но впоследствии решение было обжаловано, и проблема осталась в плоскости правовой неопределенности. В июле 2022 г. появилась новость, что представители нескольких политических партий в Нидерландах подали ходатайство [16], согласно которому «лутбоксы» должны быть серьезно урегулированы (ограничены) в стране [17].

Любопытный подход можно наблюдать в Китае и Южной Корее [3. С. 264–265]. Игровые компании обязаны знакомить игроков с шансами выпадения ценностей из лутбоксов. Разумеется, целью таких предписаний является побуждение пользователя задуматься, стоит ли ему отдавать деньги за мизерный шанс получения желаемого. В свою очередь, это противодействует известному психологическому воздействию, когда азартному человеку кажется, что с каждой попыткой математическая вероятность успеха повышается.

Попытки законодательного регулирования существуют и в иных странах (некоторые штаты США, Австралия, Испания и пр.). Однако, как правило, дальше инициатив и рекомендаций они не продвигаются.

Существует еще одна грань понимания правовой регламентации лутбоксов в контексте баланса интереса сторон. Игровым компаниям выгоднее уйти с рынка и не соблюдать национальные законы малочисленных государств, чем соглашаться с ними. Например, на острове Мэн «коробки с наградами» также были приравнены к азартным играм. Как отмечает Л. Ю. Сяо, вряд ли разработчики пойдут на уступки в таком случае, ведь, по сравнению с крупными государствами, количество потребителей на острове крайне мало [18. P. 5]. Действительно, страх потерять китайский рынок, а вместе с ним и миллиарды долларов в таком случае несоизмерим. В дополнение существует интересный факт, что западные игроки узнали настоящую вероятность получения предметов в игре Counter-Strike: Global Offensive только после нововведения от «Valve» для китайской версии клиента «Steam».

Автор зарубежного исследования также проанализировал опыт бельгийского запрета. Оказалось, что пользователи Бельгии быстро нашли обходы для доступа к лутбоксам, например, регистрация британских аккаунтов Apple ID и использование VPN [18. P. 7]. Л. Ю. Сяо также подчеркивает, что нормативный запрет лутбоксов может создать чувство «ложной безопасности», когда в плоскости фактической его эффективность будет стремиться к нулю [18. P. 16].

Взгляд авторов настоящей работы на проблемные аспекты регулирования оборота лутбоксов. Что касается точки зрения авторов настоящей работы, думается, что рациональный путь решения проблем мог бы состоять не в запретительном методе правового регулирования, а в ограничительном (при котором достигается компромисс между участниками общественных отношений). Например, в осуществлении предварительного контроля игр (а не последующего) перед их допуском на национальный рынок. Мы поддерживаем косвенные методы решения проблемы: аналогичные китайским, осуществление пропаганды о вреде подобной

формы лудомании, проведение психологической работы с нуждающимися в ней и пр. [18. P. 20]

Также мы считаем, что сам принцип работы большинства «сундучков с наградой» аналогичен слот-машинам в классических казино. Игрок, совершив вложение денежных средств напрямую или через покупку «донатной валюты» (не желая ее зарабатывать или не имея такой возможности в силу правил игры), открывает лутбокс с желанием получить очень редкий предмет. Мотивация у пользователя может быть неоднородной: продажа предмета/аккаунта (даже если это запрещено пользовательским соглашением), коллекционирование, получение высокой социальной оценки «коммьюнити» (от англ. Community – «сообщество, социальная группа». Широко используемое обозначение пользователей видеоигр) и др.

Действительно, многие игроки, в том числе несовершеннолетние, проявляя свой азарт, тратят зачастую колоссальные суммы на покупку лутбоксов. Например, один пользователь в Diablo Immortal осуществил микротранзакции на сумму около 100 тыс. долларов, чтобы получить редкие руны. Но игра посчитала его слишком «сильным» и не позволяла ему сражаться против других игроков (из-за автоматического баланса) [19]. Безусловно, такие сюжеты выделяются как отклонения от общего правила, хотя и являются показательными.

Можно приводить еще бесчисленное множество примеров, но все они лишь являются средством гносеологического исследования явлений и процессов. В первую очередь, следует сформировать конкретные ориентиры. На наш взгляд, ключевыми вопросами в данном исследовании являются следующие:

Какие интересы в отношениях, связанных с предметом исследования, существуют?

Каким интересам мы желаем отдать приоритет? А какие проигнорировать? (вопрос достижения разумного компромисса)

Какие существуют разумные пути для достижения поставленной задачи?

Стоит ответить сразу, что не существует верного ответа на каждый из этих вопросов. Где-то отдается строгий приоритет публичному интересу, а где-то во внимание обязательно берется интерес частный, коммерческий.

Какие интересы мы можем выделить? Во-первых, стремление защитить общество от неразумных затрат, развития психологических проблем. Во-вторых, у компаний существуют свои собственные интересы, которые заключаются в желании получить прибыль. В-третьих, необходимо помнить и об интересах пользователей игрового контента, ведь существенные ограничения могут коснуться даже тех, кто открытием лутбоксов не занимается вовсе.

Целеполагание субъектов правотворчества и правоприменения так или иначе коррелирует с публично значимыми идеалами, такова специфика права. По данной причине игнорировать публичный интерес не представляется возможным. Но является ли полный запрет всего, что может «вредить» обществу, наилучшим способом достижения общественной цели?

Авторы настоящей работы полагают, что такой путь не является верным, особенно в контексте регулирования лутбкосов. Зарубежная практика и исследования показывают, что как бы они ни воспринимались государством и ни преподносились обществу, даже при их полном запрете азартные пользователи находят легкие

способы обхода ограничений. Таким образом, можно сделать очевидный вывод, что, если игрок имеет волю испытывать свою удачу, формальные запреты не смогут подавить такое желание. Более того, проблема не заканчивается на лутбоксах, ведь они являются лишь частным проявлением «способов заработка», основанных на уникальной человеческой эмоции – азарте. Не существует и гарантий, что, запретив «коробки с наградами», зависимый индивид не найдет им альтернативу, в том числе в сферах, не связанных с компьютерными играми.

Из сказанного можно заключить, что стоит бороться не со следствиями, а с причинами появления неконтролируемой страсти к азарту (важно напомнить, что именно спрос рождает предложение). В борьбе за предотвращение детской и подростковой лудомании на первом плане должно выступать воспитание несовершеннолетнего, его здоровая социализация. Безусловно, многие вопросы тесно взаимосвязаны с областью психиатрии и психологии, поэтому на них может ответить только специалист. Однако нам, как юристам, кажется очевидным, что необходимо нивелировать бесконтрольное желание нерационально тратить финансы, а не «запрещать Интернет».

Бесспорно, в тематике азартных игр, даже виртуальных, циркулирует огромное количество денежных средств. Следовательно, существует риск лоббирования, коррупции и проявления прочих пороков общества. Напомним, что цель настоящей работы заключается в рассмотрении лишь правовой стороны. Но факт остается фактом, общество – это сложная система, где все сферы тесно взаимосвязаны, поэтому, чтобы решить одну проблему, нужно уделять внимание и остальным.

Вернемся к способам достижения баланса интересов. При прямом запрете лутбоксов существует риск, что игровая компания прекратит реализацию своего продукта на национальном рынке, ведь может оказаться так, что убытки на содержание серверов для конкретного региона будут превышать прибыль (без основного элемента монетизации). Напомним, что только страны с широкой целевой аудиторией компьютерных игр (например, Китай) или с обеспеченным населением, готовым вкладывать большие суммы денежных средств в «донаты», могут навязать свои условия. В остальных же случаях перед государством будет стоять выбор: либо компромисс, либо запрет с игнорированием любых последствий.

Разумеется, лутбоксы, или формы агрессивной монетизации, не благо, ведь все это является продуктом жестокой конкуренции на рынке. Самая действенная модель борьбы с подобными явлениями строится вокруг сплочения международного сообщества для общего влияния на «аппетит» игровых корпораций. Однако в связи с современными тенденциями и не слишком глобальным значением проблемы нужно признать, что данный путь является утопией.

Таким образом, задача решается на национальном уровне, каждое государство по-своему, в силу множества причин, выбирает путь законодательного регулирования лутбоксов. Не удивительно, что российские исследователи занимают позиции полного запрета «сундучков», ведь компьютерные игры зачастую «демонизируются» в отечественном информационном пространстве. Авторы же считают, что игры могут быть как благом – способом эмоциональной разрядки и погружения в мир фантазий и развлечений, так и злом – при развитии различных девиаций (зависимость и пр.).

По нашему мнению, самым рациональным и компромиссным выходом будет реализация множества косвенных методов, которые в совокупности могут привести к значительному положительному эффекту. Так, к социальным методам могут относиться: здоровое воспитание несовершеннолетних; создание условий для обучения и деятельности квалифицированных специалистов по психолого-психиатрической помощи, компетентных в борьбе с зависимостями; поддержка друзей и близких, которые страдают от зависимости; ограничение пропаганды лутбоксов (фейковой рекламы) и пр.

Как непосредственные методы можно выделить: обязывание разработчиков раскрывать шансы выпадения ценностей; введение ограничений на открытие n-го количества лутбоксов в день; возрастной ценз; борьба со сторонними площадками для продажи игровых предметов (здесь также возникает множество «подводных камней»); повышение налоговой ставки для разработчиков, реализующих «цифровой азартный контент»; предварительный контроль перед допуском продукта на рынок и др.

Данный перечень является примерным, показывающим общую стратегию борьбы с лутбоксами и схожими механиками монетизации. Конкретную же тактику в определенном обществе (государстве) необходимо реализовывать выборочно, с учетом детального анализа социально-экономических и иных значащих для решения проблем явлений.

Итак, в настоящей работе мы постарались показать, что проблема законодательного регулирования лутбоксов является многогранной, требующей для разрешения детального анализа множества аспектов общественной жизни и поиска компромиссов. Уникальным элементом настоящего исследования является обоснование невозможности обеспечения интересов с помощью одностороннего регулирования: исключительного запрета или дозволения. В дополнение нами были разработаны собственные терминология и классификация, которые могут помочь другим исследователям при научном обосновании, описании сути процессов и явлений. В заключение хочется выразить надежду, что общество сможет найти рациональный компромисс между публичными и коммерческим интересами, сохранив при этом масштабную, интересную и развивающуюся культуру видеоигр.

Список литературы

1. Диденко К. Н. Внутренние микротранзакции в игровой индустрии как новый риск для детей и подростков // Детство – территория безопасности: сборник материалов конференции, Москва, 08 октября 2021 г. / Московский городской педагогический университет. Саратов: Саратовский источник, 2022. С. 145–148.

2. Махортов С. Подходы к регулированию внутриигровой собственности и обороту игровой валюты в странах мира // Научно-технический центр ФГУП «ГРЧЦ». 22.11.2022. URL: https://rdc.grfc.ru/2022/11/game_property_regulation

3. Варчук А. А. Зарубежный и российский опыт регулирования лутбоксов // Вопросы российской юстиции. 2020. № 5. С. 262–272.

4. Родионов И. А. Особенности гражданско-правового регулирования видеоигр с использованием лутбоксов // Modern Science. 2021. № 12–1. С. 311–317.

5. Дроздов Д. Е., Генералова Е. В., Николаев В. В. Проблема правового регулирования лутбоксов, как аналога казино в игровой индустрии // Заметки ученого. 2021. № 13. С. 477–480.

6. Федеральный закон от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменения в некоторые законодательные акты Российской Федерации» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_64924/

7. Решение Чертановского районного суда по делу № 02–4488/2018 // Официальный портал судов общей юрисдикции г. Москвы. URL: https://www.mos-gorsud.ru/rs/chertanovskij/services/cases/civil/details/b2fac727–0490–443f-acb0–21306e0c6663?caseNumber=02–4488/2018

8. Бурханова А. О., Червяков М. Э. Лутбоксы как разновидность азартных игр // Modern Science. 2019. № 5–1. С. 185–188.

9. Киселева Л. Ю. Правовое регулирование лутбоксов в видеоиграх // Научные записки молодых исследователей. 2021. Т. 9, № 4. С. 34–40.

10. Денисова А. И. Компьютерные игры как феномен современной культуры // Аналитика культурологии. 2010. № 3(18). С. 18–20.

11. Брушкова Л. А., Владимиров И. А. Лутбокс-монетизация в онлайн-видеоиграх как социально- экономическая проблема современного общества // Modern Economy Success. 2023. № 1. С. 181–185.

12. Постановление Пленума Верховного Суда РФ от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации» // Российская газета. 2015. № 140. 30 июня.

13. Мамедов Ю. В. Проблемы законодательного регулирования практики продажи лутбоксов игровыми компаниями // Молодые ученые в решении актуальных проблем науки: материалы IX Международной научно-практической конференции. Владикавказ, 12–14 декабря 2019 года. Владикавказ: Веста, 2019. С. 469–472.

14. Андреев Н. Субъективный учебник по праву компьютерных игр. Страсти вокруг лутбоксов и азартные игры // Zakon.ru. 25.01.2021. URL: https://zakon.ru/blog/2021/01/25/subektivnyj_uchebnik_po_pravu_kompyuternyh_igr_strasti_vokrug_lutboksov_i_azartnye_igry

15. Архипов В. В. Индустрия компьютерных игр: ключевые правовые проблемы // Открытое Образование. URL: https://openedu.ru/course/spbu/GAMIND/

16. Motie van het lid Bontenbal c.s. over loot boxes in videogames ook in Nederland verbieden. 30 juni 2022 26643–881 // tweedekamer.nl. URL: https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022Z13927&did=2022D28743

17. Alex Bes. Нидерланды движутся по пути к полному запрету лутбоксов // IXBT.com. 07.07.2022. URL: https://www.ixbt.com/live/games/niderlandy-dvizhutsya-k-polnomu-zapretu-lutboksov.html

18. Xiao L. Y. Breaking Ban: Belgium's Ineffective Gambling Law Regulation of Video Game Loot Boxes // Collabra: Psychology. 2023. № 9(1), 57641. DOI: https://doi.org/10.1525/collabra.57641

19. Шатухин Д. Фанат Diablo Immortal потратил на игру 100 тысяч долларов и стал «слишком сильным» // dtf.ru. 01.08.2022. URL: https://habr.com/ru/news/680288

А. Р. Зарипов,
магистрант,
Московский государственный университет
имени М. В. Ломоносова

ВЛИЯНИЕ ЭКСПЕРИМЕНТАЛЬНЫХ ПРАВОВЫХ РЕЖИМОВ В СФЕРЕ ЦИФРОВЫХ ИННОВАЦИЙ НА КОНКУРЕНТНУЮ СРЕДУ

Аннотация. В условиях стремительно растущих цифровых рынков, появляющихся на базе регулятивных песочниц, возникает угроза нарушения хозяйствующими субъектами принципов конкурентного права путем ведения монополистической деятельности и недобросовестной конкуренции. Цель данного исследования – анализ влияния экспериментальных правовых режимов на конкурентную среду и выявление недостатков в регулировании российских «песочниц». В статье представлены точки зрения по данному вопросу отечественных и зарубежных специалистов, приведен международный опыт, а также предложены способы для поддержания конкуренции при внедрении IT-технологий с помощью экспериментальных режимов.

Ключевые слова: право, цифровые технологии, экспериментальный правовой режим, регулятивные песочницы, конкуренция, группа компаний, экосистемы, искусственный интеллект, саморегулируемые организации

IMPACT OF EXPERIMENTAL LEGAL REGIMES IN DIGITAL SPHERE ON THE COMPETITIVE ENVIRONMENT

Abstract. In the context of rapidly growing digital markets which were formed in regulatory sandboxes there is a threat that business entities may violate the principles of competition law by carrying out monopolistic activities and unfair competition. The purpose of this research is to analyse the impact of experimental legal regimes on the competitive environment and to identify weaknesses in the regulation of Russian sandboxes. The article contains the opinions of domestic and foreign experts regarding this issue, cites international experience and suggests ways to maintain competition during the introduction of IT-technologies by means of experimental regimes.

Keywords: law, digital technologies, experimental legal regime, regulatory sandboxes, competition, corporate group, digital ecosystems, artificial intelligence, self-regulatory organisations

Конкуренция как основа рыночной экономики, безусловно, играет важную роль в сфере развития цифровых инноваций. Однако в условиях стремительно развивающегося прогресса появилось множество пробелов в правовом регулировании вновь возникающих digital-областей [9]. В качестве решения были созданы экспериментальные правовые режимы (далее также – ЭПР, или регулятивная песочница), которые добавили гибкости в нормотворчество, введя ряд послаблений, состоящих в «полном или частичном отказе от применения определенной группой лиц или на определенной территории обязательных требований либо в отказе

от осуществления разрешительной деятельности в отношении объекта разрешительной деятельности» [16].

Согласно пп. 2 п. 1 ст. 3 Федерального закона от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», одной из целей ЭПР является развитие конкуренции [17]. Тем не менее ряд экспертов, как отечественных, так и зарубежных, придерживаются мнения о негативном влиянии данного юридического инструмента на конкурентную среду, так как в течение срока действия специального режима субъекты – участники эксперимента получают определенные преимущества, которые при ординарных условиях вполне могли бы привести к доминирующему положению данных субъектов на рынке.

Так, Е. Ю. Баракина на основании анализа международного опыта выделила несколько недостатков регулятивных песочниц: «Во-первых, предоставление доступа к "песочнице" лицензированных и нелицензированных участников уже создает трудности с обоснованием справедливости участия тех и других на одинаковых условиях в "песочнице". Во-вторых, "песочница" – это среда искусственная, вне настоящего рынка. Она создает искусственные преимущества для пользователя на рынке, не позволяет полноценно отследить функционирование компании в текущих рыночных условиях. В-третьих, "неконкурентность" механизма принуждает регулятора тщательно отбирать проект, так как отдельные компании могут злоупотреблять своим положением» [3. С. 64–67].

Схожую точку зрения высказывают и западные коллеги: fictious competition distortion [29]. Упомянутый тезис говорит об искаженности или фиктивности конкуренции в условиях экспериментального режима. В сущности, возникает ситуация, при которой происходит дублирование рынка: с одной стороны, существует действующий порядок, выраженный через «соперничество хозяйствующих субъектов» в рамках текущих экономических процессов, с другой – наслаивающийся поверх «инкубатор», который готовит новых производителей в обход полноценной конкурентной борьбы. Гораздо важнее тот факт, что предприниматели после окончания специального режима, по сути, создают новый товарный рынок (или рынок услуг), а это, в свою очередь, означает их потенциально более выгодное положение по сравнению с лицами, которые впоследствии также захотят войти на этот рынок и представить свою продукцию.

Кроме того, разработка и развитие инноваций требуют высоких затрат, поэтому зачастую этим направлением занимаются крупные компании. В результате возникают определенные риски, связанные с образованием или укрупнением групп компаний и «экосистем». Очевидно, как следствие, получение таких преимуществ также дестабилизирует конкурентную среду. Указанные риски определены в «Концепции общего регулирования деятельности групп компаний, развивающих различные цифровые сервисы на базе одной «Экосистемы»», опубликованной на официальном сайте Минэкономразвития [6]. В первую очередь они касаются монополизации данных. В «Концепции» риски сгруппированы по следующим категориям: для граждан – в виде злоупотребления отношениями с клиентами путем введения в заблуждение, навязывание товаров и услуг, ущемления прав

потребителей и т. д.; для бизнеса – в форме недобросовестной конкуренции; для экономики и государства – в качестве снижения конкурентоспособности национальной экономики, утраты контроля за использованием данных, а также киберрисков, технологических рисков и рисков безопасности персональных данных.

Е. А. Громова в своем научном труде также указывает на проблему неравного доступа к персональным данным пользователей различных платформ и приводит в качестве примера жалобу, поданную на корпорацию Google рядом хозяйствующих субъектов: «по их мнению, потеря возможности отслеживать онлайн-активность пользователей негативно отразится на их доходах, а корпорация Google продолжит собирать огромные объемы пользовательских данных, что даст ей неоспоримое конкурентное преимущество» [5. С. 41–51; 21. С. 23–26]. Кроме этого, в доказательство того, что некоторые участники ЭПР могут создавать барьеры для входа на рынок потенциальных конкурентов, автор приводит доводы зарубежных экспертов, например: «FinTech-компании в состоянии предсказать, кто будет их будущими конкурентами, и исключить их с рынка путем проведения упреждающих слияний. Злоупотребление рыночной властью со стороны FinTech-компаний может практиковаться в форме отказа от предоставления лицензий или предоставления конкурентам доступа к важнейшим финансовым данным или средствам» [23. С. 5].

Необходимо также отметить особую роль искусственного интеллекта (далее также – ИИ) в вопросе разработки и внедрения различных цифровых систем. Не только подразумеваемые выше, но и многие другие технологии, в отношении которых вводятся экспериментальные правовые режимы, так или иначе связаны с ИИ, занимающимся обработкой данных (BigData), управлением сложных механизмов (высокоавтоматизированных транспортных средств или беспилотников), торговлей финансовыми инструментами (высокоскоростная алгоритмическая торговля) и пр. С точки зрения экспертов, указанные инновации дают конкурентное преимущество субъектам предпринимательской деятельности, использующим их [27].

Намеченная в России тенденция на цифровизацию экономики значительно укрепила положение искусственного интеллекта во многих сферах общественной жизни. Главным образом это касается области бизнес-процессов. Так, судя по аналитическим данным, собранным в отношении «развертывания» ИИ в Российской Федерации и опубликованным в июле 2023 г. [1], совокупный объем выручки компаний, занимающихся активным развитием и внедрением в свою деятельность систем искусственного интеллекта, которые в свою очередь значительно влияют на финансовый оборот данных участников рынка цифровых инноваций, составил в 2021 г. 552 млрд руб. (что на 28 % больше, чем в 2020 г.) и 647 млрд руб. в 2022 г. (рост рынка составил 17,3 % относительно 2021 года). Несмотря на заметное увеличение доли рынка ИИ в экономике страны, количество конкурирующих субъектов снижается – на 2022 г. около 29 компаний, использующих технологии искусственного интеллекта, были ликвидированы или состоят в процессе ликвидации на данный момент. При этом начиная с 2020 г. поддержка разработки и развития систем ИИ через государственное финансирование выросла почти в 3 раза с момента запуска федеральной программы «Искусственный интеллект» [15].

Таким образом, возникает ситуация, когда крупные «игроки» еще больше расширяют свое влияние и тем самым монополизируют рынок. Ярчайшим примером является картина, сложившаяся в мире благодаря западным IT-гигантам. Доминирующее положение цифровых компаний из Кремниевой долины стало своего рода нормой для общественности – практически все электронные девайсы или сервисы создаются и продвигаются при их непосредственном участии. Естественно, для конкурентной среды такая действительность крайне пагубна, так как приводит к недобросовестным практикам, злоупотреблениям правом и системным сбоям, когда проблемы одного гиганта впоследствии влияют на всех участников рынка. По мнению специалистов, для нормализации экономических процессов уже сейчас необходимо принять соответствующие антимонопольные меры [14]. По всей видимости, российские компании развиваются по тому же пути, поэтому очень важно сократить отрыв отечественных монополистов от более мелких начинающих предприятий, пока это еще возможно. Представляется, что добиться такого эффекта можно с помощью введения специальных послаблений малым IT-компаниям в рамках экспериментального правового режима. Например, в Великобритании для осуществления указанных целей разработан специальный инструмент – regulatory nursery [26]. Такие мини экспериментальные правовые режимы призваны предоставлять дополнительную поддержку и рекомендации для начинающих в IT-сфере фирм. Кроме того, британский Financial Conduct Authority (далее – FCA), или Управление по финансовому регулированию и надзору, предоставляет case manager [30], т. е. специального помощника, для организаций, которые имеют право на участие в регулятивной песочнице. К обязанностям курирующего различные фирмы лица относится содействие в подготовке и реализации «эксперимента». Также FCA оказывает консультационные услуги и дает толкование правил, установленных в рамках конкретного ЭПР.

Отдельного внимания требует следующий факт: искусственный интеллект наделен особыми свойствами, позволяющими рассматривать его не только как объект эксперимента, но и как субъект или «квазисубъект» права [4. С. 3–9; 20. С. 32–36]. В вопросах разработки и внедрения новых технологий ИИ имеет особое преимущество благодаря своим производственным мощностям, поэтому в процессе обучения он способен генерировать гораздо больше идей, чем человек. Как следствие, компании, использующие данные идеи, могут создавать барьеры для входа конкурентов на рынок, например, с помощью вспомогательных патентов.

По мнению А. В. Хрусталевой, наиболее остро эта проблема развита в медицинской сфере и выражается в наличии препятствий для появления аналогов запатентованного лекарственного средства, которые могли быть представлены по более выгодным для потребителей ценам. В таком случае образовавшаяся монопольно высокая цена делает медикаменты не такими доступными для пациентов и требует больше затрат из бюджетных средств при закупках лекарственных препаратов для государственных и муниципальных нужд, что на практике экономически нецелесообразно. Как утверждает автор: «ВП [вспомогательный патент] является актом недобросовестной конкуренции на фармацевтическом рынке

Российской Федерации, который препятствует обеспечению доступности и прозрачности обращения лекарственных препаратов» [18. С. 30–34].

Исходя из международной практики, выработанной, в частности, комиссией по финансовому надзору Китайской Республики (Тайвань), заявка на участие в экспериментальном правовом режиме, поданная IT-компанией может быть отклонена, если представленная продукция будет лишена «инновационности» [23]. При этом наличие критерия «инновационность» вызывает критику среди ученых-юристов в связи с возникновением трудностей по доказыванию данного признака. Наиболее вероятной моделью аргументирования в таком случае станет отсылка на приобретенный патент [32]. Однако именно этот инструмент создаст исключительное право на разрабатывающуюся технологию, а вместе с ним и условия, не допускающие потенциальных конкурентов как к участию в регулятивной песочнице, так и впоследствии на рынок инноваций. Сложно рассчитать масштаб последствий в сфере конкурентной борьбы при участии искусственного интеллекта в процессе создания новых разработок, которые позднее могут быть запатентованы владельцами ИИ.

По данным статистического анализа [10], а также официального реестра экспериментальных правовых режимов в сфере цифровых инноваций [12], представленных Министерством экономического развития, на данный момент (август 2023 г.) во всей Российской Федерации установлено девять ЭПР, в которых участвуют около пятидесяти компаний. Однако с января 2021 г. всего было подано семьдесят пять заявок на введение регулятивной песочницы. Из них, помимо уже принятых, двадцать проектов находятся в разработке, в отношении еще четырнадцати работа приостановлена, а двадцать четыре – отклонены, как не соответствующие требованиям Федерального закона от 31.07.2020 № 258-ФЗ. Показатели едва ли говорят об эффективности использования «песочниц» в российском формате. Наоборот, создается впечатление существования неких препятствий в проведении экспериментов и низкой доступности участия в них для небольших организаций. Как уже было сказано ранее, это довольно пагубно для конкурентной среды.

Причина такого положения дел вполне может находиться в определении целей экспериментального правового режима. Так, по мнению департамента развития цифровой экономики РФ и Банка России, регулятивные песочницы направлены на преодоление правовых барьеров [8]. Следовательно, при разработке и внедрении инноваций регуляторы исходят не из экономических, а из юридических предпосылок. Другими словами, за основу выработки норм государственного управления ими взяты не общественные отношения, а стремление поддержать контролируемую среду. Такой подход является достаточно узким, так как подразумевает, что правоотношения, связанные с возникновением новых объектов гражданского оборота (цифровых технологий), складываются только в рамках установленных в законном порядке норм и не выходят за их пределы. Подобный позитивизм несколько консервативен, потому что не учитывает темпы экономико-правового прогресса и таким образом игнорирует возможность видоизменения социально-правовой парадигмы. Так, рассматриваемые общественные отношения возникают не с момента их нормативного закрепления. Они появляются с созданием

объекта-инновации, причем не только в форме ранее неизвестных юридических практик, но и в образе стандартного правового опыта, который впоследствии может преобразиться и потребовать формирования «нео»-регулирования.

На официальном сайте Банка России регулятивная песочница определяется как «механизм для пилотирования, моделирования процессов новых финансовых сервисов и технологий в изолированной среде, требующих изменения правового регулирования» [11]. Рекомендуется изменить подход, заменив формулировку «требующих изменения правового регулирования» на «которые требуют или могут потребовать в будущем изменения правового регулирования». Разумеется, речь не идет о поголовном допуске всех поданных на рассмотрение заявлений к участию в ЭПР. Необходимо, чтобы компетентные органы тщательно отбирали заявки, анализируя потенциальные риски, но при этом расширительное толкование «песочницы» позволит большему количеству фирм принять участие в эксперименте, обеспечив благоприятные условия для защиты конкуренции, а также создаст возможность превентивного реагирования на возможные изменения в социально-правовой среде. Мировой опыт как раз демонстрирует именно такие тенденции. Так, в Южно-Африканской Республике целью регулятивной песочницы считают развитие наиболее перспективных отраслей, в которых инновации бросают вызов существующему законодательству (innovation is challenging regulation) [25]. Страна-первопроходец в становлении ЭПР – Великобритания – также склоняется к тому, что «песочницы» в первую очередь нужны для проведения безопасных тестов над появляющимися цифровыми технологиями, чтобы сократить срок выхода продукта на рынок и сопутствующие с этим затраты [31]. Как указывает П. Шуст, в основе сингапурских регулятивных песочниц тоже «лежит стремление предоставить инновационным компаниям возможность тестировать свои продукты и модели на небольшом, изолированном участке реального рынка» [22], а после завершения «проверочного периода» предприниматели смогут полноценно реализовать свой продукт на территории Сингапура [24].

Таким образом, проблема защиты конкуренции в рамках проведения экспериментальных правовых режимов в сфере цифровых инноваций в Российской Федерации становится все заметнее. Повышаются экономические риски. Следовательно, уже сейчас необходимо предпринимать меры по урегулированию данных сфер общественной жизни. В качестве решения Е. А. Громова предлагает «привлечь антимонопольные органы к процессу принятия решений об установлении, изменении и прекращении экспериментального режима» [5. С. 41–51], соответственно, наладить взаимодействие ФАС с участниками ЭПР и использовать систему антимонопольного комплаенса в организация – субъектах эксперимента.

Антимонопольный комплаенс как инструмент способствует снижению случаев привлечения хозяйствующих субъектов к ответственности за несоблюдение антимонопольного законодательства, так как служит своего рода превентивным механизмом, побуждающим участников рынка внимательнее относиться к мерам по предупреждению нарушений. Кроме того, он позволит выявлять такие нарушения на ранних этапах, чем уменьшит нагрузку на антимонопольные органы [2; 13. С. 15].

Схожее мнение по поводу развития конкурентно-ориентированной направленности применения регулятивных песочниц можно увидеть и у зарубежных специалистов: «Shifting the focus towards a kind of anticipatory competition policy, leading competition authorities to the forefront of market governance and assigning them greater responsibilities with respect to nascent markets» [28]. Иными словами, при введении экспериментального правового режима необходимо акцентировать внимание на «упреждающей политике» в области защиты конкуренции, и при этом антимонопольные органы должны расширить зону своего влияния на рынке одновременно с увеличением степени их ответственности.

Проведенный анализ указывает на присутствие некоторых недостатков в регулировании российских ЭПР в сфере цифровых инноваций. Главным образом они касаются антимонопольного права и защиты конкуренции. Несмотря на новизну рассматриваемого института, он подвергается критике далеко не в первый раз. Поэтому, чтобы регулятивная песочница функционировала должным образом, регуляторам следует проводить «работу над ошибками» на постоянной основе. В августе 2023 г. Центральный Банк России уже предпринял шаги по оптимизации экспериментальных режимов: «В результате форму заявки сделали проще, а срок рассмотрения заявок и пилотирования проектов сократился сразу в три раза» [19]. Сохранение столь положительной тенденции послужит отличным стимулом в развитии ЭПР.

Также в работе были предложены способы решения выявленных проблем. Однако согласиться с ними можно лишь отчасти. Активное участие антимонопольных органов и использование «комплаенса», безусловно, даст свои плоды. Тем не менее рекомендуется также создать условия для конкурентной борьбы внутри регулятивной песочницы. Так как экспериментальный правовой режим создает искусственный рынок, важно, чтобы на нем дублировались основные экономические процессы. Следовательно, потребуется и большое количество субъектов предпринимательской деятельности. Для обеспечения их участия предлагается ввести институт частно-публичного регулирования, а именно передать часть функций государственных органов саморегулируемым организациям путем выдачи установленной в законном порядке лицензии. В Великобритании этот инструмент получил название «зонтичные песочницы» [7; 22].

Список литературы

1. Альманах «Искусственный интеллект». 2022. № 12. URL: https://aireport.ru/ai_index_russia-2022

2. Антимонопольный комплаенс: текущая практика и перспективы развития: доклад Аналитического центра при Правительстве Российской Федерации. URL: http://ac.gov.ru/files/publication/a/7838.pdf

3. Баракина Е. Ю. К вопросу об установлении экспериментального правового режима в области применения искусственного интеллекта // Российская юстиция. 2021. № 2. С. 64–67.

4. Блинов В. С. Новые технологии – старые проблемы. Искусственный интеллект как субъект права // Право и бизнес. 2022. № 4. С. 3–9.

5. Громова Е. А. Экспериментальные режимы создания цифровых инноваций и проблемы обеспечения добросовестной конкуренции // Журнал российского права. 2022. № 10. С. 41–51.

6. Концепция общего регулирования деятельности групп компаний, развивающих различные цифровые сервисы на базе одной «Экосистемы». 28.05.2021. URL: https://economy.gov.ru

7. Международный опыт применения «песочниц». Обзор Коллегии Евразийской экономической комиссии по внутренним рынкам, информатизации, ИКТ. 2018. URL: https://eec.eaeunion.org/upload/directions_files/291/2915ed626ad3b69f1116ca897fa28b7f.pdf

8. Основные направления развития финансового рынка Российской Федерации на 2023 год и период 2024 и 2025 годов (разработаны Банком России) // Вестник Банка России. 2022. № 63. 29 декабря.

9. Пробелы в праве в условиях цифровизации: сборник научных трудов / под общ. ред. Д. А. Пашенцева, М. В. Залоило. М.: Инфотропик Медиа, 2022. 472 с.

10. Развитие экспериментальных правовых режимов. Департамент развития цифровой экономики (Минэкономразвития). URL:https://itforum.admhmao.ru/upload/iblock/1af/o6r6a9qfonel2nvteq7yirrigb2ik2pv/Razvitie-EPR.pdf

11. Регулятивная «песочница». Официальный сайт Банка России. URL:https://cbr.ru/fintech/regulatory_sandbox/#highlight=%D0%BF%D0%B5%D1%81%D0%BE%D1%87%D0%BD%D0%B8%D1%86%D0%B0

12. Реестр экспериментальных правовых режимов в сфере цифровых инноваций. URL: https://www.economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/normativnoe_regulirovanie_cifrovoy_sredy/eksperimentalnye_pravovye_rezhimy/reestr_eksperimentalnyh_pravovyh_rezhimov

13. Спиридонова А. В. Принцип взаимодействия антимонопольных органов и бизнес-сообщества в обеспечении добросовестной конкуренции в Российской Федерации // Конкурентное право. 2019. № 1. С. 15.

14. Тимофеев А. Чем опасна власть цифровых гигантов. 2020. URL: https://www.gazeta.ru/tech/2020/07/15_a_13152859.shtml?ysclid=l3kq0uja7w

15. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

16. Федеральный закон от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

17. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

18. Хрусталева А. В. Вспомогательные изобретения, создаваемые искусственным интеллектом, как инструмент недобросовестной конкуренции // ИС. Промышленная собственность. 2023. № 2. С. 30–34.

19. ЦБ оптимизировал работу своей регулятивной «песочницы». Газета «Ведомости». URL: https://www.vedomosti.ru/finance/news/2023/08/10/989453-tsb-optimiziroval-rabotu-regulyativnoi-pesochnitsi

20. Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32-36.
21. Черешнева И. А. Цифровые платформы: от защиты конкуренции к защите данных // Конкурентное право. 2023. № 2. С. 23–26.
22. Шуст П. Регулятивные песочницы: регулирования как сервис. Ассоциация участников рынка электронных денег и денежных переводов. 2016.
23. Chen A. Regulatory Sandbox and Competition of Financial Technologies in Taiwan. Competition Policy International, 2019.
24. Consultation Paper on Fintech Regulatory Sandbox Guidelines // Monetary Authority of Singapore. 06.06.2016.
25. Feedback on the Intergovernmental Fintech Working Group's first regulatory sandbox initiative. Intergovernmental Fintech Working Group (IFWG), 2022.
26. Glossop A. Regulatory sandbox: 5 key things to know, 2021.
27. LegalTech в сфере предпринимательской деятельности: монография / Р. Н. Адельшин, Е. И. Андреева, Л. В. Андреева и др.; отв. ред. И. В. Ершова, О. В. Сушкова. М.: Проспект, 2023. 200 с.
28. Poncibò C., Zoboli L. Regulatory Sandboxes: ex ante regulation or competition policy?. 2023. URL: https://www.competitionpolicyinternational.com/wp-content/uploads/2023/04/7-REGULATORY-SANDBOXES-EX-ANTE-REGULATION-OR-COMPETITION-POLICY-Cristina-Poncibo-Laura-Zoboli.pdf
29. Poncibò C., Zoboli L. The Methodology of Regulatory Sandboxes in the EU: A Preliminary Assessment from a Competition Law Perspective // Stanford-Vienna Transatlantic Technology Law Forum: EU Law Working Papers. 2022. № 61.
30. Regulatory Sandbox // Financial Conduct Authority. March 2022. URL: https://www.fca.org.uk/firms/innovation/regulatory-sandbox
31. Regulatory Sandbox // Financial Conduct Authority. November 2015. URL: https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf
32. «Regulatory sandboxes in artificial intelligence» // OECD Digital Economy Papers, № 356, OECD Publishing, Paris, 2023.

Ю. В. Засеева,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

К ВОПРОСУ О НОВЫХ ФОРМАХ КОММЕРЧЕСКОГО ПОДКУПА

Аннотация. В статье рассматривается появление новых форм коммерческого подкупа в контексте развития криптовалют и технологии блокчейн. По мере роста популярности инновационных цифровых активов и децентрализованных систем они также привлекают внимание преступников, стремящихся использовать их для осуществления незаконной деятельности. В исследовании выявлены проблемы, связанные с анонимным характером криптовалют, которые могут способствовать совершению сделок, связанных со взяточничеством и коммерческим подкупом.

Кроме того, в статье рассматривается потенциал технологии блокчейн для противодействия этой незаконной деятельности путем повышения прозрачности.

Ключевые слова: коммерческий подкуп, криптовалюты, технология блокчейн, коррупция, анонимность, уголовное право

TO THE QUESTION OF THE NEW FORMS OF COMMERCIAL BRIBERY

Abstract. This article examines the emergence of new forms of commercial bribery in the context of the development of cryptocurrencies and blockchain technology. As these innovative digital assets and decentralized systems grow in popularity, they also attract the attention of criminals seeking to exploit them for illicit activities. The study examines the challenges posed by the anonymous nature of cryptocurrencies, which may facilitate bribery-related transactions. In addition, the article examines the potential of blockchain technology to counter these illicit activities by increasing transparency.

Keywords: commercial bribery, cryptocurrencies, blockchain technology, corruption, anonymity, criminal law

Актуальность данной статьи заключается в комплексном исследовании взаимосвязи криптовалют, технологии блокчейн и коммерческого подкупа. В ней подчеркивается необходимость принятия проактивных мер для использования потенциала этих технологий и смягчения последствий их использования в противоправной деятельности.

Данная тематика становилась предметом исследования многих российских ученых в области уголовного права. В частности, в статье Д. Г. Ткаченко рассматривается вопрос о квалификации посредничества во взяточничестве и коммерческом подкупе с использованием современных цифровых технологий [6]. В другой статье А. А. Тарновский и другие исследователи рассматривают вопросы, касающиеся определения правового статуса криптовалюты в российском праве, возможность криптовалюты выступать в качестве предмета преступления, способы определения размера взятки, полученной в криптовалюте [5]. Отметим также статью О. А. Науменко и Н. А. Бутяевой, где рассматривается понятие и правовое регулирование криптовалюты, а также проблемы поиска и установления личности преступника, использующего криптовалюты при совершении преступлений [4].

Цель исследования – изучить влияние криптовалют и технологии блокчейн на возникновение новых форм коммерческого подкупа.

Задачи исследования:

– исследовать и оценить масштабы коммерческого подкупа с использованием криптовалют;

– изучить преимущества и ограничения технологии блокчейн в борьбе с коммерческим подкупом;

– проанализировать нормативно-правовые проблемы, связанные с мониторингом и предотвращением коммерческого подкупа с помощью криптовалют.

Для достижения задачи и решения поставленных целей применяются различные подходы к познанию, включая общенаучные и частно-юридические методы

исследования. Среди них можно выделить историко-правовой, компаративистский и системно-структурный анализ, а также методы индукции, дедукции, сравнения, сопоставления, обобщения, герменевтики, диалектики и формальной юриспруденции.

Эмпирическая база исследования будет включать анализ существующих норм уголовного права, а также судебной практики по делам, связанным с коммерческим подкупом и смежными составами преступлений при помощи криптовалют.

Хронологические рамки данного исследования начинаются с момента создания действующей правовой базы, регулирующей коммерческий подкуп, до даты окончания исследования – август 2023 года. Оно не охватывает любые возможные правовые изменения или изменения, которые могли произойти после этой даты.

Коммерческий подкуп как одна из форм коррупции является проблемой для многих стран. С появлением криптовалют и блокчейна возникли новые возможности и проблемы, связанные со коммерческим подкупом. Децентрализованный характер криптовалют и прозрачность, обеспечиваемая технологией блокчейн, потенциально могут быть как благом, так и препятствием для борьбы с коррупцией.

Криптовалюта – это цифровая или виртуальная форма валюты, использующая криптографические методы для обеспечения безопасности финансовых операций, контроля за созданием новых единиц и проверки передачи активов. В отличие от традиционных фиатных валют криптовалюты работают в децентрализованных сетях, основанных на технологии блокчейн.

На сегодняшний день существует множество видов криптовалют. Одними из наиболее популярных являются Bitcoin, Ethereum, Tether, Binance Coin, USD Coin, XRP, Cardano, Solana, Dogecoin и Polkadot. Выделяют также стейблкоины – это криптовалюты, которые привязаны к стабильному активу, например к доллару США, для снижения волатильности.

Bitcoin, Ethereum, Tether и Monero – это наиболее часто используемые виды криптовалют, обладающие уникальными свойствами и характеристиками.

Биткоин – это децентрализованная цифровая валюта, которую можно покупать, продавать и обменивать напрямую, без посредников вроде банков. В ней используется децентрализованная система бухгалтерских книг, известная как блокчейн, которая защищена консенсусом по принципу proof-of-work (PoW). Биткоин предназначен для использования в качестве денег и формы оплаты, не зависящей от какого-либо одного человека, группы или правительства. Его объем ограничен 21 млн монет. Биткоин когда-то считался приватным, но сейчас это не так.

Ethereum – это сеть компьютеров по всему миру, которые следуют набору правил, называемых протоколом Ethereum. Он позволяет людям совершать сделки и общаться без контроля со стороны центрального органа. В сети существует собственная криптовалюта Ether, которая используется для оплаты определенных действий в сети Ethereum.

Tether – это стейблкоин, который пытается поддерживать привязку стоимости к базовой валюте, такой как доллар или евро. Он построен на базе Mastercoin (Omni). Tether помогает инвесторам перемещать средства между криптовалютными рынками и традиционной финансовой системой, минимизируя волатильность за счет привязки к базовой валюте в соотношении 1 к 1.

Monero – это криптовалюта, ориентированная на конфиденциальность и специализирующаяся на приватных транзакциях. В ней используется кольцевое шифрование подписей, которое позволяет скрыть отправителя, получателя и сумму каждой транзакции. Это единственная крупная криптовалюта, в которой каждый пользователь по умолчанию анонимен.

Криптовалюты произвели революцию в финансовой сфере, обеспечив безопасные и децентрализованные транзакции по всему миру. Однако характеристики, которые делают криптовалюты привлекательными для обычных пользователей, такие как анонимность, привлекают и преступников. Эти характеристики создают благодатную почву для операций, связанных со взяточничеством, позволяя преступникам скрывать свою личность при проведении незаконных финансовых операций.

Использование криптовалют для коммерческого подкупа вызывает особую обеспокоенность, поскольку они обходят традиционные финансовые институты, что затрудняет отслеживание и предотвращение таких операций. Такая анонимность способствует укреплению позиций коррупционеров, поскольку они могут реализовывать схемы подкупа, не опасаясь быть идентифицированными или задержанными.

Закон «О финансовых цифровых активах», который вступил в силу в начале 2021 г. [2], фактически приравнивает криптовалюты к имуществу и запрещает их использование в качестве платежного средства. В феврале 2022 г. Правительство РФ выпустило «Концепцию законодательного регламентирования механизмов организации оборота цифровых валют», которая предусматривает регулирование оборота таких финансовых активов с жесткими обязательствами для всех участников профессионального рынка и с акцентом на защиту прав рядовых инвесторов [7].

Постановление Пленума Верховного Суда РФ от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» определяет предметом взяточничества деньги, ценные бумаги, иное имущество, оказание услуг имущественного характера, предоставление имущественных прав [3]. Соответственно, криптовалюта является имуществом, а значит, она может быть предметом преступления.

«Есть примеры передачи в качестве взятки криптовалюты, хотя они пока не столь распространены», – отметил в интервью ТАСС генеральный прокурор РФ Игорь Краснов. При этом Краснов заметил, что такие преступления представляют повышенную общественную опасность, поскольку использование криптовалюты в криминальных расчетах зачастую свидетельствует о связи с организованной преступностью [8]. В связи с этим также возникает множество проблем и в процессуальном плане. Так, непонятно, каким образом налагать на криптовалюту арест, конфисковывать ее, и обращать ее в доход государства.

Криптовалюты создают новые проблемы в борьбе с коррупционными преступлениями, однако технология блокчейн, лежащая в основе этих цифровых активов, предлагает потенциальные решения. Блокчейн работает как неизменяемая распределенная система учета, фиксирующая все транзакции в доступной и децентрализованной форме. Такая прозрачность может помочь выявить коррупционную деятельность, поскольку обеспечивает постоянную запись транзакций.

Кроме того, решающую роль в снижении уровня взяточничества может сыграть внедрение смарт-контрактов. Это так называемые самоисполняющиеся

договоры, построенные на платформе блокчейна с прописанными в коде условиями. Исполнение условий в автоматическом режиме приведет к исполнению контракта. Человеческое участие тут минимально, что поможет исключить коррупционный фактор, когда для исполнения контракта в экономических отношениях сторона требует исполнения дополнительных условий, не оговоренных в контракте.

Несмотря на потенциальные преимущества, регулирование криптовалют и технологии блокчейн остается сложной задачей для многих стран. Децентрализованный характер этих систем означает, что ни один субъект не имеет полного контроля, что затрудняет установление юрисдикции и введение обычных правил.

Правоохранительные органы разных стран пытаются найти способы эффективного контроля и регулирования криптовалютных бирж и транзакций, чтобы соблюсти баланс между необходимостью обеспечения конфиденциальности и безопасности пользователей и необходимостью предотвращения преступной деятельности.

Для эффективного решения проблем, связанных с новыми формами коммерческого подкупа, необходимо развивать комплексную нормативно-правовую базу, включающую криптовалюты и технологию блокчейн.

Можно рассмотреть следующие меры:

1. Усиление мер по борьбе с отмыванием денег и идентификации пользователей криптовалют (KYC – «знай своего клиента»). Криптовалютные биржи и поставщики услуг должны быть обязаны внедрять надежные процедуры KYC для выявления и предотвращения потенциальных операций, связанных с преступной деятельностью.

2. Сотрудничество между государством и технологическими компаниями. Государственные органы должны сотрудничать с компаниями, работающими в сфере криптовалют и блокчейн-технологий, для разработки инновационных решений, способствующих повышению прозрачности и подотчетности финансовых операций.

3. Международное сотрудничество. Учитывая трансграничный характер криптовалют, международное сотрудничество между правоохранительными органами разных стран является жизненно важным для эффективной борьбы с коррупцией.

Таким образом, появление криптовалют и технологии блокчейн, несомненно, изменило коммерческий ландшафт. Однако оно породило и новые проблемы, особенно в сфере коммерческого подкупа. Анонимный характер криптовалют создает идеальные условия для коррупционной деятельности незаконных субъектов. Тем не менее прозрачная и децентрализованная природа технологии блокчейн предлагает инновационные решения для смягчения этих проблем.

Для эффективного решения проблемы новых форм коммерческого подкупа в эпоху криптовалют и блокчейна необходим согласованный подход, сочетающий правовые, регулятивные и технологические меры. Только при таком взаимодействии общество сможет в полной мере использовать потенциал этих технологий и одновременно защитить себя от их неправомерного использования в преступной деятельности, например во взяточничестве.

Список литературы

1. Генпрокурор РФ сообщил о выявлении в России первых случаев взяток криптовалютой. URL: https://tass.ru/ekonomika/16544839

2. Концепция законодательного регламентирования механизмов организации оборота цифровых валют. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Науменко О. А., Бутяева Н. А. Криптовалюта как предмет и средство совершения преступлений // Вестник Краснодарского университета МВД России. 2022. № 2(56). С. 47–51.

4. Постановление Пленума Верховного Суда РФ от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях». Доступ из справ.-правовой системы «КонсультантПлюс».

5. Тарновский А. А., Коваленко Е. В., Мазняк В. К. Проблемы квалификации преступления при даче взятки в криптовалюте // Образование и право. 2022. № 11. С. 303–306.

6. Ткаченко Д. Г. Особенности квалификации посредничества во взяточничестве и коммерческом подкупе с использованием современных цифровых технологий // Вестник Хабаровского государственного университета экономики и права. 2021. № 1(105). С. 130–132.

7. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25. Ст. 2954.

8. 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 Российской Федерации от 3 августа 2020 г. № 31 (часть I). Ст. 5018.

К. С. Злищева,
студент,
Северо-Кавказский филиал
Российского государственного университета правосудия

ВЛИЯНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ НА ЗАЩИТУ ТРУДОВЫХ ПРАВ УЧАСТНИКОВ УГОЛОВНОГО ПРОЦЕССА

Аннотация. В статье рассматриваются основные проблемы действующего законодательства, которые не позволяют в достаточной степени гарантировать соблюдение трудовых прав подозреваемых, обвиняемых, реабилитированных. Цифровизация учетов, которые ведут различные министерства и ведомства, правоохранительные органы, суды, позволит при ликвидации законодательных пробелов устранить несправедливость в реализации трудовых прав отдельных участников уголовного судопроизводства, сделать их полноценными субъектами экономической деятельности.

Ключевые слова: подозреваемый, обвиняемый, реабилитированный, трудовые права, судебное решение, приговор, постановление следователя

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE PROTECTION OF LABOR RIGHTS OF PARTICIPANTS IN CRIMINAL PROCEEDINGS

Abstract. The article highlights the main problems of the current legislation, which do not sufficiently guarantee the observance of the labor rights of suspects, accused, rehabilitated. Digitalization of records maintained by various ministries and departments, law enforcement agencies, and courts will make it possible, when eliminating legislative gaps, to eliminate injustice in the exercise of labor rights of individual participants in criminal proceedings, to make them full-fledged subjects of economic activity.

Keywords: suspect, accused, rehabilitated, labor rights, court decision, sentence, investigator's decision

Цифровизация во всех сферах общественной жизни призвана существенно облегчать человеку реализацию в жизни его возможностей. Уголовно-процессуальный кодекс РФ (далее – УПК РФ) [1] называет одним из назначений уголовного судопроизводства защиту личности от незаконного и необоснованного обвинения, ограничения ее прав и свобод (п. 2 ч. 1 ст. 6).

К лицу, предположительно виновному в совершении преступления, могут применить меры пресечения, которые выражаются в определенной степени изоляции или преднамеренном ограничении прав и возможностей лица. Они влияют и на состояние трудовых прав подозреваемого (обвиняемого).

Например, заключение под стражу (ст. 108–110 УПК РФ) выражается в принудительной изоляции лица в институциональных учреждениях с особым режимом, который определяется Законом о содержании под стражей подозреваемых и обвиняемых в совершении преступлений [2] и Правилами внутреннего распорядка следственных изоляторов уголовно-исполнительной системы [3]. Заключение под стражу может применяться до 18 месяцев – ст. 108, 109 УПК РФ). Работодателя при этом не уведомляют, что работник находится под стражей, что зачастую становится причиной расторжения трудового договора из-за прогула.

Прогул, согласно пп. «а» п. 6 ст. 81 ТК РФ [4], – отсутствие на рабочем месте без уважительных причин в течение всего рабочего дня (смены), независимо от его (ее) продолжительности; отсутствие на рабочем месте без уважительных причин более 4 часов подряд в течение рабочего дня (смены). Очевидно, что заключение лица под стражу является именно уважительной причиной, поскольку никоим образом не зависит от воли самого лица [5]. Поэтому мы считаем, что следователь (дознаватель) обязан уведомить работодателя лица, к которому применена мера пресечения.

Трудовая функция в рассматриваемых нами случаях лицом не осуществляется, поэтому ему не выплачивают заработную плату. Статьи 27, 41 Закона о содержании под стражей, пп. 339–343 Правил внутреннего распорядка СИЗО дают заключенным под стражу лицам возможность трудиться с соблюдением требований трудового законодательства, в том числе права на оплату труда. Кроме того, в случае совпадения периода содержания под стражей и ежегодного оплачиваемого отпуска средний заработок должен сохраняться (ст. 114 ТК РФ).

При временном отстранении от должности трудовые права лица защищает ч. 6 ст. 114 УПК РФ путем установления необходимости выплаты подследственному государственного пособия, являющегося составной частью процессуальных издержек (п. 8 ч. 2 ст. 131 УПК РФ).

Мера пресечения в виде запрета определенных действий (ст. 1051 УПК РФ) в этом смысле урегулирована хуже. Она не предусматривает механизма обеспечения права для случаев, когда лицу запрещено осуществлять действия, которые непосредственно связаны с его трудовой функцией. Для подобных ситуаций также необходима выплата ежемесячного государственного пособия.

В соответствии с ч. 1 ст. 133 УПК РФ право на реабилитацию включает в себя право на возмещение имущественного вреда, устранение последствий морального вреда и восстановление, помимо прочего, в трудовых правах.

Реабилитация, в сущности, начинается незамедлительно, так как об этом праве должно быть указано в процессуальном акте, которым лицо выводится из орбиты уголовного процесса (ч. 1 ст. 134 УПК РФ). Одновременно должны быть даны разъяснения о порядке возмещения вреда.

В случае уголовного преследования лица могут иметь место факты его увольнения вопреки смыслу п. 4 ч. 1 ст. 83 ТК РФ, которая распространяется только на случаи наличия обвинительного приговора суда, вступившего в законную силу. Согласно п. 5 Положения, утвержденного Указом Президиума ВС СССР от 18 мая 1981 г. № 4892-X [7], в таких ситуациях в процессе реабилитации лицу должна быть предоставлена прежняя работа или должность. Если это объективно невозможно, то реабилитированному должна быть предоставлена иная равноценная работа или должность.

Те же правила действуют и в случае, когда лицо хотя и было осуждено, но применено такое наказание, которое не исключает продолжение осуществления трудовой функции по прежнему месту работы (п. 4 ч. 1 ст. 83 ТК РФ). В случае если наказание назначено в виде исправительных работ, увольнение работника и вовсе недопустимо, поскольку это противоречит смыслу порядка исполнения такого наказания (ч. 1, 2 ст. 50 УК РФ) [8].

В глобальном разрезе трудовые права подозреваемых и обвиняемых в уголовном процессе России являются достаточно защищенными. В то же время существует множество пробелов, которые снижают степень такой защиты. Не секрет, что работодатели, узнав, что лицо подвергалось ранее уголовному преследованию, из различных учетов в электронном формате, ведущихся правоохранительными и иными государственными органами и учреждениями, либо отказывают в восстановлении на работе, либо предлагают лицу должность, не соизмеримую с прежней. Для эффективной защиты трудовых прав этих участников уголовного процесса необходимы изменения УПК РФ, ТК РФ и иных подзаконных нормативно-правовых актов, позволяющие по заявлению таких лиц изменять на основании постановлений следователя/дознавателя, суда сведения в учетах, ведущихся в цифровом формате по поводу дальнейшей возможности реализации их права на труд.

Список литературы

1. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001. № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. 1). Ст. 4921.

2. О содержании под стражей подозреваемых и обвиняемых в совершении преступлений: Федеральный закон от 15.07.1995 № 103-ФЗ // Законы, кодексы и нормативно-правовые акты Российской Федерации [сайт]. URL: https://legalacts.ru/doc/federalnyi-zakon-ot-15071995-n-103-fz-o

3. Об утверждении Правил внутреннего распорядка следственных изоляторов уголовно-исполнительной системы, Правил внутреннего распорядка исправительных учреждений и Правил внутреннего распорядка исправительных центров уголовно-исполнительной системы: Приказ Минюста России от 04.07.2022 № 110 // Законы, кодексы и нормативно-правовые акты Российской Федерации [сайт]. URL: https://legalacts.ru/doc/prikaz-miniusta-rossii-ot-04072022-n-110-ob-utverzhdenii

4. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // СЗ РФ. 2002. № 1 (ч. 1). Ст. 3 // СПС «Гарант». URL: https://base.garant.ru/10105655/#

5. Постановление Президиума Московского областного суда от 13.10.2004 № 631 по делу № 44г-562/04 (извлечение) // СПС «Гарант». URL: https://base.garant.ru/28941112

6. О порядке и размере возмещения процессуальных издержек, связанных с производством по уголовному делу, издержек в связи с рассмотрением дела арбитражным судом, гражданского дела, административного дела, а также расходов в связи с выполнением требований Конституционного Суда Российской Федерации и о признании утратившими силу некоторых актов Совета Министров РСФСР и Правительства Российской Федерации (вместе с «Положением о возмещении процессуальных издержек, связанных с производством по уголовному делу, издержек в связи с рассмотрением дела арбитражным судом, гражданского дела, административного дела, а также расходов в связи с выполнением требований Конституционного Суда Российской Федерации»): Постановление Правительства РФ от 01.12.2012 № 1240 // СЗ РФ. 2012. № 50 (ч. 6). Ст. 7058.

7. О возмещении ущерба, причиненного гражданину незаконными действиями государственных и общественных организаций, а также должностных лиц при исполнении ими служебных обязанностей: Указ Президиума ВС СССР от 18 мая 1981 г. № 4892-X (утв. Законом СССР от 24 июня 1981 г. № 5156-X) // СПС «Гарант». URL: https://base.garant.ru/10105655

8. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954 // СПС «Гарант». URL: https://base.garant.ru/10105655

Э. Р. Ибатуллина,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Аннотация. В статье анализируются проблемы правового регулирования защиты персональных данных в глобальной сети Интернет, поскольку в постиндустриальном обществе возрос оборот информации, связанный с персональными данными и требующий законодательного урегулирования. Быстрое развитие информационных технологий позволяет иметь доступ к различным данным не только операторам, обслуживающим субъектов персональных данных, но и злоумышленникам. Целью исследования является рассмотрение видов персональных данных и законодательной базы, регулирующей отношения в данной области.

Ключевые слова: персональные данные, информационная безопасность, Интернет, хищение данных, конфиденциальность, файлы-cookie, информационные технологии

PROBLEMS OF LEGAL REGULATION OF PERSONAL DATA PROTECTION ON THE GLOBAL INTERNET

Abstract. This article analyzes the problems of legal regulation of personal data protection on the global Internet, since the number of relations related to personal data requiring legislative regulation has increased in post-industrial society. The rapid development of information technologies allows access to various data not only to operators serving personal data subjects, but also to intruders. The purpose of the study is to consider the types of personal data and the legal framework governing relations in this area.

Keywords: personal data, information security, the Internet, data theft, privacy, cookie files, information technology

В современном мире каждый из нас сталкивается с тем, что выражает согласие на обработку персональных данных, к примеру, при регистрации в социальных сетях, но не все задумываются над тем, для чего это необходимо и где персональные данные хранятся.

Сейчас, в век цифровых технологий, существует большое количество сайтов и социальных сетей, на которых размещены те или иные данные о человеке: имя гражданина, возраст, включая паспортные данные, место проживания и т. д. Вопрос о защищенности данной информации до сих пор остается открытым, поскольку ежедневно сайты в сети Интернет подвергаются атакам со стороны мошенников, использующих полученные данные в корыстных целях, следовательно, персональные данные и вопрос об их защите в глобальной сети и обеспечении информационной безопасности [12] являются актуальными проблемами.

Понятие персональных данных закреплено как в международных источниках права, так и в отечественных. Статья 4 регламента Европейского парламента и Совета Европейского союза 2016/679 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС определяет понятие персональных данных как любую информацию, относящуюся к распознаваемому лицу [7]. Согласно Федеральному закону от 26 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ № 152) [10], к персональным данным относится любая информация по физическому лицу. Статья 2 Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [4] также раскрывает упомянутое выше понятие.

Обобщая, персональные данные – сведения, характеризующие физическое лицо: инициалы, в том числе фамилия, имя и отчество гражданина, дата рождения, профессия, доходы субъекта персональных данных и иная информация, которая относится к этой категории.

Законодатель обращает внимание еще на биометрические персональные данные, и раскрывает их как сведения, указывающие на физиологические и биологические особенности человека, устанавливающие личность. Стоит акцентировать внимание на том, что оператор также использует вышеупомянутый вид для идентификации личности, и обработка данных осуществляется, только если имеется согласие субъекта персональных данных в письменной форме. Важным моментом является, что используются биологические особенности физического лица – дактилоскопическая информация (отпечатки пальцев), изображение радужной оболочки глаза, изображение человека (фото) или его голос и т. д.

Для обработки таких данных, согласно п. 2 ст. 11 ФЗ № 152, необязательным является выражение согласия субъекта персональных данных. Тем самым законодатель акцентирует внимание на этом, ссылаясь на имплементацию международных договоров Российской Федерации о реадмиссии, обязательное проведение дактилоскопии и регистрации ее результатов и в других случаях, предусмотренных законом.

Следует отметить тот факт, что на основании пункта 3 статьи 11 ФЗ № 152, если субъект данных отказывается от обработки биометрических персональных данных, то оператор, допустим банк, не имеет права отказать в обслуживании, если такое согласие обязательным не является.

Однако если субъект персональных данных предоставил документ, удостоверяющий личность, или передал его для последующего сканирования для подтверждения осуществления определенных действий конкретным лицом, или имеется изображение в виде фотографии в личном деле (например, сотрудника) и иные случаи не относятся к биометрическим персональным данным, поскольку информация в дальнейшем для не используется в целях установления личности [5].

Законодатель также уделяет внимание специальным категориям персональных данных, включающим информацию о принадлежности субъекта персональных данных к национальности, расе, о наличии или отсутствии судимости, о состоянии здоровья и т. д.

Следующий вид – персональные данные, на которые есть разрешение от субъекта персональных данных на распространение. К примеру, это сведения, на которые было получено отдельное письменное согласие на обработку для неограниченного круга лиц. Так, согласно статье 10.1 ФЗ № 152, субъект имеет право самостоятельно определять перечень персональных данных для каждого вида, указанного в согласии на обработку персональных данных.

Субъекту также предоставляется возможность установить запрет на обработку разрешенных персональных данных неограниченным кругом лиц, тем самым оператор обязан своевременно информировать таких лиц об изменениях: запретах и условиях.

Конкретное содержание согласия на обработку персональных данных и требования к нему изложены в приказе Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения» [6].

Так, законодатель выделил несколько видов персональных данных, и, согласно статистике больше всего хищений и утечек персональных данных происходит именно в Интернете. К примеру, за 2022 г. в России увеличилась утечка персональных данных и платежной информации в 2,67 раза в сопоставлении с 2021 г., таким образом, число утекших записей составило 667 млн [1]. Насчет этого у экспертов по кибербезопасности есть свои выводы: ценная утекшая информация представляет объем только персональных данных и платежную информацию субъектов персональных данных, в то время как внутренняя информация (коммерческая тайна, проекты, формулы предприятий и компаний) не являются ценной утекшей информацией по сравнению с персональными данными [9].

Так, например, одной из площадок утечки персональных данных являются интернет-магазины, маркетплейсы, на которых большая часть из всех нас зарегистрирована. Как правило, для оплаты заказа изначально создается личный кабинет на сайте или в приложении, на котором отражаются персональные данные покупателя, и затем уже производится оплата товара. Для этого субъекты персональных данных вводят информацию о себе в виде реквизитов банковских карт, контактных данных. Такие сведения злоумышленники могут получить путем взлома личного кабинета потребителя или же базы данных оператора, обслуживающего потребителя.

Помимо этого, основным способом утечки данных являются телефонные звонки от мошенников, представляющихся различными компаниями и операторами, ставя в известность потребителя, что у него появились проблемы, например, с банковским счетом, или, наоборот, делая «выгодное» предложение для потребителя, субъекта персональных данных. Опираясь на вышеупомянутое, информация по субъектам персональных данных из клиентской базы данных была получена незаконным путем третьими лицами.

Несомненно, законодатель регулирует вопрос о защите персональных данных в Интернете, однако отслеживание злоумышленников вызывает определенные

трудности, поскольку преступления в сети Интернет характеризуются зачастую анонимностью исполнителя, латентностью, так как не все жертвы заявляют о фактах мошенничества и утечке данных.

И Уголовный кодекс Российской Федерации (далее – УК РФ) [8] лишь упоминает персональные данные, но отдельного состава преступления и уголовной ответственности за хищение персональных данных не устанавливает. Некоторые авторы полагают, что урегулировать данный вопрос возможно путем введения нормы в УК РФ о похищении конфиденциальной информации, следовательно, для конструктивного применения нормы необходимо правильно обозначить признаки деяния в составе посягательства на персональные данные и общественно опасные последствия, наступающие в результате посягательства [2].

В глобальной сети существует еще одна особенность – файлы-cookie, небольшие текстовые документы, с помощью которых браузер сохраняет информацию о пользователе на компьютере [11]. С помощью таких файлов о пользователе гаджетов можно узнать многое: к примеру, как часто он заходит на тот или иной сайт, последнее время посещения браузера, какую информацию искал в Интернете, товары в корзине в приложении или на сайте. Файлы-cookie могут содержать в себе персональные данные: информацию о владельце гаджета/личного кабинета, к ней относится логин, пароль, электронная почта, информация об устройстве, с которого был выполнен вход на сайт и т. д. [3].

Файлы-cookie – это вид таргетированной рекламы (англ. target – «цель»), которая выстраивается на основании этих файлов, информации, содержащейся в них, предпочтениях пользователя.

Таким образом, Интернет, безусловно, выполняет важную роль в современном мире, однако не стоит забывать об информационной безопасности. Вопрос о безопасности персональных данных в глобальной сети остается открытым, поскольку случаи хищения и утечки персональных данных увеличились, и данная проблема требует решения, необходимо укрепить защиту данных.

Список литературы

1. В России за год утекло более 660 млн записей с персональными данными. URL: https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21 с.

2. Бегишев И. Р., Кирпичников Д. В. Проблемные вопросы уголовно-правовой охраны персональных данных // Уголовная юстиция. 2020. № 15. С. 11–16.

3. Гадельшин А. А., Степанов М. М. Cookie-файлы как объект персональных данных и способ нарушения конфиденциальности персональных данных // Вопросы российской юстиции. 2021. № 16. С. 516–531.

4. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных ETS № 108 от 28 января 1981 г. // СПС «Гарант». URL: https://base.garant.ru/2559798

5. Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28.08.2020 № ЛБ-С-074-24059 «О методических рекомендациях» // СПС «Гарант». URL: https://base.garant.ru/74585566

6. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 г. № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения // СПС «Гарант». URL: https://base.garant.ru/400668442

7. Регламент Европейского парламента и Совета Европейского союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС // СПС «Гарант». URL: https://base.garant.ru/71936226

8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954; Российская газета. 2023. № 413. Ст. 174 (9119).

9. Утеген Д., Рахметов Б. Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 825–844. EDN: DRGDDJ

10. Федеральный закон от 26 июля 2006 года № 152-ФЗ «О персональных данных» // Российская газета. 2006. № 165; 2023. № 29 (8974).

11. Что такое файлы cookies? URL: https://trends.rbc.ru/trends/industry/5f4e8d719a794788d1c8b49f#:~:text=Cookies%20(«куки»%2C%20в%20переводе%20с,товарами%20интересовался%20и%20так%20далее

12. Жарова А. К. Риски информационной безопасности и возможности правового регулирования криптовалюты в России // Информационное право. 2018. № 4. С. 11–16. EDN: YPNFET

Л. Р. Ибрагимова,
студент,
Казанский инновационный университет
имени В. Г. Тимирясова

ВЛИЯНИЕ ПРОЦЕССОВ ЦИФРОВИЗАЦИИ НА ВНУТРИСЕМЕЙНОЕ НАСИЛИЕ

Аннотация. Цель исследования заключается в обосновании корреляции процессов цифровизации на внутрисемейное насилие. В настоящее время цифровизация общества привнесла также и негативные факторы, а именно речь идет про отсутствие должного контроля информации, в том числе про информацию, которая культивирует насилие в семье. В статье рассматривается проблема существования даркнета как площадки для распространения запрещенной информации, которая может побудить либо поспособствовать совершению внутрисемейного насилия. Также затрагивается проблема отсутствия контроля в отношении видеоигр, в которых присутствуют сцены насилия.

Ключевые слова: право, цифровые технологии, процессы цифровизации, внутрисемейное насилие, даркнет, контроль видеоигр

IMPACT OF DIGITALIZATION ON DOMESTIC VIOLENCE

Abstract. The aim of the study is to substantiate the correlation of digitalization processes with domestic violence. At present, the digitalization of society has also introduced negative factors, namely the lack of proper control of information, including information that cultivates domestic violence. The study examines the issue of the existence of the Dark Net as a platform for the dissemination of prohibited information that may cause or contribute to domestic violence. The study also raises the issue of the lack of control over video games that contain violent scenes.

Keywords: law, digital technologies, digitalization processes, domestic violence, dark net, video game control

Актуальность темы исследования обусловлена тем, что в настоящее время процессы цифровизации затрагивают практически все аспекты жизнедеятельности, и, несомненно, существует множество преимуществ от них, но в то же время стоит отметить и негативные стороны данного явления, одной из таковых является отсутствие должного контроля информации со стороны государства. Именно в этой связи создаются благоприятные условия для культивирования насилия, что в конечном итоге отражается на членах семьи.

Наличие даркнета позволяет лицу заполучить доступ к информации, которая может спровоцировать его на насильственное поведение в отношении своих членов семьи, более того на просторах Интернета можно найти множество обсуждений способов совершения преступлений, а также способы сокрытия следов преступления, следовательно, крайне важно предпринимать меры, направленные на борьбу с даркнетом, осуществляя тем самым превенцию внутрисемейного насилия.

Другой проблемой являются наличие большого количества видеоигр, в которых используются сцены насилия, что также может спровоцировать лицо на внутрисемейное насилие, а потому данная область общественных отношений нуждается в особом контроле со стороны государства.

Стоит объективно признать, что проблема внутрисемейного насилия является одной из ключевых в России. Существует множество детерминантов внутрисемейного насилия и одним из таковых является отсутствие должного контроля информации в сети Интернет.

К примеру, в настоящее время существует даркнет – скрытый сегмент Интернета, который доступен с помощью специального браузера. Tor-браузер является одним из самых распространенных, который позволяет получить доступ к даркнету. В результате его использования лицо остается анонимным, а возможность его обнаружения сводится к нулю [3. С. 380].

Именно в даркнете существует множество обсуждений вопросов совершения преступлений, их способов, орудий, сокрытия следов совершения преступления и т. д. Некоторые сайты имеют возможность осуществлять трансляцию, следовательно, могут транслировать факты насилия, совершения различных преступлений, что неизбежно влияет на психику пользователя, который рано или поздно захочет повторить увиденное [1. С. 168].

Следовательно, пользователь даркнета может быть склонен к совершению внутрисемейного насилия, а также может узнать для себя информацию, которая будет ему полезна в ходе совершения преступлений, относящихся к внутрисемейному насилию.

Таким образом, неконтролируемая доступная информация может либо побудить, либо облегчить совершение внутрисемейного насилия. В этой связи крайне важно принимать меры, направленные на борьбу с даркнетом, т. е. речь идет как про блокировку соответствующих форумов, так и про деанонимизацию авторов, которые распространяют соответствующую информацию.

Также для борьбы с даркнетом используют специальные программы для перехвата IP-адресов, сотрудники правоохранительных органов тщательно изучают профиль тех или иных пользователей, пытаются найти определенные ошибки, которые позволят идентифицировать лицо [5. С. 387].

Однако процесс идентификации лица все же характеризуется в таких условиях повышенной сложностью, следовательно, для эффективной борьбы с информацией, которая распространяется в даркнете, необходимо повышать техническую грамотность сотрудников правоохранительных органов.

Стоит также отметить, что блокировка веб-сайтов не всегда может принести желаемый результат, так как в настоящее время практически у каждого человека на телефоне имеется VPN (Virtual Private Network), который позволяет обходить локальные ограничения и оставаться анонимным.

Следовательно, существующие информационные технологии создают препятствия для борьбы с распространением насилия в Интернете, что делает профилактику внутрисемейного насилия крайне затруднительной [2. С. 84].

Другой проблемой является наличие множества видеоигр, которые способствуют пропаганде жестокости и агрессивности. Лицо, которое проводит большое количество времени за такими жестокими видеоиграми, начинает привыкать к использованию насилия для решения возникших проблем, терять связь с реальностью, а потому реализует «игровую механику» в повседневности, где в первую очередь страдают именно члены семьи.

Первое, что необходимо сделать для контроля видеоигр, – вести маркировку по возрасту как для производителей, так и для дистрибьюторов. Маркировка будет означать наличие либо текстового предупреждения (к примеру, «содержит сцены насилия»), либо цифрового (например, «18+»). Маркировка видеоигр уже давно существует во многих государствах, а потому Россия не должна отставать в этом вопросе [4. С. 79].

Стоит отметить, что данная инициатива поступила относительно недавно от Минэкономразвития и направлена на то, чтобы предупредить лицо о наличии элементов насилия и непристойного содержания в том или ином цифровом контенте. На данный момент критерии маркировки все еще разрабатываются, однако крайне важно, чтобы данные требования в действительности соблюдались на практике, а потому необходимо осуществлять контроль со стороны уполномоченных на то государственных органов и привлекать лиц к установленной юридической ответственности в случае нарушения законодательства о маркировке видеоигр.

Помимо прочего, в настоящий момент обсуждается идея создания реестра запрещенных видеоигр. В данный реестр предлагают включать такие видеоигры, которые негативным образом влияют на человека. На наш взгляд, игры с использованием чрезмерного насилия необходимо вносить в такой реестр, чтобы предотвратить появление насилия в семье. Так как игры в основном распространяются на специальных онлайн-платформах (к примеру, Steam), то необходимо осуществлять контроль соблюдения данного требования.

Также необходимо стимулировать российских разработчиков на создание таких видеоигр, которые будут положительным образом влиять на умы людей.

Таким образом, можно сделать следующие выводы.

В ходе исследования было выявлено, что доступ людей к даркнету может спровоцировать внутрисемейное насилие или же облегчить его совершение, а потому государство должно направлять больше усилий на блокировку соответствующих сайтов, на деанонимизацию пользователей, которые распространяют соответствующую информацию. Данные меры должны включать в себя как использование современных информационных технологий, а также обучение сотрудников правоохранительных органов информационно-технической грамотности.

Видеоигры со сценами насилия также могут выступать детерминантами внутрисемейного насилия, а потому предлагается в ближайшее время принять соответствующие поправки в законодательство и ввести маркировку видеоигр. Крайне важно, чтобы данное положение соблюдалось на практике, а потому необходимо осуществлять постоянный контроль и привлечение лиц к установленной юридической ответственности.

Также нами положительно оценивается идея о введении реестра запрещенных игр, т. е. речь идет про блокировку таких игр, которые негативным образом влияют на человека, в том числе речь идет про игры с использованием чрезмерного насилия, что также, несомненно, скажется на профилактике внутрисемейного насилия.

Список литературы

1. Антонян Ю. М. Причины насилия в семье // Пенитенциарная наука. 2020. Т. 14, № 2. С. 167–176.

2. Батюкова В. Е. Насилие в семье. Проблемы и пути решения // Закон и право. 2021. № 1. С. 83–85.

3. Москалева Е. Н. Проблемы противодействия семейному насилию в условиях цифровизации // Юридическая деятельность в условиях цифровизации: сборник статей по результатам Международной научно-практической конференции. Симферополь, 23 марта 2021 г. / под ред. Е. В. Евсиковой, В. С. Тихомаевой. Симферополь: Издательство Типография «Ариал», 2021. С. 378–382.

4. Никандров Н. Д. Цифровизация: потенциал, достижения, риски // Мир психологии. 2021. № 1–2(105). С. 75–88.

5. Шалагин А. Е. Предупреждение преступлений в эпоху цифровизации // Державинские чтения: сборник статей XVI Международной научно-практической конференции. Казань, 23–26 мая 2021 года. М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2021. С. 385–387.

С. С. Иванова,
студент,
Северо-Западный филиал
Российского государственного университета правосудия

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ТЕХНОЛОГИИ 3D-БИОПРИНТИНГА

Аннотация. В статье уделяется внимание такой перспективной цифровой технологии, как 3D-биопринтинг, которая рассматривается как новация. Спрогнозированы отдельные аспекты использования технологии 3D биопринтинга, которые потребуют правового регулирования и закрепления на уровне международных актов и национального законодательства.

Ключевые слова: 3D-биопринтинг, цифровые технологии, медицинское право, правовое регулирование, тканевая инженерия, трансплантационная медицина

PROBLEMS AND PROSPECTS OF TECHNOLOGY DEVELOPMENT 3D BIOPRINTING

Abstract. The article talks about such a promising digital technology as 3D bioprinting, which should be considered as an innovation. The data confirming the importance of its application in the future are given. Certain aspects of the use of 3D bioprinting technology are predicted, which will require legal regulation and consolidation at the level of international acts and national legislations, and may also cause problems when using it.

Keywords: 3D bioprinting, digital technologies, medical law, legal regulation, tissue engineering, transplant medicine

Введение. В современном мире стремительно появляются разнообразные цифровые технологии. Некоторые из них показывают нецелесообразность дальнейшего их развития и использования, другие же становятся полезной и удобной составляющей человеческой жизни.

Одной из таких подающих надежды технологий является 3D-биопринтинг [8]. В пользу его перспективности свидетельствуют данные о состоянии рынка био 3D-печати (на 2022 г. размер рынка 3D-биопринтинга составил 1,5 млрд долларов, а по прогнозам экспертов к 2028 г. этот показатель может составить 4,44 млрд долларов [2]. В развитие технологии заинтересованы компании многих стран (корпорация 3D systems (США), Regemat (Испания), «Энвижн тэк GMBH» (Германия) [2], частная лаборатория 3D Bioprinting Solution (Россия)) [3].

Таким образом, технология 3D-биопринтинга является довольно перспективной цифровой технологией [10], о чем свидетельствует размер рынка био 3D-печати и заинтересованность бизнеса.

Итак, теперь стоит определить, что в современном мире принято вкладывать в данное понятие [9].

Основная часть. 3D-биопринтинг – это технология создания органов и тканей из клеток живого организма при помощи 3D-печати. Данное определение довольно простое, однако позволяет понять, что представляет собой 3D-биопринтинг. Стоит сразу указать: на данном этапе биопринтинг – лишь развивающаяся технология. На темпы ее развития влияют два основных фактора. Во-первых, скорость совершенствования 3D-принтеров, а во-вторых, уровень развития тканевой инженерии. Совершенствование технологии 3D-принтинга на определенном уровне развития коренным образом повлияет на фармакологию, косметологию и, что является целью большинства исследователей в этой сфере, трансплантологию.

Говоря об этом, стоит понимать, что введение технологии 3D-биопринтинга в широкое употребление чревато возникновением огромного количества различных последствий и проблем. Рассмотрим их подробнее.

Для начала следует заметить, что, как уже стало ясно из вышеуказанных данных, в настоящий момент в развитие биопринтных технологий инвестируют лишь крупные частные предприниматели (исключение составляют Соединенные Штаты Америки, где инвестирование в 3D-биопринтинг производится в том числе из бюджета страны), располагающие большим количеством свободных денежных средств, нежели государства.

В то же время правовое регулирование тех или иных процессов и явлений обеспечивается последним, тем более когда речь идет о здоровье населения (главной целью исследователей в данной сфере является печать донорских органов и тканей). Именно государство должно определить виды организаций, которые будут вправе применять данную технологию.

Будет ли 3D-принтинг только в ведении государственных учреждений? Или же вся сфера будет основываться на частном предпринимательстве? Первый вариант довольно маловероятен, так как сейчас рассматриваемая отрасль развивается благодаря частной инициативе. Второй вариант тоже нельзя признать верным, если иметь в виду 3D-печать человеческих органов и тканей и учесть специфику такой деятельности.

Вероятнее всего предположить, что государство и частные предприниматели, иные частные организации будут совмещать и координировать свою деятельность в данной сфере в форме государственно-частного партнерства.

Тем более что известны успешные случаи применения данного подхода в медицинской сфере. Так, к примеру, на данный момент в Российской Федерации «...реализуется около 200 проектов в сфере здравоохранения и санаторно-курортного лечения» [4].

В странах Западной Европы доля государственно-частного партнерства в сфере здравоохранения составляет более 30 %, притом такая форма партнерства широко используется в сфере трансплантационной медицины [4].

Если рассмотреть сферы государственно-частного партнерства в различных странах, то можно прийти к выводу, что в основном это строительство объектов здравоохранения, внедрение информационных технологий, разработка и производство инновационного медицинского оборудования [4].

Но на все это еще только предстоит обратить внимание законодателю. Если же обратиться к действующему законодательству Российской Федерации,

то единственное положение, которое может способствовать формированию правовой базы для применения 3D-биопринтинг в настоящее время, содержится в ст. 14 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»: «К полномочиям федеральных органов государственной власти в сфере охраны здоровья относятся... организация оказания гражданам... специализированной, в том числе высокотехнологичной медицинской помощи» [6].

3D-биопринтинг гипотетически можно отнести к средствам оказания «высокотехнологичной медицинской помощи», однако данный термин никак не раскрыт законодателем, поэтому об официальном признании технологии речи пока еще нет.

Но независимо от того, как распределятся роли между государством и частным предпринимательством, первому все-таки необходимо будет выработать некие требования, которые будут предъявляться к лицам, осуществляющим деятельность в сфере 3D-биопечати. Главной проблемой тут выступит то, что в процессе создания биопринтного органа или ткани задействованы представители различных профессий: начиная от IT-дизайнера и заканчивая генетиком. Уровень профессионализма представителей разных специальностей измеряется по-разному: отличаются критерии и требования.

Существуют и более существенные вопросы. К примеру, кто будет нести ответственность, если изготовленная биопринтная ткань или орган будут ненадлежащего качества? Генетик, под руководством которого делились клетки, образуя материал для печати, IT-дизайнер, спроектировавший 3D-модель на компьютере, изготовитель 3D-принтера, на котором был напечатан орган, хирург, непосредственно трансплантировавший биопринтное изделие?

Готового ответа у человечества нет, так как до сих пор с подобными проблемами мы не сталкивались. Но из этого основного вопроса вытекает другой, дополнительный. Какой биопринтный орган и какую биопринтную ткань можно считать надлежащего качества, а какую нет? Для решения этой проблемы нужно определить критерии, которым должны будут соответствовать орган или ткань, изготовленные с использованием технологии 3D-биопринтинга.

Но важно не только законодательно определить, кто будет нести ответственность, но и стоит учесть сложности с установлением этапа создания биопринтного органа или ткани, на котором произошел сбой: из-за многоэтапности процесса изготовления биопринтных изделий почти невозможно определить, когда что-то пошло неправильно. Если это не было замечено сразу, то по готовому органу определить этап, на котором произошел сбой, нельзя. Вероятно, когда подобная проблема потребует непосредственного решения, критерии, которым должен соответствовать орган или ткань на каждом этапе, будут определены. Будет также найдена форма контроля за соблюдением требований к биопринтным изделиям.

Следующим важным аспектом станет то, что биопринтные ткани и органы требуют привлечения значительных финансовых вложений. В связи с этим в ближайшие десятилетия они вынужденно будут объектами купли-продажи. В большинстве государств по понятным причинам торговля органами и тканями человека запрещена.

Поэтому во многих государствах необходимо будет внести поправки в законодательство и сделать исключение для биопринтных органов. Если говорить о России, то в нашей стране предусмотрена уголовная ответственность за торговлю людьми «с целью изъятия... органов или тканей» [5], а не за торговлю органами или тканями вообще, также уголовная ответственность за убийство «...в целях использования органов или тканей потерпевшего» [5], но биопринтных изделий это никак не коснется.

В ст. 15 Закона «О трансплантологиии органов и (или) тканей человека» установлен запрет для медицинских организаций на продажу «...органов и (или) тканей у трупа» [7]. В настоящий момент это фактически единственный способ получения биоматериала для трансплантации, но позднее, когда будет возможна торговля органами или тканями, которые не были изъяты у человека, а напечатаны, это положение не будет создавать препятствий для признания биопринтных органов объектом купли-продажи. Более того, «действие настоящего закона не распространяется на препараты и пересадочные материалы, для приготовления которых использованы тканевые компоненты» [7]. Для создания биопринтных изделий используются клетки живого организма, а не органы или ткани, изъятые у трупа. Поэтому логично предположить, что запрет на продажу на напечатанные органы не распространяется. И это главнейшее из многочисленных преимуществ 3D-биопринтинга перед трансплантологией.

А в пока еще далекой перспективе, когда технология создание биопринтных органов и тканей станет более дешевым, человечество получит все шансы минимизировать такую глобальную проблему, как торговля людьми, с целью изъятия у них органов или тканей, так как этот вид деятельности станет неприбыльным.

Более того, биопринтные органы и ткани обладают еще одним важным свойством. Основой для них служит, в зависимости от технологии, группа клеток или готовая ткань, которые выращивают из родных клеток живого организма того, для кого создается орган. Поэтому в отличие от донорских органов и тканей биопринтные не вызывают отторжения.

Итак, для успешного использования 3D-биопринтинга в дальнейшем необходимо признать органы и ткани, изготовленные по указанной технологии, объектами гражданско-правовых отношений, но лишь до тех пор, пока они не были трансплантированы человеку.

И, наконец, возникает еще один довольно важный вопрос: как будет осуществляться взаимодействие участников создания биопринтных изделий, выполняющих определенные задачи на разных этапах. Будут ли это различные организации, заключившие между собой договоры или все этапы, будут осуществляться в одной и той же организации?

Если допустить последний вариант, то все работы должны будут осуществляться в медицинских учреждениях, так как трансплантация готового органа или ткани может проводиться только в таких учреждениях, и тогда появятся необычные должности типа IT-дизайнера, специалиста по 3D-принтерам и т. д.

На данный вопрос пока ответить довольно сложно. Наверное, это можно будет узнать лишь тогда, когда 3D-биопринтинг прочно войдет в повседневную жизнь.

Скорее всего, один из названных вариантов начнет превалировать. Какой именно – сказать сейчас сложно. Поэтому этот аспект нельзя однозначно считать ни недостатком, ни достоинством 3D-биопринтинга.

Заключение. Таким образом, можно сделать вывод, что, хотя пока ни в одном государстве 3D-биопринтинг не был отражен в праве, однако многие крупные частные предприятия уже инвестируют в развитие данной технологии. В будущем технология должна получить правовое обоснование и регулирование своего использования. Отсутствие последних может привести к бесконтрольному использованию 3D-биопринтинга, что чревато новыми проблемами.

Список литературы

1. Об основах охраны здоровья граждан в Российской Федерации: ФЗ от 21.11.2011 № 323-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_121895

2. Обзор отчета о рынке 3D биопечати. URL: stratviewresearch.com/2070/3D-bioprinting-Market.html

3. Токарев Б. Е., Токарев Р. Б. Анализ рыночных перспектив технологий 3D-биопечати // Науковедение. 2016. Т. 8, № 2. С. 9. URL: cyberleninka.ru

4. Тощенко В. Государственно-частное партнерство: роль, формы и сферы использования – социальные последствия экономического кризиса в России. 2009. 34 с. URL: Cyberlenenka.ru

5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699

6. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства Российской Федерации. 2011. № 48. Ст. 6724.

7. Закон Российской Федерации от 22 декабря 1992 г. № 4180-I «О трансплантации органов и (или) тканей человека // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. № 2. Ст. 62.

8. Шутова А. А. Регулирование и охрана отношений в сфере биопринтных технологий. М.: Проспект, 2022. 104 с. EDN: RQFNTB

9. Шутова А. Юридико-терминологический анализ понятия «3D-биопринтинг» // Юрислингвистика. 2022. № 26(37). С. 40–47. EDN: ZWLZLS

10. Шутова А. А. 3D-биопринтинг: этико-правовой аспект // Безопасность бизнеса. 2022. № 4. С. 60–64. EDN: UFQOGU

А. Д. Кирилова,
студент,
Вологодский государственный университет

ВНЕДРЕНИЕ DATA MATRIX НА ВСЕ КАТЕГОРИИ ТОВАРА

Аннотация. В статье представлены основные характеристики и особенности цифровой маркировки, основания внедрения Data Matrix (двумерного матричного штрихкода) на все категории товаров, суть которых заключается в том, что для каждого товара генерируется персональный код, устойчивый к фальсификации. Задачей персонального кода является увеличение собираемости налогов за счет прозрачности бизнеса, со стороны потребителя будет уверенность в качестве товара и его подлинности.

Ключевые слова: матрица данных, налоговые поступления, фальсификация, система «Честный знак», контрафакт, кодирование данных, двухмерный код

IMPLEMENTATION OF DATA MATRIX FOR ALL CATEGORIES OF GOODS

Abstract. Consider the implementation of Data Matrix for all categories of goods in the Vologda region. The bottom line is that for each product a personal code is generated that is resistant to falsification. The task of the two-dimensional code is to increase the collection of taxes, due to the transparency of the business, the consumer will be confident in the quality of the product and its authenticity. The article also presents the main characteristics and features of digital marking.

Keywords: data matrix, tax revenues, falsification, “Honest Sign” system, counterfeit, data coding, two-dimensional code

В настоящее время актуален вопрос маркировки товара. Начиная с 2018 г. в России начали использовать Data Matrix, активное использование началось с 2022 г. и по сей день, с каждым годом обхват товаров увеличивается. Маркировка товара позволяет избавиться от контрафакта, поддержать отечественных производителей и увеличить собираемость налогов в бюджет.

Data Matrix – это двумерный матричный штрихкод, который состоит из черно-белых элементов, представлен в форме квадрата или прямоугольника, размещенного в прямоугольной или квадратной группе. Data Matrix предназначен для кодирования данных, созданный код является уникальным, подделать его невозможно. Data Matrix состоит из кода идентификации (в нем содержатся данные о товаре) и кода проверки (обеспечивает защиту от копирования). Чаще всего в промышленности и торговле применяются битовые матрицы, кодирующие от нескольких байт до 2 килобайт данных. В России Data Matrix активно используют в виде наклейки на определенном виде товара. При производстве товаров код наносится один раз. Уникальный штрихкод служит сокращению теневой экономики, увеличению налоговых поступлений, борьбы с контрафактом и позволяет отследить местонахождение товара.

Data Matrix код представляет собой уникальный ключ к информации о товаре в базе данных системы «Честный знак» [1. С. 16]. «Честный знак» – это единая национальная система цифровой маркировки и прослеживания товаров. Специальный цифровой код гарантирует подлинность и качество товара. Основная задача системы – повышение уровня безопасности россиян, борьба с контрафактом и некачественными аналогами [2]. Основные преимущества: надежность, простота использования, широкий перечень товаров, доступность.

Разберем на примере вариант, когда отсутствует маркировка на товаре, предположим гражданка А в магазине Б решила приобрести товары для ремонта на большую сумму, кассир магазина выдал гражданке А чек, который не ушел на платформу фискальные данные (ОФД). Кассир магазина в свою очередь договаривается с организацией В, что готов пробить чек на большую сумму, данную сумму организация отразит у себя на затратах, кассир получит вознаграждение за проделанные манипуляции. В этом случае государство недополучит налоговых поступлений.

Таким образом, маркировка товаров положительно повлияет на производителей, потребителей, бюджет государства. Увеличатся налоговые поступления в бюджет, бизнес станет прозрачнее, произойдет легализация рынка, что повлечет увеличение выручки легальных производителей, потребитель будет уверен в качестве товара. В итоге следует отметить, что необходимо внедрить Data Matrix на все категории товара.

Список литературы

1. Холбан О. Цифровая маркировка товара как защита от контрафакта // Тенденции развития науки и образования. 2020. № 61–6. С. 15–18. DOI: 10.18411/lj-05-2020-110. EDN: LVAMVP

2. Бочаров Д. И. Механизмы налогового стимулирования малого инновационного предпринимательства в России и за рубежом: проблемы и перспективы // Экономика и бизнес: теория и практика. 2021. № 10-1(80). С. 47–51.

А. В. Козлов,
студент,
Российский университет дружбы народов
имени Патриса Лумумбы

ОСОБЕННОСТИ ЦИФРОВИЗАЦИИ АДМИНИСТРАТИВНОГО ПРАВА В СФЕРЕ ОКАЗАНИЯ ПОМОЩИ НЕСОВЕРШЕННОЛЕТНИМ

Аннотация. Одной из тревожащих проблем Российской Федерации является снижение рождаемости у населения. Помощь государства в данном вопросе нашла свое отражение в мерах административного характера с применением механизмов цифровизации. Статья раскрывает ведущие государственные меры, направленные на сохранение, рождение детей, их благополучие. Социальная защита

выражена в материальных благах и органах, имеющих здравоохранительный характер (фондах), которые стимулируют семьи России на рождение новых граждан. Рассматриваются виды государственной помощи и способы их получения.

Ключевые слова: государство, цифровизация, фонд, семья, документы, несовершеннолетние, социальная политика

PECULIARITIES OF DIGITALIZATION OF ADMINISTRATIVE LAW IN THE SPHERE OF ASSISTANCE TO NON-ADULTS

Abstract. One of the alarming problems of the Russian Federation is childbearing. The article reveals the leading state measures aimed at the preservation, birth of children and their well-being. Social protection is expressed in material benefits and bodies having a health character (funds), which stimulate Russian families to give birth to new citizens. Types of state aid and ways of their reception are disclosed.

Keywords: state, digitalization, fund, family, documents, minors, social policy

Цифровизация административного права является одним из ключевых направлений развития современного общества. Она позволяет ускорить и упростить процесс оказания помощи несовершеннолетним, повысить качество и доступность государственных услуг, а также улучшить контроль за соблюдением законодательства.

Одной из особенностей цифровизации в административном праве является использование электронных баз данных и информационных систем, которые позволяют автоматизировать процесс сбора, обработки и анализа данных о несовершеннолетних. Это дает возможность сократить время на обработку запросов и ускорить процесс принятия решений. Наиболее актуальным выразителем данной мысли выступит Комиссия по делам несовершеннолетних и защите их прав как в субъектах Федерации, так и в органах местного самоуправления, цифровизация данных структур помогла их более корректной работе благодаря большей систематизации данных, направленных на контроль и профилактику детской преступности и безнадзорности.

Кроме того, цифровизация позволяет улучшить качество оказания помощи несовершеннолетним. Например, использование электронных форм заявлений и онлайн-сервисов для записи на прием к специалистам позволяет избежать очередей и сократить время ожидания. Мы видим данное применение, например, в Тульской области, где при поддержке министерства здравоохранения была разработана техническая программа «Доктор 71», упрощающая получение медицинских услуг у любого профильного специалиста, более того, мы видим развивающийся функционал возможностей, направленный на улучшение сервиса и получение дополнительных возможностей. Также возможно использование онлайн-консультаций и видеосвязи для оказания помощи несовершеннолетним на расстоянии, примером этого может выступать телемедицина [3], в частности, мы можем отметить реализацию данной технологии в местах Крайнего Севера или труднодоступных территорий, данные технологии помогают избежать проблем со здоровьем и не допустить развития тяжелых заболеваний.

Не стоит забывать о том, что в особом внимании со стороны государства нуждаются дети, имеющие тяжелые заболевания, в том числе врожденные. Для сбора средств на лечение тяжелобольных детей в соответствии с Указом Президента Российской Федерации был основан фонд «Круг добра» [7], его основополагающей целью выступает исполнение расширенных методов выполнения и бюджетирования при оказании медицинской помощи детям с тяжелыми заболеваниями, которые могут угрожать жизни и здоровью ребенка. Государство зарегистрировало 44 таких заболевания и взяло на себя обязательство обеспечения больных детей медикаментозными средствами и средствами индивидуальной мобильности, в том числе не имеющими официального разрешения на использование в России, а также техническими средствами, направленными на реабилитацию детей. Все это стало возможно благодаря созданию цифровых баз данных, в которых хранится информация о заболеваниях.

Заявление в Фонд для получения оперативной помощи при условии согласования у лечащего врача необходимо подать через Единый портал государственных услуг, более того, также через региональный орган управления здравоохранением. В последнем случае орган здравоохранения совместно с медицинской организацией собирает необходимый комплект документов, формирует заявку и направляет ее в Фонд. Ответ Фонда можно узнать как у сотрудников регионального органа управления здравоохранением, через который было подано заявление [2], так и по информационной телефонной линии, где можно также получить информацию по вопросам консультации врачей, назначения лечения и лекарственных препаратов. Заявителю, кроме того, приходит уведомительное письмо с решением Фонда. Ответ может быть также вывешен на сайте Фонда в разделе отработанных заявлений.

Кроме того, Фонд организует услуги народной поддержки по сбору пожертвований. Не все одобряют сбор средств населения на лечение детей, полагая, что государство обязано обеспечивать защиту здоровья своего народа, как это закреплено Конституцией Российской Федерации. Однако народную помощь и милосердие трудно переоценить, ведь они способствуют единению людей вокруг ценностей, значимых не только для государства, но и для общества.

Социальная государственная политика отражена также в системе социальных пособий, предусмотренных в Федеральном законе «О государственных пособиях гражданам, имеющим детей» [4], в нее входят различные социальные гарантии начиная многообразными выплатами и заканчивая помощью в получении различных льгот.

Наша страна ввела понятные механизмы назначения и выплаты различных пособий. Так, в соответствии с Постановлением Правительства Российской Федерации от 2022 г. № 2330, право на это пособие появляется, если размер дохода семьи не выше величины прожиточного минимума, действующего в субъекте Российской Федерации по месту жительства или фактического проживания заявителя [1]. Заявления на получение ежемесячной выплаты рассматривает Фонд пенсионного и социального страхования РФ и выплачивает ее за счет средств бюджета субъекта Федерации. Сам прожиточный минимум устанавливается

согласно ФЗ № 134 от 1997 г., исходя из потребностей людей в каждом конкретном субъекте [5].

Вся необходимая информация и критерии применения для получения материальной поддержки семьям сформированы в ФЗ № 44 от 2003 г. Так, расчет необходимого уровня дохода производится из таких условий, как доход на одного человека, среднее количество человек в семье и наличие имущества. Временной критерий допускает изучение вышеуказанной информации за три месяца. Отдельно отметим, что в учет дохода будет зачтено и получение прибыли от бизнеса или ведения подсобного хозяйства. При всем выше сказанном, обязательно отметим, что общая денежная сумма рассчитывается до уплаты необходимых налогов [6].

Также необходимо учитывать, что при цифровизации необходимо обеспечить безопасность данных несовершеннолетних, конфиденциальность и защиту их прав и интересов. Для этого необходимо использовать соответствующие меры защиты и контроля, а также обучать специалистов правилам работы с электронными базами данных.

В целом цифровизация административного права имеет множество преимуществ, но также требует тщательного планирования и контроля. В сфере оказания помощи несовершеннолетним имеется множество преимуществ и потенциала для улучшения качества услуг. Однако необходимо проводить систематический мониторинг и анализ результатов внедрения цифровых технологий, чтобы учесть потребности и особенности каждого несовершеннолетнего и обеспечить полноценное участие их и их родителей в процессе оказания помощи.

Список литературы

1. Постановление Правительства Российской Федерации от 16.12.2022 № 2330 «О порядке назначения и выплаты ежемесячного пособия в связи с рождением и воспитанием ребенка» // СЗ РФ. 2022. № 52. Ст. 9602.

2. Указ Президента Российской Федерации от 05.01.2021 № 16 «О создании Фонда поддержки детей с тяжелыми жизнеугрожающими и хроническими заболеваниями, в том числе редкими (орфанными) заболеваниями, «Круг добра» // СЗ РФ. 2023. № 73.

3. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ccf02734a76e335943ae86f86b319d6035cca374

4. Федеральный закон от 19.05.1995 № 81-ФЗ «О государственных пособиях гражданам, имеющим детей» // СЗ РФ. 1995. № 21. Ст. 1929.

5. Федеральный закон от 24.10.1997 № 134-ФЗ «О прожиточном минимуме в Российской Федерации» // СПС КонсультантПлюс.

6. Федеральный закон от 05.04.2003 № 44-ФЗ «О порядке учета доходов и расчета среднедушевого дохода семьи и дохода одиноко проживающего гражданина для признания их малоимущими и оказания им государственной социальной помощи» // СЗ РФ. 07.04.2003. № 14. Ст. 1257.

7. Фонд «Круг добра». URL: https://фондкругдобра.рф

В. В. Колупаева,
студент,
Томский университет систем управления и радиоэлектроники

ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Аннотация. Статья посвящена изучению процесса внедрения цифровых технологий в практику работы государственных органов, выявлению основных проблем, препятствующих процессу их эффективного применения как со стороны населения, так и в деятельности должностных лиц, которые используют их при выполнении своих должностных обязанностей. Выявлена суть понятия «государственное управление», а также характеристики отдельных видов технологий, применяемых в государственном управлении.

Ключевые слова: управление, государственное управление, цифровые технологии, цифровизация, государственные услуги, портал государственных услуг Российской Федерации, Центр государственных и муниципальных услуг, база данных

THE USE OF DIGITAL TECHNOLOGIES IN PUBLIC ADMINISTRATION

Abstract. The article is devoted to the study of the process of introducing digital technologies into the practice of government agencies, identifying the main problems that hinder the process of their effective application both by the population and in the activities of officials who use them in the performance of their official duties. The essence of the concept of “public administration” is revealed, as well as the characteristics of certain types of technologies used in public administration.

Keywords: management, public administration, digital technologies, digitalization, public services, portal of public services of the Russian Federation, Center of State and Municipal Services, database

В наше время многие области жизни дошли до цифрового мира, и, конечно, государственное управление не стало исключением. На данный момент цифровизация не завершена в государственном управлении, в связи с этим возникают определенные проблемы, но и цифровые технологии не стоят на месте и постоянно совершенствуются. Чтобы раскрыть сущность темы необходимо понять, что значит «государственное управление». Обратимся к Федеральному закону «О стратегическом планировании в Российской Федерации», в котором регламентировано, что государственное управление – деятельность органов государственной власти по реализации своих полномочий в сфере социально-экономического развития Российской Федерации и обеспечения национальной безопасности Российской Федерации [3].

Развитие цифровых технологий в современном мире приводит к повышению интереса [2] и увеличению возможностей для повышения эффективности деятельности государственных органов, что проявляется в двух основных аспектах [10].

С одной стороны, их активное внедрение в государственное управление, связанное с появлением автоматизированных справочных систем, справочно-правовых систем упрощает профессиональную деятельность, предоставляя государственным служащим дополнительные инструменты по поиску, обобщению правовой информации, обмену данными, обращением в судебные органы и т. д. Благодаря современным информационным технологиям государственные служащие могут не только оперативно получать актуальные сведения, но и имеют возможность быстро отыскать статические данные, без которых иногда невозможно обойтись при решении разных вопросов. С другой стороны, цифровизация государственного управления позволяет населению получать сведения о деятельности государственных органов, делая ее более прозрачной и открытой.

Повышению эффективности профессиональной деятельности государственных служащих способствует совершенствование компьютерной техники, программного обеспечения, улучшение автоматизированной системы обработки информации, электронных баз, работы справочно-правовых и экспертных систем, а также бурное развитие разнообразных телекоммуникационных сетей, в том числе Интернет.

Российская Федерация на современном этапе, следуя прогрессивному направлению развития цифровых технологий, стремится к тому, чтобы повысить эффективность государственного управления. Цифровизация в сфере государственного управления позволяет с помощью онлайн-инструментов (электронная подпись, электронный документооборот и др.) упростить взаимодействие государства и граждан. В частности, это можно увидеть на примере развития сервиса для быстрого оказания помощи при обращении граждан в государственные органы.

Внедрение технологий делает государственное и муниципальное управление более открытым. На сайтах субъектов размещаются отчеты о проделанной работе, что делает деятельность государственных органов прозрачнее, а следовательно, доверие к работе органов власти у граждан будет возрастать. Например, если зайти на официальный сайт Правительства Российской Федерации и перейти во вкладку «Отчеты», то там можно увидеть все итоги деятельности данного органа. На сайте есть возможность посмотреть все отчеты: ежемесячные, ежегодные. На официальном сайте Администрации города Санкт-Петербурга, как пример государственного управления на региональном уровне, тоже есть возможность посмотреть отчеты должностных лиц, например, отчет губернатора, доклад уполномоченного по правам человека и т. д. [6].

Значимость процесса внедрения цифровых технологий способствует увеличению вовлеченности граждан и заинтересованности к реализации своих прав на управление государством. Так, если зайти на официальный сайт Президента Российской Федерации, есть возможность отправить обращение Президенту в форме электронного документа [11]. Такой документ может быть написан в форме жалобы, просьбы, предложения или пожелания. Данная функция полезна тем, что позволяет поднять важные темы, привлечь внимание к насущным вопросам, что впоследствии приведет к конструктивному обсуждению и их решению.

На официальных сайтах субъектов Российской Федерации тоже есть возможность обращения граждан онлайн по какому-либо вопросу. Рассмотрим на примере Томской области. На официальном интернет-портале Администрации Томской области есть раздел «Открытый регион», где необходимо выбрать «Обращение граждан» [5]. В данной вкладке каждый гражданин имеет возможность ознакомиться с общей информацией об отправке обращения в форме электронного документа, отправить письмо губернатору онлайн, записаться на личный прием. На официальном сайте есть возможность изучить аналитический обзор обращений граждан. Данные публикуются с 2011 г. Если рассматривать аналитический обзор каждого года об обращениях граждан, поступивших в Администрацию Томской области, то количество поступивших обращений каждый год менялось – то увеличивалось, то уменьшалось, например, в 2020 г. общее количество обращений составляло 11 316 обращений, в 2022 г. – 10 093 обращения. Впервые электронное обращение граждан в Администрацию Томской области упоминается в 2014 г. Далее ежегодно увеличивалась доля таких обращений, и сокращалась доля письменных обращений.

Рассмотрим конкретные цифровые технологии, которые используются в государственном управлении. Часто используемым электронным ресурсом является портал государственных услуг Российской Федерации. На Госуслугах предоставляются разнообразные услуги для граждан. Например, из раздела «Справки, выписки» человек может заказать справку об отсутствии судимости, которая необходима при устройстве на работу (это облегчает жизнь гражданам, так как можно получить данную услугу, не выходя из дома); или у гражданки Российской Федерации родился ребенок в 2020 году, и ей предоставляется право получения материнского капитала за первого ребенка. Чтобы подтвердить данное право и иметь возможность им воспользоваться, то необходимо получить сертификат на материнский капитал, который можно оформить в электронном виде. Далее в течение пяти дней сертификат оформляет Социальный фонд, а электронный сертификат загружается в личный кабинет родителя на портале Госуслуг. В разделе «Штрафы, долги» есть возможность узнать о штрафах и оплатить их. При оплате штрафа банки передают информацию в систему государственных платежей, чтобы ведомство смогло зафиксировать оплату штрафа. Если штраф оплачивается через Госуслуги, то он автоматически перенесется из списка штрафов к оплате в список платежей. Информация о передаче данных об оплате в систему государственных платежей появится в личном кабинете [8].

Рассмотрим, как используется сайт Центра государственных и муниципальных услуг (МФЦ) в государственном управлении. Например, онлайн можно получить услугу «государственный кадастровый учет недвижимого имущества и (или) государственной регистрации прав на недвижимое имущество». На сайте есть возможность ознакомиться со всей нужной информацией: стоимостью услуги, какое ведомство занимается данной услугой, перечнем необходимых документов, какие основания для отказа в оказании данной услуги.

Однако, несмотря на значимость цифровизации государственного управления, можно выделить ряд проблем, которые препятствуют процессу. В первую

очередь речь идет о цифровой неграмотности значительной части населения страны. Это связано с проблемами недостаточного уровня владения техникой, сведениями об информационных ресурсах, что зачастую усугубляется самим несовершенством используемых технологий. Некоторые граждане совсем оказываются изолированными от цифровизации по причине отсутствия компьютера, сенсорных телефонов и Интернета. Из данной ситуации можно найти выход. Например, для той части населения, которая не умеет пользоваться компьютерами и телефонами, организовать обучение. Объяснить, как устроены официальные сайты, как и где найти необходимую информацию, каким способом оформить государственную услугу онлайн. В России с 2014 г. запустили обучение по компьютерной грамотности. Изначально был формат пособия, дальше проводили вебинары с подробным объяснением и очное обучение в компьютерных классах [1]. Также некоторые люди старшего поколения не хотят подключать Интернет из-за его стоимости, так как она не оправдает его использования. В среднем мобильный Интернет стоит от 500 рублей. В таком случае можно разработать специальный тариф, где Интернета в месяц будет хватать на посещение официальных сайтов (например, Президента, Правительства, области, города и т. д.), на использование Госуслуг, а стоимость такого тарифа не будет превышать 300 рублей.

Еще одна проблема цифровизации государственного управления – ее малоразвитость. Если зайти на официальные сайты, например, Томской области и Алтайского края, то очень сложно что-либо найти [7]. Отчеты вовремя не публикуются, интерфейс неудобен. На официальном сайте Алтайского края не удалось найти вкладку с отчетами, только через «поиск». Но даже через «поиск» предоставилось возможным изучить отчеты только до 2016 года, за последующие года никаких результатов о деятельности не имеется. Если рассмотреть официальный сайт Томской области, то выявлено неполное соответствие Федеральному закону «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [4]. Например, на сайте не найдена информация о состоянии защиты населения и территории от чрезвычайных ситуаций и принятых по обеспечению их безопасности, и не найдена информация о результатах проверок, проведенных государственным органом, его территориальными органами, органом местного самоуправления (статья 13 пункты 4, 5). Решение в данной ситуации может быть только одно: необходимо задуматься о том, чтобы увеличить штат сотрудников, в функции которых будет входить развитие сайта. Кроме этого, следует прислушиваться к мнениям пользователей путем проведения общественного опроса на тему о том, какие функции они хотели бы видеть на сайте.

Когда речь идет о цифровом мире остро стоит вопрос о кибербезопасности. В таких реалиях всегда есть вероятность хакерских атак и киберпреступлений. Слаборазвитая кибербезопасность приведет, во-первых, к утечке и изменению конфиденциальных данных, которые обрабатывают государственные структуры (паспортные данные граждан, данные налогоплательщиков и др.). Во-вторых, угроза кибератак. Такое явление может привести к нарушению работы государственных систем и служб. В целях снижения уровня угрозы утечки информации или иными проявлениями противоправной деятельности государственным

структурам необходимо предусмотреть ряд дополнительных мер, в том числе использование различных цифровых кодов, расширения сферы применения электронных подписей, канальных шифратов и т. д. Перечисленные меры позволят обеспечить безопасность процессу создания, хранения, накопления и обработки информации, что является одной из важнейших задач применения цифровых технологий в государственном управлении. Таким образом, главная задача при использовании цифровых технологий в государственном управлении – это обеспечение кибербезопасности.

В заключение следует отметить, что в нашем мире уже невозможно не пользоваться цифровыми технологиями, они глубоко проникли в нашу жизнь. Технологии очень облегчают сферу государственного управления, так как увеличивают эффективность работы государственных органов, гражданам проще получить необходимую для них услугу, сокращается сложность в обработке большого количества бумажных документов, увеличивается прозрачность работы государственных структур, несмотря на имеющиеся проблемы.

Список литературы

1. Азбука интернета. URL: https://www.company.rt.ru/social/programms/education/azbuka/?utm_campaign=3263c6717bdb01612ec27ee797047662&utm_source=admitad&utm_content=442763

2. Интересы в механизме публичной власти: проблемы теории и практики: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2023.

3. О стратегическом планировании в Российской Федерации: Федеральный закон от 28.06.2014 № 172-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=439977&dst=1000000001&cacheid=18EBCCD39A8424E30F4B214694CD6DA7&mode=splus

4. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=422007&dst=0&edition=etD&rnd=vCKhPoTqOk1roE5w#XsThPoTaRIMDP1XF

5. Официальный интернет-портал Администрации Томской области. URL: https://tomsk.gov.ru

6. Официальный сайт Администрации Санкт-Петербурга. URL: https://www.gov.spb.ru

7. Официальный сайт Алтайского края. URL: https://www.altairegion22.ru

8. Портал государственных услуг Российской Федерации. URL: https://www.gosuslugi.ru

9. Портал Правительство Российской Федерации. URL: http://government.ru/activities

10. Правовое управление в кризисных ситуациях: монография / С. Б. Бальхаева, Х. И. Гаджиев, С. А. Грачева и др.; отв. ред. Ю. А. Тихомиров. М.: Проспект, 2022.

11. Президент России. URL: http://www.kremlin.ru

К. К. Косовская,
студент,
Сибирский федеральный университет
Д. Д. Долгозвягов,
студент,
Сибирский федеральный университет
Г. А. Тихонов,
студент,
Сибирский федеральный университет

МЕЖГОСУДАРСТВЕННОЕ УПРАВЛЕНИЕ КИБЕРПРОСТРАНСТВОМ: ВОПРОСЫ ПРАВА И КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ КРИЗИСА

Аннотация. В статье обозначаются современные проблемы, порождаемые стремительным развитием информационно-коммуникационных технологий и киберпространства. Рассматривается уже существующий ландшафт международного права и степень, в которой оно обеспечивает самостоятельный механизм регулирования в киберпространстве. Исследуются три ключевых индикатора кризиса, отражающихся в области международного права кибербезопасности. Особое внимание уделяется нормотворческим инициативам по данным вопросам. Утверждается, что формирующийся свод необязательных норм представляет собой критическое окно возможностей для возвращения государствам центральной правотворческой позиции.

Ключевые слова: цифровые технологии, кибербезопасность, управление, международное право, международные нормы, цифровая экономика, атрибуция

INTER-STATE GOVERNANCE OF CYBERSPACE: ISSUES OF LAW AND CYBERBUSSECURITY IN A CRISIS

Abstract. The article examines the contemporary challenges posed by the rapid development of information and communication technologies and cyberspace. It examines the already existing landscape of international law and the extent to which it provides an independent regulatory mechanism in cyberspace. Three key indicators of crisis reflected in the field of international cybersecurity law are explored. Particular attention is paid to normative initiatives on these issues. It is argued that the emerging body of non-binding norms represents a critical window of opportunity for states to regain a central lawmaking position.

Keywords: digital technology, cybersecurity, governance, international law, international norms, digital economy, attribution

В контексте международного права правовые нормы устанавливают общие границы приемлемого поведения в международных отношениях, сохраняя при этом важное пространство для маневра, усмотрения и переговоров. Чтобы очертить эту зону свободы для государств и других международных акторов в отношении нового явления международного значения, необходимо идентифицировать,

интерпретировать и применять к нему соответствующие правовые нормы. Киберпространство в широком понимании является именно таким явлением. Важно отметить, что использование и злоупотребление этим сложным виртуальным пространством без границ затрагивают жизненно важные интересы государства в физическом мире, включая национальную безопасность, общественную безопасность или экономическое развитие. Таким образом, киберпространство выходит далеко за пределы внутренних дел любого государства.

Эксперты (GGE), учрежденные Генеральной Ассамблеей Организации Объединенных Наций (ООН). На тот момент в группу входили представители 15 государств – членов ООН, включая три «кибер-сверхдержавы»: Китай, Россию и США. Таким образом, ее позицию можно рассматривать как подтверждение общего понимания в международном сообществе.

Выделяются индикаторы очевидного кризиса международного права. Во-первых, сфера кибербезопасности, которая сопротивляется кодификации применимых правил в рамках всеобъемлющего многостороннего соглашения. Во-вторых, государства, которые не вносят свой вклад в разработку международных правил, специфичных для кибербезопасности. Было бы неверно утверждать, что государства полностью отказались от установления стандартов. Наиболее отчетливо эту тенденцию можно увидеть в контексте работы ГПЭ ООН. Эксперты (GGE), учрежденные Генеральной Ассамблеей Организации Объединенных Наций (ООН). На тот момент в группу входили представители 15 государств – членов ООН, включая три киберсверхдержавы: Китай, Россию и США.

В своем последнем отчете группа декларировала преимущества «добровольные, необязательные нормы ответственного поведения государства». В докладе утверждается, что такие нормы предотвращают конфликты в киберпространстве, способствуют международному развитию и снижают риски для международного мира и безопасности. В отчете также рекомендовано 11 норм.

В совокупности эти показатели обозначают тенденцию отхода от создания юридических норм международного права в классическом понимании. Вместо разработки обязательных договоров или обычных норм государства прибегают к нормативной деятельности, выходящей за рамки традиционного международного права. В теории права это явление описывается как «плюрализация международного нормотворчества», которое характеризуется наблюдением, что «лишь ограниченная часть осуществления публичной власти на международном уровне в настоящее время материализуется в создание норм, которые можно считать международно-правовыми нормами в соответствии с классическим пониманием международного права». Чтобы понять, какое влияние эта ситуация оказывает на международно-правовое регулирование кибербезопасности, нам следует немного отойти от масштаба и рассмотреть более широкий контекст существующего международного права. Отсутствие системы норм международного права, специфичной для кибербезопасности, не означает, что не существует правовых норм, применимых к кибердеятельности.

В дополнение к этим общепримениым нормам международного права относятся: устав Международного союза электросвязи 1992 г.; Будапештская конвенция

2001 г. о киберпреступности и протокол от 2006 г. о ксенофобии и расизме; соглашение по информационной безопасности Шанхайской организации сотрудничества 2009 г.; конвенция Африканского союза по кибербезопасности 2014 г.

Безусловно, перечисленные международные соглашения важны, но они регулируют лишь небольшую часть деятельности, связанной с киберпространством. Кроме того, могут иметь очень ограниченное членство – шесть государств, в случае соглашения Шанхайской организации сотрудничества, и ни одного в конвенции Африканского союза. Проблема усугубляется тем, что цифровая революция совпала с очередным обострением геополитической ситуации, одним из проявлений которого являются так называемые цифровые войны.

Таким образом, хотя киберпространство не является беззаконной территорией, находящейся вне досягаемости международного права, на данный момент не существует сложного регуляторного механизма, который способен обеспечить стабильную кибердеятельность государств. Более того, государства, похоже, неохотно участвуют в развитии и интерпретации международного права, применимого к кибербезопасности.

Переходя к анализу международно-правовых механизмов обеспечения цифровой безопасности, следует отметить, что среди важнейших угроз выделяется высокий уровень зависимости России в сфере цифровых технологий, обусловленный преимущественно полупериферийным характером отечественной экономики. Однако Россия обладает мощным научным потенциалом, что позволяет надеяться на то, что перспективы создания суверенного сегмента Интернета вполне реальны. Формальным правовым основанием для такого вывода является принятие ряда специальных нормативных актов, направленных на обеспечение безопасности отечественного сектора Интернета. Базовым актом является Закон о суверенном Интернете.

Следует отметить, что эксперты обоснованно утверждают, что одним из ключевых факторов обеспечения долгосрочной международной стабильности в условиях становления и быстрого развития современного цифрового общества является формирование режима коллективной ответственности в сфере функционирования глобальной сети Интернет [1–4]. Однако экономически развитые страны на сегодняшний день проводят политику поляризации международной безопасности. Для обеспечения международной стабильности необходимо создание международно-правовых механизмов, позволяющих защищать суверенные права государств на регулирование информационного пространства, в том числе в национальном сегменте Интернета.

Специальными актами постсоветских стран являются Конвенция о преступности в сфере компьютерной информации и Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. Следует отметить, что позиция Российской Федерации в отношении Конвенции о преступлениях в сфере компьютерной информации испытывала определенные колебания. Российская Федерация подписала этот документ, но затем отозвала его, поскольку в конвенции содержатся положения, которые можно считать нарушением суверенитета государства.

Международное право кибербезопасности сегодня находится на критическом этапе. Нерешительность государств в отношении участия в разработке и применении международного права привела к возникновению вакуума власти, способствующего появлению негосударственных нормотворческих инициатив. Однако говорить о кризисной ситуации было бы преждевременно. В ближайшие несколько лет станет понятно, увидим ли мы постепенный упадок межгосударственного управления киберпространством или фундаментальную перекалибровку правовых подходов, когда государства снова займут центральное место [5–6].

Среди важнейших угроз для страны можно выделить высокий уровень зависимости России в сфере цифровых технологий. Эта зависимость обусловлена, главным образом, полупериферийным характером отечественной экономики. В связи с этим существует уязвимость информационной инфраструктуры, кибертерроризм, кибершпионаж и вмешательство во внутренние дела других стран, которое может осуществляться посредством неправомерного использования информационных и коммуникационных технологий.

В настоящее время идет процесс создания международно-правового механизма обеспечения цифровой безопасности. Основные контуры архитектуры обозначены главным образом в региональных актах. Тем не менее подавляющее большинство универсальных актов носит рекомендательный характер. Следовательно, не существует универсального международно-правового механизма, который мог бы обеспечить безопасность в цифровой сфере.

Учитывая тот факт, что международные отношения вступают в очередную фазу острой конфронтации, нельзя ожидать ее разрешения в обозримом будущем. В связи с этим России необходимо разработать и принять свою стратегию цифровой безопасности. Она должна включать в себя меры по снижению зависимости от иностранных технологий и разработке отечественных аналогов, а также усиление мер по защите информационной инфраструктуры и борьбе с киберугрозами.

Список литературы

1. Bulyga R. P. Business audit: issues of theory and methodology / / Innovative development of the economy. 2011. 2(3). Pp. 113–155.

2. Dai J., Vasarhelyi M. A. Toward Blockchain-Based Accounting and Assurance // Journal of Information Systems/ 2017. 31(3). Pp. 5–21.

3. Kubo M. Is the International Law of Cyber Security in Crisis? // 8th International Conference on Cyber Conflict. NATO CCD COE Publications. 2016. 8(2). Pp. 127–139.

4. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672.

5. Правовое управление в кризисных ситуациях: монография / С. Б. Бальхаева, Х. И. Гаджиев, С. А. Грачева и др.; отв. ред. Ю. А. Тихомиров; М.: Проспект, 2022.

6. Интересы в механизме публичной власти: проблемы теории и практики: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2023.

А. В. Криушина,
курсант,
Московский университет Министерства внутренних дел
Российской Федерации
имени В. Я. Кикотя

СМАРТ-КОНТРАКТ И ЭЛЕКТРОННАЯ СДЕЛКА: СООТНОШЕНИЕ ПОНЯТИЙ

Аннотация. Целью исследования являются выявление и анализ существенных различий между понятиями «электронная сделка» и «смарт-контракт», определение возможности их соотношения друг с другом. Особое внимание обращается на схожесть данных категорий в части недостаточной теоретической и законодательной проработанности. Рассматриваются такие особенности смарт-контракта, как содержание, возможное отсутствие юридической силы, необходимость в привлечении специалиста, автоматизированный характер, трудности восприятия пользователями и др. Делается вывод о невозможности причисления смарт-контракта ни к одному из видов сделки и предлагается выделять его исключительно как новый способ исполнения обязательств.

Ключевые слова: смарт-контракт, электронная сделка, цифровые технологии, программный код, договор, обязательство, автоматизация, юридическая сила

SMART CONTRACT AND ELECTRONIC TRANSACTION: THE RELATIONSHIP OF CONCEPTS

Abstract. The purpose of this article is to identify and analyze significant differences between the concepts of “electronic transaction” and “smart contract”, to determine the possibility of their relationship with each other. The author pays special attention to the similarity of these categories in terms of insufficient theoretical and legislative elaboration. Considering such features of a smart contract as the content, possible lack of legal force, the need to involve a specialist, automated nature, difficulties of perception by users, etc., the author comes to the conclusion that it is impossible to classify a smart contract to any type of transaction and proposes to single it out exclusively as a new way of fulfilling obligations.

Keywords: smart contract, electronic transaction, digital technologies, program code, contract, obligation, automation, legal force

В науке и практике с большой периодичностью употребляются понятия «смарт-контракт», «электронный контракт», «электронный договор» и т. п. В настоящее время их трактовка вызывает значительные трудности, поскольку все они охватывают отношения в рамках информационной среды и не нашли своего закрепления в действующем законодательстве.

Сейчас большую актуальность приобретает вопрос сущности смарт-контракта как юридического факта, а именно возможность его сопоставления с электронной сделкой: соотносятся ли они как целое и часть, как составная часть и целое,

либо вообще не сопоставимы друг с другом. В связи с этим предлагается более детальное рассмотрение сущности и отличительных признаков смарт-контрактов в сравнении с некоторыми особенностями электронных сделок.

Смарт-контрактом является «криптографический договор, непосредственно находящийся в цепочке блоков блокчейн, подкрепленный автоматизированным исполнением условий договора за счет данной технологии» [9. С. 2292–2293]. В. С. Рухтина отмечает, что их использование расширяется и является особенно эффективным при периодическом заключении однородных соглашений, не требующих существенных изменений, к каким можно отнести договоры аренды или поставки. Примером являются автоматизированные «торговые операции между оператором авиатопливного бизнеса Газпромнефть-Аэро и S7 Airlines с Альфабанком» [6. С. 410].

Действующее законодательство не закрепляет понятие смарт-контракта, его правовой режим и место в системе способов исполнения обязательств. Однако, опираясь на опыт применения смарт-контрактов, можно выделить основные признаки, отличающие их от смежных определений:

– заключение в форме письменного кода;

– заключение с использованием технологии блокчейн;

– оплата встречного предоставления цифровым финансовым активом;

– самостоятельное и автоматизированное исполнение обязательств [4. С. 27].

Ориентируясь на суждения, приводимые Л. Г. Ефимовой [3. С. 129], электронную сделку можно охарактеризовать как особую, заключаемую субъектами в простой письменной форме категорию гражданско-правовой сделки с помощью электронных или других технических средств при возможности воспроизвести впоследствии ее содержание на материальном носителе, а также достоверно определить контрагентов.

Д. А. Турицын разделяет смарт-контракты в соответствии с наличием юридической силы. Он признает фактическое существование не имеющих юридической силы контрактов, объясняя это отсутствием их направленности на приобретение юридической силы и на осуществление контроля за взаимодействием вступающих в правоотношения субъектов. Таким образом, автор говорит о «действительном выражении договорного соглашения» как об исключительной прерогативе тех смарт-контрактов, которые обладают юридической силой [8. С. 225]. Именно это и определяет одно из отличий смарт-контракта от электронной сделки, условием признания недействительности которой является нарушение установленных гражданским законодательством требований о соблюдении формы, прав и интересов иных лиц и др., в то время как некоторые категории смарт-контрактов изначально не имеют установок на контроль деятельности сторон, оформленный юридически.

Значительные различия можно выявить в структуре содержания сравниваемых единиц. Следует учитывать, что смарт-контракт имеет форму, которая, как правило, не является привычной и понятной простым пользователям. Если рассматривать строение смарт-контрактов в соотношении с электронными сделками, то говорить о его соотношении с электронной сделкой как общего

и входящего в него частного не представляется возможным по причине того, что и в смарт-контракте допустимо отсутствие положений, имеющихся в обычном договоре. Согласимся с позицией Турицына, связывающего такое отсутствие не столько со слабой технической проработанностью смарт-контрактов, выраженной в невозможности включения аспектов, «которые неявно подразумеваются в договоре», сколько с отсутствием в этом объективной необходимости или нежелательностью автоматизации таких составляющих сделки [8. С. 226].

В качестве еще одной отличительной особенности создания смарт-контрактов можно выделить то, что в силу сложной технической составляющей и неясности механизмов их функционирования, а также трудностей при создании, расшифровке и проведении иных манипуляций с программными кодами сторонам в обязательном порядке требуется привлечение компетентного специалиста, который должен обеспечить техническую сторону проводимых действий. При этом, как отмечает В. М. Камалян, привлекаемое лицо несет ответственность сугубо за неправильное составление смарт-контракта, т. е. неисполнение либо ненадлежащее исполнение им каких-либо действий, связанных с объективной необходимостью обеспечения соответствия «текста договора программному коду (содержанию смарт-контракта)» [5. С. 35]. Следовательно, можно установить, что такое лицо не обязано обладать юридическими знаниями и владеть юридической техникой, поскольку ответственности за содержание заключаемого соглашения в области грамотного выражения волеизъявления сторон специалист рассматриваемой категории не несет.

Таким образом, участие специалиста в составлении смарт-контракта является отличительным от электронной сделки признаком, поскольку создание электронной сделки (как многосторонней, так и односторонней) может быть свободно осуществлено и без участия третьих лиц, вовлечение которых в процесс заключения и исполнения электронной сделки носит диспозитивный характер и подлежит урегулированию преимущественно за счет волеизъявления сторон. Автор считает, что роль «специалиста» как при заключении электронных сделок, так и при составлении смарт-контрактов достаточно велика, потому что именно на данную категорию участников гражданских правоотношений возложена ответственность технического обеспечения необходимых в рамках соглашений процессов, при неграмотном подходе к которому возникают существенные риски неверной интерпретации содержания сделки или контракта, что неминуемо повлечет искажение реальных интересов сторон, а также значительные трудности при доказывании в рамках процессуальной деятельности. В связи с этим предлагается закрепить в виде отдельной статьи либо пункта статьи в главе 9 Гражданского кодекса Российской Федерации [2] положения, выделяющие специалистов в качестве отдельной категории участников при заключении сделок, регламентирующие его основные права, обязанности и ответственность за ненадлежащее исполнение возложенных функций. Предполагается, что специалист не будет принадлежать к какой-либо из сторон сделки, а будет независимым лицом, которое может приглашаться любой из сторон по взаимному согласию или назначаться соответствующими органами или должностными лицами (если, например,

в качестве стороны выступает публично-правовое образование, казенное предприятие или учреждение).

И, наконец, ключевым отличием рассматриваемых объектов является то, что при заключении сделки (как в устной, так и в простой письменной или электронной форме) требования по соблюдению содержащихся в ней условий и исполнения соответствующих обязательств возлагаются непосредственно на конкретных участников, когда смарт-контракт предполагает автоматизированный способ исполнения обязательств без какого-либо вовлечения сторон. А. Я. Ахмедов раскрывает действие данного механизма следующим образом: при наступлении определенных, заранее установленных участниками обстоятельств «программный код обеспечивает автоматизированное последовательное совершение действий, направленных на исполнение обязательств» [1. С. 149–150]. В связи с этим логичным является возникновение вопроса относительно ответственности при некачественном исполнении обязательств или их неисполнении вообще. Так, А. И. Савельев считает, что именно действия должника будут являться ядром понятия «обязательство», что делает вопрос исполнения обязательств за счет автоматизации неактуальным, так как «все параметры исполнения уже заранее и однозначным образом определены в программном коде» [7. С. 32–34]. Следовательно, каждое действие, производимое программным кодом, изначально будет являться «надлежащим» в силу отсутствия возможности участников и третьих лиц каким-либо образом повлиять на установленную последовательность компьютерных операций.

Итак, сопоставив понятия «электронная сделка» и «смарт-контракт» путем рассмотрения ключевых особенностей смарт-контракта относительно осуществляемой в рамках электронных сделок деятельности, можно заключить, что данные понятия, несмотря обязательное применение специальных технических средств и механизмов, не являются тождественными по причине наличия ряда факторов, совокупность которых не является исчерпывающей. Правовой режим смарт-контрактов не стал объектом официального толкования и признан предметом многочисленных дискуссий. Кроме того, в отличие от электронных сделок, заключаемых практически повсеместно, смарт-контракты имеют несколько ограниченный круг лиц из-за более сложной процедуры пользования и отсутствия понимания механизмов их функционирования значительной долей пользователей.

Рассуждая о дискуссионности вопроса касательно соотношения смарт-контракта с электронной сделкой по причине множества существенных различий между ними, автор согласился с позицией А. И. Савельева, который не причисляет смарт-контракт ни к одному из видов сделки, а воспринимает его исключительно как новый способ исполнения обязательств. На формирование данной точки зрения оказал влияние существенный довод данного ученого об отсутствии волевого компонента сторон при автоматизированном исполнении обязательства, что в корне противоречит сущности гражданско-правовой сделки, которая практически полностью основана на реализации волеизъявления участников.

Список литературы

1. Ахмедов А. Я. К вопросу о признаках смарт-контракта // Правовая политика и правовая жизнь. 2020. № 2. С. 146–154.
2. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // Российская газета. № 238–239. 1994.
3. Ефимова Л. Г. Еще раз о понятии и правовой природе электронной формы сделки // Совершенствование законодательства. 2019. № 8(153). С. 129–137.
4. Ефимова Л. Г., Сиземова О. Б. Правовая природа смарт-контракта // Банковское право. 2019. № 1. С. 21–28.
5. Камалян В. М. Правовые риски использования цифровых технологий в банковской деятельности // Актуальные проблемы российского права. 2019. № 9. С. 32–39.
6. Рухтина В. С. Эдектронная форма сделки // Вопросы российской юстиции. 2022. № 17. С. 406–413.
7. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32–59.
8. Турицын Д. А. К вопросу о форме автоматизированных цифровых контрактов в современном договорном праве: электронные контракты и смарт-контракты // Право и практика. 2019. № 4. С. 224–228.
9. Christidis K., Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things // IEEE Access. 2016. № 6. Pp. 2292–2293.

О. В. Кротикова,
студент,
Международный юридический институт

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРЕДОСТАВЛЕНИЯ ГОСУДАРСТВЕННЫХ И МУНИЦИПАЛЬНЫХ УСЛУГ В СФЕРЕ ГРАЖДАНСКО-ПРАВОВОЙ ПОДДЕРЖКИ МНОГОДЕТНЫХ СЕМЕЙ

Аннотация. В статье рассмотрены правовые основы реализации и поэтапного внедрения информационных систем автоматизации процесса оказания государственных и муниципальных услуг в рамках осуществления государственных программ помощи многодетным семьям. Обозначены ключевые фазы перехода оказания мер социальной поддержки муниципалитетами указанной категории граждан на цифровые услуги. Проанализированы центральные проекты, функционирующие в настоящий момент при помощи цифровых технологий.

Ключевые слова: цифровизация, цифровые платформы, межведомственный информационный обмен, проактивное обращение, идентификация, аутентификация, авторизация

DIGITAL TRANSFORMATION OF THE LEGAL REGULATION OF THE PROVISION OF STATE AND MUNICIPAL SERVICES IN THE FIELD OF CIVIL LEGAL SUPPORT FOR LARGE FAMILIES

Abstract. In this article, we have investigated the legal basis for the use and phased implementation of information systems for automating the processes of providing state and municipal services within the framework of the implementation of state assistance programs for large families. The key phases of the transition of the provision of social support measures by municipalities of this category of citizens to digital services are outlined. The central projects currently being implemented with the help of digital technologies are analyzed.

Keywords: digitalization, digital platforms, interdepartmental information exchange, digital code, proactive appeal, identification, authentication, authorization

В настоящий момент в условиях формирования единого информационного цифрового пространства в стране [5] наиболее важно, на наш взгляд, сформировать действенный механизм правового регулирования предоставления государственных и муниципальных услуг [14]. В первую очередь предлагается обратить внимание на нормативно-правовую базу социальных служб, призванных обеспечить качественный уровень социальной поддержки наиболее уязвимой категории граждан, а именно многодетных семей [16. С. 56-58].

Внедрение цифровых технологий в системы государственного управления в Российской Федерации началось с момента разработки концепции административной реформы [6] во исполнение распоряжения Правительства РФ [9], в рамках обеспечения механизмов доступности, экстерриториальности и проактивности еще с 2006 года. Вышеуказанные меры по внедрению цифровых информационных технологий имели своей целью:

– сокращение непрофильных направлений,

– повышение узконаправленных специалистов путем обеспечения межведомственного информационного обмена между органами власти без участия заявителя,

– перевод предоставления государственных и муниципальных услуг в электронный вид.

Несмотря на то, что мероприятия по трансформации подходов к предоставлению государственных и муниципальных услуг начались еще с 2007 г. [8] с появлением первых экспериментальных многофункциональных центров (МФЦ), а также с создания интернет-портала www.gosuslugi.ru в 2009 году, но до принятия ФЗ № 210 [2] единых стандартов указанный правовой институт в себе не содержал [1]. Данным ФЗ были закреплены такие дефиниции, как «государственные услуги», «муниципальные услуги», «портал государственных и муниципальных услуг», «межведомственное информационное взаимодействие», а также «многофункциональный центр» (МФЦ). Первый же подмосковный офис «Мои документы» открылся в Балашихе все в том же 2009 году.

Следующим важным этапом цифровизации государственного и муниципального управления в рамках межведомственного взаимодействия явилось создание

единой системы идентификации и аутентификации (ЕСИА) [7], функциями которой законодатель установил идентификацию, аутентификацию, авторизацию участников, органов и организаций информационного взаимодействия.

Единые нормы, регламентирующие порядок, форму, сроки предоставления электронных услуг федеральной государственной информационной системой «Единый портал государственных и муниципальных услуг», порталов государственных и муниципальных услуг субъектов РФ, официальных сайтов органов государственной власти и органов местного самоуправления, установлены Постановлением Правительства в 2016 г. [9].

Реализуемая в настоящий момент Правительством Московской области государственная программа «Цифровое Подмосковье» [11], являющаяся обеспечивающей подпрограммой государственной программы «Цифровая экономика РФ» [11] в рамках федерального проекта «Цифровое государственное управление», направлена на снижение административных барьеров, повышение качества и доступности предоставления государственных и муниципальных услуг [15. С. 46–75], в том числе на базе МФЦ с целью развития информационной и технической инфраструктуры экосистемы цифровой экономики Московской области.

Таким образом, МФЦ становится площадкой-посредником между заявителем и ведомственной структурой, управомоченной государством на предоставление конкретных государственных и муниципальных услуг. В настоящий момент в рамках исполнения Концепции Правительства РФ [13] реализуется поэтапный переход к предоставлению абсолютного большинства государственных и муниципальных массово социально значимых услуг в режим 24/7 без личного присутствия граждан. Реализация указанной законодательной нормы осуществляется на базе основных органов исполнительной власти и государственных внебюджетных фондов [12], таких как Росреестр, Федеральная миграционная служба России, МВД России, Федеральная налоговая служба, Пенсионный фонд РФ, ФССП России, Росимущество, Роспотребнадзор. Однако практика реализации в ходе интеграции ведомственных баз данных в единую систему продемонстрировала существующие недочеты при реализации инициативы, связанные, прежде всего, с недостаточной информированностью особенностей правового регулирования данного относительно нового для России правового института. В этой связи услуги Росреестра, ФМС России и МВД России были исключены из обязательного списка.

Наиболее удачной оказалась оптимизация муниципальных и госуслуг по двум направлениям: моносервисы (отдельные виды муниципальных и госуслуг) и суперсервисы (комплексы услуг) [18. С. 64–72]. Безусловное удобство для многодетных семей здесь представляет комплексный запрос, учитывающий жизненную ситуацию и индивидуальные особые потребности заявителя. Будь то юридически значимые, материально-вещественные либо информационные действия.

В паспорте федерального проекта «Цифровое государственное управление» [14], помимо ключевых показателей, обозначены и обязательные характеристики суперсервисов, это и типизация (стандартизация) услуг, реестровая модель, многоканальность, проактивность, экстерриториальность, машиночитаемое описание

процесса оказания услуг, а также исключение участия человека из процесса принятия решений. Каждый суперсервис предполагает тестовый режим работы непосредственно перед внедрением, имеет свои сроки внедрения и, в соответствии с вышеуказанным проектом, к концу 2024 г. все 25 суперсервисов должны выполнять свои функции в полном объеме. В связи с чем законодателем активно формируются цифровые административные регламенты предоставления муниципальных и госуслуг.

Данная законодательная новация видится нам спорной в связи с недостаточностью нормативного обеспечения реализации принципа проактивности, его противоречивостью в отношении основного заявительного принципа предоставления государственных и муниципальных услуг, отличающего его тем самым от услуг гражданско-правовых. Помимо прочего, в установлении ст. 7.3 ФЗ № 210 [2] беззаявительной формы предоставления муниципальных и госуслуг нами усматривается попытка «размывания» основных категорий законодательства о предоставлении государственных и муниципальных услуг, закрепление законодателем «правового дуализма».

Вместе с тем нельзя не отметить примеры положительного опыта по реализации проактивного режима предоставления налоговых льгот, вычетов (в соответствии со ст. 391 НК РФ), государственного и регионального сертификата на материнский капитал (на основании сведений ФГИС «ЕГР ЗАГС» [10]).

С другой стороны, практикой применения измененных норм ФЗ № 104 [3] был сформирован прецедент повсеместного применения нового подхода к осуществлению социальных выплат в проактивной форме, что в большинстве случаев на практике стало приводить к множественным коллизиям.

Кроме того, реализация принципа проактивности вступает в противоречие с принципом неприкосновенности частной жизни, нарушая тем самым конституционные права граждан.

Не менее противоречивым этапом цифрового развития оказания государственных и муниципальных услуг представляется создание единого федерального информационного регистра (ЕФИР) граждан РФ, иностранных граждан и лиц без гражданства, проживающих на территории РФ, а также граждан РФ, проживающих на территории других государств [4], сформированного на основе записи актов гражданского состояния, в соответствии с чем будет сформирован эталонный цифровой профиль гражданина.

В связи с тем, что реализация государственной семейной политики в отношении многодетных семей – многосубъектная деятельность с участием и федеральных, и органов власти субъектов, и органов местного самоуправления [13], цифровая трансформация социальных услуг видится нам довольно положительной новеллой, имеет долгосрочные перспективы.

Таким образом, процесс цифровизации сферы государственных и муниципальных услуг явился продолжением концепции формирования сервисного государства [17. С. 189–192], где особое значение придается формированию высокого уровня удовлетворения граждан качеством государственных и муниципальных услуг, в том числе путем реализации различных механизмов административно-правовой и гражданско-правовой направленности.

Список литературы

1. Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // СЗ РФ. 2003. № 40. Ст. 3822.

2. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // СЗ РФ. 2010. № 31. Ст. 4179.

3. Федеральный закон от 01.04.2020 № 104-ФЗ «Об особенностях исчисления пособий по временной нетрудоспособности и осуществления ежемесячных выплат в связи с рождением (усыновлением) первого или второго ребенка» // СЗ РФ. 2020. № 14. Ст. 2034.

4. Федеральный закон от 08.06.2020 № 168-ФЗ «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» // СЗ РФ. 2020. № 24. Ст. 3742.

5. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901.

6. Постановление Правительства РФ от 16.05.2011 № 373 «О разработке и утверждении административных регламентов осуществления государственного контроля (надзора) и административных регламентов предоставления государственных услуг» // СЗ РФ. 2011. № 22. Ст. 3169.

7. Постановление Правительства РФ 28.11.2011 № 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // СЗ РФ. 2011. № 49 (V). Ст. 7284.

8. Постановление Правительства РФ от 15.04.2014 № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество» // СЗ РФ. 2014. № 18 (часть II). Ст. 2159.

9. Постановление Правительства РФ от 26.03.2016 № 236 «О требованиях к предоставлению в электронной форме государственных и муниципальных услуг // СПС «Гарант». URL: https://base.garant.ru/71362988

10. Постановление Правления ПФР от 31.05.2019 № 312 п «Об утверждении Административного регламента предоставления Пенсионным фондом Российской Федерации и его территориальными органами государственной услуги по выдаче государственного сертификата на материнский (семейный) капитал» // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335192/

11. Постановление Правительства Московской области от 04.10.2022 № 1059/35 «О досрочном прекращении реализации государственной программы Московской области «Цифровое Подмосковье» на 2018-2024 годы и утверждении государственной программы Московской области «Цифровое Подмосковье» на 2023-2030 годы» // СПС «Гарант». URL: https://base.garant.ru/405853523

12. Распоряжение Правительства РФ от 25.10.2005 № 1789-р «О концепции административной реформы в Российской Федерации в 2006–2010 годах» (утративший силу) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_56259

13. Распоряжение Правительства РФ от 11.04.2022 № 837-р «О концепции перехода к предоставлению 24 часа в сутки 7 дней в неделю абсолютного большинства государственных и муниципальных услуг без необходимости личного присутствия граждан» // СЗ РФ. 2022. № 17. Ст. 2941.

14. Цифровое государственное управление: паспорт федерального проекта (утв. Президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28.05.2019 № 9) // СПС «Гарант». URL: https://base.garant.ru/72302270

15. Бит-Шабо И. В. Современные тенденции развития законодательства зарубежных государств и направления совершенствования финансовой сферы социального обеспечения в Российской Федерации в сфере деятельности государственных социальных внебюджетных фондов // Труды кафедры финансового права российского государственного университета правосудия: сборник научных трудов / под ред. И. А. Цинделиани. М.: Проспект, 2019. С. 46–75.

16. Олейник С. А., Чмеленко И. А. Государственные и муниципальные образования как участники гражданских правоотношений // Журнал Закон и власть. 2020. № 2. С. 56–58.

17. Лозовой М. М. Понятие государственных (муниципальных) услуг (работ), оказываемых (выполняемых) государственными, муниципальными учреждениями // Вестник экономики, права и социологии. 2016. № 2. С. 189–192.

18. Организация предоставления государственных и муниципальных услуг: учеб. пособие / под ред. С. Н. Костиной. М-во науки и высш. образования Рос. Федерации, Урал. федер. ун-т. Екатеринбург: Изд-во Урал. ун-та, 2019. 128 с.

А. В. Кулагина,
студент,
Московский государственный университет
имени М. В. Ломоносова

ОЦЕНКА РАБОТНИКОВ С ПОМОЩЬЮ АЛГОРИТМОВ

Аннотация. В статье рассматриваются актуальные тенденции оценки персонала при помощи алгоритмов и автоматизированных систем. Обсуждается возможная эффективность и результативность таких мер и их соотношение с требованиями законодательства об уважении частной жизни. Отдельно отмечается проблема «непрозрачности», эффект «черного ящика», предвзятость алгоритмов и способы их решения. Описаны примеры применения алгоритмов в России и зарубежных странах. Даны рекомендации по постепенному повсеместному внедрению алгоритмов и автоматизированных систем во многие области производства.

Ключевые слова: оценка работников, алгоритм, квалификация, критерии оценки, наблюдение, непрозрачность, тестирование

EMPLOYEE EVALUATION USING ALGORITHMS

Abstract. The article adresses the latest trends in personnel evaluation by means of algorithms and automated systems. It discusses the possible effectiveness and efficiency of such measures and their correlation with the requirements of legislation on respect for privacy. The problem of "non-transparency", "black box" effect, bias of algorithms and ways of solving such conflicts are separately noted. The author describes actual examples of algorithms application in Russia and foreign countries and gives recommendations for gradual widespread implementation in many areas of production.

Keywords: employee evaluation, algorithm, qualification, evaluation criteria, observation, non-transparency, testing

Как алгоритмизация может влиять на поведение людей и оценивать его? Каким образом она упрощает систему оценки и наблюдения за рабочей деятельностью? Такими вопросами уже давно задаются специалисты, занимающиеся внедрением алгоритмов в рабочий процесс. В литературе, посвященной управлению алгоритмами в гиг-экономике, выделяют пять функций, в отношении которых технология может поддерживать управленческий контроль: наблюдение за трудовым процессом, сбор данных для оценки производительности, автоматическое принятие решений, автоматизированные системы обмена сообщениями и архитектура цифрового выбора [10. P. 1049]. Новую модель управления работниками концептуализировали в понятии «алгократии» (algocracy).

Нестабильная экономическая ситуация приводит к тому, что профессиональные и квалификационные требования к работникам возросли, тем самым делая вопрос автоматизирования и сокращения участия человека в оценке персонала все более актуальным [5. С. 354]. Что же касается оценки работников, то под этим термином принято понимать «комплекс мероприятий по выявлению профессиональных, деловых и индивидуально-типологических качеств работника» [1. С. 82]. Иными словами, это процесс, в ходе которого отдельные специалисты и руководители обсуждают результаты работы сотрудников, их производительность и развитие, а также поддержку, в которой они нуждаются в своей работе. Она также используется для оценки результатов работы за определенный период времени и позволяет сосредоточиться на будущих целях, возможностях и необходимых ресурсах [17]. Стоит отметить, что оценка персонала не закреплена Трудовым кодексом РФ, следовательно, по ее результатам к сотруднику не может быть применено дисциплинарное взыскание или понижение в должности. Она дает возможность определить соответствие сотрудника занимаемой им должности, выявить слабые и сильные стороны работников, выявить наиболее перспективных сотрудников, сформировать квалифицированный кадровый резерв. Не менее важным аспектом достоверной оценки персонала представляется

грамотное финансирование и распределение бюджета предприятия на обучение сотрудников, что обеспечивает компании достойный уровень конкурентоспособности [7. С. 90]. Алгоритмизированная система оценки позволяет вести мониторинг как за отдельным сотрудником, так и за штатом в целом.

В самом общем виде структуру оценки можно представить так: определение критериев оценки, этап непосредственной оценки работников, анализ результатов и принятие по ним управленческих решений. Алгоритмизация в значительной степени упрощает работу руководителя или менеджера по персоналу в силу автоматического сбора данных, безошибочной обработки и качественных подсчетов, когда вероятность возникновения человеческого фактора растет пропорционально скорости исполнения задач [2. С. 75]. Алгоритмы также сокращают время, затрачиваемое на подготовку документов, обеспечивают структурированное отображение результатов, избавляют от бумажной волокиты.

В пользу все большего использования алгоритмических механизмов говорят также статистические данные. Так, по данным опроса Forbes, из 350 российских и международных компаний, работающих как внутри страны, так и за ее пределами, наем новых сотрудников в 2023 г. планируют 58 % компаний. Годом ранее этот показатель был 81 % [6]. Из чего следует логичный вывод, что первоочередной задачей становятся сохранение полезных и продуктивных сотрудников и углубленное развитие программ горизонтальной мобильности. На первое место выдвигается оценка индивидуальных способностей, потенциала роста, ориентации на достижение результата, гибкости в поведении и мышлении, развитии творческого потенциала и иных мероприятий, для стимулирования деятельности перспективных сотрудников, повышения их квалификации и др.

Наиболее распространенные алгоритмы оценки персонала подразделяются на два вида: оценку компетенций и оценку результативности. Под первой понимается оценка знаний и умений сотрудника, способность применять их в нестандартных и стрессовых ситуациях, к примеру, работнику дают ситуационное задание и ожидают наиболее соответствующее его должности исполнение. Второй метод – оценка результативности – основан на сравнении показателей работы конкретного сотрудника с запланированными для данного периода работы и должности показателями.

В оценочные мероприятия также зачастую входят: своевременное проведение аттестации, быстрое исправление недоработок, оперативный контроль, установление единых критериев оценивания деятельности, ранжирование сотрудников по полученным результатам [9. С. 142]. Наиболее часто применяемые критерии оценки: профессиональные (опыт, квалификация), деловые (дисциплина, организованность), морально-психологические (стрессоустойчивость), специфические (черты характера, отношение в коллективе). На данный момент функционируют следующие системы алгоритмической оценки работников, например, StartExam. Эта система основывается на методе «360 градусов», включающем в себя различные тестирования, анкетирования, мониторинг продуктивности работы, времени использования компьютера [16]. Тесты автоматизированы, т. е. предоставляются и проверяются алгоритмом. А до полной автоматизации интервью еще далеко,

так как на данный момент есть неустранимые несовершенства алгоритмов по распознаванию и обработке голоса и речи.

Интересно, что оценку работника проводят не только специалисты, но и все его окружение – непосредственный руководитель и коллеги [4]. При этом критерии оценки должны соответствовать здравому смыслу и ценностям компании. Цели для каждой должности должны находиться в согласованности с целями других должностей и политикой компании в целом, поскольку получаемые данные непосредственным образом отражаются на благополучии компании. Так, например, ненадлежащее исполнение задач работником своей трудовой функции знаний может привести компанию к денежным потерям, а его отрицание корпоративной культуры негативно отразится на психологической атмосфере в коллективе, вот почему оценка персонала необходима.

Не менее интересным способом оценки представляется так называемый ассессмент-центр. Это комплексная оценка персонала по компетенциям, включающая в себя взаимодополняющие инструменты, например, деловые игры, анкетирование и тестирование. Тест-ассессмент состоит из двух этапов: 1) комплексного психологического тестирования с различными заданиями и вопросами; 2) наблюдения опытного эксперта за всем процессом прохождения тестов с подготовкой итогового отчета. На настоящий момент в таком методе оценки применяется автоматизированная расшифровка интервью, подготовка тестов и заданий алгоритмами, стандартизированные критерии. Сотрудники отмечают, что оценки на основе игр или иных интерактивных заданий воспринимаются как более увлекательные, удовлетворяющие и захватывающие [12. P. 5]. Работники заявляют, что такие методы являются менее агрессивными и навязчивыми [11].

Тем не менее, несмотря на всю быстродейственность и кажущуюся объективность алгоритма, возникают серьезные проблемы. Первая из них – атеоретичность и недостаточная прозрачность. К примеру, алгоритм может прийти к выводу, что работники с определенным цветом глаз показывают более высокие результаты труда, и в свою очередь рекомендовать поощрять кандидатов с таким цветом глаз. Очевидно, что такой подход вовсе не соответствует требованиям объективности и недопустимости дискриминации. Возникает так называемый эффект черного ящика, когда непонятно, какие именно процессы происходят во время обработки исходной информации. Именно поэтому так важны справедливые, релевантные и соответствующие законами алгоритмы, обрабатывающие данные с оценкой сотрудников [13].

Вторая из них – это специфичность методов оценки на онлайн-платформах. Исследуя цифровизацию труда, специалисты по общественным наукам обнаружили новые группы работников, возникших на почве цифрового капитализма [18]. Можно рассмотреть в качестве примера платформу по предоставлению услуг такси Uber, где в первую очередь после окончания поездки водителя оценивает клиент. В специальном приложении потребитель по своему личному усмотрению ставит оценки в соответствии с определенными критериями, затем эти данные отправляются агрегатору платформы [14]. При этом чем ниже рейтинг водителя, тем меньше заказов ему поступает и тем меньше его заработок. В этом смысле

о непредвзятости алгоритмов не может вестись и речи. Клиент по своему субъективному восприятию влияет на рейтинг исполнителя, а полученные результаты не оцениваются в дальнейшем человеком и сразу начинают отражаться на количестве заказов таксиста и оплате труда.

Непрозрачность и в определенной степени субъективность алгоритмов увеличивают шансы на судебные иски со стороны работников [15. P. 55]. Обобщая все вышесказанное, можно констатировать, что для корректной и объективной работы механизмов алгоритмической оценки требуется следующее: ввести детально проработанные шкалы и параметры оценки персонала, мероприятия по оценке должны проводиться с регулярной периодичностью. Более того, лицам, отвечающим за управление персоналом, следует тщательно проверять все результаты.

Кроме того, стоит отметить недавно распространившееся мнение о том, что государство вскоре станет основным заказчиком в сфере оценки персонала. Ярким примером служат все возрастающие запросы от федеральных и региональных министерств на стандартизированные и сформированные машиной опросники и иные инструменты оценки. Иными словами, начинает намечаться перекос в сторону государственных организаций, что оставляет в стороне частные предприятия [8]. Наиболее ощутимы изменения в Китае, где действуют различные социальные и личностные рейтинги, которые напрямую влияют как на возможность трудоустройства, так и на возможность сохранения места работы [3].

Таким образом, можно сделать вывод, что алгоритмизация оценки персонала – весьма полезное и перспективное явление, которое может объективно и беспристрастно давать характеристику оцениваемым субъектам и упростить весь процесс. Однако для бесперебойной и безупречной работы таких алгоритмов необходимо соблюдать этические и правовые нормы, а для большей безопасности вручную перепроверять полученные результаты.

Список литературы

1. Берулава М. Н. Психология и педагогика менеджмента. Бийск: НИЦ, Б и ГПИ, 1995. 115 с.

2. Веретехина С. В. Автоматизированные системы оценки персонала // УПИРР. 2015. № 5. С. 72–77.

3. «Образцовые» и «ненадежные»: как работает китайский социальный рейтинг. URL: https://style.rbc.ru/life/643d3f839a7947afd12e9f35

4. Оценка персонала: цели, задачи и методы. URL: https://www.hr-director.ru/article/67845-otsenka-personala-tseli-zadachi-i-metody 08.09.2021

5. Паламова С. И. Формирование модели управления кадровым потенциалом предприятия // Молодой ученый. 2022. № 7(402). С. 253–255.

6. Почти четверть компаний в России отказались от планов найма сотрудников в 2023 году. URL: https://www.forbes.ru/biznes/482731–23-kompanij-v-rossii-otkazalis-ot-planov-najma-sotrudnikov-v-2023-godu

7. Романова Н. П. Управление человеческими ресурсами как форма использования человеческого потенциала // Вестник ЗабГ У. 2019. № 2. С. 88–95.

8. Форум «Оценка персонала 2020. Осенняя сессия». URL: http://www.hrmedia.ru/node/1812

9. Чэнь Ш. Концепция стратегического управления человеческими ресурсами предприятия // ИСОМ. 2019. № 5. С. 138–146.

10. Gandini A. Labour Process Theory and the Gig Economy // Human Relations. 2019. Vol. 72, Is. 6.

11. Kaibel C., Koch-Bayram I., Biemann T., Mühlenbock M. Applicant perceptions of hiring algorithms – Uniqueness and discrimination experiences as moderators // Proceedings of the 79th Annual Meeting of the Academy of Management. 2019.

12. Li L., Lassiter T., Lee M. K., Oh, J. Algorithmic hiring in practice: recruiter and hr professional's perspectives on AI use in hiring // Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society (New York, NY: Association for Computing Machinery). 2021. 11 p.

13. Qian Yuan, Yin Jiemin. Study on Employee Performance Evaluation Based on Adaptive Feature Selection Fuzzy Algorithm, 2022. 13 p.

14. Rahman H., Valentine M. A. How client managers restrain control to keep control: Evidence from technologically-mediated 'Gigs'. Working Paper. Stanford University. 2019.

15. Smither J. W., Reilly R. R., Millsap R. E., Pearlman K., Stoffey R. W. Applicant reactions to selection procedures // Personnel Psychology. 1993. 46(1). Pp. 49–76.

16. StartExam – самая гибкая платформа для оценки персонала. URL: https://www.startexam.ru/360/

17. Wang B. Evaluation Method of the Excellent Employee Based on Clustering Algorithm // Dai H. N., Liu X., Luo D. X., Xiao J., Chen X. (eds) Blockchain and Trustworthy Systems. 2021.

18. Riczu Z., Melypataki G., Mate D. A. Concepts of Work: from Traditional Social-Labor Ideas to Modern Effects of Digital Transformation // Journal of Digital Technologies and Law. 2023. № 1(1). Pp. 175–190. EDN: ZENNZF

Н. С. Купцов,
студент,
Российский государственный университет правосудия

ОТСУТСТВИЕ СУБЪЕКТА С ПРАВОВЫМ СТАТУСОМ АВТОРА КАК ОСОБЕННОСТЬ АВТОРСКИХ ПРАВООТНОШЕНИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННОЙ СЕТИ

Аннотация. В статье рассматривается особенность современных правоотношений, возникающих в связи с созданием визуального произведения алгоритмами нейросети. Выявляются достоинства и недостатки существующих подходов к отнесению статуса автора произведения самой нейросети к субъектам, принимающим фактическое участие в его создании. Отмечается принципиальная новизна оформляющихся интеллектуальных правоотношений с использованием

нейронных сетей. Делается вывод о невозможности оперирования правовой категорией «автор» применительно к рассматриваемому виду правоотношений.

Ключевые слова: авторское право, автор произведения, произведение искусства, нейросеть

ABSENCE OF A SUBJECT WITH THE LEGAL STATUS OF THE AUTHOR AS A FEATURE OF COPYRIGHT RELATIONS USING A NEURAL NETWORK

Abstract. This article examines an essential feature of modern copyright relations arising in connection with the fact of creating a visual work using neural network algorithms, which consists in the complete absence of the author as a subject of legal relations in them. In particular, the advantages and disadvantages of existing approaches to attributing the status of the author of the work to the neural network itself and the subjects taking actual part in its creation are revealed; the fundamental novelty of the emerging intellectual legal relations using neural networks is noted; it is concluded that it is impossible to operate with the legal category of «author» in relation to the type of legal relations under consideration.

Keywords: copyright, author of the work, work of art, neural network

Стремительное развитие информационных технологий на рубеже XX–XXI вв., ознаменовавшее переход человечества к принципиально новым формам взаимодействия и жизнедеятельности, вне всякого сомнения, еще не исчерпало своего потенциала. При этом стоит признать: разного рода технологические новшества на современном этапе оказывают такое ощутимое воздействие на политические, экономические, социальные и духовные общественные процессы, что игнорировать множество возникающих в связи с этим проблем теоретического и прикладного характера, вызванных неизбежными коллизиями между устоявшимися подходами и вызовами сегодняшней реальности, попросту невозможно. В этой связи представляется бесспорным, что в самое ближайшее время человечеству придется вести активную работу по поиску путей обновления всех сфер общественной жизни с учетом фактического формирования уже сегодня новой модели мироздания, впервые в истории не просто столкнувшейся с существованием цифровой (т. е. по существу – альтернативной) реальности, но и, что более важно, вынужденной считаться с ее широчайшими возможностями.

Безусловно, такое обновление не должно пройти мимо всей разветвленной системы национального и международного права. Запоздалое изменение правовых норм, не поспевающее за гораздо более стремительным темпом развития технологий, все сильнее ощущается в самом широком спектре правовых отраслей. При этом в правовой системе Российской Федерации указанная тенденция ощущается еще более остро: относясь к романо-германской правовой семье, она лишена возможности свободно использовать для регулирования развивающихся правоотношений судебный прецедент как более маневренный и гибкий правовой источник. В связи с этим любое обновление отечественного правопорядка возможно только

путем законотворчества – не в пример более затяжной и бюрократически осложненной процедуры. Как следствие, в России уже сегодня одинаково актуальны проблемы привлечения к уголовной ответственности за гибель человека в ДТП с участием беспилотного автотранспорта и, к примеру, признания предметов виртуального мира полноправными объектами гражданского оборота [4. С. 393–401].

Впрочем, одной из наиболее актуальных и любопытных с исследовательской точки зрения проблем правовой модернизации представляется дальнейший путь развития правоотношений, возникающих в сфере авторского права. Обширное влияние современной технологической революции на эту отрасль отмечалось многими исследователями-правоведами: В. Л. Энтин, в частности, убежден, что нормальное функционирование норм авторского права в будущем невозможно без «переформатирования традиционных представлений» [10. С. 5], преобладающих в данной отрасли сегодня. При этом один из наиболее ощутимых ударов по устоявшимся догмам отечественного авторского права, несомненно, наносит искусственный интеллект, все более расширяющий сферу своего использования.

На сегодняшний день область применения одной из наиболее распространенных технологий, содержащих элементы «цифрового разума» – нейронной сети, – поражает своей широтой. Вместе с тем в течение последних двух лет повседневное использование нейросети окончательно утратило статус научно-прикладной и исследовательской деятельности и перешло в достояние общественности. Сказанное верно, прежде всего, для так называемых графических нейросетей, задачей которых является создание высококачественного изображения по текстовому запросу конкретного пользователя; при этом получаемое в ходе работы искусственного интеллекта изображение уникально и неповторимо, не имеет исторических аналогов. Следовательно, имеет смысл вести речь о том, что в результате выполнения такого рода нейронной сетью запроса пользователя формируется графическое изображение, которое в силу формального соответствия п. 1 ст. 1259 Гражданского кодекса РФ [1] вполне относимо к категории объектов авторского права, т. е. имеются основания для возникновения авторского правоотношения.

Однако дальнейшее рассуждение в указанном направлении неизбежно наталкивается на непреодолимое препятствие: поскольку известно, что абсолютное авторское правоотношение всегда возникает вследствие создания произведения [5. С. 86], одним из субъектов такого правоотношения обязательно должен быть автор (субъект, обладающий правовым статусом непосредственного создателя произведения). Иное противоречило бы не только базовым основам актуальной теории авторского права, но и формальным законам логики, ведь функционирование данной правовой отрасли направлено прежде всего на защиту охраняемых законом интересов автора конкретного произведения как «центральной фигуры российского авторского права» [2. С. 55]. В этой связи первоочередное значение для исследователей приобретает вопрос о том, кто именно из субъектов, так или иначе участвующих в создании такого произведения (сама нейронная сеть; конкретный пользователь, оформивший текстовый запрос; разработчик нейронной сети или ее владелец), может выступать его автором. Далее автору представляется необходимым проанализировать каждый из перечисленных подходов подробнее.

Мысль о возможности предоставления статуса автора произведения искусства самой нейросети, создавшей его, оформилась сразу после широкого распространения нейросетевых технологий: во многом потому, что фактически именно алгоритм нейронной сети без вмешательства извне самостоятельно моделирует результат текстового запроса пользователя, формирует соответствующее текстовому описанию графическое изображение. При этом существование и активная научная разработка указанного подхода (который, к слову, затрагивает куда более фундаментальную проблему – возможность наделения технологии искусственного интеллекта правосубъектностью как таковой) опираются в первую очередь на само существо нейронных сетей: известно, что они обладают свойством самостоятельно «выполнять творческо-когнитивные функции, которые до сих пор были исключительным правом человека» [8. С. 49]. В этой связи речь идет о развитии едва ли не равносильного (а в чем-то, возможно, и превосходящего) аналога человеческого мозга – до сегодняшнего момента наиболее совершенного изобретения природы. Разумеется, если рассматривать анализируемую в работе частноправовую проблему на таком абстрактном уровне, поиск ответа на вопрос о возможности авторской правосубъектности нейронной сети уходит на второй план, а утвердительный ответ на этот вопрос предполагается чем-то само собой разумеющимся.

Вместе с тем автор считает необходимым предостеречь от столь поспешных выводов. На сегодняшний день идея о признании технологий искусственного интеллекта полноправным носителем активного правового статуса в целом и авторско-правового статуса в частности, несмотря на возможную привлекательность и потенциал развития в будущем, выглядит чрезвычайно фантастично, а существенные недостатки такого подхода обнаруживаются при самом непритязательном анализе. Отметим прежде всего, что любая, даже самая совершенная нейронная сеть, не существует в вакууме, ее создание и обеспечение функционирования – итог целенаправленной человеческой деятельности. Иными словами, формирование нейросетью уникального изображения является, по существу, процессом выполнения специального алгоритма, пусть и наделенного рядом специфических признаков, позволяющих обеспечить неповторимость выполняемого результата и самостоятельный его анализ с целью совершенствования.

В этой связи гораздо более правильно на сегодняшний день говорить о нейросети как объекте права: в частности, вполне логично отнести ее к категории программ для ЭВМ, которые с позиции пп. 2 п. 1 ст. 1225 ГК РФ выступают охраняемыми результатами интеллектуальной деятельности. Более того, наделение нейросети правовым статусом автора, по сути, бессмысленно, поскольку, даже приобретя номинальное наименование автора, она не сможет самостоятельно распоряжаться всеми правами и обязанностями, которые собственно этот статус и составляют. Грубо говоря, в этом случае речь пойдет о формировании нежелательной правовой фикции, что не сможет не оказать негативного воздействия на систему правового регулирования. Наконец, невозможность признания нейронной сети автором произведения сегодня закреплена в отечественном законодательстве: ст. 1257 ГК РФ недвусмысленно указывает на возможность обретения

статуса автора только гражданином, чьим творческим трудом создано конкретное произведение литературы, науки или искусства.

Отечественными исследователями предлагаются и другие доводы в пользу невозможности признания искусственного интеллекта как субъектом авторского права, так и субъектом права вообще. Автор полностью соглашается с позицией И. А. Филиповой и В. Д. Коротеева, отмечающих в качестве препятствующих факторов также абстрактность довода о наличии у искусственного интеллекта сознания и самосознания, несущего в себе риски негативного воздействия на оперирование подобными категориями в отношении людей; неизбежность разрушительных последствий идеи признания правосубъектности искусственного интеллекта для всей антропоцентрической системы права, основополагающих правовых положений, формировавшихся со времен Римской империи [7. С. 371–372]. Ценность представляет и замечание А. Ю. Шешукова и Е. А. Княжевой, указывающих на отсутствие у нейронных сетей критически важного признака «осознанности», заключающегося в самостоятельном вложении смысла в создаваемое произведение, «определении его идеи или концепции»; более того, исследователи справедливо указывают на полную невозможность применения относительно нейросети категории «смерти», что делает проблематичным решение вопроса о возможности и сроках перехода произведения в общественное достояние [9. С. 97–98]. Автор полагает, что даже перечисленных выше тезисов достаточно для утверждения однозначного вывода: подход к наделению нейросети правовым статусом автора на создаваемое ей произведение в настоящее время несостоятелен.

Поскольку признание непосредственного создателя графического изображения – нейронной сети – его автором сегодня невозможно, имеет смысл проанализировать целесообразность наделения авторско-правовым статусом принимающего участие в процессе создания рассматриваемого произведения гражданина.

Теоретически в качестве такового возможно рассматривать двух различных субъектов: конкретного пользователя, сформулировавшего текстовый запрос, на основании которого алгоритм нейронной сети создал соответствующее графическое изображение, или же разработчика нейронной сети (и/или ее владельца) как лица, создавшего саму нейросеть и алгоритм ее работы или же осуществляющего обслуживание работы нейронной сети, владеющего определенной цифровой платформой, на ресурсах которой функционирует нейросеть.

Главным достоинством обоих подходов в свете вышесказанного является их соответствие признаку антропоцентричности права, что автоматически снимает с актуальной повестки трудности, возникшие при попытке наделить присущими человеку ментальными качествами искусственный интеллект. К сожалению, автор вынужден констатировать, что это обстоятельство выступает едва ли не единственной их положительной характеристикой; в остальном эффективность обозначенных подходов вызывает сомнения по ряду причин. Так, идея о наделении статусом автора произведения пользователя нейросети представляется несостоятельной, поскольку деятельность по оформлению текстового запроса для последующего генерирования изображения не соответствует признаку «творческого труда», обозначенного в качестве обязательного в диспозиции ст. 1257

ГК РФ: иными словами, конечный пользователь лишь формирует примерный замысел произведения, не принимая никакого личного участия в его непосредственном создании. Более того, поскольку графическое изображение в данном случае оформляется при помощи функционирования алгоритма нейросети, пользователь не имеет объективной возможности точно предсказать результат работы нейронной сети, добиться абсолютной степени соответствия полученного изображения его персональным представлениям. Думается, что возможность четко представлять конечный результат творческой работы и совершать направленные действия по его реализации – один из важнейших признаков автора как создателя произведения искусства. В этой связи говорить о пользователе нейронной сети как об авторе произведения нельзя.

Кстати, по этой же причине автор полагает невозможным вести речь о наделении авторско-правовым статусом пользователя с признанием алгоритма нейросети рядовым инструментом для создания произведения (наподобие кистей и красок для художника; музыкального инструмента для композитора и пр.): в отличие от «традиционных» средств создания произведения искусства, в данном случае лицо не использует их, а фактически полностью поручает нейросети создание изображения. Очевидно, что в этом смысле признание нейронной сети инструментом в руках автора противоречит самому смыслу авторской деятельности; использование нейросети в качестве инструмента «должно сопровождаться человеческим замыслом, внутренней оценкой результата, его корректировкой» [9. С. 99].

Наиболее благоприятным с точки зрения действующего правового регулирования может показаться подход, согласно которому статус автора нейросетевого произведения будет принадлежать разработчику этой нейросети и/или владельцу цифровой площадки, на которой нейросеть размещена. Не в последнюю очередь это связано с наличием в гражданском законодательстве действенных правовых конструкций: так, если допустить, что нейросеть как объект интеллектуальной собственности относится к категории программ для ЭВМ (пп. 2 п. 1 ст. 1225 ГК РФ), то логично, что все создаваемые такой нейросетью изображения (поскольку они формируются при помощи программного кода – алгоритма, созданного разработчиком) могут выступать в качестве новообразованных элементов нейронной сети, т. е., по существу, объектами права интеллектуальной собственности разработчика.

Вместе с тем данная позиция не решает проблему отсутствия непосредственного творческого труда разработчика в создании конкретного произведения; более того, в отличие от пользователя нейронной сети, который, по крайней мере, моделирует замысел изображения, создатель алгоритма нейронной сети не принимает вообще никакого прямого участия в его формировании. Строго говоря, разработчик нейросети имеет отношение к созданию ею конкретного произведения лишь косвенно – одним фактом написания технического алгоритма. Такое рассуждение прямо указывает на несостоятельность идеи признания правого статуса автора за таким «косвенным» участником процесса создания графического изображения. По аналогичной причине не может идти речи о признании авторами нейросетевого

произведения владельца портала информационного размещения, оператора нейросети и других подобных субъектов.

В свете приведенного выше анализа допустимо вести речь о наличии крайне нехарактерной для сформировавшихся устоев отечественного авторского права проблемы: с одной стороны, факт создания нейросетью уникального графического изображения, выполненного в определенной изобразительной технике, сам по себе является достаточным поводом для возникновения авторского правоотношения с целью защиты прав, свобод и законных интересов его создателя; с другой же – ни один из субъектов, так или иначе принимающих участие в создании нейросетевого изображения, по разным причинам не может обладать правовым статусом его автора (не говоря уже о невозможности признания такого статуса за самой нейронной сетью). Иными словами, перед нами фактически предстает авторское правоотношение без автора – немыслимое с точки зрения сложившегося правового регулирования. Не будет преувеличением отметить, что с подобного рода проблемой отрасль авторского права сталкивается впервые за всю историю своего развития.

Необходимо, однако, указать, что в условиях отсутствия в настоящее время сколько-нибудь устойчивого доктринального подхода к решению рассматриваемой проблемы и, как следствие, законодательного регулирования конкретные участники подобных правоотношений вынуждены самостоятельно конструировать модели их оформления. Показательны в этой связи положения, содержащиеся в пользовательском соглашении российской графической нейросети Kandinsky [6], разработанной под эгидой акционерного общества СБЕР. Так, пп. 5.7 и 5.8 соглашения четко разделяют права на сформированное изображение и права на элементы нейросети и информационного портала: если первые принадлежат конкретному пользователю, то вторые – компании СБЕР. При этом категорией «автор» текст соглашения не оперирует: вместо нее и пользователь, и собственник нейросети именуются правообладателями. Важно отметить также, что п. 3.1 соглашения устанавливает прямую обязанность пользователя сервисом использовать его исключительно в некоммерческих целях, для личного потребления. В случае, если пользователь имеет желание использовать полученное изображение для получения имущественной выгоды, соглашение обязывает его обращаться в СБЕР для решения вопроса в частном порядке путем заключения отдельного договора. Думается, что такая модель индивидуального правового регулирования объясняется нежеланием разработчика нейросети самостоятельно, на свой страх и риск вводить новые правовые инструменты и конструкции в отсутствие действующих конкретных правовых норм. Обращает на себя внимание п. 5.4 соглашения, обязывающий пользователя при размещении изображения на сторонних ресурсах указывать на факт создания изображения с использованием алгоритма нейросети Kandinsky. Данное положение указывает на заинтересованность разработчика нейросети не столько в защите права авторства на изображение как таковое, сколько в распространении информации о действии нейросетевого алгоритма (своего рода рекламирования нейросети путем прямого размещения результатов ее работы). Вероятно, такой законный интерес создателя нейросети может выступать

в качестве еще одного характерного признака нового рода правоотношений с использованием искусственного интеллекта в сфере авторского права.

С точки зрения современного вектора развития сферы использования изображений, сформированных нейросетями, интерес представляет точка зрения А. В. Гурко, полагающего возможным применительно к подобного рода правоотношениям оперировать категорией «бенефициара», т. е. лица, получающего выгоду от использования нейросети и ее возможностей. В этом случае в качестве выгодоприобретателя может выступать как пользователь (в случае получения выгоды от использования изображения), так и разработчик нейросети (при появлении в результате работы нейросети дополнений алгоритма) [3. С. 140]. При такой постановке вопроса возможно говорить о наличии правоотношения, производного от авторского, однако находящегося в то же время в лоне отрасли авторского права [5. С. 90].

Таким образом, все большее распространение нейронных сетей, алгоритм которых позволяет создавать графические изображения на основе текстового запроса конкретного пользователя, с неизбежностью вызывает ряд проблем, заключающихся в явном несоответствии характеристик таких принципиально новых правоотношений устоявшимся правовым нормам и доктринальным моделям, в том числе отрасли авторского права. Ни один из участников процесса создания нейросетевого произведения не может быть наделен правовым статусом его автора, что, однако, не препятствует возникновению правоотношения, которое системно и сущностно должно быть отнесено к авторско-правовым. Такая коллизия никогда ранее не возникала в силу отсутствия субъекта, способного к созданию произведений искусства, помимо человека; сегодня ситуация кардинально изменилась. В этой связи правовое регулирование авторских правоотношений с использованием искусственного интеллекта должно в ближайшее время оформиться в качестве нового, самостоятельного элемента отрасли авторского права. Существенная роль в этом, как и ранее, должна быть отведена научному сообществу.

Список литературы

1. Гражданский кодекс Российской Федерации. Часть четвертая: Федеральный закон от 18.12.2006 № 230-ФЗ // Собр. законодательства РФ. 2006. № 52. Ст. 5496.

2. Калятин В. О. Право интеллектуальной собственности. Правовое регулирование баз данных: учебное пособие для вузов. М.: Юрайт, 2023. 186 с. (Высшее образование) // Образовательная платформа Юрайт. URL: https://urait.ru/bcode/515537

3. Коданева С. И. Трансформация интеллектуальной собственности под влиянием развития искусственного интеллекта // Социальные новации и социальные науки. 2021. № 2(4). С. 132–141.

4. Купцов Н. С. Проблема определения теоретико-правовой сущности некоторых элементов виртуального мира в контексте отнесения их к объектам гражданских прав // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило,

И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 4. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. 412 с. EDN: KSNIFB. DOI: 10.21202/978-5-8399-0770-6_2022_4_412

5. Литвина А. И. О понятии авторского правоотношения // Вестник Пермского университета. Юридические науки. 2014. № 2(24). С. 84–93.

6. Нейронная сеть Kandinsky 2.2: [сайт]. 2023. URL: https://www.sberbank.com/promo/kandinsky

7. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 359–386. EDN: IMMOAM

8. Человек и «Искусственный интеллект»: антропо-социальные контексты / Г. П. Ковалева, О. Н. Ефремова, В. Н. Порхачев, Н. Н. Ростова // Вестник общественных и гуманитарных наук. 2020. Т. 1, № 2. С. 48–53.

9. Шешуков А. Ю., Княжева Е. А. Автор мертв. Почему нейросеть не может стать субъектом авторских прав // Труды по интеллектуальной собственности. 2023. Т. 45, № 2. С. 95–102.

10. Энтин В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи). М.: Статут, 2017. 216 с. URL: https://znanium.com/catalog/product/1013817

В. В. Куренкова,
студент,
Национальный исследовательский университет
«Высшая школа экономики»
Я. Д. Стрелецкая,
студент,
Национальный исследовательский университет
«Высшая школа экономики»

ПРАВОВЫЕ ОСНОВАНИЯ ИСПОЛЬЗОВАНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ В МАШИННОМ ОБУЧЕНИИ

Аннотация. Цель статьи – выявить основные тенденции в сфере использования интеллектуальной собственности в машинном обучении. Актуальность работы обусловлена всплеском популярности различных искусственных интеллектов, как текстовых, так и визуальных. В работе освещаются не только основные особенности работы авторского права с искусственным интеллектом, но формулируются предложения по усовершенствованию законодательства.

Ключевые слова: искусственный интеллект, интеллектуальная собственность, объекты интеллектуальной собственности, авторское право, машинное обучение, базы данных, цифровизация

LEGAL BASIS FOR THE USE OF INTELLECTUAL PROPERTY IN MACHINE LEARNING

Abstract. The purpose of this article is to identify the main trends in the use of intellectual property in machine learning. The relevance of the work is due to the surge in popularity of various AI, both textual and visual. Due to the fact that the topic of AI is acute all over the world, we also gave examples from international legislation. In this paper, we not only highlighted the main features of the work of copyright with AI, but also offered our ideas for improving legislation.

Keywords: artificial intelligence, intellectual property, intellectual property objects, copyright, machine learning, databases, digitalization

Машинное обучение, нейросети и искусственный интеллект в наши дни приобретают все большую значимость для общества и государства. Известны многие случаи использования машинного обучения в повседневной, творческой, научной и даже политической деятельности. Человечество стоит на пути масштабного прорыва в сфере технологий. Безусловно, на первом месте будут алгоритмы, коды и другие задачи программирования. Однако без большого массива данных, без баз данных, вряд ли получится хоть чему-то обучить машину.

Для обучения искусственного интеллекта (далее – ИИ) разработчикам необходимы качественные материалы, которые зачастую защищены правами интеллектуальной собственности. Чтобы получить возможность использования этих материалов, необходимо согласие создателей (правообладателей). Ввиду большого объема используемых баз данных издержки получения согласия могут стать серьезным барьером для развития технологий ИИ. В этих условиях встает вопрос об оптимальном подходе к правовым основаниям использования интеллектуальной собственности в машинном обучении.

Перед нами стоит задача разобраться в определениях (начиная от машинного обучения и заканчивая TDM), рассмотреть реальные примеры того, как законодательство регулирует использование объектов интеллектуальной собственности в составе больших данных в нейросетях, а также определить возможные направления изменения правового регулирования.

Объекты интеллектуальной собственности являются материалом для создания алгоритмов для машинного обучения. Для обучения ИИ необходимо загружать в базу данных огромный объем материалов (фото, тексты, видео, музыку, песни, шутки и многое другое), эта информация, в свою очередь, попадает под определение объектов авторского права.

Авторское право в каждой стране регулируется законом примерно схоже. Например, в четвертой части ГК РФ авторское право – это интеллектуальные права на произведения науки, литературы и искусства; авторскими правами являются: исключительное право на произведение, право авторства; право автора на имя, право на неприкосновенность произведения и право на обнародование произведения.

В США же Закон об авторском праве предоставляет авторам исключительное право производить и продавать копии своих работ, право на создание

производных произведений, а также защищает правообладателя. У авторских прав в Соединенных Штатах есть срок, и, как правило, он истекает спустя 70 лет после смерти автора. После этого произведения переходят в общественное достояние.

Самих методов использования объектов интеллектуальной собственности существует большое множество: считывание, воспроизведение, копирование, доведение до общего сведения и иные способы. Сам по себе интеллектуальный анализ текста и данных [3] является обширным определением того, как можно взаимодействовать с объектами авторских прав. Так как есть возможность совмещения разных методов машинного обучения (например, сканирование, а после доведение до общего сведения), появляется проблема незаконного обнародования баз данных авторского права. К сожалению, случаи свободного использования объектов искусственного интеллекта не полностью регулируются законодательством, из-за чего возникают разногласия.

На данный момент споры по поводу использования интеллектуальной собственности в машинном обучении ведутся очень активно: многие авторы и компании пытаются оспорить правильность и точность ст. 1260 ГК РФ так как согласно этой статье, изготовленные программы могут делиться на «составные», те которые включают в себя другие материалы и источники, и на полностью авторские. Если материал признается составным, то его могут использовать и другие пользователи, согласно п. 3 ст. 1260 ГК РФ. Руководствуясь этими данными, Конституционный Суд РФ постановил, что данный пункт противоречит Конституции РФ, а именно статьям 17 (часть 3), 19 (части 1 и 2), 34 (часть 1), 44 (часть 1), 45 (часть 1), 46 (часть 1) и 55 (часть 3) – препятствует защите авторских прав на ЭВМ в суде [5].

Авторские права стали камнем преткновения в сфере использования интеллектуальной собственности в машинном обучении. Если в обозначенном выше деле предметом спора стали авторские права программиста, то часто встречаются случаи, когда нарушаются права пользователей в результате использования больших баз данных, без их согласия. Так, например, в решении от 19 декабря 2019 г. по делу № А40-183412/2019 по данным Заявителя (сайта «Авито») были нарушены авторские права продавцов, которые размещали на сайте свои объявления о продаже машин. Третье лицо брало с сайта «Авито» номера этих пользователей и предлагало разместить свое объявление и на сайте Авто.ru. Но суд посчитал номер телефона не личной информацией, что довольно логично, потому что номер телефона используется не только его обладателем, но и сторонними людьми, поэтому права пользователей не были нарушены и иск был отклонен. Также было дело «ВКонтакте» и «Дабл»: «Дабл», используя технологии Big Data, брали информацию о пользователях в соцсетях и во «ВКонтакте». Это нарушало права пользователей приложения и самих разработчиков, так как пользователи не давали согласия на использования их персональных данных. Данные, собранные «Дабл», были выложены на сайте стороннего банка АО, и один из пользователей, заметивший это, написал заявление в полицию. Но иски ВК и пользователя не были удовлетворены, потому что ВК не смогли доказать, что произвели затраты на создание датасета, поэтому их права и права пользователей не смогли защитить. Это существенный минус ГК РФ [1].

Также в пример нельзя не привести системы Botkin.AI, которая использует результаты медицинских обследований для диагностирования рака. Эта технология практикуется как в России, так и за рубежом. Также ИИ являются дроны, которые довольно удачно функционируют.

На данный момент интеллектуальная собственность активно используется в машинном обучении: соцсети используют свои базы данных для создания алгоритмов рекламы, больница – для диагностики заболеваний и т. д. Но они сталкиваются с множеством препятствий как в ГК, так и в сознании обывателей. В ГК РФ авторы статей стараются защитить авторские права, но при этом затормаживают процесс или делают его вовсе невозможным. В США в машинном обучении с точки зрения права ушли немного дальше. Например, ввели такое понятие, как «добросовестное использование», когда люди могут использовать интеллектуальную собственность без каких-либо лицензий, но с соблюдением определенных правил, а также, как было сказано ранее, был введен срок действия – 70 лет. Это позволяет действовать таким системам, как All Prior Art, Ambercite AI, Google Auto Draw, Humtap, Cyborg Writer и т. д.

Общество постепенно движется к внедрению положений о работе ИИ в закон. Законодательство должно быть принято на достаточно общем уровне, чтобы положения об авторских правах могли быть применимы к непредвиденным ситуациям [3]. Мы предлагаем ввести ответственность и для ИИ, и для разработчиков, а также ввести срок действия прав для определенного вида ИИ, потому что ИИ делятся на сильные, способные на самостоятельные действия, и слабые, которые действуют только по заданной схеме.

Искусственному интеллекту необходимы данные, на основе которых он будет функционировать, а также это сопрягается с главной целью создания многих ИИ – обработкой информации. На данный момент такого рода использование баз данных и иной интеллектуальной собственности регулируется четвертой частью ГК: в ней устанавливается определение интеллектуальной собственности, а также детали работы с ней. Если мы говорим про зарубежное право, то там, как было показано выше, наблюдается постановка целей на развитие сферы машинного обучения. Эту тенденцию мы можем наблюдать в США и других европейских странах: помощники DARPA, принятие ФЗ об ИИ США, политика, направленная на поддержку разработчиков ИИ, в том числе и на уровне законодательства [4].

С учетом всех данных можно утверждать, что Россия также движется к цифровизации и развитию искусственного интеллекта, выдвигается множество инициатив, связанных с интеллектуальной собственностью и цифровизацией. Эти инициативы сталкиваются с проблемами, связанными с авторским правом. Но законотворцы стараются их решить.

Список литературы

1. ВКонтакте v. Дабл // Buzko Krasnov. URL: www.buzko.legal /content-ru/vkontakte-protiv-dabl-polnyy-obzor-keysa-parsing-zapreshchen

2. Использование объектов интеллектуальной собственности (базы данных и ее элементов) в машинном обучении // Российский центр оборота прав на

результаты творческой деятельности. URL: https://рцис.рф/research/ispolzovanie-obektov-intellektualnoj-sobstvennosti-bazy-dannyh-i-ee-elementov-v-mashinnom-obuchenii

3. Meeûs d'Argenteuil J., Triaille J. P., Francquen A., March, 2014. Study on the legal framework of text and data mining (TDM), De Wolf & Partners Date Views. URL: op.europa.eu/en/publication-detail/-/publication/074ddf78-01e9-4a1d-9895-65290705e2a5/language-en

4. Defense Advanced Research Projects Agency (DARPA). URL: https://www.dar-pa.mil

5. Постановление Конституционного Суда РФ от 16.06.2022 № 25-П «По делу о проверке конституционности пункта 3 статьи 1260 Гражданского кодекса Российской Федерации в связи с жалобой гражданина А. Е. Мамичева».

Д. А. Лужков,
магистрант,
Государственный институт экономики, финансов, права и технологий

ПРОБЛЕМА ЦИФРОВЫХ (ЭЛЕКТРОННЫХ) ДОКАЗАТЕЛЬСТВ В ГРАЖДАНСКОМ ПРОЦЕССЕ

Аннотация. В статье рассматриваются актуальные проблемы, сложившиеся в судебной практике, вызванные широким использованием электронных документов и информационных систем в гражданском обороте. В настоящее время участники гражданского оборота все чаще направляют предложения, требования, претензии своим контрагентам не посредством почтовой связи, а на адрес электронной почты, через личный кабинет, в чатах технической поддержки, по телефонам горячих линий. В связи с этим необходимо определить место цифровых (электронных) доказательств в процессе доказывания, а в дальнейшем, возможно, выделение их в отдельную категорию судебных доказательств, что позволит установить в действующем процессуальном законодательстве порядок их предоставления в судебном процессе.

Ключевые слова: право, процессуальное законодательство, процесс доказывания, судебные доказательства, цифровые технологии, цифровые доказательства, электронные доказательства

THE PROBLEM OF DIGITAL (ELECTRONIC) EVIDENCE IN CIVIL PROCEEDINGS

Abstract. The article deals with the actual problems that have developed in judicial practice, caused by the widespread use of electronic documents and information systems in civil circulation. Currently, participants in civil circulation are increasingly sending proposals, demands, claims to their counterparties not by mail, but to an email address, through a "personal account", in "technical support" chats, by calling "hot lines", to an email address mail. In this regard, it is necessary to comprehensively study and determine the place of digital (electronic) evidence in the process of proving,

and in the future, it is possible to separate them into a separate category of forensic evidence, which will make it possible to establish in the current procedural legislation the procedure for their provision in the trial.

Keywords: law, procedural law, process of proof, judicial evidence, digital technologies, digital evidence, electronic evidence

Доказательства необходимы для вынесения судом правосудного и обоснованного решения по делу, вне зависимости от того, к какой юрисдикции относится судебное разбирательство. Развитие цифровых технологий в последнее время позволило применять в современном судопроизводстве новые виды доказательств, которые не использовались еще совсем недавно [5–7]. В связи с этим назрела необходимость изучения и определения места цифровых (электронных) доказательств в процессе доказывания.

Цифровые доказательства стали неотъемлемой частью современного общества, где все оставляют следы своей деятельности в Интернете. Однако использование на практике таких доказательств в гражданском процессе возможно только при определенных условиях.

Одним из главных препятствий является недостаточность регулирования в данной области; законодательство не всегда адекватно реагирует на новые технологические решения, и отсутствуют четкие правила о возможности принятия цифровых доказательств в качестве основы дела.

Еще одной проблемой является техническая сложность анализа и исследования цифровых доказательств. Часто возникает необходимость проведения специальной экспертизы, которая также становится объектом обсуждения и сомнения сторон.

Наконец, третьей проблемой является защита цифровых доказательств от подделки. Современным технологиям ничего не стоит подделать медиа-файлы, изменить дату создания документа или наложить эффекты на фотографии. Помимо этого, вопрос о качестве доказательств также требует внимания: устаревшие или слабо защищенные технологии могут привести к потере или изменению информации.

Однако, несмотря на все проблемы, цифровые доказательства имеют все большее значение в гражданском процессе. Необходимость быстрого и точного сбора информации заставляет стороны использовать именно такие доказательства, также они могут увеличить объем доказательств и повысить их точность.

Актуальность использования цифровых (электронных) доказательств обусловливается широким использованием электронных документов и информационных систем в гражданском обороте.

На данный момент понятий «электронное доказательство», «цифровое доказательство» в нормативных правовых актах Российской Федерации не существует. Между тем в юридической литературе есть определение рассматриваемого понятия: под электронным доказательством понимается информация, полученная с помощью компьютерных средств и имеющая значение для дела [2. С. 197].

Также электронное доказательство может быть определено как новый вид доказательств, который позволяет установить истинность юридических фактов в процессе [4. С. 28].

На основании вышеуказанных определений может быть непосредственно сформирован подход к изучению электронных (цифровых) доказательств как совокупности сведений, зафиксированных на цифровом носителе информации и позволяющих установить подлежащие доказыванию обстоятельства рассматриваемого судом гражданского дела. В настоящее время законодательство относит электронные доказательства, согласно ст. 71 ГПК РФ, к письменным доказательствам.

Между тем такое определение электронных доказательств не может считаться исчерпывающим. Основным признаком письменного доказательства является его фиксация на бумажном носителе. А электронный документ может как обладать такой фиксацией (электронный образ документа), так и не быть зафиксированным указанным способом. При этом электронные (цифровые) доказательства создаются с помощью кодирования, позволяющего сохранить информацию без изменения.

В настоящее время при создании электронных доказательств используется система двоичного кодирования, обладающая дискретным (непрерывным) способом передачи информации, в результате чего искажение данных маловероятно. При этом сведения о попытках фальсификации (изменения) электронного (цифрового) доказательства оставят следы в метаданных файла.

Электронные доказательства могут быть разделены на несколько видов: цифровые доказательства, электронные сообщения, интернет-источники, электронные образы документов.

К цифровым доказательствам следует отнести информацию, созданную на базе современных цифровых технологий, зафиксированную двоичным кодированием.

Электронные сообщения – это материалы, содержащие, например, переписку покупателя с продавцом, которые могут быть зафиксированы в виде скриншота и являются основанием для принятия объективного решения по делу. Важность данного вида электронного (цифрового) доказательства обуславливается, например, тем, что в настоящее время все больше договоров заключаются без соблюдения простой письменной формы договора, например, все больше розничных покупок товаров для личного потребления происходит в интернет-магазинах и даже в социальных сетях. При этом фактически единственным доказательством заключения договора розничной купли-продажи на конкретных условиях и в конкретное время является электронная переписка продавца и покупателя.

Интернет-источники – это сайты, официальные порталы, которые содержат какую-либо информацию, необходимую в процессе доказывания. Это могут быть облачные хранилища, архивы данных, сайты интернет-магазинов, страницы продавцов в социальных сетях [3. С. 128].

Электронные образцы документов – это документы, которые были созданы на бумажном носителе и в последующем переведены в электронный вид.

Таким образом, в науке доказательственного права назрела необходимость включить электронные (цифровые) доказательства в качестве отдельного вида доказательств в действующее процессуальное законодательство. Таким образом,

суд будет иметь возможность истребовать электронное (цифровое) доказательство не только в виде бумажного документа, но и виде файла при помощи электронной почты, мессенджера или системы электронного документооборота (ГАС «Правосудие»). Это значительно сократит время направления доказательств в суд и существенно ускорит рассмотрение гражданских дел.

Кроме того, в настоящее время при предоставлении скриншотов переписки покупателя (потребителя) с продавцом суд может потребовать представить их в виде нотариально удостоверенных документов в соответствии со ст. 102 и 103 «Основ законодательства Российской Федерации о нотариате» [1], что для покупателя (потребителя) может оказаться весьма затратным и обременительным.

Таким образом, выделение электронных (цифровых) доказательств в отдельную категорию доказательств в том числе позволит установить в процессуальном законодательстве порядок их предоставления в суд, исследования и оценки.

В судебной практике не сформировался единый подход к принятию в качестве доказательств по делу электронных (цифровых) доказательств, что затрудняет объективное, полное и всестороннее рассмотрение гражданских дел судом.

В настоящее время суды нуждаются в использовании электронных (цифровых) доказательств в судопроизводстве по гражданско-правовым спорам как отдельного вида доказательств. Они помогут облегчить и ускорить процесс доказывания и исследования материалов дела в гражданском процессе. Вышеизложенное указывает на то, что электронное (цифровое) доказательство должно стать отдельной категорией доказательств в процессуальном законодательстве Российской Федерации.

Также в завершение следует отметить, что в силу развития цифровых технологий уже объективно возникла возможность применять при отправлении правосудия новые виды доказательств, которые не использовались ранее. Однако действующее законодательство отстает от сложившихся реалий.

Актуальность данного вопроса вызвана широким использованием электронных документов и информационных систем в гражданском обороте, поскольку как юридические, так и физические лица все чаще направляют свои предложения, требования и претензии контрагенту не посредством почтовой связи, а в цифровом формате.

В связи с этим необходимо всестороннее изучение и определение места цифровых (электронных) доказательств в процессе доказывания, а в дальнейшем возможно выделение их в отдельную категорию судебных доказательств, что позволит установить в действующем процессуальном законодательстве порядок их предоставления в судебном процессе.

Таким образом, подводя итог, можно обозначить основные проблемы представления цифровых (электронных) доказательств в гражданском процессе.

Первая проблема заключается в том, что цифровые доказательства могут быть подделаны или изменены. Это связано с тем, что электронная информация легко копируется и передается. Кроме того, необходимо убедиться, что электронные доказательства не были изменены в процессе передачи или хранения.

Вторая проблема состоит в том, что определение подлинности электронных доказательств может быть трудным. Существует ряд критериев, которые могут

использоваться для подтверждения подлинности электронных документов, таких как цифровая подпись или дата создания. Однако, даже если такие критерии применяются, они не могут дать гарантии подлинности без дополнительных проверок.

Третья проблема связана с тем, что цифровые доказательства могут быть трудными для восприятия. Электронная информация может быть сложной и технической, что может затруднить понимание ее значимости судьей или коллегией присяжных.

Наконец, четвертая проблема связана с тем, что использование цифровых доказательств может существенно увеличить время и стоимость процесса. Необходимость проведения дополнительных экспертиз их подлинности может потребовать дополнительного времени и ресурсов.

В целом использование цифровых доказательств в гражданском процессе имеет как плюсы, так и минусы. Чтобы успешно использовать электронные доказательства, необходимо учитывать и решать указанные проблемы.

Следовательно, необходимо разработать четкие правила и нормы использования и признания цифровых доказательств в гражданском процессе, проводить обучение юристов в этой области и совершенствовать существующие технологии и инструменты для контроля и защиты цифровых доказательств.

Список литературы

1. Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11 февраля 1993 г. № 4462-1) // СПС «КонсультантПлюс».

2. Браилко А. Ю. Особенности оценки электронных доказательств в суде // Молодой ученый. 2022. № 48(443). С. 197.

3. Довгополая М. Ю. Проблема определения электронных доказательств в гражданском процессе // В сборнике: Власть и общество: история, современное состояние и тенденции развития: сборник материалов Всероссийской научно-практической конференции / науч. ред. В. В. Наумкина, отв. ред. В. Н. Козлова. Абакан, 2023. С. 128.

4. Одерий А. В. Электронные доказательства в гражданском и арбитражном процессе // Инновационная наука. 2022. № 6. С. 28.

5. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295.

6. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497.

7. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022. С. 15.

А. С. Лузина,
магистрант,
Казанский (Приволжский) федеральный университет

ПРОБЛЕМЫ ГРАЖДАНСКО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ, ВОЗНИКАЮЩИХ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Целью исследования является выявление проблем гражданско-правового регулирования, возникающих в сфере использования информационных технологий. Существенные особенности исследования заключаются в выявлении следующих правовых проблем: отсутствия однозначного правового регулирования смарт-контрактов в российской правовой системе; скорости развития технологий и правовых регуляторных механизмов; законодательного определения единой концептуальной правовой регламентации гражданско-правовых отношений, осуществляемых с использованием информационных технологий.

Ключевые слова: право, информационные технологии, смарт-контракт, правовая регламентация, правовые регуляторные механизмы, искусственный интеллект

PROBLEMS OF CIVIL LEGAL REGULATION OF RELATIONS ARISING IN CONNECTION WITH THE USE OF INFORMATION TECHNOLOGIES

Abstract. The article reveals and observes main problems of civil legal regulation in relations that arise in the usage of information technologies. The essential features of this investigation are to identify and recognize the following legal problems: the non-availability of the legal regulation of smart contracts in Russian legal system, the problem of the speed of technology's development and legal regulators of the mechanisms, the problem of legislative definition as a single concept that allows regulating civil law relations provided by using information technology.

Keywords: law, information technologies, smart contract, legal regulation, legal regulatory mechanisms, artificial intelligence

Современный мир переживает бурное развитие информационных технологий (далее – IT), которые активно применяются во всех сферах общественных отношений. В этой связи особую актуальность приобретают вопросы, связанные с правовым регулированием отношений, осложненных IT-элементом.

Гражданско-правовые отношения невозможны без заключения соглашений, в связи с чем проблемы договорного права занимают особое место в современной цивилистике. В условиях развития цифровой экономики информационные технологии оказывают непосредственное влияние на механику заключения гражданско-правовых договоров. В качестве примера такого влияния можно привести заключение так называемых смарт-контрактов. Как правило, смарт-контракты заключаются на специальных онлайн-платформах и шифруются при

помощи технологии блокчейн. Преимуществом таких соглашений является возможность адаптирования под изменяющиеся коммерческие условия. Как отмечают В. С. Белых, М. О. Болобонова, в зарубежном гражданском праве устоялась позиция о том, что смарт-контракт является скорее техническим понятием и представляет собой компьютерную программу, нежели самостоятельный гражданско-правовой институт [2. С. 56]. Между тем, по мнению автора настоящего исследования, смарт-контракт следует рассматривать с позиции гражданско-правового соглашения, заключенного с использованием средств информационных технологий.

В данном исследовании выявим основные проблемы в применении смарт-контрактов, правовом регулировании использования заключения сделок в информационной среде, дистанционных гражданско-правовых сделках, наследовании цифровых активов, передаче прав доступа к цифровым аккаунтам.

Наиболее очевидной представляется проблема, связанная с применением смарт-контрактов в российской правовой системе, которая заключается в отсутствии какого-либо однозначного правового регулирования данного правового института. В этом отношении российское законодательство отстает, в том числе от законодательства соседних государств. Так, законодательство Республики Беларусь определяет смарт-контракт в качестве программного кода [6]. В Российской Федерации определение смарт-контракта было предложено авторами Проекта Федерального закона № 419059-7 «О цифровых финансовых активах», как договора, заключаемого в электронной форме [6]. Однако в окончательную редакцию Федерального закона соответствующее определение не вошло. В настоящее время определение смарт-контракта содержится только в нормативных актах, издаваемых Банком России [1]. При этом действующая правоприменительная практика рассматривает смарт-контракт, прежде всего, в качестве самостоятельного вида договора, а не технического решения. Вместе с тем без должного нормативного правового регулирования дальнейшее развитие смарт-контрактов в Российской Федерации представляется затруднительным.

Следует отметить, что не любая сделка, заключаемая с применением информационных технологий, является смарт-контрактом. Основной проблемой, связанной с заключением сделок в информационной среде, является, на наш взгляд, проблема идентификации ее участников. Одним из средств идентификации является верификация субъектов гражданско-правовых отношений с помощью государственных информационных систем. Ряд авторов указывают на проблемы, связанные с идентификацией определенных субъектов гражданско-правовых отношений – в частности, индивидуальных предпринимателей [17. С. 43–45]. Так, в Едином государственном реестре индивидуальных предпринимателей (ЕГРИП) не содержатся сведения о местонахождении предпринимателя, что затрудняет анализ возможности исполнения сделки потенциальным контрагентом.

Безусловно, действующие ограничения в части предоставления информации публичными сервисами установлены в целях защиты персональных данных физических лиц. На наш взгляд, представляется обоснованным расширить сферу применения Единой системы идентификации и аутентификации (ЕСИА) и Единого портала государственных и муниципальных услуг («Госуслуги»), позволив

участникам гражданско-правовых отношений заключать сделки при помощи указанных систем, а именно осуществлять взаимную идентификацию. Стоит отметить, что соответствующая техническая возможность существует, поскольку при помощи портала «Госуслуги» в настоящее время можно заключать договоры обязательного страхования гражданской ответственности владельцев транспортных средств, а также договоры банковского вклада и кредитные договоры.

В связи с широким распространением сделок, совершаемых с применением информационных технологий, хотелось бы отметить, что проблема идентификации сторон сделки не является единственной. Так, при совершении дистанционной гражданско-правовой сделки (например, заключении инвестиционного соглашения посредством онлайн-платформы) возникает проблема определения места совершения сделки и, как следствие, действующей юрисдикции. Д. С. Карлаш указывает на отсутствие соответствующего законодательного регулирования в Российской Федерации [8. С. 22–28]. Зачастую онлайн-сделки заключаются посредством акцептирования стороной предложенной оферты. Поскольку информационное пространство является глобальным, не имеет значения физическое местонахождение оферента. В этой связи, на наш взгляд, уместным было бы установление законодательного императива о привязке места совершения сделки к месту жительства акцептора – физического лица или месту государственной регистрации компании, участвующей в сделке. Безусловно, такой подход является невыгодным для оферента, являющегося по умолчанию сильной стороной сделки, поскольку он посредством формирования и направления оферты определяет основные параметры и существенные условия сделки.

В литературе встречаются и другие позиции относительно определения места совершения сделки. Д. Е. Матыцин предлагает определять юрисдикционную принадлежность по адресу веб-сайта или веб-сервера стороны сделки [11. С. 68]. На наш взгляд, такая позиция является разумной, поскольку, как правило, веб-серверы, на которых размещаются крупные инвестиционные площадки, отличаются статичностью, вследствие чего осуществляемые с их помощью гражданско-правовые сделки могут характеризоваться определенной стабильностью. Вместе с тем автор не учитывает проблему использования VPN-сервисов, которые позволяют маскировать местонахождение исходного веб-сервера и таким образом менять юрисдикцию сделки при статичности серверного оборудования. Кроме того, не стоит забывать об общих принципах свободы волеизъявления сторон, позволяющих им самим определять место совершения сделки. В этой связи уместно предположить, что рост популярности сделок, совершаемых с использованием информационных технологий (например, инвест-платформ) будет сопровождаться усилением неравенства между участниками сделки в пользу владельца инвестиционной площадки и оферента.

Определение юрисдикции посредством местонахождения веб-сайта также несет под собой риск, связанный с возможными действиями кибермошенников, которые могут подменить оригинальное доменное имя поддельным. Например, использовав в названии сайта вместо буквы «о» цифру «0». При этом визуальное оформление мошеннического сайта может полностью совпадать с оригинальным.

Используя такие фишинговые схемы, мошенники могут завладеть учетными данными пользователей инвестиционных платформ и тем самым вывести денежные средства. Д. Е. Матыцин видит решение данной проблемы в создании специального реестра интернет-сайтов [11. С. 71]. В настоящее время в Российской Федерации действует реестр сайтов, содержащих запрещенную информацию (https://eais.rkn.gov.ru/), куда после специальной проверки вносятся неблагонадежные сайты. По нашему мнению, создание реестра «благонадежных» сайтов не столько поможет решить проблему кибермошенничества, сколько осложнит деятельность добросовестных администраторов доменных имен, коих, безусловно, большинство: создание реестра потребует за собой описание определенной процедуры включения интернет-сайта в этот реестр, проведение проверочных мероприятий. То есть, по сути, добросовестный владелец интернет-сайта должен будет подтверждать свою добросовестность, что фактически приводит к нарушению презумпции добросовестности участников гражданских правоотношений, установленный пунктом 5 статьи 10 ГК РФ [3].

Информационные технологии могут выступать не только в качестве средства осуществления гражданско-правовых отношений, но в качестве объекта соглашений. В частности, государство заинтересовано в инвестировании в развитие информационных технологий, для чего разрабатывают механизмы государственно-частного партнерства в данной сфере. Между тем ряд исследователей отмечают определенные недостатки правового регулирования такого партнерства в части судьбы результатов интеллектуальной деятельности. Например, Е. А. Громова отмечает, что терминология, используемая в законодательстве о государственно-частном партнерстве в сфере ИТ связана с правами на объект информационных технологий, а не с результатом интеллектуальной деятельности в целом [5. С. 35]. С указанной позицией не соглашается О. В. Егоров, отмечая, что объект информационных технологий вполне может представлять самостоятельный результат интеллектуальной деятельности, в связи с чем терминологическая неопределенность в данном случае не возникает [7. С. 42]. Определенный консенсус в литературе имеется по поводу необходимости установления открытого перечня объектов информационных технологий, которые могут быть предметом государственно-частного партнерства. Автор настоящего исследования разделяет указанную точку зрения, при этом хотелось бы добавить, что отсутствие законодательных ограничений относительно состава и перечня объектов информационных технологий позволит улучшить инвестиционный климат в государстве, поскольку законодатель не в состоянии предусмотреть все возможные виды объектов ИТ в условиях их постоянного развития и совершенствования.

С проблемой регулирования результатов интеллектуальной деятельности и исключительных прав на них субъекты гражданско-правовых отношений сталкиваются в тот момент, когда объектом отношений выступают результаты интеллектуальной деятельности, созданные с использованием цифровых технологий и технологий искусственного интеллекта. Основная сложность в таком случае связана с определением автора произведения, поскольку законодательство в качестве основного критерия для признания объекта произведением называет использование

творческого труда при создании [4]. В настоящее время среди специалистов в данной области идет активная дискуссия, связанная с определением автора произведения, сгенерированного компьютерной программой.

К. К. Таран исключает саму возможность признания авторства за искусственным интеллектом, поскольку это кардинальным образом изменит концептуальное направление всей системы гражданского права в Российской Федерации [16. С. 24]. Между тем, исследуя зарубежный опыт, нельзя не упомянуть о прецеденте признания части прав автора произведения за искусственным интеллектом, произошедшем в КНР. В то же время в США художница Кристина Каштанова была лишена прав автора на произведение «Рассветная заря», поскольку было установлено, что используемые в нем изображения полностью сгенерированы искусственным интеллектом.

Таким образом, представляется разумным при определении автора произведения, созданного с использованием технологий искусственного интеллекта, исследовать, прежде всего, техническую сторону программы с целью определения творческой составляющей в ее создании: принадлежит ли основной творческий вклад разработчикам программного обеспечения, либо пользователю, либо в определенном соотношении распределяется между ними. Представляется необходимым в этой связи законодательно регламентировать алгоритмы определения творческого участия в создании произведения. Использование цифровых информационных технологий оказало определенное влияние на систему правовых отношений в сфере наследственного права, в котором основные проблемы правового регулирования связаны с наследованием цифровых активов, передачей прав доступа к цифровым аккаунтам (прежде всего, в социальных сетях), а также составлением электронных завещаний.

Наиболее распространенными видами цифровых активов в настоящее время являются токены (в том числе невзаимозаменяемые (NFT)) и криптовалюта [21]. С помощью технологии блокчейн владелец соответствующего цифрового актива может зашифровать доступ к нему. При этом доступ к зашифрованному объекту третьих лиц полностью исключается. По мнению Т. С. Яценко, технология блокчейн является наиболее надежным способом защиты цифрового актива [18. С. 13]. Однако, на наш взгляд, указанный способ шифрования создает определенные сложности, связанные с получением доступа к активу наследниками в отсутствие необходимого распоряжения наследодателя.

Стоит отметить, что в Российской Федерации в настоящее время не определен порядок передачи цифровых активов по наследству. Вместе с тем российское законодательство идет в сторону развития системы регуляции отношений в сфере информационных технологий. В частности, законодатель легализовал цифровые права, определив их как обязательственные и иные права, содержание и условие размещения которых определяются в соответствии с правилами информационной системы [13]. То есть фактически правовая регламентация цифровых прав должна соответствовать требованиям информационной системы, в которой размещены объекты. По нашему мнению, такой законодательный подход следует считать адекватным, поскольку ввиду широкого разнообразия, а также тенденций

к изменению категорий цифровых прав и активов наличие их перманентного статичного статуса, установленного определенным нормативным правовым актом, привело бы к постоянному отставанию механизмов правового регулирования отношений от фактического содержания правоотношений.

В гражданско-правовых отношениях все большую роль приобретают социальные сети, которые выполняют не столько коммуникативную функцию, сколько коммерческую и зачастую используются в процессе осуществления предпринимательской деятельности. В этой связи особую ценность приобретают аккаунты в социальных сетях, используемые при осуществлении предпринимательской деятельности. Как и любой коммерчески значимый актив, аккаунты в социальных сетях, представляют особый интерес при наследовании, при этом порядок доступа к аккаунтам определяются не законодательством, а правилами соответствующей социальной сети. Т. С. Яценко приводит ссылку на судебный спор, возникший в США, в котором наследники требовали обязать социальную сеть предоставить доступ к аккаунту наследодателя [18. С. 9]. В конечном итоге, судебное решение было принято в пользу наследников, поскольку правилами пользовательского соглашения социальной сети не запрещено передавать информацию об аккаунтах пользователей третьим лицам в порядке наследования.

Принятый в конце 2019 г. Федеральный закон № 480-ФЗ внес значительный вклад в повышение качества нотариальных услуг, предусмотрев возможность оказания услуг удаленным способом [12]. По мнению Т. В. Андроповой на сферу наследственного права данный Федеральный закон не оказал значительного влияния, поскольку нотариальные услуги, оказываемые в наследственных правоотношениях, требуют ясного и четкого установления волеизъявления наследодателя, которое затруднительно получить в удаленном формате [1. С. 4].

Исследуя зарубежный опыт, следует отметить рост популярности использования электронных завещаний: в частности, с использованием специальных приложений для смартфонов, позволяющих верифицировать пользователя и сохранить созданное им завещание. В других случаях наследодатели создают видеозавещание и размещают его в открытом доступе (например, на популярной видеоплатформе YouTube). Стоит отметить, что ни одна из действующих правовых систем не признает легальность таких форм завещаний, однако нельзя отрицать, что ввиду развития цифровой и технологической грамотности населения подобные формы завещаний будут пользоваться все большей популярностью, в связи с чем правовые системы должны будут каким-то образом адаптироваться под изменяющиеся гражданско-правовые отношения. Более того, при помощи цифровых технологий у наследодателя появится больше возможностей зашифровать завещание (в том числе при помощи вышеописанной технологии блокчейн). Законодателю, однако, следует иметь в виду, что не все формы завещаний, сделанных с использованием современных технологий, следует переводить в правовое поле. Так, к использованию видеозавещаний следует, на наш взгляд, относиться скептически, поскольку подлинность видеозаписи и волеизъявление наследодателя могут вызвать определенные сомнения, учитывая стремительное развитие технологий искусственного интеллекта (в том числе технологии «дипфейк»).

В сфере предпринимательской деятельности, в частности в области оказания юридических услуг, существует большой спрос на информационные технологии и программное обеспечение, позволяющие оперативно проанализировать большой объем данных или сделать выборку по заданным критериям. П. Д. Константинов указывает на два типа алгоритмических программ такого рода: 1) программы типа COIN позволяют анализировать договоры и соглашения определенного вида; 2) программы типа Ross позволяют формировать юридические заключения [10. С. 20]. С одной стороны, использование программ подобного вида позволяет существенно сократить время специалиста, которое он потратит на ознакомление и анализ документа. С другой стороны, использование соответствующих программ должно происходить под контролем специалиста. Автор предостерегает от излишней автоматизации и алгоритмизации юридической деятельности, в частности, от использования алгоритмов при отправлении правосудия. На наш взгляд, правовое регулирование использования вспомогательных программ должно основываться на следующих аспектах. Во-первых, технологическая составляющая программы должна учитывать возможное изменение законодательства, которое неминуемое влечет за собой изменение правоприменительных подходов. Во-вторых, вспомогательные программы должны быть направлены именно на помощь специалисту в решении поставленных задач, но ни в коем случае не должны решать задачи за него.

Важнейшей формой осуществления гражданско-правовых отношений является проведение собраний. При этом собрания проводятся как для коммерческих целей (например, в хозяйственных обществах), так и в иных целях, не связанных с коммерческой деятельностью (например, собрания собственников помещений в многоквартирном доме). Основная проблема, с которой сталкиваются организаторы проведения общих собраний, – обеспечение кворума. Особенно эта проблема актуальна для собраний жильцов многоквартирного дома (с учетом современных тенденций к многоэтажной поквартальной застройке).

Использование информационно-коммуникационных технологий позволяет решить проблему наличия кворума при проведении собраний. Особую популярность использование таких технологий приобрело в период острой фазы эпидемии новой коронавирусной инфекции COVID-19 в 2020 г. [20], когда многие граждане перешли на удаленный формат работы. Между тем возможность проведения общих собраний с использованием телекоммуникационных технологий не в полной мере отражена в российском законодательстве. И Жилищный кодекс Российской Федерации (далее – ЖК РФ), и Федеральный закон «Об акционерных обществах» (далее – Закон об АО) предусматривают возможность проведения собраний в заочной форме. При этом, как отмечает Ю. Н. Коваленко, законодательство не совсем четко и однозначно оперирует понятиями «форма собрания» и «форма голосования», часто смешивая их [9. С. 32]. Например, электронная или письменная форма голосования может использоваться как при очной, так и при заочной формах собрания.

Заочная форма проведения собраний не сильно приветствуется российским законодателем. Так, ЖК РФ позволяет проводить заочное собрание только в том

случае, если очное не состоялось по каким-либо причинам (п. 1 ст. 47 ЖК РФ). На наш взгляд, такой законодательный подход не выглядит эффективным, поскольку: а) заочная форма таким образом выглядит более «слабым» способом принятия решений; б) требует больших организационных затрат на проведение собрания. Предполагается, что смысл очной формы проведения собрания заключается в возможности обмена мнениями и аргументами относительно вопросов, вынесенных в повестку дня собрания. В этой связи законодателю следует разработать эффективный правовой механизм реализации обмена мнениями и аргументами участниками собраний, в частности, с помощью информационных технологий (участие в онлайн-конференции или обсуждение в мессенджерах посредством создания общих чатов).

Таким образом, по результатам исследования основных проблем гражданско-правового регулирования отношений, связанных с использованием информационных технологий, можно сделать вывод о том, что в настоящее время развитие технологий опережает «обрастание» правоотношений правовыми регуляторными механизмами. При этом данная особенность свойственна не только российской правовой системе, а является глобальной мировой тенденцией. В таком случае уместно говорить о необходимости определения единой концептуальной правовой регламентации гражданско-правовых отношений, осуществляемых с использованием информационных технологий, с возможностью определенными цифровыми платформами устанавливать на основе общих требований конкретные регламенты взаимодействия.

Список литературы

1. Андропова Т. В. Информационные технологии в наследственном праве // Наследственное право. 2020. № 2. С. 3–6.

2. Белицкая А. В., Белых, В. С., Беляева, О. А. и др. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография; отв. ред. В. А. Вайпан, М. А. Егорова. М.: Юстицинформ, 2019. 376 с.

3. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства РФ. 1994. № 32. Ст. 3301.

4. Гражданский кодекс Российской Федерации (часть четвертая) от 18 декабря 2006 г. № 230-ФЗ // Собрание законодательства РФ. 2006. № 52 (1 ч.). Ст. 5496.

5. Громова Е. А. Государственно-частное партнерство в цифровую эру: поиск оптимальной правовой формы // Юрист. 2018. № 10. С. 31–39.

6. Декрет № 8 «О развитии цифровой экономики». URL: http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716

7. Егоров О. В. Проблемы правового регулирования соглашений о государственно-частном партнерстве и концессионных соглашений, объектом которых выступают информационные технологии, и пути их решения // Хозяйство и право. 2022. № 11. С. 39–49.

8. Карлаш Д. С. Электронный документооборот: вопросы правового регулирования // Право и экономика. 2019. № 8. С. 22–28.

9. Коваленко Ю. Н. Развитие альтернативных форм проведения общих собраний сособственников // Гражданское право. 2022. № 1. С. 30–33.

10. Константинов П. Д. Анализ цифровых технологий, направленных на помощь в осуществлении юридических услуг // Арбитражный и гражданский процесс. 2022. № 7. С. 19–20.

11. Матыцин Д. Е. Методологический базис гражданско-правового регулирования дистанционных инвестиционных сделок // Актуальные проблемы российского права. 2022. № 4. С. 65–75.

12. О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации: Федеральный закон от 27 декабря 2019 г. № 480-ФЗ // Собрание законодательства РФ. 2019. № 52 (ч. 1). Ст. 7798.

13. О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации: Федеральный закон от 18 марта 2019 № 34-ФЗ // Собрание законодательства РФ. 2019. № 12. Ст. 1224.

14. О государственно-частном партнерстве, муниципально-частном партнерстве в Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 13 июля 2015 г. № 224-ФЗ // Собрание законодательства РФ. 2015. № 29 (ч. 1). Ст. 4350.

15. О цифровых финансовых активах: проект Федерального закона № 419059-7 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PRJ&n=170084

16. Таран К. К. Предпосылки правового регулирования результатов интеллектуальной деятельности, созданных с использованием искусственного интеллекта // Право и экономика. 2023. № 1. С. 20–27.

17. Трофимов А. А. Использование государственных информационных систем для идентификации субъектов при заключении гражданско-правовых договоров // Гражданское право. 2022. № 5. С. 43–45.

18. Яценко Т. С. Наследование цифровых прав // Наследственное право. 2019. № 2. С. 9–14.

19. Яценко Т. С. Наследственное право в цифровую эпоху: вызовы и тенденции развития // Наследственное право. 2020. № 2. С. 8–11.

20. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

21. Жарова А. К. Риски информационной безопасности и возможности правового регулирования криптовалюты в России // Информационное право. 2018. № 4. С. 11–16. EDN: YPNFET

В. А. Лукинова,
слушатель,
Уфимский юридический институт
Министерства внутренних дел
Российской Федерации

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Аннотация. Исследование посвящено анализу мошенничества по телефону, а именно выделяются способы телефонного мошенничества, особенности работы мошенников, средства обеспечения безопасности пользователей, и рассматривается ответственность операторов связи.

Ключевые слова: телефонное мошенничество, телефонный звонок, текстовое сообщение, способы телефонного мошенничества, средства обеспечения безопасности, оператор связи

DIGITAL TECHNOLOGIES AND TELEPHONE FRAUD

Abstract. The study is devoted to the analysis of telephone fraud, namely, methods of telephone fraud, features of the work of fraudsters, means of ensuring user safety are highlighted, and the responsibility of telecom operators is considered.

Keywords: telephone fraud, telephone call, text message, methods of telephone fraud, security measures, telecom operator

Часто встречаются преступления в телекоммуникационной среде с использованием телефонной связи. Преступники совершают мошеннические действия через телефонный звонок или посредством отправки текстового сообщения.

Телефонное мошенничество – особый вид мошенничества в области информационных технологий, представляющий собой несанкционированные действия и неправомерное пользование ресурсами и услугами, хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, модификации информации или другого вмешательства в работу средств обработки или передачи данных информационно-телекоммуникационных сетей [4].

Мобильное мошенничество происходит через телефонный звонок. Современные технические возможности средств сотовой связи также позволяют проводить адресную рассылку БМБ-сообщений [2].

Мошенник применяет различные способы для обмана пользователей сотовых телефонов, в частности, манипуляцию.

Вишинг, также известный как голосовой фишинг, представляет собой киберпреступление, при котором злоумышленники используют телефон для кражи личной информации в своих целях. При вишинг-атаке киберпреступники используют тактику социальной инженерии, чтобы убедить жертв предоставить личную информацию, как правило, с целью доступа к финансовым счетам [3].

Вот некоторые способы телефонного мошенничества:

– используя похожий номер службы безопасности банка, злоумышленник говорит о том, что с карты пользователя снята определенная сумма денег, и для разблокирования банковской карты необходимо назвать CVC-код;

– мошенники могут позвонить на мобильный телефон и предложить помочь близкому человеку, который попал в беду, за некоторую сумму. Иногда злоумышленники звонят с неизвестного номера, представляясь близким человеком, прося перевести им деньги. Потерпевшие говорят о том, что голос был очень похож на голос близкого человека, и в панике они перевели сумму денег;

– телефонный вызов, который сбрасывается при ответе абонента, понуждает перезвонить на неизвестный номер, за что будет взиматься плата;

Мошенничество с использованием текстовых сообщений:

– сообщение с просьбой перевода денежной суммы близкому человеку;

– пополняется баланс номера или карты банка, далее приходит сообщение, что деньги перевели по ошибке и требуют перевести их обратно;

– рассылка текстовых сообщений о большом денежном выигрыше, для подтверждения необходимо отправить текстовое сообщение с кодом на неизвестный номер, за что взимается плата.

Также, преступник может взять микрозаем в Интернете, используя паспортные данные абонента. Данные лица предоставляются при заключении договора об оказании услуг сотовой связи [5].

Преступников тяжело идентифицировать из-за того, что используется подменный номер и для хранения денег используют криптовалюту. Они применяют VPN, прокси-серверы с целью маскировки своего адреса.

Особенности работы мошенников:

– звонят первыми;

– ведут разговор о деньгах;

– пытаются узнать личные данные: паспорт, номер карты, пароль, код из банковских уведомлений;

– используют техники манипуляции, пытаются ввести в замешательство, говоря о трагедии с близким человеком;

– оказывают давление, ограничивая во времени, чтобы абонент незамедлительно совершил указанные действия.

Средством обеспечения безопасности своей банковской карточки является установление лимитов на переводы. Будет определена незначительная сумма денег. Если посредством звонка банковский работник просит увеличить или убрать лимит, стоит задуматься о том, что позвонил мошенник.

В случае звонка о несчастном случае близких людей стоит проверить подлинность сведений. Необходимо уметь противостоять мошенникам путем бдительности и понимания вероятных рисков. Стоит внимательно прислушаться к акценту и интонации позвонившего лица. Зачастую звонки совершаются из-за границы с использованием российских сим-карт.

Есть возможность определять неизвестные номера через поисковую систему Интернета и специальные приложения. Диагностика номера позволит определить имя позвонившего.

Будет ли привлечен оператор связи из-за телефонного мошенничества? При помощи ст. 13.2.1 КоАП РФ оператор связи будет привлечен к административной ответственности, если не отключит подменные номера мошенников, которые используют российские номера, делая вызов из-за рубежа.

В надзорном органе рассматривается вопрос об аннулировании лицензии при злостных нарушениях сотового оператора [1]. И, таким образом, это позволит закрыть компании сотовой связи, которые незаконно выполняют свои функции, допуская деятельность мошенников.

Итак, мошенники часто используют телефон для совершения преступления. Для профилактики преступлений в данной сфере следует быть предусмотрительным, применять способы определения неизвестного номера. Стоит незамедлительно обращаться в правоохранительные органы о телефонном мошенничестве. Для операторов связи предусмотрена административная ответственность ст. 13.2.1 КоАП РФ, что должно уменьшить число телефонных мошенников.

Список литературы

1. Вопросы борьбы с интернет-мошенничествами / В. А. Емельянова, А. М. Салимова, М. Л. Цвет, И. А. Биккинин // Russian Studies in Law and Politics. 2022. Т. 6, № 1–2. С. 58–62. EDN: XBMTNM

2. Гаврилова А. А. Sms-оповещение населения: подходы к оценке коммуникативной эффективности // Технологии гражданской безопасности. 2008. № 4.

3. Куренная В. О. Фишинг и вишинг в информационной безопасности // StudNet. 2022. № 6.

4. Леваков А. К. Телефонное мошенничество: трудности противодействия // Вестник связи. 2020. № 12. С. 15–16.

5. Цвет М. Л., Биккинин И. А. Телефонное и интернет мошенничества: феномен малой раскрываемости // XVII Акмуллинские чтения: материалы Международной научно-практической конференции. Уфа, 2–3 декабря 2022 года. Т. 1. Уфа: Башкирский государственный педагогический университет им. М. Акмуллы, 2022. С. 229–231.

В. Ю. Мамкин,
магистрант,
Московский государственный юридический университет
имени О. Е. Кутафина

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ БОЛЬШИХ ДАННЫХ В ФИНАНСОВОЙ И БАНКОВСКОЙ СФЕРАХ: ЗАДАЧИ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. В статье анализируются внедрение и задачи правового регулирования использования технологий больших данных в финансовую и банковскую сферы. Применение Big Data в таких областях, как финансовая и банковская, нацелено на повышение работоспособности банков, улучшение бизнес-процессов, однако формирует новые рисковые факторы и требования к компетенциям персонала, определяет необходимость трансформации регулятивных подходов, сотрудничества банков. Законодателю рекомендуется разработать нормативно-правовую базу, регулирующую формирование и использование экономическими агентами открытых данных.

Ключевые слова: правовое регулирование, большие данные, банковская сфера, сфера финансов, закон, технологии, нормативно-правовая база

APPLICATION OF BIG DATA TECHNOLOGIES IN FINANCIAL AND BANKING SPHERES: CHALLENGES OF LEGAL REGULATION

Abstract. The scientific article is aimed at analyzing the application of big data technologies in the financial and banking spheres, as well as at considering the challenges associated with their legal regulation. The analysis shows that the use of data in these areas can have a significant impact on security, privacy, competition and user rights. To address these issues, it is necessary to develop effective legal regulation.

Keywords: legal regulation, big data, banking, finance, law, technology, regulatory framework

В нынешней цифровой экономике сквозные технологии проникают во все сферы, а цифровая трансформация служит одной из национальных целей развития России согласно Указу Президента Российской Федерации от 21 июля 2020 г. № 474. Банки активно участвуют в этих процессах и получают преимущества от применения цифровых технологий и платформенных решений, что позволяет им сокращать затраты на рутинные операции, изменять банковские бизнес-модели и создавать новую ценность для клиентов.

Поддержанию финансовой стабильности, участию в конкуренции, повышению доступности финансовых услуг способствуют цифровые технологии на макроуровне. Тем не менее процессы цифровой трансформации, которые одновременно происходят в сфере банков, соединены с новыми проблемами, требующими обоснованного наукой решения, создающими очередные рисковые факторы, влекущими вызвать системные риски и определить необходимость преобразования регулятивных подходов. Одной из сквозных цифровых технологий, внедрение которой обеспечивает цифровую трансформацию банков, банковского сектора и финансового рынка в целом, является технология больших данных (Big Data). Регулярные изменения происходят благодаря обусловленным значительным превосходствам банков и некредитных финансовых организаций, которые они получают от использования технологии Big Data.

Цель этой научной статьи заключается в разработке рекомендаций по применению таких технологий в банковском секторе, включая заключение сделок не без помощи финансовой платформы, с учетом обеспечения стабильности банковского сектора на макро- и микроуровне, а также развития финансового рынка [4].

Для достижения этой цели были поставлены и решены следующие задачи, определившие структуру настоящей статьи: описать исследовательскую программу, связанную с преобразованием работы банка с информацией на основе технологии Big Data; изучить направления и преимущества использования Big Data в банках; выявить проблемы, связанные с использованием этой технологии в банковской сфере; определить тенденции взаимодействия между банками, финансовыми платформами и провайдерами услуг из небанковского сектора при

использовании этой технологии; критически рассмотреть практики, направленные на развитие применения Big Data в банках.

Большие данные – это массивы информации, которые включают в себя разные средства и методы обработки значительных объемов сформированных и несформированных сведений [9. С. 50]. С помощью этой технологии можно результативно применять данные для выполнения разных задач и достижения конкретных целей. Один из существенных плюсов применения Big Data – быстрая скорость обработки информации, что является одной из важнейших составляющих для банковских организаций, где время имеет большое значение для людей и банков, в которых уже успешно используются Big Data. В качестве примера можно привести то, что раньше рассмотрение информации о людях, которые подавали заявку на кредитную карту, могло занимать достаточное количество дней. Тем не менее, с применением Big Data такой процесс теперь охватывает незначительное количество времени. В банковской сфере активно применяются Big Data, чтобы анализировать поведение людей и изучать их предпочтения. Это способствует банкам точнее понимать своих людей и предлагать им наиболее подходящие услуги. Примером успешного применения Big Data в банках служит анализирование Сбербанком сведений о своих пенсионерских клиентах [10. С. 1]. С помощью Big Data выявлено, что наибольшую часть важных депозитов открывают люди в возрасте 50–55 лет. После 68 лет структура их использования становится менее разнообразной. Также были выявлены различия в поведенческих моделях пенсионеров и предпенсионеров. Банки РФ также применяют технологию больших данных для сегментации людей. Для регистрации людей и обнаружения их активности в банковской сфере уже давно применяются программные механизмы [5. С. 33].

Тем не менее с применением больших данных они могут более точно определить потребности и желания каждого человека или группы людей, что предоставляет им возможности предлагать наиболее персонализированные услуги и улучшать общее качество обслуживания. Технология Big Data имеет огромный потенциал в банках и продолжает развиваться. Для получения максимального для себя результата из такой технологии в банковской сфере активно исследуются новые методы и подходы к обработке и анализу данных.

Сбербанк, как один из крупнейших банков в России, обладает обширной информацией о своих клиентах. Банк обладает информацией о региональных кредитах государства, долях расходов на разные услуги и товары, а также доступом к сведениям о склонности людей к расходам или сбережениям, их доходах, прибыли организаций. Эти данные позволяют банку анализировать поведение клиентов на рынке и определять их финансовые потребности. Сбербанк предлагает наиболее подходящие банковские услуги и делает классификацию клиентов по определенным группам, используя современные аналитические инструменты и технологии. К примеру, клиенту могут предложить выгодные условия по депозитам, если он проявляет склонность к сбережениям. Банк может предложить клиенту выгодный кредит для покупки товаров или услуг, если клиент активно тратит деньги на определенные товары или услуги. Технологии анализа сведений также помогают банку предвидеть возможное банкротство юридических

лиц-клиентов. Таким образом, в банковской сфере могут быть приняты конкретные действия для минимизации своих рисков в условиях резкого и стабильного снижения доходов, которые могут служить предупреждением о проблемах с выплатой кредита. Скорость обработки сведений является одним из ключевых преимуществ применения аналитических технологий в банковской сфере. Это дает банкам принимать решения по выдаче кредитов или предоставлению других услуг в кратчайшие сроки. Клиенты способны приобрести необходимые финансы без существенных затрат времени и усилий благодаря онлайн-кредитованию, которое стало доступным и удобным. Ручная оценка, которая базируется на опыте и интуиции работников банка является менее объективным подходом, чем применение аналитических технологий в сфере банков при определении кредитоспособности людей [6]. Скрытые тренды и закономерности могут быть вполне невидимы при традиционном подходе. Они выявляются при помощи больших объемов данных и алгоритмов анализа. При нейтрализации преступлений в сфере финансов, таких как сомнительные сделки и вывод капитала, технология больших данных играет существенную роль. Анализ данных о поведении клиентов и их банковских операциях позволяет выявлять подозрительные ситуации и принимать меры для предотвращения возможных финансовых мошенничеств или террористического финансирования.

По итогу обработки данных сформировался ряд показателей (анализ, синтез, актуальность информации и выводы), которые составляют потенциальную ценность технологии. Такое явление предоставляет возможность эвальвировать работу Big Data как Value (ценность) [11].

Помимо коммерческих банков, эта технология является также актуальной для Центрального банка Российской Федерации (ЦБ РФ), который проводит анализ большого количества сведений, ежеминутно поступающих от банков в виде отчетов. Если выявятся существенные нарушения требований, с помощью анализа ЦБ РФ принимает соответствующие меры о санации банка или лишении его лицензии. Помимо этого, ЦБ РФ анализирует уровень кредитного снабжения населения, экономику государства и т. д.

Использование больших данных делает такой процесс заметно проще и ускоряет его. Также Big Data способствует ЦБ РФ в своевременном предупреждении потенциальных нарушений и осуществлению надзора за деятельностью кредитных организаций. Из-за этого Центральный банк Российской Федерации принял «Основные направления развития финансовых технологий на 2018–2020 годы», где содержится информация о том, что технология Big Data является перспективной и планируется разработать предложения и рекомендации по ее применению для ЦБ РФ и участников финансового рынка [7. С. 3].

Технология больших данных широко применяется многими, но в настоящее время не существует официальной законодательной базы для ее использования. Федеральный закон «Об информации, информационных технологиях и о защите информации» [1] не отражает, по нашему мнению, требований банковского сектора в регулировании использования больших данных. Считаю, что через развитие института персональных данных, должно происходить регулирование Big Data.

Для полной реализации Федерального закона «О персональных данных» [2] необходимо расширить понятие персональных данных, включив в него метаданные, позволяющие косвенно идентифицировать субъекта, такие как данные о местоположении, сетевых адресах и т. д., история посещений веб-страниц. Следует усилить организацию обработки добровольно предоставляемых данных, в том числе разъяснять действия по обезличиванию и обработке данных после обезличивания – с согласия или без согласия лица, предоставляющего персональные данные.

Банки могут потерять большую часть своих клиентов в ближайшем будущем, если не будут использовать самые современные стратегии анализа данных, способствующих удовлетворению потребностей людей. То есть технологии больших данных необходимы для того, чтобы идти в ногу с мировыми тенденциями. Чтобы обеспечить успешное внедрение и последовательное применение больших данных кредитными организациями, государство должно постоянно расширять использование больших данных посредством законодательного регулирования.

В связи с популярностью технологии блокчейн в финансовой сфере большинство экономик активно рассматривает вопросы нормативного регулирования и развития этой технологии. Среди недавних примеров рекламы технологии блокчейн – анонс Сбербанком 20 мая 2021 г. своей блокчейн-платформы, предоставляющей создателям полнофункциональный API и библиотеки для работы с общедоступными токенами. Она предназначена для подготовки возможности простых в использовании программ для клиентов, способных работать с блокчейн-платформой, применяя определенную расчетную единицу, интегрированную с банком. Благодаря этому возможно применять расчетные действия, основу которых составляют рублевые смарт-контракты. Именно через привлечение участников-валидаторов, которые привлекаются для проверки точности и правильности транзакций, хотя доступ к защищенным сведениям в таких транзакциях для них закрыт, обеспечивается децентрализованная структура платформы [3].

Банки и финансовые платформы используют аналитику Big Data для решения различных задач, связанных с предоставлением финансовых услуг, как указывается в литературе. Исследователи Европейского банковского управления (EBA) отмечают, что банки применяют аналитику Big Data для управления рисками, взаимодействия с клиентами, анализа рынка и оптимизации внутренних процессов. Применение больших данных может принести значительные преимущества финансовым институтам в различных областях их деятельности. Они могут повысить эффективность, сократить издержки и увеличить прибыль. Благодаря объему и скорости обработки данных, а также автоматизации, технологии больших данных предоставляют финансовым институтам возможности управления рисками, оптимизации операционной деятельности, улучшения работы финансового рынка. Они также позволяют предлагать клиентам более индивидуальные услуги и расширять круг потребителей. Технологии больших данных связаны с некоторыми рисками для пользователей, даже если финансовые учреждения, клиенты финансовых услуг и финансовая система в целом застрахованы от опасностей.

К таким относятся риски, связанные с методологическими опасностями, с защитой персональных данных, антиконкуренции и дискриминации, с работой третьих сторон, а также существование серых зон в регулировании.

Превосходство Big Data признано в финансовых учреждениях, и эта точка зрения подкрепляется примерами, представленными ранее.

Во-первых, из социальных сетей и прессы, такая технология предоставляет возможность получать сведения из разных внешних источников, а также анализировать внешние и внутренние данные в режиме реального времени с использованием методов машинного обучения.

Big Data увеличивает скорость транзакций на высокоразвитых и широко применяемых рынках, к примеру, фондовые, поскольку люди пользуются ими для применения инвестиционных решений, прогнозирования будущих цен, управления своими инвестиционными портфелями и определения комиссий за предоставляемые услуги, одновременно повышая скорость операции на технологически развитых и популярных рынках.

Во-вторых, применение больших данных улучшает качество управления рисками путем анализа значительного объема данных, включающие в себя неструктурированные внешние данные, которые ранее не учитывались. При использовании обыденных средств невозможно обнаружить закономерности и взаимосвязи, но эту проблему можно решить путем внедрения технологий искусственного интеллекта. Кредитный скоринг на основе больших данных повышает точность оценки, включая выдачу кредитов, делая ставки более беспристрастными с точки зрения риска.

В-третьих, из-за нехватки сведений, нужных для оценивания кредитоспособности потенциальных заемщиков, в ряде растущих и перспективных стран и стран с развивающейся рыночной экономикой происходит нехватка кредитов для домохозяйств и МСП. По некоторым расчетам, население Китая зачастую проходит через трудности при получении кредита, несмотря на то, что процент кредитов для МСП всего 20–25 % от общего объема корпоративного кредитования, хотя вложение сектора в ВВП – примерно 60 %, содействие созданию рабочих мест – 80 %. Большие данные могут улучшить кредитоспособность заемщиков путем анализа данных, касающихся происхождения кредита, статуса кредита, времени обработки платежей, коммунальных услуг, операторов сотовой связи и других связанных показателей.

Big Data дают возможность институтам, касающимся финансов, увеличить и распространить базу клиентов с помощью домашних хозяйств и МСП, которые не имеют никакой кредитной истории, но тем не менее их кредитоспособность может оцениваться с применением альтернативных источников, содержащих сведения (арендная плата, платежи за коммунальные услуги для домашних хозяйств, объемы продаж для предприятий). В результате таких действий может повыситься доступность услуг в сфере финансов в пределах границ финансовой системы.

На основе анализа рынка потребительских кредитов в Соединенных Штатах Америки становится понятно, что неправильное оценивание кредитоспособности заемщиков на основе неточных больших данных или ошибочных моделей ведет

к отсутствию улучшения финансовой доступности для некоторых заемщиков из-за неполных и неточных моделей. Помимо этого, применение моделей Big Data может привести к дефициту экономических услуг, которые доступны заемщикам, из-за возможности дискриминации по конкретным параметрам.

В-четвертых, огромному количеству клиентов предоставляется возможность использовать персонализированные услуги: в прошлом для понимания потребностей людей нужно было персональное общение с представителями финансовой организации, но в настоящее время анализ Big Data дает возможность давать персональные услуги миллионам людей.

Финансовые учреждения применяют аналитику расходов людей, активности в социальных сетях и сведения геолокации, чтобы лучше понимать в чем больше всего нуждаются пользователи. Big Data делают лучше таргетинг компаний и цен, особенно в страховой сфере, за счет точного сегментирования возможных клиентов.

Таким образом, в общей сложности применение технологий больших данных позволяет более результативно переработать сведения в разных областях рынка финансов, редактировать данные, что приводит к снижению рисков с точки зрения их управления и обслуживания людей.

Преимущества использования Big Data в банковской сфере включают:

– повышение эффективности маркетинга и управления рисками;

– существенное улучшение результатов оценки и расширение объема данных для анализа с использованием различных источников и типов данных;

– снижение затрат на управление рисками кибербезопасности, выявление мошенничества и выполнение надзорных требований «Знай своего клиента» (Know your customer);

– предоставление дифференцированных и настроенных под потребности клиентов услуг, персонализация обслуживания, что способствует созданию новой ценности и повышает доходность банковской деятельности;

– возможность повысить оценку уязвимостей банковской области, увеличить выбор переменных для последствий реализуемых регулирующих мер и анализа финансовой стабильности, обеспечивая устойчивость других участников и рынка в целом. Это также способствует установлению справедливого ценообразования и исключению ложной информации.

Чтобы достичь преимуществ и устранения недостатков использования Big Data, рекомендуется разделять функцию управления данными, которые уменьшают непрозрачность взаимоотношений, информационную асимметрию в отношениях между клиентами и банками, создает потребность в новых высококвалифицированных сотрудниках, изменении бизнес-процессов, мышления руководства банка, регламентов и процедур.

При образовании, проверке и коррекции моделей банков, базирующихся на больших данных, регуляторам нужно увеличивать свои подходы и принципы к применению и защите данных, создать новый регулятивный инструментарий для предотвращения монополизации рынка банков и концентрацию его сегментов, которые реализуют экосистемную модель, обратить внимание на

микропруденциальные инструменты регулирования банковских рисков для предотвращения дискриминации потребителей услуг операторов финансовых платформ, которые предлагают новые денежные продукты, содержащие основу Big Data.

Оказывать неблагоприятное влияние на конкуренцию и ограничивать доступ малых и средних банков может экосистемная деятельность на банковском рынке, тем самым создавая опасность справедливого образования цен и предложения высокого качества банковских продуктов и услуг, которые соответствуют нуждам людей.

В качестве рекомендаций также следует сделать сертификацию специализированных поставщиков, которые сотрудничают с банками, продолжить разработку нормативно-правовой базы, регулирующей формирование и применение открытых сведений агентами в сфере экономики, направленной на уменьшение рисков, создание условий для денежной доступности, доверительных отношений между рыночными участниками, конкуренции и общего снабжения стабильности и эволюции рынка финансов.

Воздействие основанного на данных подхода на банковскую деятельность отражается в бизнес-стратегиях, рисках и операциях банков. Традиционный подход банков к анализу основан на использовании данных, собранных о клиентах, контрагентах и рынках, на которых они действуют. Понимание важности расширения объема анализируемых данных ставит перед банками новые вопросы относительно источников данных, их структурирования и обработки.

Технология Big Data включает работу с большим объемом данных, поступающих из разных источников и в разном формате. Работа с данными в банке проходит через несколько этапов. Сначала анализируются бизнес-процессы и определяются производственные задачи, для решения которых используются Big Data. Затем происходят сбор данных и их подготовка, включающая очистку, гибридизацию и переформатирование данных. Очистка данных предполагает исключение недостоверной информации, которая непригодна для анализа. Гибридизация включает объединение Big Data с другими данными, включая малые данные (small data), которые можно понять и обработать без использования машин. Переформатирование данных предполагает приведение различных типов данных (например, изображения, текст, аудио, финансовые данные и т. д.) к формату, с которым можно работать с помощью аналитических алгоритмов. В научной литературе предложена классификация данных в зависимости от их формата. Так, данные могут быть жесткими и мягкими, где жесткие данные представляют количественную информацию в числовом виде. Их легко собирать, хранить, анонимизировать и обмениваться; к работе с жесткими данными можно применять регламенты, минимизируя риски, связанные с субъективностью действий персонала.

Таким образом, с развитием цифровых платформ и платформенных решений, являющихся основой цифровой экономики, технология Big Data получает возможность применения в банковской сфере. Внедрение больших данных в практику банков предъявляет новые требования к компетенциям сотрудников, что ставит перед руководством банков, рынком труда, образованием и наукой новые задачи.

Переход к использованию Big Data подразумевает, что данные создаются и собираются разными участниками рынка. Это означает необходимость параллельных затрат на сбор, обработку и реализацию этапов Big Data, таких как разработка, тестирование и использование различных аналитических моделей, создание аналитических отчетов и т. д. В масштабах экономики такие процессы мешают созданию положительных эффектов от единого информационного пространства, сокращению затрат на работу с данными, улучшению качества моделей и управленческих решений, созданию равных конкурентных условий для разных банков.

Одновременно изолированность данных внутри каждого банка или экосистемы мешает удовлетворению клиентской потребности в удобном получении банковских и финансовых услуг, управлении личными финансами. Клиент может обратиться в банк за услугой, например, кредитом, даже если он не является клиентом этого конкретного банка, но будет вынужден понести расходы на предоставление информации о себе, которая уже есть у другого обслуживающего банка. Клиент, обслуживаемый разными банками, нуждается в одном приложении, где он может видеть все свои счета в разных банках и управлять ими. Возможность решения таких задач предоставляется концепцией открытого банкинга (Open banking), согласно которой обслуживающий банк как третья сторона, как финтех компания, предоставляет банковские данные клиента с его согласия. Реализация этой концепции осуществляется через использование открытых API.

В странах ЕС Open banking имеет юридическую основу. В соответствии со второй Директивой ЕС о платежных услугах (PSD2) крупнейшие банки Великобритании обязаны с 2018 г. раскрывать информацию о счетах и транзакциях клиентов. Обмен финансовой информацией между банками и другими организациями, с соблюдением требований по защите и конфиденциальности, позволяет повысить эффективность оценки рисков и сократить затраты и время на принятие решений. В Российской Федерации система открытого банкинга поддерживается регулятором по рекомендации. Центральный банк Российской Федерации создал стандарты для извлечения сведений о банковских счетах и транзакциях пользователей, предполагающих предоставление сведений при взаимодействии между банком, клиентом, участниками перевода денег и разработчиками программного обеспечения. Использование таких стандартов добровольное. В зарубежных странах преимущества, получаемые участниками взаимодействия с применением открытых API в соответствии с концепцией открытого банкинга, привели к последовательному формированию еще двух концепций: открытых финансов (Open finance) и открытых данных (Open data).

Положительные итоги применения Big Data в банковской сфере определяются несколькими условиями:

1. Наличие квалифицированного персонала с необходимыми техническими и профессиональными навыками в банковской сфере.

2. Финансирование расходов на внедрение технологии.

3. Создание необходимой инфраструктуры и выбор соответствующих технологий для работы с Big Data.

Также существует ряд сложностей, включая правильный выбор методов и алгоритмов для работы с этой технологией.

Можно выделить ряд рисков:

1. Стремительное развитие Big Data и введение новых решений со стороны поставщиков программного обеспечения и технологических услуг (несоответствие между заявленной надежностью и результативностью может привести к ошибочном принятым решениям).

2. Риск зависимости от поставщиков услуг, необходимых для функционирования финансовых платформ, который следует рассматривать как компонент операционного риска (может проявиться в нарушении договорных обязательств, защиты данных или неэтичном поведении, послужить потерей операционной устойчивости банка). Европейские регуляторы возлагают ответственность за управление им на банки.

Для выбора наилучших поставщиков программного обеспечения, облачных хранилищ и других нужных компонентов для воплощения Big Data банки и операторы в финансовой сфере должны иметь свой персонал.

Интеграция внешних сервисов между собой служит еще одной проблемой, которую банки должны устранить при их выборе. Важно обозначить точные критерии для сотрудничества с поставщиками и отказа одному поставщику в пользу другого.

Значение модельного риска повышается при работе с большими данными. На него влияют качество и количество данных, на которых основаны модели. Он тесно связан с кибератаками и техническими сбоями, являющихся новыми факторами риска, которые внедряются в аналитические модели. К ним предъявляются определенные требования:

1. Соответствие регулятивным нормам и стандартам профессионального сообщества.

2. Результаты и допущения моделей должны быть понятными, прозрачными и наглядными.

Законодательного регулирования в сфере Big Data в настоящее время нет. В Федеральном законе от 7 июля 2003 г. № 126-ФЗ «О связи» существует важная информация в области обработки больших данных, которая рассматривается в соответствии с государственной программой «Цифровая экономика». В рамках этого закона существуют мероприятия на период до 2024 года.

АНО «Право роботов» ответственна за формирование и согласованность такой группы, объединяющей всех заинтересованных лиц IT-рынка Российской Федерации и экспертов в правовой сфере. Сферы по использованию Big Data могут регулировать ФЗ от 27.07.2006 № 152-ФЗ «О защите персональных данных» и ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

«Элементы доверия» наделяют конкретные принципы и процедуры, которые должны быть включены во всестороннее регулирование применения больших данных банками и организациями. Они содержат в себе этические вопросы, объяснимость и интерпретируемость данных, отслеживаемость, возможность их аудита,

качества, защиту и безопасность, предотвращение предвзятости, а также защиту прав потребителей банковских и финансовых услуг.

Для полноценной стабильности в сфере банков важным направлением является развитие поведенческого надзора.

Основным инструментом для решения большого количества задач является технология Big Data. Тем не менее законодателю лучше всего акцентировать свое внимание не только на алгоритме или технологии передачи личных сведений, но и на последующем применении этих данных. Необходимо принять меры по обеспечению неприкосновенности частной жизни людей, а также улучшить нынешнее актуальное законодательство в цифровой отрасли, разработав конкретный НПА. В целях нейтрализации монополизации применения Big Data можно предложить внедрение дополнительных преград при приобретении таких технологий. Монополия на рынке больших данных может представлять угрозу, поэтому особенно важно обратить внимание на меры для защиты от атак хакеров и утечек персональных сведений.

Мировая практика внедрения финтехпродуктов показывает, что нормативно-правовое регулирование остается важным вопросом, так как зачастую требуется внесение изменений в действующую нормативную базу.

Организация ежегодных событий по сбору, представлению и анализу финтехпродуктов играет важную роль в продвижении финансовых технологий на финансовом рынке.

Особенностью опыта применения финансовых технологий в банковской сфере России является то, что российские финансовые компании часто сами модернизируют традиционные финансовые услуги, в отличие от зарубежных стран. Одним из общих факторов развития финансовых технологий является рост уровня доступности Интернета.

Отличия российских и западных банков во многом связаны с длительностью их работы. В западных странах существуют банки, которые существуют уже 200 лет, сохраняя отделения и принимая бумажные документы, в то время как в России произошел резкий перелом в банковской отрасли.

Успех внедрения финансовых технологий в ежедневную деятельность банка во многом зависит от государственного регулирования данной сферы. В некоторых странах были созданы рабочие группы для разработки нормативно-правовой базы, регулирующей финансовые технологии. Приведем несколько примеров.

В Великобритании был создан отдельный орган Payment Systems Regulator – для мониторинга платежных систем с целью обеспечения их эффективности для бизнеса и граждан. Также был реализован проект «Управление регулированием финансовых рынков», в рамках которого созданы и запущены финтехпесочницы для финансовых институтов. Для привлечения ведущих компаний в разработку финансовых технологий был запущен финтехакселератор.

В Соединенных Штатах существует разветвленная сеть деловых связей в области финансовых технологий под названием California Fintech Network. Кроме того, в Университете Дрейпера проводятся специализированные курсы для начинающих предпринимателей, где изобретатели могут создать свои собственные

компании и получить финансирование. В Нью-Йорке функционирует акселератор для инновационных предприятий, а также специальная облачная платформа для продвижения финтехбизнеса. Законодательным органам рекомендуется продолжать разработку нормативно-правовой базы, которая будет регулировать формирование и использование открытых данных экономическими агентами. Важной частью этой базы будет обязанность агентов публиковать данные и использовать их для проверки моделей. Разработанные рекомендации по использованию технологии Big Data в банковской сфере направлены на сокращение рисков, создание условий для развития финансовой доступности, установление доверия между участниками рынка, усиление конкуренции и в общем – обеспечение стабильности и развития финансового рынка.

Правовое регулирование применения технологий больших данных в сфере финансов и банковских услуг имеет ряд задач и вызывает неотложные вопросы, которые требуют правового анализа и регулирования.

Ниже приведены некоторые из них:

1. Защита информации и приватность: сбор, хранение и обработка больших объемов данных в сферах финансов и банков служения представляет угрозу для приватности клиентов и обработки их личной информации. Суть задачи заключается в разработке и использовании правовых механизмов, таких как НПА о защите сведений и законы, гарантирующие тайну личных сведений, и устраняют нелегальный доступ или потерю данных клиентов.

2. Борьба с мошенниками и идентификация: для обнаружения и ликвидации денежных мошенничеств Big Data открывают возможности. Несмотря на это, нуждаемость в законодательном урегулировании для установления правил и условий применения сведений людей, устранения нелегального доступа или злоупотребления их личными данными остается актуальной.

3. Антимонопольное регулирование: несмотря на то, что применение больших данных способно неблагоприятно влиять на малые и средние мероприятия, оно также может обеспечить преимуществами крупных игроков. На наш взгляд, законодательство должно обеспечить справедливую конкуренцию и устранять монопольные практики, в которых используются Big Data.

4. Согласие пользователей и их права: сбор, хранение, применение сведений пользователей в денежной сфере должно обеспечиваться с их согласия. Политика прозрачности должна базироваться на правовых нормах.

5. Аспекты этики и правовая ответственность: в законодательстве существует необходимость для установления ответственности для сторон, связанных с применением Big Data в рассматриваемых в этой статье областях. Помимо этого, необходимо установить этические принципы и ограничения, которые должны соблюдаться при работе с такими данными.

6. Безопасность данных и приватности. Клиентские сведения должны быть доступны исключительно уполномоченным лицам, обеспечены надежной защитой. Для недопущения и устранения злоупотребления или несанкционированного пользования личными данными очень важно создать ограничения и правила применения сведений клиентов.

Изменение обыденных моделей реализации деятельности, введение нынешних новый цифровых технологий – в этом и заключается информатизация мировой экономики. Неотделимой частью развития экономики России, включая банковский сектор, является техническая сторона модернизации. «Индустрия 4.0» – прогнозируемое событие, приравненное к четвертой промышленной революции, основная составляющая которого – переход к информационной среде [8].

На основе проведенного анализа можно сделать вывод о том, что нынешние законы, касающиеся персональных данных, не соответствуют современным запросам применения и управления большими данными. При создании федерального закона важно учесть меры наказания за его нарушение, зарубежную практику, применяемую для успешного решения проблем, подробно продумать детали регулирования отношений между субъектами.

Ответственность и этические вопросы также заслуживают внимания при создании правового регулирования. Необходимо учитывать разделение ответственности между сторонами, связанными с использованием больших данных, и установить этические принципы и ограничения, чтобы обеспечить справедливый и безопасный доступ к данным.

В целом эффективное правовое регулирование использования технологий больших данных в финансовой и банковской сферах необходимо для обеспечения безопасности данных, конфиденциальности, честной конкуренции и защиты прав пользователей. Оно должно учитывать долгосрочную перспективу с быстро меняющейся природой технологий и требованиями финансовой и банковской сферы.

Список литературы

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

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 31.07.2006. № 31 (1 ч.). Ст. 3451.

3. Винья П. Машина правды. Блокчейн и будущее человечества. М.: МИФ, 2018. С. 320.

4. Васильев С. А., Никонова И. А., Мирошниченко О. С. Банки, финансовые платформы и Big Data: тенденции развития и направления регулирования // Финансовый журнал. 2022. Т. 14, № 5. С. 105–119. URL: https://doi.org/10.31107/2075–1990–2022–5–105–119

5. Казаков Р. И. Использование технологии Big Data при реализации функции банка по сбору просроченной задолженности // Бизнес-образование в экономике знаний. 2016. № 1(3). С. 33–36.

6. Локтионова Е. А., Рагозина А. В. Особенности применения систем анализа больших данных в деятельности коммерческого банка // Baikal Research Journal. 2017. № 2.

7. Основные направления развития финансовых технологий на период 2018–2020 годов // Центральный Банк Российской Федерации. 2018. URL: https://www.cbr.ru/Content/Document/File/85540/ON_FinTex_2017.pdf

8. Пакова О. Н., Коноплева Ю. А., Дедук А. И. Особенности и проблемы реализации «Индустрии 4.0» в современном банковском секторе // Вестник Северо-Кавказского федерального университета. 2021. № 2(83). С. 98–106.

9. Пшеничников В. В. Влияние финансовых технологий на изменение модели банковского обслуживания клиентов // Теория и практика сервиса: экономика, социальная сфера, технологии. 2018. № 1(35). С. 48–52.

10. Что говорит Big Data Сбербанка о жизни пенсионеров? URL: https://www.sberbank.ru/common/img/uploaded/files/pdf/analytics/big_data_sber_pens.pdf

11. Recent Applications of Big Data in Finance / Balkiss Tekaya, Sirine El Feki, Tasnim Tekaya, Hela Masri. 2021.

Н. О. Маслаков,
студент,
Национальный исследовательский университет ИТМО

К ВОПРОСУ О СОДЕРЖАНИИ ПОНЯТИЙ КИБЕРПРОСТРАНСТВА И КИБЕРПРЕСТУПНОСТИ

Аннотация. В статье рассматриваются существующие доктринальные подходы к содержательному определению дефиниций «киберпространство» и «киберпреступность». Делается вывод о том, что сегодня не выработана единая научная позиция в понимании данных терминов, это связано с тем, что информационные технологии начали свое бурное развитие относительно недавно, в результате чего современная наука так пока и не сформулировала единообразного преставления о сущности киберпространства. Кроме того, не существует универсального термина для обозначения инструментов и программного обеспечения, которые используются при совершении определенных киберпреступлений. На основе анализа российской и зарубежной доктрины в рассматриваемой области были выделены основные компоненты, формирующие структуру киберпространства и его существенные признаки. Сделана попытка типологизации проблем безопасности в киберпространстве и угроз, с которыми сталкиваются отдельные граждане, организации и государства в эпоху цифровых технологий. Приводятся рекомендации по минимизации этих угроз.

Ключевые слова: киберпространство, киберпреступность, Интернет, информационное пространство, телекоммуникационные сети, кибератаки, глобальная компьютерная сеть

ON THE QUESTION OF THE CONTENT OF THE CONCEPT OF CYBERSPACE AND CYBERCRIME

Abstract. The article discusses the existing doctrinal approaches to the meaningful definition of the definitions of “cyberspace” and “cybercrime”. It is concluded that today a unified scientific position in understanding these terms has not been developed, this is due to the fact that information technologies began their rapid development

relatively recently, as a result of which modern science has not yet formulated a unified conception of the essence of cyberspace, except Moreover, there is no universal term for the tools and software that are used in the commission of certain cybercrimes. Based on the analysis of Russian and foreign doctrine in the area under consideration, the main components that form the structure of cyberspace and its essential features were identified. An attempt has been made to typify the security problems in cyberspace and the threats faced by individual citizens, organizations and states in the digital age. Recommendations are given to minimize these threats.

Keywords: cyberspace, cybercrime, Internet, information space, telecommunications networks, cyber-attacks, global computer network

Интернет – одно из самых важных изобретений двадцатого века, которое оказало значительное влияние на нашу жизнь. В современном мире Интернет произвел революцию в различных сферах нашей жизни, разрушив барьеры и коренным образом изменив ее. Интернет стал незаменимым инструментом в жизни каждого человека. Всепроникающее влияние глобальной компьютерной сети оказало глубокое воздействие на общество, повысив удобство коммуникации внутри него. Наш мир становится все более сетевым, все более зависимым от оцифрованной информации, лежащей в основе ключевых услуг и современной инфраструктуры. Различные государства, организации и частные пользователи сетей обеспокоены угрозами конфиденциальности, целостности и доступности оцифрованной информации. В данный момент киберпространство имеет огромное значение в современном мире. Разнообразная человеческая деятельность связана с киберпространством, которое позволяет налаживать коммуникацию между людьми, совершенствовать бизнес-процессы, а также повышать эффективность деятельности государственных и коммерческих организаций.

Сам процесс развития киберпространства занял достаточно большой промежуток времени. В начале 1980-х годов в США появилась локальная сеть Milnet, а также множество других локальных сетей, которые, как правило, обеспечивали задачи по передаче информации между различными университетами и научными центрами. Со временем данные разрозненные локальные сети были объединены в общую сеть под название Internet. Уже к середине 1990-х годов сеть Интернет получила всеобщую популярность и стала массово использоваться рядовыми гражданами. На данное явление обратили внимание законотворцы большинства стран мира. Россия не стала исключением, и в 1996 г. в нашей стране был принят новый Уголовный кодекс, который уже включал в себя главу 28, посвященную преступлениям в сфере компьютерной информации.

В настоящее время более 4 млрд человек регулярно пользуются Интернетом для выполнения работы, покупок и общения, ожидается, что к 2030 г. эта цифра превысит 7,5 млрд пользователей, что составит более 90 % населения Земли [6. С. 201]. Такое колоссальное количество пользователей в сети Интернет говорит о том, что значительная часть населения разных стран вовлечена в глобальную сеть.

На данный момент не существует единого подхода к пониманию термина «киберпространство». Это связано с тем, что информационные технологии начали свое бурное развитие относительно недавно, в результате чего современная наука так и не выработала единого преставления о сущности киберпространства. Указанный термин впервые было упомянут Уильямом Гибсоном в произведении «Нейромант». В нем он описывает киберпространство следующим образом: «… графическое представление данных, извлекаемых из банков памяти любого компьютера в человеческой системе…» [7. С. 103].

Само понятие «киберпространство» широко распространено в англоязычной научной среде. Среди российских ученых до сих пор нет единого мнения относительно того, какой термин следует использовать при обсуждении сферы, образуемой глобальными компьютерными сетями и совершаемыми в ней преступлениями. Например, такие ученые, как В. А Номоконов и Т. Л. Тропина предпочитают использовать термины «киберпреступление» и «киберпространство» [10], в то же время Е. А. Русскевич ставит под сомнение использование терминологии, дословно заимствованной из зарубежного научного сообщества [9].

В российских нормативных актах используется понятие «информационная структура». Так, согласно Указу Президента РФ от 5 декабря 2016 г. № 646, под «информационной структурой Российской Федерации понимается совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации» [1]. Полагаем, что в указанном содержании этот термин синонимичен понятию «киберпространство».

По мнению Р. И. Вылкова, «киберпространство – это принципиально новый вид проективного пространства культуры, который соединяет знаковую реальность и современную технологию, облегчающую и существенно ускоряющую мыслительную деятельность людей» [5. С. 11].

Китайский ученый Цзян-син Ву отмечает, что «киберпространство – это пятая граница, помимо четырех границ суши, моря, неба и космоса, и исследования киберпространства все еще находятся в зачаточном состоянии. Государства по-разному понимают, как применять правила суверенитета в киберпространстве, но все чаще раздаются голоса, призывающие уделять больше внимания сетевому суверенитету. Таким образом, переход от традиционного киберпространства к новому киберпространству неизбежен. В будущем киберпространство будет обладать многими важными характеристиками, такими как открытость, гетерогенность, мобильность, динамизм и безопасность» [4. С. 1460].

Ж. Липтон считает, что «киберпространству присущи следующие черты: глобальное распространение сети Интернет; специальные нормы, регулирующие поведение в онлайн-среде отличные от норм, регулирующих поведение в обычном, “физическом” мире; специфический вид ущерба, понесенного в результате недобросовестного поведения в онлайн-среде» [3. С. 121].

Резюмируя вышесказанное, можно сделать вывод, что киберпространство состоит из следующих основных компонентов:

1. Сети связи – сеть Интернет, локальная сеть, беспроводные сети и прочее.

2. Компьютерная техника – серверы, маршрутизаторы, мобильные устройства, системные блоки и прочее.

3. Программное обеспечение – операционные системы, приложение и иные программы для обработки данных.

4. Информация.

5. Пользователи.

В целом киберпространство является очень динамичным и быстро развивающимся миром, который требует постоянного обновления технических и организационных мер безопасности, чтобы защитить пользователей и их данные от различных угроз.

Проанализировав научные подходы к сущностному содержанию понятия «киберпространство», можно выделить его существенные признаки:

1. Существует в информационной среде.

2. Образуется из совокупности множества различных телекоммуникационных сетей.

3. Присутствует возможность взаимодействия людей друг с другом посредством телекоммуникационных сетей.

Таким образом, мы считаем, что киберпространство – это множество соединенных между собой различных телекоммуникационных сетей и техники, которые формируют единую информационную среду, позволяющую людям взаимодействовать друг с другом.

Следует отметить, что на сегодняшний день существуют различные проблемы безопасности в киберпространстве и угрозы, с которыми сталкиваются отдельные лица, организации и правительства в эпоху цифровых технологий. Ниже перечислены некоторые из них:

1. Атаки вредоносных программ и программ-вымогателей. Вредоносные программы и программы-вымогатели стали одними из наиболее распространенных и разрушительных угроз в киберпространстве. Вредоносное программное обеспечение, такое как вирусы, черви и трояны, может проникать в системы, компрометировать конфиденциальные данные и нарушать работу технических устройств. Программа-вымогатель, разновидность вредоносного ПО, шифрует данные жертвы и требует выкуп за отказ от их обнародования. Такие атаки могут парализовать критически важные инфраструктуры, предприятия и даже целые экономики.

2. Фишинг и социальная инженерия. Фишинговые атаки и методы социальной инженерии используют человеческие уязвимости, а не технические недостатки. Киберпреступники часто используют тактику обмана, чтобы заставить людей раскрыть конфиденциальную информацию, такую как пароли, финансовые реквизиты или личные данные. С помощью мошеннических электронных писем, поддельных веб-сайтов или обмана в социальных сетях злоумышленники манипулируют доверием людей, чтобы получить несанкционированный доступ к персональным данным или совершить мошеннические действия.

3. Утечка данных и кража личных данных. Утечка данных становится все более серьезной проблемой как для организаций, так и для отдельных лиц.

Киберпреступники нацеливаются на базы данных, содержащие ценную личную, финансовую или корпоративную информацию. После взлома эти данные могут быть проданы в темной сети или использованы для финансового мошенничества или других вредоносных действий. Утечка данных не только наносит ущерб гражданам и организациям, но и подрывает доверие общественности к цифровой экосистеме.

4. Продвинутые постоянные угрозы (APT) – это изощренные и скрытные кибератаки, нацеленные на конкретные объекты, часто осуществляемые в течение длительного времени. Эти угрозы включают в себя комбинацию вредоносных программ, социальной инженерии и целенаправленных методов взлома для получения несанкционированного доступа, мониторинга действий и извлечения ценной информации. APT обычно осуществляются хорошо финансируемыми организованными группами или национальными государствами, стремящимися к экономическим, политическим или военным преимуществам.

5. Уязвимости интернета вещей (IoT). Быстрое распространение устройств Интернета вещей (IoT) привело к возникновению новых проблем в области безопасности. Благодаря миллиардам взаимосвязанных устройств, включая умные дома, носимые устройства и промышленные системы, интернет вещей расширил возможности киберпреступников для атак. Слабые меры безопасности, отсутствие стандартизации и недостаточное количество обновлений указанных механизмов делают устройства интернета вещей уязвимыми для взлома, что потенциально может привести к нарушениям конфиденциальности, сбоям в работе или даже физическому ущербу.

6. Атаки на цепочки поставок приобрели известность как средство косвенной компрометации защищенных систем. Проникая к надежным поставщикам, злоумышленники могут внедрять вредоносное ПО или бэкдоры в программные или аппаратные компоненты. Эта тактика позволяет им взламывать хорошо защищенные системы и получать несанкционированный доступ к конфиденциальной информации или нарушать критически важные операции. Недавние громкие атаки на цепочки поставок подчеркнули далеко идущие последствия этой угрозы.

7. Спонсируемый государством кибершпионаж и военные действия. Киберпространство стало ареной спонсируемой государством деятельности, включая кибершпионаж и военные действия. Страны прибегают к целенаправленным атакам с целью кражи конфиденциальных данных, разрушения инфраструктуры или получения стратегических преимуществ. Червь Stuxnet и вредоносная программа NotPetya служат примечательными примерами кибероружия, разработанного некоторыми государствами. Эскалация спонсируемой государством кибердеятельности создает значительные риски для глобальной безопасности и стабильности.

Несмотря на то, что сегодня слово «киберпреступность» прочно вошло в обиход, многим людям было бы трудно дать точное определение этому понятию. Кроме того, не существует универсального термина для обозначения инструментов и программного обеспечения, которые используются при совершении определенных онлайн-преступлений. Это означает, что в научном сообществе так и не смогли прийти к единому понимаю содержания термина «киберпреступность».

Так, например, Дж. Доусон утверждает, что «для того, чтобы дать определение киберпреступности, нам необходимо понять влияние информационных и коммуникационных технологий на наше общество и то, как они изменили наш мир» [2. С. 749].

И. М. Рассолов считает, что киберпреступление это «общественно опасное деяние, которое совершается с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в «Интернете»» [8. С. 144].

По мнению Т. Л. Тропиной, под киберпреступлением следует понимать «виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные общественно опасные деяния, совершаемые с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера пространству» [10. С. 76].

На основании изложенного можно прийти к выводу, что на данный момент существующие определения киберпреступности значительно отличаются друг от друга и зависят от научных убеждений их авторов. Но несмотря на это, можно выделить следующие существенные признаки киберпреступности:

– киберпреступление всегда совершается умышленно;
– наличие информационно-телекоммуникационных сетей;
– трансграничность;
– высокая латентность;
– анонимность и неперсонифицированность;
– причинение имущественного или неимущественного вреда;
– несанкционированный доступ к чужим данным.

Таким образом, мы считаем, что киберпреступность – это целенаправленная деятельность, направленная на причинение имущественного или неимущественного вреда посредством несанкционированного доступа к чужим данным через информационно-телекоммуникационные сети.

Развитие киберпреступности оказывает значительное влияние на общество. С появлением новых технологий и увеличением количества людей, использующих Интернет, возможности для совершения киберпреступлений значительно расширились. Так, И. М. Рассолов отмечает то, что «сформировались следующие категории киберпреступлений:

1. Информационные преступления, которые включают в себя перехват информации, изменение информации и кражу информации.

2. Сетевые преступление, которые включают несанкционированный доступ и распространение вирусов.

3. Пособничество и подстрекательство к киберпреступлению.

4. Подделка документов и мошенничество, связанное с компьютерами» [8. С. 151].

В условиях глобализированной экономики риск киберпреступных атак весьма значителен, и именно по этой причине его не следует игнорировать. Киберпреступления имеют далеко идущие последствия, затрагивающие

как отдельных граждан, так и организации, государство и общество в целом. Концепция киберпространства и распространенность киберпреступности подчеркивают настоятельную необходимость принятия надежных мер кибербезопасности как на индивидуальном, так и на коллективном уровнях. Правотворческие, правоохранительные органы и технологические компании должны сотрудничать в разработке и обеспечении соблюдения эффективных нормативных актов и политики, которые сдерживают киберпреступников и защищают киберпространство. Аналогичным образом отдельным гражданам необходимо уделять приоритетное внимание цифровой грамотности и внедрять передовые методы, такие как использование надежных паролей, средств шифрования и других. Кроме того, повышение осведомленности о киберугрозах и формирование культуры кибербезопасности имеют важное значение для снижения рисков, связанных с киберпространством. Следует внедрять образовательные и обучающие программы, чтобы сформировать у граждан компетенции, необходимые для защиты себя и своих цифровых активов. Более того, международное сотрудничество и обмен информацией между странами имеют решающее значение для борьбы с киберпреступностью, поскольку киберугрозы чаще всего носят трансграничный характер и требуют скоординированного реагирования.

В заключение хотелось бы отметить, что хотя киберпространство предлагает беспрецедентные возможности, оно также несет с собой и проблему киберпреступности. Признавая важность киберпространства и принимая упреждающие меры, мы можем коллективно снизить риски, связанные с киберпреступностью, и создать более безопасную цифровую среду. Благодаря сотрудничеству, осведомленности и надежным методам обеспечения кибербезопасности мы можем ориентироваться в особенностях использования киберпространства и защищать наше цифровое будущее.

Список литературы

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

2. Dawson J. The future cybersecurity workforce: going beyond technical skills for successful cyber performance // Frontiers in psychology. 2022. Т. 9. С. 744–751.

3. Lipton J. Rethinking Cyberlaw: A New Vision for Internet Law / Edward Elgar Publishing LTD, 2019. 176 p.

4. Wu J., Li J., Ji X. Security for cyberspace: challenges and opportunities //Frontiers of Information Technology & Electronic Engineering. 2018. Т. 19. С. 1459–1461.

5. Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проективная идея: автореф. дис. … канд. филос. наук: 09.00.01. Екатеринбург, 2009. 24 с.

6. Острейкина Н. В. Основные тенденции развития интернет-коммуникаций и социальных сетей в российском обществе за последние пять лет // Смыслы, ценности, нормы в бытии человека, общества, государства. 2020. С. 199–205.

7. Пратына Д. А. Киберрелигия: проблема интерпретации // Религиоведение. 2008. № . 4. С. 104–117.

8. Рассолов И. М. Право и интернет: теоретические проблемы: дис. … д-ра юрид. наук. 12.00.14. М, 2008. 357 с.

9. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650–672. EDN: FISEET.

10. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. 12.00.08. Владивосток, 2005. 235 с.

Д. А. Матвеев,
магистрант,
Нижегородский государственный университет
имени Н. И. Лобачевского

О ВОЗМОЖНОСТИ РАЗДЕЛЕНИЯ ЦИФРОВЫХ СЛЕДОВ ПОЛЬЗОВАТЕЛЯ

Аннотация. С технологическим развитием и интеграцией прогресса в нашу повседневную жизнь все острее встает вопрос о предоставлении гарантий безопасности для данных, причем не только в процессе передачи их 3-м лицам для обработки, хранения и т.п., но и при повседневном использовании их же на своих персональных устройствах. Законодательство в сфере защиты и использования данных активно меняется с целью более удобного и безопасного их использования, однако количество угроз увеличивается с каждым годом и это вызвано не только развитием технологий, но и повышением спроса на данные со стороны злоумышленников, занимающихся социальной инженерией. В статье проанализированы современные киберугрозы, приведены оценки специалистов, а также требования законодателя к защите персональных данных. Помимо этого, предложена собственная классификация информации, позволяющая ранжировать данные с целью их защиты таким образом, что при утечке данных, наиболее далеких от первоисточника, злоумышленники фактически не получают никакой ценной информации о человеке.

Ключевые слова: развитие технологий, кибербезопасность, прогнозы специалистов, уязвимости, обработка информации, законодательство в сфере работы с персональными данными, классификация информации

ON THE POSSIBILITY OF SEPARATING THE USER'S DIGITAL FOOTPRINTS

Abstract. With technological development and the integration of progress into our daily lives, the question of providing security guarantees for data is becoming more and more acute, and not only in the process of transferring them to 3rd parties for processing, storage, etc., but also in everyday use them on their personal devices. Legislation

in the field of data protection and use is actively changing in order to make it more convenient and safe to use it, however, the number of threats is increasing every year and this is caused not only by the development of technology, but also by an increase in demand for data from social engineering attackers. The article analyzes modern cyber threats, provides expert assessments, as well as requirements for the protection of personal data of the legislator. In addition, their own classification of information is proposed, which allows ranking data in order to protect it in such a way that when data is leaked that is the furthest from the original source, attackers actually do not receive any valuable information about a person.

Keywords: technology development, cyber security, experts' forecasts, vulnerabilities, information processing, legislation in the field of working with personal data, information classification

На сегодняшний день разработка и внедрение новых информационных систем, программного обеспечения, технологических решений в техническую составляющую вычислительных машин идет настолько быстро, что полное обновление рабочего места специалиста занимает от 3-х до 5 лет.

С технологическим развитием вышеуказанного комплекса, с его повсеместным внедрением все острее встает вопрос о гарантиях безопасности для информации, содержащейся как на внешних носителях, так и в процессах, используемых в вычислительных машинах. Актуальной выступает задача повышения защищенности данных пользователя как от внешних угроз, так и от угроз, вызванных технологическими решениями комплектующих частей. В то же время поиск оптимального решения не должен вызывать деструктуризацию уже действующей системы как технической, так и правовой, решение должно быть действенным и не ресурсозатратным.

Если на заре развития всемирной сети Интернет угрозу представляло лишь программное обеспечение в виде троянов и так называемого WinLock-а или программы-вымогателя, то в настоящее время их перечень существенно расширился. Различное программное обеспечение, использующее вычислительные мощности вашего персонального компьютера для майнинга криптовалют или перенаправляющее трафик на сомнительные ресурсы с целью заработка, является лишь вершиной айсберга и не может сравниться с программами, способными украсть персональные данные, представленные в виде цифрового следа.

Вредоносные программы в большинстве случаев заражают систему в результате контакта с «инфицированным» источником и передают данные, содержащиеся в куки-файлах браузера из различных программ и папок с документами. Однако чтобы вредоносная программа стала действовать по назначению, ей необходимо сначала обойти встроенные средства защиты операционной системы, что не является проблемой для новых версий вирусного ПО. По своей сути противостояние антивируса и вируса занимается «заделыванием брешей» и поиском новых путей уязвимости. Игра в кошки-мышки, где вредоносное ПО на шаг впереди. Примечательно, что некоторые программы-вредители используют не уязвимости самой системы, а особенности технической составляющей устройств для получения данных.

Так, в начале августа компания Intel сообщила об уязвимости под кодовым названием Downfall, позволяющая красть данные на компьютерах с процессорами Intel 2015–2019 годов: от Skylake 6-го поколения до Rocket Lake и Tiger Lake 11-го. Это могут быть ключи шифрования, пароли, переписка, банковские сведения. Уязвимость использует архитектуру процессора, которая ускоряет его быстродействие [7].

Аналогичная проблема наблюдается и в процессорах от компании AMD. Уязвимость под названием Inception также позволяет получить злоумышленникам конфиденциальные данные путем изменения внутренних инструкций процессора [9].

Видится, что подобных заявлений будет становиться больше с каждым годом, поскольку все чаще архитектуры комплектующих персонального компьютера и серверов имеют различные апскейлеры, ускоряющие общее быстродействие, системы в целом, но при этом держащие в кэше чрезмерно большой объем информации о файлах пользователя.

С повсеместным внедрением технологии AI многие современные графические адаптеры уже стали использовать сглаживание и масштабирование с названной технологией, однако при этом сам процесс создания дополнительных кадров является коммерческой тайной компании и говорить о ее безопасности так же с уверенностью нельзя, поскольку происходит взаимодействие с памятью устройства.

Из-за повсеместной цифровизации и внедрения электронных систем сбора, учета и систематизации данных, в том числе и персональных, встает необходимость в использовании современного оборудования, обладающего достаточной вычислительной мощностью для работы с большими объемами данных при этом с высокой скоростью. Поэтому отказ от работы с новейшим оборудованием представляется не самым правильным решением. В то же время использование облачных сервисов остается под знаком вопроса, так как, во-первых, даже при наличии сертификатов защиты и прохождении аттестации на серверах компании-хоста будут храниться данные множества клиентов, что делает хранилище более желанной целью для злоумышленников; во-вторых, в ряде случаев, например, при передаче персональных данных, облачный сервер будет выступать третьим лицом, а передача некоторых данных третьим лицам невозможна даже с целью хранения. Необходимо искать компромисс между производительностью, изолированностью и итоговой ценой решения.

В марте компания Gartner представила доклад, в котором изложила основные тенденции развития мирового рынка кибербезопасности. Помимо повышения важности отрасли в целом, был также отмечен потенциальный рост числа сотрудников, использующих новые/модифицированные технологии в личных целях вне поля зрения IT-отдела. В 2022-м значение таких сотрудников равнялось 41 %. В такой ситуации организациям рекомендуется переосмыслить операционную модель кибербезопасности с целью более тесного взаимодействия с работниками [4].

В то же время во многих бизнес-отраслях и государственных структурах наблюдается дефицит квалифицированных специалистов в сфере кибербезопасности. Данный недостаток зачастую пытаются исправить путем повышения

квалификации сотрудников, что хоть и может улучшить общее положение, но в полной мере заменить специалиста в области киберугроз не в состоянии.

Перед специалистами довольно остро встают вопросы уязвимостей данных. В декабре 2022 г. «Лаборатория Касперского» представила прогноз в области киберугроз. Был отмечен рост утечек персональных данных, при этом тенденция получила новый виток: злоумышленники не просто «сливают» базы, но и совмещают информацию из различных источников. В результате получается подробное «досье» на человека. Так удобнее реализовать более продвинутые таргетированные схемы социальной инженерии и кибершпионажа [6]. Вышеприведенные факты свидетельствуют о росте интереса к персональным данным и данным, представляющим коммерческий интерес как со стороны компаний, занимающихся безопасностью, так и со стороны мошенников.

В настоящее время все больше конфиденциальной информации находится в электронной форме, а допуск к некоторым продуктам требует предоставления биометрических данных. Если еще 5 лет назад речь шла о разблокировке смартфона при помощи отпечатка пальца или объемно-геометрического сканера, распознающего ваше лицо, то сейчас существует целая криптовалюта, для операций с которой требуется использовать сканер сетчатки глаза. Центральным элементом проекта является сфера Ord, которая предназначена для сканирования глаз пользователя и подтверждения личности [8].

Сбор и предоставление подобной информации должны быть урегулированы на законодательном уровне, а также должны быть предоставлены гарантии безопасности в части хранения этих данных. Возникает вопрос: как данные, имеющие информацию о нас, хранятся и надежно ли они защищены?

В связи с активным развитием цифровых технологий 28 октября 2020 г. вступило в действие Постановлением Правительства № 1750, содержащее перечень технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций [3]. К приоритетным отраслям были отнесены технологии работы с большими данными в области обработки, утилизации данных с использованием машинного обучения, сбора, хранения и обработки и анализа данных, в том числе децентрализованных.

В России действуют следующие федеральные законы: об информации, информационных технологиях и о защите информации № 149 ФЗ [1] и 152 ФЗ «О персональных данных» [2], в которых прописаны основные правила хранения и обработки, передачи и удаления данных для государственных структур и компаний. Приказами ФСТЕК и УФСБ РФ урегулирована процедура и форма лицензирования на осуществление деятельности по технической защите, контроля и надзора. Постановлениями Правительства определены требования к ГИСам, требования к защите персональных данных, их передаче и прочее. Также многие структуры имеют дополнительные требования к защите информации: начиная с установки антивирусов до обязательного использования, модифицированного или специально разработанного ПО, в том числе и ОС.

Для реализации защитных функций используется ПО, позволяющее обезопасить систему от атак извне, однако, в случае неудачи программы-защитника,

злоумышленник получает доступ к базе данных, содержащей не только не зашифрованную информацию о пользователе, но и собранную в одном месте. Стоит отметить, что повышение общей защиты путем дополнительного шифрования данных также не кажется оптимальным, так как существенно увеличило бы время на их общую обработку.

На данный момент законодатель предусматривает сбор и хранение информации для целей, обработки, однако требования к самому хранению данных не соответствуют современным реалиям киберугроз, а внедрение новых технологий в сфере защиты и децентрализации данных невозможно ввиду жестких требований законодателя. Представляется, что повышение объемов информации будет все сложнее защитить привычным путем, однако использование смежных технологий может решить эту проблему.

В то же время санкция за нарушение обработки персональных данных и за их разглашение несоизмерима с тем ущербом, который способна нанести человеку или организации утечка этих данных. Так, по данным редакции InfoWatch в 2022 г. в России «утекло» более 667 млн записей с персональными данными пользователей, содержащую различную информацию: от ФИО и номера телефона до адреса проживания. Как констатируют эксперты, число скомпрометированных записей в прошлом году более чем в 4,5 раза превысило население страны. Причем каждая утечка в 2022 г. по объему выросла на треть по сравнению с годами ранее и содержала около 940 тыс. записей [5]. При всей важности этих данных и с учетом того ущерба, который потенциальный злоумышленник способен нанести, ответственность за нарушения в сфере обработки ПД должна быть колоссальной. Однако в настоящее время КоАП закрепляет максимальный размер штрафа в 500 тыс. рублей (статья 13.11). Однако два года назад ответственность также была ужесточена, но меньше «утечек» от этого не стало.

На данный момент для защиты и хранения данных компаниям и учреждениям приходится идти на некоторые компромиссы. В частности, невозможно обеспечить максимальный уровень защиты большого количества данных на всех стадиях работы с ними без потери вычислительной мощности, да и постоянные обновления защиты требуют все больше средств для работы и обслуживания, поэтому либо работа с данными идет медленно, но защищенно, либо быстро, но не безопасно. Исходя из вышесказанного будет логичным предложить деление персональных данных на группы для возможного предоставления разных степеней защиты для конкретных групп. Данный подход позволит не только снизить нагрузку на оборудование, но и оптимизировать процесс защиты, так как более приоритетная информация будет лучше защищена или же вовсе не будет храниться на постоянной основе в общей базе.

Ввиду того, что к настоящему времени человечество перестало быть единственным «создателем» информации, следует учитывать характер произведенной информации, устройства, с помощью которого она была создана, а также насколько точно данные позволяют установить информацию о человеке, который пользовался программой или устройством. Разнообразие гаджетов, накапливающих cache-информацию о событиях, передающих данные через сервера

со всевозможным сбором cookie-файлов, хеша, кеша и других подобных данных привела к тому, что, помимо того, что человек хотел бы записать целенаправленно, создается еще ряд «остаточной» информации, которая может представлять интерес для широкого круга лиц.

Предлагается введение классификации информации, где деление происходит в зависимости от возможности установить насколько далеко цифровой след о человеке находится от первоисточника. На данный момент такая классификация отсутствует, что является неверным, поскольку иерархия информации позволила бы более оперативно решать поставленные задачи: не только определять, каким образом была создана конкретная информация, но и насколько она ценна для идентификации человека, к которому она имеет отношение. Предложенная классификация имеет следующие группы: первичная, первичная-измененная, производная, остаточная и систематизированная (обработанная).

Источником возникновения информации, как уже отмечалось ранее, может выступать человек и результаты его деятельности (цифровой след), хешированные устройствами, при условии, что факт использования конкретным человеком данного устройства подтвержден. Так, данные, воспроизведенные человеком и записанные в электронной форме, предлагается считать наиболее приближенными к человеку и вычитать из данного Абсолюта критерии, которые так или иначе могут обработать и видоизменить информацию и с помощью которых можно восстановить исходные действия и данные.

Таким образом, информацию, произведенную человеком и не подвергшуюся никаким из нижеперечисленных критериев обработки и изменений, предлагается считать первым типом информации – первичной.

Использование фильтров, таких как машинный перевод, фильтры графики, фильтры поиска, ограничения поиска и т. д. части информации, первоначально воспроизведенные человеком, не изменяются кардинально, однако в них смещаются акценты. В зависимости от объекта обработки это может быть подбор более контрастных цветов в картине или изображении, замена синонимами слов или словосочетаний, даже исключение или сокрытие информации, которую можно трактовать двояко или которая способна нанести вред. Подобные «мягкие фильтры» не способны изменить исходную информацию кардинальным образом, однако она все равно будет отлична от исходной и в некоторых случаях, таких как с подбором более контрастных цветов, будет отличаться для восприятия по отношению к оригиналу.

Использование фильтров может привести к более грубому искажению информации, и даже формированию отличного от оригинала отношения к восприятию. Можно считать, что фильтры, способные исказить информацию до изменения отношения к ее восприятию следует считать «жесткими фильтрами».

Деление на «мягкий» и «жесткий» фильтры весьма условно, потому что влияет лишь на восприятие исходной информации человеком, а так как человек субъективен в своих суждениях, то воспринятую им информацию с использованием фильтра также следует считать субъективной, однако из-за произведенного изменения данный тип следует выделить в отдельную группу – первичную-измененную информацию.

При занесении информации в базу данных происходит систематизация в соответствии с алгоритмом базы или программы, которая производит шифровку. В зависимости от целей и вида информации исходная (первичная) информация видоизменяется, из нее могут выделяться основные критерии, необходимые для цели, с которой они заносились в базу, а иные элементы отсеиваться за своей ненужностью. Установить первоисточник информации по-прежнему можно, однако для более точного расчета необходимо обладать способом шифрования и трассировки действий исходника, что представляется невозможным без бекапа или алгоритма шифрования. Наглядный пример: смысл книги «А» и «Б» состоит в борьбе с фашисткой Германией. Однако, как узнать, что под книгой «А» скрыт роман Альбера Камю «Чума», а под книгой «Б» – работа Николая Чуковского «Балтийское небо»?

Подобное «усреднение» информации в сборнике существенно отличается от информации в ее первоначальном виде, однако связь с первоисточником все еще можно установить.

Результаты нашей работы, подобно черновикам писателя, остаются в устройствах, на которых мы воспроизводим и создаем информацию. Остаточные данные сохранятся в браузерах, файлах операционной системы, программах. Процесс кеширования необходим большинству компьютерных устройств и программ ввиду своей архитектуры, для ускорения быстродействия. При желании подобные системные данные можно удалить, или попытаться восстановить. Качество и объем их сохранения зависят от способа шифровки и от давности работы с информацией. В большинстве случаев при помощи кеша и хеша возможно восстановить информацию, которая была утеряна, однако не всегда в полном объеме.

Предлагается считать подобный способ воспроизводства исходной информации остаточной, т. е. восстановленной из метаданных. Остаточная информация по своей сути не является прямым указателем на личность, которая воссоздала информацию, однако данным способом можно установить, с какого устройства, аккаунта была получена информация, и, в зависимости от имеющихся средств дешифровки информации, восстановить определенную часть информации, которая уже может являться указателем на личность создателя.

Хешированная информация, остающаяся на устройстве или сайте, может быть автоматически собрана иными программами с целью оптимизации дальнейшей работы. Как и производная информация, из кеша или хеша выбирается только «общий смысл», который аккумулируется с иными данными. Собранные и систематизированные таким образом данные позволяют предложить пользователю другие похожие материалы на основании его предыдущей активности или же служить для анализа действий человека.

Предлагается считать такой вид информации систематизированной. Как и остаточная, она не способна указать на человека, который генерирует информацию, и определяет лишь устройство взаимодействия. Восстановление исходной информации для данного типа представляется возможным лишь в редких случаях, сведенных к минимуму, однако собранных и систематизированных таким

образом данных достаточно для формирования косвенных выводов о точках интереса человека.

Сбор данных представляет собой автоматический процесс, основанный на классической архитектуре программ ML, однако для качественного анализа и моделирования возможных сфер интереса до недавнего времени требовался человек. Сейчас же все чаще системно-анализирующую функцию выполняют программы, использующие алгоритмы, которые основаны на типе архитектуры нейронных сетей и, как отмечалось ранее, этим все чаще будут пользоваться злоумышленники.

Подводя итог вышеприведенному анализу и подходу к классификации цифровых следов, можно сформулировать следующие выводы:

1. Повышение безопасности для данных пользователя является основной задачей не только в рамках цифровизации, но и при повсеместном использовании устройства или сайта самим пользователем.

2. Исходя из правовой составляющей вопроса, необходимо более активно внедрять так называемые экспериментальные правовые режимы с целью нахождения наиболее удобного и эффективного для интеграции и дальнейшего использования варианта реформы. Идеальным выглядит сценарий защиты, при котором можно извлечь набор данных из обрабатываемого файла, без которого ценность самого файла сводится к нулю. Какой смысл от данных, их кражи, если нет возможности их продать, опубликовать, использовать? Количество утечек информации будет расти с каждым годом – это закономерно для развивающейся и такой потенциально выгодной отрасли. Отсюда также следует, что и смысла в повышении санкции за «утечку» данных нет.

3. Отойти от концепции повышения защищенности данных путем использования дорогостоящего ПО для защиты, использования серверов с повышенным классом защищенности и т. п.: намного эффективнее выглядит идея децентрализации данных, изложенная в статье. В таком случае ценность данных будет ранжирована и применять новые способы защиты для ключевых, наиболее приближенных к человеку цифровых следов будет проще не только для законодателя, но и для разработчика, так как это позволит точно определить перечень данных для защиты, называя их характеристики.

С технической точки зрения необходимо обратить внимание на использование алгоритмов нейронных сетей, так как именно они способны классифицировать данные по специфическим параметрам или кластерам. Именно такое деление, а затем и извлечение из начальной информации способно сделать данные бесполезными для злоумышленника, так как без их восстановления они будут иметь нечитаемый вид. Самое интересное, что похожий подход уже реализован в базе Image.Net для анонизации человеческих лиц.

Хочется верить, что дифференциация в хранении информации позволит уменьшить вероятность и объемы утечек, а также создать более безопасную среду для пользователей с наименьшими рисками распространения персональных данных.

Список литературы

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 2006. № 31. Ч. I. Ст. 3448.
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 2006. № 31. Ч. I. Ст. 3451.
3. Постановление Правительства РФ от 28.10.2020 № 1750 «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций» // Собрание законодательства РФ. 2020. № 44. Ст. 7003.
4. IDC: 10 прогнозов в сфере защиты корпоративных данных // Tadviser.ru. URL: https://www.tadviser.ru/index.phpСтатья: Главные_тенденции_в_защите_информации#
5. В России за год утекло более 660 млн. записей с персональными данными // Comnews.ru. URL: https://www.comnews.ru/content/225506/2023–04–17/2023-w16/rossii-za-god-uteklo-bolee-660-mln-zapisey-personalnymi-dannymi#
6. Как будут проходить атаки на корпорации в 2023 году. Прогноз «Лаборатории Касперского» // Tadviser.ru. URL: https://www.tadviser.ru/index.php/Статья: Главные_тенденции_в_защите_информации#
7. Уязвимость Downfall // Overclockers.ru. URL: https://overclockers.ru/blog/Scorpion81/show/102694/uyazvimost-downfall-v-processorah-intel-pozvolyaet-krast-personalnye-dannye
8. Sam Altman Wants to Scan Your Eyeball in Exchange for Cryptocurrency // Bloomberg. URL: https://www.bloomberg.com/news/articles/2021–06–29/sam-altman-s-worldcoin-will-give-free-crypto-for-eyeball-scans
9. Zenbleed // lock.cmpxchg8b. URL: https://lock.cmpxchg8b.com/zenbleed.html#:~: text=that%20includes%20it.-, Workaround,-It 20is%20highly

И. А. Мекерова,
магистрант,
Санкт-Петербургский государственный университет

ОТ ЦИФРОВИЗАЦИИ К ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. Цифровизация играет значительную роль в развитии бизнеса, превращая традиционные процессы и системы в современные и эффективные. Важность цифровой трансформации и ее влияние на нашу жизнь, работу и экономику возрастают с каждым годом. В данной статье рассматриваются преимущества и возможности цифровизации для бизнеса и общества.

Ключевые слова: цифровизация, цифровая трансформация, роль, бизнес, организация, технологии, компания, инновации

FROM «DIGITALIZATION» TO «DIGITAL TRANSFORMATION»

Abstract. Digitalization plays a significant role in business development, transforming traditional processes and systems into modern and efficient ones. In recent years, we have been hearing more and more about the importance of digital transformation and its impact on our lives, work and economies. In this article, we will look at the benefits and opportunities that digitalization opens up for business and society.

Keywords: digitalization, digital transformation, role, business, societies, organization, technologies, company, innovations

В современном мире невозможно представить себе жизнь без цифровых технологий, представляющих собой «технологии сбора, хранения, обработки, поиска, передачи и представления данных в электронном виде» [17]. Они позволяют компаниям работать более эффективно, снижать затраты, повышать качество продукции и услуг, принимать обоснованные решения и находить новые возможности для роста, а также адаптироваться к меняющимся требованиям рынка и оставаться конкурентоспособными в современном бизнес-мире.

Кроме того, цифровые технологии вызывают вопросы этики и приватности, требуют большей гибкости и обучения «для соответствия новым профессиям и приобретения навыков, необходимых для современного общества» [1], поэтому «для того, чтобы успешно функционировать в условиях цифровизации и вызванных ею новых бизнес-моделей, компании вынуждены пересматривать свою структуру и осваивать новую культуру ведения бизнеса» [20].

Цифровизация тесно связана с цифровыми технологиями, которые позволяют создавать новые возможности для развития и инноваций, оптимизировать рабочие процессы, улучшать продукты и услуги, а также повышать уровень конкурентоспособности.

Одной из ключевых ролей цифровизации в бизнесе является улучшение операционной эффективности. С появлением новых технологий и программного обеспечения, компании могут автоматизировать и оптимизировать множество бизнес-процессов, значительно снижая время и затраты на их выполнение. Например, автоматизация систем управления складом позволяет упростить инвентаризацию, отслеживание поставок и управление запасами товаров. Это помогает сократить время, снизить вероятность ошибок и повысить общую эффективность операций.

Цифровизация также открывает бизнесам новые возможности для достижения широкой аудитории и улучшения своего маркетинга, что «приводит к совершенствованию качества обслуживания клиентов и повышению результативности основных показателей деятельности компании, увеличивает ее операционную гибкость в целом» [12]. Онлайн-реклама, социальные сети и другие цифровые платформы предоставляют компаниям инструменты для продвижения товаров и услуг, а также для привлечения новых клиентов. Благодаря цифровому маркетингу компании «могут получить важные сведения о поведении, предпочтениях, интересах и потребностях потребителей» [10], что помогает повысить лояльность клиентов и объем продаж, «установить с клиентами более тесную связь и увеличить клиентскую базу».

Кроме того, цифровизация позволяет бизнесам улучшить взаимодействие с клиентами и качество обслуживания. Мобильные приложения, онлайн-чаты и социальные сети предоставляют компаниям возможность получить более глубокое понимание потребностей и предпочтений своих клиентов, благодаря чему компании могут улучшить свою репутацию, обеспечить удовлетворенность клиентов и получить конкурентные преимущества.

СберПро совместно с РБК выяснили, что собой представляет цифровизация и как этот процесс выглядит на практике. СберПро информирует о том, что «цифровизация – внедрение цифровых технологий в конкретный бизнес-процесс организации, направленное на его оптимизацию и приводящее к росту продуктивности и доходности» [23].

Как сообщает РБК, «цифровизация – это процесс перевода данных и процессов в цифровой формат, который способствует оптимизации операций и повышению эффективности» [14].

Аналитики компании Boston Consulting Group (BCG) определяют цифровизацию как «полное внедрение и максимальное использование цифровых технологий во всех аспектах деловой деятельности компании» [2].

Е. И. Рузина считает, что «цифровизация – это качественно новый уровень развития экономики, на котором инициируются технологический сдвиг и прогресс, повышается точность и эффективность работы на производственных процессах» [18].

Аналитики i-SCOOP заявляют, что «цифровизация означает использование цифровых технологий и данных для получения доходов, улучшения бизнеса, преобразования бизнес-процессов» [11].

В узком смысле «цифровизация является процессом преобразования информации в цифровую форму, что обычно приводит к снижению издержек и созданию новых возможностей, а в широком смысле цифровизация рассматривается как глобальный тренд эффективного развития, охватывающий различные сферы жизни и деятельности» [6].

Согласно Глоссарию Gartner IT, «цифровизация – это использование цифровых технологий для изменения бизнес-модели и предоставления новых возможностей получения дохода и создания ценности; это процесс перехода к цифровому бизнесу».

Цифровизация создает новые возможности для образования и развития. Онлайн-курсы, электронные библиотеки и другие цифровые платформы предоставляют доступ к образовательным ресурсам и информации из любой точки мира. Это расширяет возможности обучения и развития для миллионов людей. Более того, цифровые технологии также помогают улучшить доступность медицинских услуг, особенно для людей, живущих в удаленных районах или имеющих ограниченные возможности доступа к медицинской помощи.

Цифровизация способствует развитию инноваций и созданию новых рабочих мест. Современные технологии и программное обеспечение открывают новые возможности для развития инновационных идей, что позволяет предпринимателям и стартапам создавать новые бизнесы и рабочие места. Кроме того, цифровизация

также создает сотни тысяч рабочих мест в сфере информационных технологий и программирования, что способствует экономическому росту и развитию.

Одним из ограничений развития новых технологий является недостаточное количество исследований мирового уровня в данной области, а также нехватка высококвалифицированных специалистов, способных «создавать эффективные стратегии и управлять их внедрением на основе принципов цифровой экономики».

Это создает вызовы для инноваций и препятствует полному раскрытию потенциала цифровых технологий. Для преодоления этого дефицита необходимо активнее инвестировать в образование и научные исследования, а также стимулировать развитие сферы IT и информационных технологий в целом. Только так можно обеспечить качественную кадровую базу и устранить препятствия перед дальнейшим развитием цифровых технологий.

Задачи цифровизации могут варьироваться в зависимости от конкретной отрасли или компании, но в основном они включают:

1. Преобразование данных и информации в цифровой формат: содержит преобразование бумажных документов, файлов и записей в электронный формат, чтобы они были доступны и управляемы в цифровом виде.

2. Автоматизацию и оптимизацию процессов: цифровизация позволяет автоматизировать рутинные и повторяющиеся задачи, что улучшает эффективность работы, сокращает время выполнения и позволяет сотрудникам сконцентрироваться на более важных и креативных задачах.

3. Внедрение цифровых технологий и инструментов: цифровизация включает в себя использование современных технологий, таких как интернет вещей, «нейронные сети, облачные вычисления» и аналитика данных. Эти инструменты могут помочь компании улучшить свои продукты, услуги и процессы.

4. Усовершенствование взаимодействия с клиентами: цифровизация позволяет улучшить коммуникацию и взаимоотношения с клиентами, предоставляя им обновленную информацию, персонализированные услуги и удобные каналы связи.

5. Обеспечение безопасности данных: при переходе к цифровой форме хранения и обработки данных необходимо обеспечить их безопасность и защиту от несанкционированного доступа.

6. Развитие цифровых навыков персонала: цифровизация требует соответствующих знаний и навыков у сотрудников. Для успешного внедрения цифровых решений организация должна инвестировать в обучение и развитие своих работников.

7. Постоянное инновационное развитие: цифровизация не является единоразовым процессом, а является постоянным процессом поиска новых возможностей, применения инноваций и улучшения уже внедренных решений.

Далее рассмотрим преимущества, которые цифровизация может предоставить бизнесу:

1. Повышение эффективности: цифровые системы позволяют сократить затраты времени и ресурсов на выполнение бизнес-процессов, увеличивая производительность и эффективность работы.

2. Улучшение качества услуг: цифровизация позволяет более точно предоставлять услуги клиентам, повышая их удовлетворенность и укрепляя лояльность.

3. Расширение рынков и увеличение продаж: цифровые технологии предоставляют возможность достигнуть новых рынков и увеличить объемы продаж за счет разработки онлайн-каналов продаж и маркетинговых стратегий.

4. Уменьшение издержек: цифровые системы могут помочь в сокращении затрат на обслуживание клиентов, управление запасами, маркетинг и другие бизнес-процессы.

5. Усиление конкурентоспособности: цифровизация может стать источником конкурентного преимущества, обеспечивая возможность быстро реагировать на изменяющиеся требования рынка и клиентов.

Однако, помимо преимуществ, цифровизация также представляет некоторые вызовы и риски. В силу обилия информации и возможности ее непрерывного потока, можно столкнуться с проблемой информационного перенасыщения, а также с угрозой кибербезопасности.

Перейдем к рассмотрению рисков, которые могут возникнуть при внедрении цифровизации, представленных в табл. 1.

Таблица 1

Риски, возникающие при внедрении цифровизации

Название риска	Характеристика риска
Риск информационной безопасности («кибербезопасность»)	Внедрение цифровых технологий требует хранения и обработки большого объема данных, что может повысить угрозу несанкционированного доступа к ним, взлома или утечки
Технологический риск	Использование новых технологий может привести к непредвиденным проблемам, связанным с совместимостью систем, отказом технологии и другими техническими проблемами
Организационный риск	Изменение бизнес-процессов и систем может привести к сопротивлению со стороны работников и затруднить их адаптацию к новым условиям работы. Кроме того, внедрение цифровизации может потребовать крупных инвестиций и вызвать финансовые проблемы для компании
Риск связи с клиентами	Внедрение новых цифровых технологий может изменить способ взаимодействия с клиентами. Некорректное использование новых каналов коммуникации или неправильное понимание потребностей клиентов может привести к потере покупателей
Риск законодательства и регулирования	Существуют различные юридические и регуляторные требования в отношении цифровых технологий. Несоблюдение этих требований может привести к юридическим проблемам и штрафам

Источник: составлено автором на основе [16, 21].

Результатом процесса цифровизации выступает цифровая трансформация.

Активное использование цифровых технологий в стратегии компании может проявляться разными способами: внедрением цифровых инструментов в существующие бизнес-процессы компании, а также изменением бизнес-модели с целью повышения ценности для клиентов путем цифровой трансформации, которая помогла многим компаниям изменить стратегии, оптимизировать системы управления основными технологическими процессами и ускорить рост бизнеса.

Предполагается, что все больше компаний будут внедрять цифровые технологии для улучшения гибкости производственных процессов и принятия решений, что способствует ускорению процесса цифровой трансформации, которая представляет собой «революционные изменения бизнес-моделей на основе использования цифровых платформ, которые приводят к радикальному росту объемов рынка и конкурентоспособности компаний.

Профессор кафедры менеджмента и инноваций Санкт-Петербургского государственного экономического университета Салимьянова Индира Гаязовна определяет цифровую трансформацию как «осознанный переход компании к цифровым технологиям и полное изменение производственных, управленческих подходов с учетом применения цифровых технологий».

Цифровая трансформация (digital transformation) – переход к цифровому бизнесу, комплексное преобразование деятельности компании, ее бизнес-процессов, компетенций и бизнес-моделей, максимально полное использование возможностей цифровых технологий с целью повышения конкурентоспособности, создания и наращивания стоимости в цифровой экономике. Как сообщает РБК, «цифровая трансформация – это не только инвестиции в новые технологии, но и глубокое преобразование продуктов и услуг, структуры организации, стратегии развития, работы с клиентами и корпоративной культуры».

По мнению автора, цифровизация и цифровая трансформация являются взаимосвязанными концепциями, но имеют свои отличия.

Автор выделяет ключевые отличия цифровизации от цифровой трансформации, представленные в табл. 2, что позволяет ясно обозначить особенности каждого подхода и его влияния на организацию.

Цифровизация означает процесс преобразования аналоговой информации в цифровой формат. Это включает в себя использование цифровых технологий и инструментов для обработки, хранения и передачи данных. Цифровизация позволяет автоматизировать процессы, улучшить эффективность и оптимизировать работу организаций.

Цифровая трансформация, с другой стороны, является широким понятием, которое охватывает изменения в бизнес-моделях, процессах и культуре организации, вызванные использованием цифровых технологий. Целью цифровой трансформации является создание новых ценностей для клиентов, улучшение взаимодействия с ними и повышение конкурентоспособности организации.

Таким образом, цифровизация является одной из составляющих цифровой трансформации. Цифровые технологии играют важную роль в обоих концепциях, но цифровая трансформация включает не только технические аспекты, но и стратегические, организационные и культурные изменения.

Таблица 2

Отличия цифровизации от цифровой трансформации

Признак	Цифровизация	Цифровая трансформация
1. Ориентация	Улучшение текущих процессов и моделей бизнеса	Глубокое изменение существующего бизнеса
2. Масштаб	Концентрируется на конкретных функциональных областях или процессах	Охватывает все аспекты бизнеса
3. Цель	Более узкая цель, такая как повышение эффективности операций или сокращение затрат	Стремится к созданию новых возможностей и созданию ценности для клиентов
4. Временная перспектива	Цифровизация, как правило, может быть завершена в относительно короткие сроки, поскольку она ориентирована на улучшение уже существующих процессов	Цифровая трансформация является более длительным и непрерывным процессом, подразумевающим постоянные изменения и приспособления к изменяющимся потребностям и технологиям
5. Участие технологий	Упор на конкретные технологии	Комплексный подход к применению современных цифровых технологий
6. Влияние на бизнес-модель	Цифровизация, в то время как она могла бы улучшить эффективность и автоматизировать процессы, обычно не приводит к принципиальным изменениям бизнес-модели	Цифровая трансформация может привести к радикальным изменениям в бизнес-модели организации, включая разработку новых продуктов или услуг, появление новых источников дохода и улучшение клиентского опыта

Источник: составлено автором на основе [21].

На сегодняшний день все больше компаний активно адаптируются к цифровому миру, внедряют новые технологии и инструменты, решающие сложные задачи и усиливающие «потенциал лидера на мировом рынке товаров и услуг». Благодаря этому можно говорить о необходимости обучения и развития цифровых навыков, чтобы быть готовыми к вызовам современной эпохи.

Список литературы

1. Аренков И. А., Салихова Я. Ю., Лизовская В. В. Развитие маркетинговых компетенций в цифровой экономике // Управление бизнесом в цифровой экономике: сборник тезисов выступлений Четвертой международной конференции, Санкт-Петербург, 18–19 марта 2021 г. / под общей редакцией И. А. Аренкова, М. К. Ценжарик. Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2021. С. 109–114.

2. Банке Барт Аналитический отчет BCG. Vlast.kz. URL: https://vlast.kz/corporation/24539-cifrovizacia-biznesa.html

3. Генералова Н. В., Соболева Г. В. Цифровизация корпоративного процесса «учет и Финансы»: ограничения и риски, российский опыт // Управление бизнесом в цифровой экономике: сборник тезисов выступлений Пятой международной конференции, Санкт-Петербург, 19 марта 2022 года. Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022. С. 138–144.

4. Голубецкая,Н. П., Бургонов О. В. Вызовы системы государственного регулирования устойчивости предпринимательских структур в условиях цифровых технологий // Актуальные проблемы менеджмента: повышение стратегической устойчивости регионов и предприятий: материалы Международной научно-практической конференции, Санкт-Петербург, 20 ноября 2020 года. Санкт-Петербург: ООО «Скифия-принт», 2021. С. 31–35.

5. Жигалов, В. М. Цифровизация стратегий компаний в условиях неблагоприятной внешней среды // Управление бизнесом в цифровой экономике: сборник тезисов выступлений Четвертой международной конференции, Санкт-Петербург, 18–19 марта 2021 г. / под общей редакцией И. А. Аренкова, М. К. Ценжарик. Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2021. С. 71–75.

6. Зайцева Т. Г., Кропивка Н. В. Цифровизация как фактор трансформации экономики // Вестник Белгородского университета кооперации, экономики и права. 2020. № 3(82). С. 166–174.

7. Коваленко Б. Б., Коваленко Е. Г. Цифровая трансформация бизнес-моделей – условие роста компаний энергетики // Управление бизнесом в цифровой экономике: сборник тезисов выступлений Пятой международной конференции, Санкт-Петербург, 19 марта 2022 года. Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2022. С. 107–113.

8. Маленков Ю. А. Стратегические препятствия и новые возможности роста производительности, эффективности и качества управления в условиях цифровизации экономики // Актуальные проблемы менеджмента: производительность, эффективность, качество: материалы Международной научно-практической конференции, Санкт-Петербург, 10 ноября 2017 года. Санкт-Петербург: Издательство Санкт-Петербургского государственного университета, 2017. С. 17–21.

9. Месропян В. Р. Цифровые платформы – новая рыночная власть: Цифровая платформа знаний АгроЭкоМиссия: [сайт]. URL: https://agriecomission.com/base/cifrovye-platformynovaya-rynochnaya-vlast

10. Никонова М. Р. Возможности и риски бизнеса в эпоху цифровизации / М. Р. Никонова // Экономика и предпринимательство. 2023. № 3(152). С. 845–847.

11. Оцифровка, цифровизация, цифровизация и трансформация: отличия. URL: https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption

12. Павель Е. В., Быкова П. А. Маркетинг и тотальное управление качеством в контексте процессов цифровизации // Управление бизнесом в цифровой экономике: сборник тезисов выступлений, Санкт-Петербург, 21–22 марта 2019 г. / под общей редакцией И. А. Аренкова, М. К. Ценжарик. Санкт-Петербург:

Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2019. С. 177–179.

13. Рачипа А. В., Суржиков М. А., Самыгин С. И. Цифровизация в управлении организацией: инновационные бизнес-модели // Государственное и муниципальное управление. Ученые записки. 2022. № 3. С. 64–69.

14. РБК Тренды. Индустрия 4.0. Как отличить цифровую трансформацию от цифровизации. URL: https://trends.rbc.ru/trends/industry/cmrm/606ae4c49a794754627d6161

15. РБК Тренды. Что такое цифровая трансформация? URL: https://trends.rbc.ru/trends/innovation/5d695a969a79476ed81148ef

16. Риски на пути к цифровой трансформации бизнеса: как их избежать? 6.11.2021. URL: https://rb.ru/opinion/riski-cifrovoj-transformacii

17. Росстат. Понятия и определения (Цифровые технологии).

18. Рузина Е. И. Цифровизация: об определении понятия, о выгодах и рисках цифровой трансформации // Горизонты экономики. 2022. № 5(71). С. 96–99.

19. Салимьянова И. Г. Цифровая трансформация бизнеса как инновационный путь развития банковской сферы // Инновационная деятельность. 2020. № 3(54). С. 91–101.

20. Скляр М. А., Кудрявцева К. В. Цифровизация сферы услуг как условие становления сервисно-цифровой экономики // Управление бизнесом в цифровой экономике: сборник тезисов выступлений Четвертой международной конференции, Санкт-Петербург, 18–19 марта 2021 г. / под общ. ред. И. А. Аренкова, М. К. Ценжарик. Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна, 2021. С. 64–70.

21. Строк О. А. Сущность понятий цифровизация и цифровая трансформация // Банковская система: устойчивость и перспективы развития: сборник научных статей двенадцатой Международной научно-практической конференции по вопросам банковской экономики, Пинск, 29 октября 2021 года. Часть II. Пинск: Полесский государственный университет, 2021. С. 205–208.

22. Ценжарик М. К., Крылова Ю. В., Стешенко В. И. Цифровая трансформация компаний: стратегический анализ, факторы влияния и модели // Вестник Санкт-Петербургского университета. Экономика. 2020. Т. 36, № 3. С. 390–420.

23. Цифровизация и цифровая трансформация: задачи и результаты 9.05.2022. URL: https://sber.pro/digital/publication/czifrovizacziya-i-czifrovaya-transformacziya-zadachi-i-rezultaty

24. Эксперт УРАЛ № 9 Бизнес в цифре 27.02.2023. URL: https://expert.ru/ural/2023/09/biznes-v-tsifre

25. Glossary Gartner. URL: https://www.gartner.com/en/glossary

А. Р. Мингажева,
студент,
Санкт-Петербургский государственный университет

МОЛОДЕЖНАЯ ПЛАТФОРМЕННАЯ ЗАНЯТОСТЬ: ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЯ

Аннотация. В статье анализируются актуальные проблемы регулирования платформенной занятости. Молодежная занятость рассматривается в контексте платформенной занятости. Приводятся проблемы платформенной занятости и механизмы, которые позволяют их решить. Констатируется, что для решения проблемы правовой неопределенности в вопросе статуса работников цифровых платформ необходимо формальное закрепление на законодательном уровне отдельной категории труда как платформенная занятость.

Ключевые слова: занятость, молодежь, платформенная занятость, пользовательское соглашение, трудоустройство, трудовое право, цифровая платформа, цифровая экономика, цифровизация

YOUTH PLATFORM EMPLOYMENT: PROBLEMS AND WAYS TO SOLVE

Abstract. The article analyzes the actual problems of platform employment regulation. Youth employment is considered in the context of platform employment. The article presents the actual problems of platform employment and the mechanisms that will allow them to be solved. The author states that in order to solve the problem of legal uncertainty regarding the status of digital platform workers, it is only necessary to formally fix platform employment at the legislative level as a separate category of labor.

Keywords: digitalization, digital economy, digital labor, digital platform, employment, future of work, labor law, law, platform employment, user agreement, youth

Растущая цифровизация экономики и общества оказывает глубокое влияние на сферу труда. Предполагается, что эта тенденция сохранится и даже ускорится в ближайшие годы. Цифровизация не затрагивает лишь несколько высокотехнологичных производственных секторов экономики. В целом, она носит массовый характер, что формирует глобальный тренд на цифровую экономику будущего. Данная тенденция влечет повсеместное появление цифровых платформ. В современном научном сообществе данное явление называется платформенной экономикой или гиг-экономикой (gig-economy). Частным следствием этого процесса является появление платформенной занятости [14].

Платформенная занятость – это гибкий формат включения работника в рынок труда, предполагающий использование онлайн-платформы (цифровой платформы) в качестве посредника между поставщиками услуг (исполнителями работ) и потребителями (клиентами).

По оценкам Международной организации труда, количество платформ цифрового труда за последние пятнадцать лет увеличилось стремительно. По состоянию

на январь 2021 года, в мире насчитывалось не менее 777 активных платформ, когда как в 2006 г. их количество не превышало и 50 [1].

Доступность цифровых платформ обеспечивает быстрое включение в трудовую деятельность граждан разных стран. Так, например, международная публичная компания Uber, специализирующаяся на поиске, вызове и оплате такси, всего за 14 лет смогла выйти на рынок в более чем 65 стран мира. Данный рост был достигнут без масштабных инвестиций в автомобили, но за счет работников, использующих собственные или арендованные автомобили и, конечно, рассматриваемую цифровую платформу. Очень многие крупные компании работают по схожей системе (DeliveryClub, ЯндексТакси и проч.). Более того, в настоящее время существует множество типов цифровых платформ (финансовые, промышленные, сельскохозяйственные, розничные и проч.), задействованных в разных секторах экономики государств, что позволяет включить в трудовую деятельность все большее число граждан.

Цифровая экономика несет в себе значительный потенциал также для содействия занятости молодежи, однако для того чтобы преобразовать данный потенциал в реальную возможность получения достойной работы молодыми специалистами, необходимы изменения в правовом регулировании этой сферы.

Значительное влияние на развитие цифровых платформ оказала пандемия Covid-19 [16], хотя еще до начала кризиса цифровые платформы активно росли и расширялись. Многие крупные компании видели потенциал в использовании цифровой рабочей силы, а работники, в свою очередь ценили возможность получения простого заработка.

Молодые люди выбирают работу на цифровых платформах по ряду причин [2].

Во-первых, получение работы онлайн стало более простым и доступным, нежели получение работы офлайн. Молодежь чаще всего подрабатывает в свободное от учебы время, а классическая модель поиска работы и прохождения собеседований занимает большее количество времени. Поиск работы онлайн позволяет ускорить данный процесс и не наносит такого же ущерба учебному процессу, как работа оффлайн.

Во-вторых, молодые люди быстрее и легче проходят обучение и включаются в рабочий процесс. На многих платформах установлена сдельная оплата труда, т. е. размер заработной платы зависит от количества выполненных задач, объем работы. Таким образом, работники разного возраста без опыта работают в равных условиях оплаты труда. Однако по мере накопления опыта время, необходимое молодым людям в отличие от их более старших коллег, выполнения отдельных задач, сокращается быстрее. Обобщая сказанное, можно сделать вывод, что самое главное в работе на цифровой платформе – быстрая обучаемость на практике.

Вдобавок платформенная занятость позволяет решить такую проблему молодежного трудоустройства, как поиск первого рабочего места, так как работа на ней обладает принципиально более низким порогом вхождения, чем любая традиционная занятость, что позволяет получить тот самый опыт, который чаще всего требуется от работника при классическом трудоустройстве. Несмотря на то что

трудовая деятельность на цифровой платформе обычно является краткосрочной и нестабильной, первые шаги в профессиональной деятельности, необходимые для будущего специалиста, становятся проще и доступнее большему числу людей благодаря цифровым платформам.

Географическая доступность платформенной занятости позволяет начинать работу без переезда, даже оставаясь в доме родителей. Одновременно с этим была обнаружена тенденция в географической мобильности молодых людей, названная "цифровым кочевничеством", эта тенденция отражает возможность совмещать страсть к путешествиям и работу на цифровой платформе.

Платформенная занятость также часто становится первым шагом в сфере предпринимательской деятельности, можно начать с основанного на ней микробизнеса. Это не требует ни сложных регистрационных процедур, ни привлечения большого стартового капитала. Лицо может попробовать себя в роли предпринимателя и безболезненно решить, подходит ли это направление для него в качестве постоянной деятельности.

Возможность смены профессиональной траектории предоставляется платформенной занятостью для поколения Z. Найти себя в новой профессии, не совпадающей с полученной первоначально, становится гораздо легче.

Глобализация цифровых платформ, способствующая увеличению занятой молодежи в разных странах, явно обладает большим потенциалом развития. На макроуровне цифровая экономика обеспечивает хорошую отдачу от инвестиций, а качество рабочих мест на цифровых платформах остается довольно высоким [3]. В то же время остаются некоторые серьезные проблемы, связанные с обеспечением всех молодых людей равными возможностями для доступа к цифровой занятости. Во многих странах с низким и средним уровнем дохода возможность подключения к Интернету по-прежнему остается острой проблемой, особенно в сельской местности. Обеспечение доступности сети Интернет в отдаленных местах требует значительных денежных вложений и временных затрат.

На данный момент международные организации (МОТ, Европейская комиссия, Европейский парламент и др.), а также профсоюзные организации активно добиваются урегулирования вопросов платформенной занятости на законодательном уровне. До настоящего времени платформенная занятость не формализована, не встроена в сложившуюся в странах мира систему трудовых и экономических отношений. Более того, проблему усложняет то, что применение норм трудового, налогового права зависит от конкретной юрисдикции, тогда как зачастую пользователь цифровой платформы и ее оператор находятся в разных странах. Однако даже при условии, что пользователь и оператор будут находиться под одной юрисдикцией, пользователь может скрыть свое местоположения при помощи различных виртуальных инструментов. Таким образом, регулирование этого сегмента экономики – растущего, развивающегося – не сложилось; в частности, остро стоит вопрос страхования предпринимательских рисков и обеспечения социальных гарантий, необходимых как для занятых посредством платформ, так и для самих платформ.

В связи с этим могут быть выявлены следующие проблемы: работники имеют неопределенный статус занятости; имеются риски ухода работников в теневой сектор, риски роста неформальной занятости и скрытой оплаты труда; низкая оплата труда, наличие неоплачиваемой работы; отсутствие гарантий минимальной оплаты труда. По данным статистики, 75 % платформенных работников США зарабатывают меньше уровня федеральной почасовой минимальной зарплаты, а 22 % работников указывали, что заработная плата была недостаточной [4].

Ввиду отсутствия формализации платформенной занятости, а также низкой правовой грамотности населения, что особенно актуально для молодого поколения, при поиске удаленной работы на различных цифровых платформах (в том числе на специализированных) граждане также могут столкнуться с разного рода мошеннической деятельностью.

Риски платформенной занятости можно рассмотреть на практических примерах.

В марте 2023 г. пункты выдачи заказов онлайн-маркетплейса Wildberries объявили забастовку по всей России [5]. Причиной, по словам владельцев ПВЗ (пункта выдачи заказов), стали незаконные условия работы, в частности штрафы. Сотрудники пунктов выдачи заказов Wildberries объявили забастовку из-за новой системы штрафов, предусматривающей удержание до 100 % заработной платы за бракованный товар. Согласно новой оферте, держателей ПВЗ лишили права оспаривать подмены. В частности, если покупатель возвращает бракованную вещь обратно в ПВЗ, с их владельцев удерживают полную стоимость товара. Кроме того, они обязаны выплатить всю цену продукции, если в полученной посылке не по их вине оказался другой предмет. По словам работников, списания за подмены начались уже 9 марта. На этом примере явно отражаются недостатки платформенной занятости. Из-за отсутствия формализации, юридического регулирования платформенной занятости, возникают подобные проблемы, когда крупный маркетплейс выставляет необоснованные штрафы, требования (в данном случае) к своим сотрудникам.

Также статистика показывает, что количество протестных акций, связанных с условиями труда работников на цифровых платформах, в мире неуклонно растет.

Ввиду того, что фактически существует явное различие между тем, как осуществляется трудовая деятельность на платформе, и тем, какой она должна быть, исходя из правового регулирования, установленного в данной сфере, важно выявить причины подобного расхождения.

В настоящее время регулирование платформенной занятости осуществляется на трех уровнях: международном, государственном и частном (платформенном).

На международном уровне существуют основополагающие правовые принципы в сфере трудового права, которые применяются ко всем трудящимся, вне зависимости от их договорного статута. Работники цифровых платформ также относятся к этой категории, вне зависимости от того, каким «статусом» занятости их наделяют государства. Такие принципы изложены в ключевых декларациях, конвенциях Международной организации труда [6–9]. К этим документам можно отнести: положения Конвенции 1930 г. о принудительном труде № 29, Конвенцию

1999 г. о наихудших формах детского труда № 182, Конвенцию 1951 г. о равном вознаграждении № 100, Конвенцию 1948 г. о свободе объединений и защите права на объединение в профсоюзы № 87 (в данном случае, работающие на цифровых платформах граждане обладают правом на ведение коллективных переговоров) и т. д. Важно отметить, что даже при том условии, что государства-участники не ратифицировали данные конвенции, они имеют определенные обязательства их соблюдения исходя из самого факта членства в Организации Объединенных Наций. Из этого проистекает следующая проблема: данные международные нормы прямо не касаются цифровых платформ, которые носят частный, негосударственный характер. Нормативно-правовые документы Международной организации труда, в первую очередь, адресованы государствам-членам ООН. Государства, в свою очередь, должны адаптировать данные нормы международного права в свою правовую систему путем имплементации или инкорпорации.

Однако государства в настоящее время по-разному определяют статус занятости работников цифровых платформ. Так, например, в 2020 году, в Индии был принят Кодекс социального обеспечения, в котором появилось определение «платформенных работников», как трудящихся вне формата традиционного подхода – «работодатель-работник», но выполняющих свою работу/предоставляющих свои услуги посредством цифровых платформ. В Испании существует особый статус занятости для работников цифровых платформ – «экономически зависимый самозанятый работник», при наличии данного статуса трудящийся обретает коллективные права, которых нет при статусе обычного самозанятого [10]. Подобная неопределенность в подходах к установлению статуса работников цифровых платформ в разных странах, а также постоянные нормативные изменения, регулирующие труд работников платформ, не способны сформировать надежное поле социальной защиты. Таким образом, права, которыми должны пользоваться все работники вне зависимости от их договорного статута, на деле распространяются лишь на наемных работников.

Для обеспечения надежной социальной защиты работников цифровых платформ необходимы изменения в правовых административных механизмах, создание системы социальных гарантий.

На уровне Российской Федерации также формируется правовое регулирование трудовой деятельности работников цифровых платформ. Термин «цифровая платформа» уже сейчас появляется во многих нормативных документах, например, ст. 16.2 Закона РФ от 19 апреля 1991 г. № 1032-1 «О занятости населения в Российской Федерации» [11]. Однако прямое закрепление в законодательстве статуса работников цифровых платформ по-прежнему отсутствует.

Совсем недавно Государственной Думой был принят в первом чтении законопроект «О занятости населения в РФ» [12]. Ключевое новшество законопроекта – введение понятия платформенная занятость наряду с самозанятостью. Если термин самозанятого уже активно используется в обиходе, то платформенная занятость – совершенно новое понятие. К ней хотят отнести людей, которые ищут заказчиков, выполняют работы или услуги с использованием интернет-платформ. Таким образом, можно сказать, что государство уже делает определенные шаги к формализации платформенной занятости, юридическому ее закреплению.

Другая сложность, с которой законодатель сталкивается, – это неопределенность в статусе самой цифровой платформы, а именно в какой роли выступает субъект, обеспечивающий деятельность цифровой платформы. Более того, именно на цифровую платформу, как на работодателя в традиционной модели трудовых отношений, будет возлагаться ответственность или же меры государственной поддержки. В правовом поле Российской Федерации уже существуют схожие термины, такие как «оператор информационной системы» или же «владелец сайта», однако данные термины не отражают в полной мере тот статус, которым обладают субъекты, обеспечивающие деятельность цифровых платформ, хотя и частично пересекаются по смыслу с ними [13].

К основным элементам, которыми оперируют цифровые платформы можно отнести информацию. Именно посредством такого ресурса, как информация государство может косвенно регулировать деятельность цифровых платформ. Сейчас в России существуют законодательные требования к операторам информационных систем, информационным ресурсам, размещаемой информации на цифровых платформах, к пользователям информационной сети Интернет и т. п. Однако важно помнить, что здесь существует разный объем требований к цифровым платформам. Так, например, объем требований к цифровой платформе повышается, если платформа достигает определенного «лимита» пользователей, таким образом, в ситуации когда небольшая платформа превышает данный лимит и становится крупной платформой с большим количеством пользователей, объем требований к ней, соответственно, увеличивается.

Помимо различных норм законодательства об информации, существуют также нормы гражданского (здесь зачастую идет речь о товарах и услугах, которые предоставляются посредством цифровых платформ), административного законодательства, которые способны косвенно регулировать деятельность цифровых платформ в России.

Наряду с государственным регулированием, существует также регулирование на уровне самой цифровой платформы. В данном случае идет речь об условиях пользовательских соглашений. Пользовательские соглашения регулируют отношения между пользователем сайта/платформы и ее владельцем/оператором. В подобном соглашении, которое составляет владелец/оператор сайта/платформы, перечислены права и обязанности сторон. Важно отметить, что условия пользовательского соглашения не могут противоречить законодательству государства. В самом соглашении могут быть предусмотрены совершенно разные условия, в зависимости от специфики платформы/сайта, например, условия копирования информации, специфики сайта, условия совершения цифровых покупок и т.п. Пользовательское соглашение носит односторонний характер, т. е. пользователь сайта/платформы может либо принять, либо отвергнуть его. Именно в одностороннем характере заключения пользовательского соглашения существует и его недостаток, сайт/платформа может устанавливать необоснованные требования к пользователям, которые не смогут воспрепятствовать этому. Отсутствие дискуссии между сторонами пользовательского соглашения, диктат условий только с одной стороны является причиной неравенства между пользователями и платформой, а также главным недостатком данного вида регулирования платформенной занятости.

С учетом быстрого развития информационных технологий, цифровизации окружающего мира, появляется необходимость быстро реагировать на изменения и адаптировать законодательство под новые реалии времени.

Цифровая платформенная занятость открывает новые возможности заработка для людей по всему миру. В России число занятых на цифровых платформах неуклонно растет, за первый квартал 2023 г. их число превысило 5 млн человек, для 96 % трудящихся на цифровых платформах это основной способ заработка [15]. Большую часть тех, кто работает на цифровых платформах в России, составляют молодые граждане до 30 лет. Таким образом, проблема цифровой занятости тесно связана с проблемами молодежного трудоустройства и должна рассматриваться в совокупности.

Вместе с тем платформенная занятость содержит множество рисков для молодых работников, ввиду отсутствия четкой формализации подобной категории труда. В подобной ситуации у многих трудящихся на цифровых платформах отсутствует львиная доля социальных гарантий, которые есть у граждан, работающих по трудовому договору.

Кроме этого, регулирование занятости на уровне платформы является недостаточным, так как те требования, которые заявляет цифровая платформа в одностороннем порядке, могут ограничивать права работников. Чтобы не допустить подобного ограничения прав, необходимым представляется только формальное закрепление платформенной занятости как отдельной категории в правовом поле. Смешение таких категорий, как «самозанятый» и платформенная занятость не сможет гарантировать соблюдение прав трудящихся на цифровых платформах.

Список литературы

1. World Employment and Social Outlook 2021: The role of digital labour platforms in transforming the world of work International Labour Office. – Geneva: ILO, 2021.

2. Платформенная занятость как инструмент трудовой социализации представителей поколения Z / Центр проектной деятельности и коммуникационных технологий РГГУ, 2021 г. URL: https://rsuh.digital/platformennaya

3. Global Employment Trends for Youth 2022: Investing in transforming futures for young people. Sukti Dasgupta. Geneva: ILO, 2022.

4. Digital labour platforms and the future of work: Towards decent work in the online world International Labour Office. Geneva, ILO, 2018.

5. РБК Новости. URL: https://www.rbc.ru/business/15/03/2023/64116c889a7947de327e0288

6. Конвенция Международной организации труда № 29 от 28 июня 1930 года «Относительно принудительного или обязательного труда».

7. Конвенция Международной организации труда № 182 от 1 июня 1999 года «О запрещении и немедленных мерах по искоренению наихудших форм детского труда».

8. Конвенция Международной организации труда № 100 от 29 июня 1953 г. «Относительно равного вознаграждения мужчин и женщин за труд равной ценности».

9. Конвенция Международной организации труда № 87 от 9 июля 1948 года «Относительно свободы ассоциаций и защиты права на организацию».

10. Платформенная занятость: определение и регулирование / Авт. коллектив: О. В. Синявская, С. С. Бирюкова, А. П. Аптекарь, Е. С. Горват, Н. Б. Грищенко, Т. Б. Гудкова, Д. Е. Карева; Национальный исследовательский университет «Высшая школа экономики», Институт социальной политики. М.: НИУ ВШЭ, 2021. 78 с.

11. Закон РФ от 19.04.1991 № 1032-1 «О занятости населения в Российской Федерации». Ст. 16.2.

12. Законопроект «О занятости населения в Российской Федерации» № 275599-8. URL: https://sozd.duma.gov.ru/bill/275599-8

13. Платформенная экономика в России: потенциал развития: аналитический доклад / Г. И. Абдрахманова, Л. М. Гохберг, А. В. Демьянова и др.; под ред. Л. М. Гохберга, Б. М. Глазкова, П. Б. Рудника, Г. И. Абдрахмановой; Нац. исслед. ун-т «Высшая школа экономики». М.: ИСИЭЗ ВШЭ, 2023. 72 с.

14. Интересы в механизме публичной власти: проблемы теории и практики: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2023.

15. Обследования населения по проблемам занятости: Федеральная служба государственной статистики. URL: https://rosstat.gov.ru/compendium/document/13265

16. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

Г. О. Михайлинский,
магистрант,
Сибирский федеральный университет

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ ЦИФРОВОГО РУБЛЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В статье рассматриваются вопросы применения в России цифровой валюты как новой формы денежного обращения. Анализируются основные положения законодательства в данной сфере, выявляются экономические и правовые предпосылки применения цифровых технологий в платежной системе. Дается оценка новейших законодательных актов, принятых по вопросам введения цифрового рубля, преимуществ и недостатков закрепленной в них модели правового регулирования соответствующих отношений. Делается вывод о возможном решении проблем коррупционного характера при помощи цифрового рубля, вероятных рисках для граждан и о необходимости доработки ряда законодательных положений в данной области.

Ключевые слова: цифровая экономика, цифровая валюта, цифровой рубль, цифровые технологии, безналичные денежные средства, денежное обращение, формы расчетов

PROBLEMS AND PROSPECTS OF THE INTRODUCTION OF THE DIGITAL RUBLE IN THE RUSSIAN FEDERATION

Abstract. The article discusses the use of digital currency in Russia as a new form of monetary circulation. The main provisions of legislation in this area are analyzed, the economic and legal prerequisites for the use of digital technologies in the payment system are identified. The assessment of the latest legislative acts adopted on the introduction of the digital ruble, the advantages and disadvantages of the model of legal regulation of the relevant relations enshrined in them is given. The conclusion is made about the possible solution of corruption problems with the help of the digital ruble, the likely risks for citizens and the need to finalize a number of legislative provisions in this area.

Keywords: digital economy, digital currency, digital ruble, digital technologies, non-cash funds, money circulation, forms of settlements

Одна из немаловажных тенденций развития современного общества касается цифровизации различных сфер жизни. В значительной степени она коснулась и экономики, т. е. фундамента общественных отношений. О масштабах этого процесса свидетельствует хотя бы появление и активное применение в доктрине и прессе термина «цифровая экономика», определяемой как «часть общего объема производства, которая целиком или в основном произведена на базе цифровых технологий фирмами, бизнес-модель которых основывается на цифровых продуктах или услугах» [1. С. 29]. Представляются вполне обоснованными все чаще встречающиеся суждения о том, что цифровая экономика представляет собой весьма серьезную альтернативу традиционной аналоговой экономики [2. С. 76], причем в долгосрочной перспективе ее преобладание вероятнее всего будет только возрастать.

Одним из наглядных и наиболее актуальных примеров названной выше тенденции является внедрение в денежное обращение цифровых финансовых активов. В РФ активно вводятся новеллы в законодательство, касающиеся цифрового рубля. Рассмотрим основные этапы данного процесса.

К числу предпосылок цифровизации денежного обращения в России относится действующий с 1 января 2021 г. 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» (далее – Закон о цифровых активах). Данный закон закрепил легальные определения цифровых финансовых активов (далее – ЦФА) и цифровой валюты [3], а также в общих чертах урегулировал правоотношения в сфере обращении ЦФА, правила деятельности системных операторов выпуска и обмена ЦФА, а также отношения, возникающие при обороте цифровой валюты в РФ. Говоря о его значении, стоит согласиться с мнением А. Барышева, считавшего данный закон является «стартом в развитии, а его принятие уже в обозримом будущем существенно преобразит повседневную экономическую среду» [4. С. 63].

Первоначально идея о введении цифрового рубля была представлена в докладе Банка России (далее – ЦБ), подготовленном в октябре 2020 года. В данном докладе цифровой рубль преподносился как «дополнительная форма российской национальной валюты» [5], т. е. как некая альтернатива наличным и безналичным деньгам, сочетающая их основные свойства.

Цифровой рубль, согласно предлагаемому проекту, может использоваться режиме оффлайн, т. е. без доступа к информационно-телекоммуникационной сети. Для реализации указанной возможности необходима разработка специализированной инфраструктуры, что представляется одной из главных проблем практического характера, которые могут возникнуть при воплощении идей о цифровом рубле в жизнь.

Уже на данном этапе можно сделать несколько важных с теоретической и практической точек зрения выводов. Следует согласиться с мнением о том, что цифровой рубль изначально задумывался как средство сохранения государством в лице ЦБ контроля над национальной платежной системой и ограничения обращения набирающих популярность «денежных суррогатов» и криптовалют [6. С. 80], от которых цифровой рубль выгодно отличается тем, что по своему характеру является обязательством ЦБ и эмитируется исключительно данным уполномоченным органом.

При этом в исследовательской среде возникли достаточно серьезные и обоснованные претензии к предлагаемым нововведениям. В частности, это касалось самой постановки вопроса об отнесении цифрового рубля к формам национальной валюты, поскольку здесь наблюдается противоречие гражданско-правовой терминологии [7. С. 11]. Решение данного вопроса связано с популярной в гражданско-правовой доктрине теорией о разделении денег на государственные, которые подразделяются на наличные деньги и электронные деньги центрального банка, и частные электронные деньги. Основываясь на данной теории, некоторые отечественные исследователи считают цифровую валюту третьей формой государственных денег [8. С. 56].

Новый виток развития концепции цифрового рубля в отечественном законодательстве связан с принятием в июле 2023 г. двух федеральных законов – Федерального закона от 24 июля 2023 г. № 339-ФЗ «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» (далее – ФЗ № 339) и Федерального закона от 24 июля 2023 г. № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ № 340). В рамках данной статьи мы рассмотрим, каким образом в рамках данных законов были разрешены вышеуказанные спорные вопросы.

Прежде всего, как следует из положений ФЗ № 339, цифровые рубли с позиции отечественного законодателя рассматриваются как разновидность безналичных денежных средств с особым правовым режимом. Таким образом законодатель решил вопрос относительно квалификации цифрового рубля, отказавшись от идеи введения альтернативной или дополнительной формы денег наряду с наличными и безналичными. Это представляется вполне закономерным и обоснованным

решением, тем более что подобный подход наблюдается и в иностранных государствах, где уже достаточно давно используется цифровая валюта (например, в КНР). На текущий момент особенности правового режима цифровых рублей сводятся к порядку расчетов ими, которые осуществляются в рамках платформы цифрового рубля [9].

На сегодняшний день вышеуказанной платформе посвящен Проект Положения ЦБ от 12 июля 2023 г. Данный проект предусматривает круглосуточный режим функционирования данной платформы, который будет обеспечиваться ЦБ как оператором платформы [10]. Также в проекте закрепляются виды цифровых кошельков (счетов цифрового рубля), которые классифицируются в зависимости от субъекта-пользователя, соответственно выделяются счета операторов по переводу денежных средств, физических лиц и юридических лиц. При этом указывается, что счета не открываются иностранным банкам и филиалам кредитных организаций. Перечень участников платформы цифрового рубля формируется в порядке, установленном Федеральный законом №161-ФЗ «О национальной платежной системе» и размещается на официальном сайте ЦБ [11]. Тарифы на услуги и сроки, в которые банки должны будут обеспечить клиентам возможность проведения таких операций, также определит Банк России. До 1 января 2025 г., когда будут введены в действие утвержденные на сегодняшний день тарифы, установлен льготный период, когда все операции с цифровыми рублями на платформе Банка России будут проводиться бесплатно [12]. К числу особенностей цифрового рубля также относится невозможность открытия вклада и выдачи кредита в данном виде валюты и неначисление процентов на остатки средств в цифровых кошельках.

Таким образом, введение цифрового рубля в РФ представляет собой одну из самых неоднозначных и в то же время перспективных законодательных новелл последних лет. Внесение изменений в ГК РФ и Закон о национальной платежной системе является лишь первым шагом в связанных с этой инициативой преобразованиях отечественного законодательства. Так, на сегодняшний день на рассмотрении в Госдуме находится проект поправок в НК РФ, целью которого является интеграция цифрового рубля в систему налогового регулирования и налогового контроля. В НК РФ внесут понятие «счет цифрового рубля». Будет предусмотрена возможность взыскания недоимок за счет цифровых рублей в ситуации, когда нет или недостаточно средств на других счетах налогоплательщика. Налоговые органы получат право приостанавливать операции по данным счетам. Кроме того, установят порядок налогообложения операций с цифровым рублем в части НДС и налога на прибыль. Для НДФЛ установят дату получения дохода при зачислении ЦР на счет. В случае принятия поправки в НК РФ, она вступит в силу с 1 января 2025 г.

На текущий момент сложно сделать однозначный вывод о том, какое влияние окажет цифровой рубль на экономическую жизнь нашего общества. Банк России 15 августа 2023 г. начал пилот цифрового рубля с участием ограниченного числа клиентов 13 банков. Он будет проходить в несколько этапов до 2025. Тем не менее можно предположить, что использование цифрового рубля вряд ли получит широкое распространение среди граждан в ближайшем обозримом будущем. Это связано не только с необходимостью тщательной проработки механизма правового

регулирования соответствующих операций, но и с не самым высоким уровнем цифровой и финансовой грамотности населения. Еще в апреле 2023 г. Банк России предпринял попытку развеять некоторые распространенные среди россиян предубеждения относительно цифрового рубля [13]. Причем если отождествление цифрового рубля с криптовалютами или связь существования цифровых рублей с наличием электричества явно связана с недостатком знаний, то опасения относительно возможности установления тотального контроля за финансами граждан или перевода зарплат бюджетников на цифровые рубли представляются не лишенными оснований, поскольку существующие на сегодняшний день проекты изменений законодательства, связанных с введением цифрового рубля, не содержат четкой системы гарантий того, что в будущем не произойдет нечто подобное.

На сегодняшний день наиболее перспективным направлением применения цифрового рубля представляется его использование при выделении бюджетных средств на исполнение государственных контрактов. Этому главным образом способствует такое свойство цифрового рубля, как прозрачность расходов и возможность отследить любые транзакции цифровыми деньгами. В современных российских реалиях это могло бы иметь очень большое позитивное значение для регулирования экономической жизни общества и снижения коррупционной угрозы. Однако условием реализации этой задачи является грамотное построение системы правового регулирования связанных с цифровым денежным оборотом правоотношений, в частности в бюджетной и налоговой сферах. Основным критерием законотворческой работы в данном направлении должна быть ориентированность на эффективное правоприменение и учет реальных потребностей общества и государства.

Список литературы

1. Белоусов Ю. В. Цифровая экономика: понятие и тенденции развития // Вестник Института экономики Российской академии наук. 2021. № 1. С. 26–43.

2. Ручкина Г. Ф. Цифровой рубль: некоторые итоги внедрения новой формы денежного обращения // Имущественные отношения в Российской Федерации. 2022. № 12. С. 76–81.

3. 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 // СПС «Гарант». URL: https://internet.garant.ru/#/document/74451466/paragraph/7:1

4. Барышев А. Обзор Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в некоторые законодательные акты Российской Федерации» // Административное право. 2021. № 2. С. 61–63.

5. Цифровой рубль: доклад для общественных слушаний от 13.10.2020 // СПС «Гарант». URL: https://internet.garant.ru/#/document/74762042/paragraph/3/doclist/407/2/0/0/%D0%B4%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4%20%D1%86%D0%B1%20%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9%20%D1%80%D1%83%D0%B1%D0%BB%D1%8C:2

6. Турбанов А. В. Цифровой рубль как новая форма денег // Актуальные проблемы российского права. 2022. № 5. С. 73–90.

7. Василевская Л. Ю. Цифровой рубль: взгляд цивилиста на проблему // Lex Russica. 2023. № 1. С. 9–19.

8. Андрюшкин С. А. Цифровая валюта центрального банка как третья форма денег государства // Актуальные проблемы экономики и права. 2021. № 1. С. 54–76.

9. Гражданский кодекс Российской Федерации. Ч. 2 // СПС «Гарант». URL: https://internet.garant.ru/#/document/10164072/paragraph/24335788:1

10. О платформе цифрового рубля: Проект Положения Банка России по состоянию на 12 июля 2023 г. // СПС «Гарант». URL: https://internet.garant.ru/#/document/407385474/paragraph/30:2

11. О национальной платежной системе: Федеральный закон от 27 июня 2011 г. № 161-ФЗ // СПС «Гарант». URL: https://internet.garant.ru/#/document/12187279/paragraph/1988597:3

12. Утверждены тарифы по операциям с цифровыми рублями: Информация Банка России от 11 июля 2023 г. // СПС «Гарант». URL: https://cbr.ru/press/event/?id=16982

13. Мифы о цифровом рубле // Сайт Центрального банка России. URL: http://www.cbr.ru/

Д. Д. Михалев,
студент,
Белорусский государственный университет транспорта
В. В. Шоман,
студент,
Белорусский государственный университет транспорта

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДИПФЕЙКОВ

Аннотация. В статье рассматривается проблема дипфейков (deepfakes) – технологии создания поддельных фото и видео с использованием искусственного интеллекта. Обсуждаются различные аспекты дипфейков, их потенциальные угрозы для информационной безопасности и национальной безопасности. Приводятся примеры реальных случаев использования дипфейков и подчеркивается неотложность принятия мер по их регулированию. Описываются законодательные инициативы в разных странах, направленные на борьбу с дипфейками, и выдвигаются предложения по защите общества от этой технологической угрозы. Подчеркивается важность информационной грамотности общества и необходимость сотрудничества на мировом уровне для борьбы с дипфейками.

Ключевые слова: дипфейк, искусственный интеллект, поддельная фотография, поддельное видео, информационная безопасность, политическая манипуляция, правовое регулирование

LEGAL ASPECTS AND REGULATION OF DEEP FAKES

Abstract. This article examines the problem of deepfakes – technologies for creating fake photos and videos using artificial intelligence. The article discusses various aspects of deepfakes, their potential threats to information security and national security. The authors give examples of real cases of using dipfakes and emphasize the urgency of taking measures to regulate them. The article also describes legislative initiatives in different countries aimed at combating defects, and puts forward proposals to protect society from this technological threat. The text emphasizes the importance of information literacy of society and the need for cooperation at the global level to combat deepfakes.

Keywords: deepfakes, artificial intelligence, fake photos, fake videos, information security, political manipulation, regulation of deepfakes

В последние годы широкое распространение получили технологии изготовления поддельных фото и видео, которые, используя методику компьютерного синтеза изображения, основанную на искусственном интеллекте, переносят черты лица с изображения человека на целевое фото (видеозапись) с высокой степенью правдоподобия. Несмотря на то, что эти изображения (видео) фиктивные, они могут быть выложены в сеть «Интернет» в качестве реальных. Речь идет о технологиях, получивших название дипфейк (deepfake), данный термин происходит от deep learning (англ. – глубинное обучение) [2].

Обычно, как отправную точку, указывают 2017 г., когда при помощи нейросетей было создано поддельное порнографическое видео с известной израильской актрисой Галь Гадот. Это видео активно распространялось в социальных сетях.

В апреле 2018 г. популярный ресурс BuzzFeed разместил видео с заголовком «Вы не поверите, что Обама скажет в этом видео». Это типичный пример сенсационного заголовка. В видео появляется «Обама», который высказывает оскорбительные комментарии в адрес Трампа. В конце видеоролика появляется реальный человек и раскрывает, что видео было поддельным. Позже были созданы подобные видео с участием спикера Палаты представителей США. При использовании искусственного интеллекта были созданы продукты, которые на первый взгляд трудно отличить от оригинала.

Дипфейки, такие как фальшивые видеоролики и аудиозаписи, представляют серьезную угрозу как для отдельного человека, так и для общества в целом. Они имеют потенциал нанести значительный вред, нарушив право на информационную безопасность [4].

Согласно статистике, представленной за 2020 г., только в Соединенных Штатах было зарегистрировано более миллиона случаев злоупотребления технологией глубокого фейкования (дипфейк). Также в том же 2020 г. был опубликован отчет Университетского колледжа Лондона, в котором эксперты пришли к выводу, что фальшивый аудио- или видеоконтент представляет собой наиболее тревожное проявление использования искусственного интеллекта в контексте его потенциального использования для совершения преступлений или актов терроризма.

Различные блогеры и медийные интернет-личности стали жертвами этой проблемы, не ограничиваясь только женщинами. Этот метод имеет фундаментальный характер и охватывает все аспекты социальной жизни потерпевших, требуя подготовки в виде анализа и изучения их социальных контактов и других аспектов.

Подделанный контент отправляется потерпевшим, а затем, под угрозой дальнейшей публикации, злоумышленники требуют выкуп. Однако часто даже после выплаты выкупа материалы все равно попадают в сеть. Кроме того, имеют место случаи подделки паспортных данных с целью последующего использования в мошеннических схемах [1].

В 2021 г. в Китае была разоблачена группа мошенников, специализирующихся на подделке паспортных данных и получении интернет-кредитов путем использования технологии глубокого фейкования. За несколько лет своей деятельности им удалось нажить себе около 75 млн долларов.

Помимо индивидуальных последствий, дипфейки могут привести к общественным проблемам. Они могут использоваться для политической манипуляции, изменения общественного мнения и даже провокации социальных конфликтов.

Важно разработать и реализовать строгие меры регулирования дипфейков, чтобы защитить права и интересы граждан и обеспечить информационную безопасность. Это включает в себя ужесточение законодательства, развитие технических средств для обнаружения и борьбы с дипфейками, а также повышение информационной грамотности общества. Без таких мер мы остаемся уязвимыми перед потенциальной угрозой, которую представляют дипфейки.

Представитель Ассамблеи Калифорнии Марк Берман, выразил обеспокоенность влиянием видеороликов, созданных с использованием технологии Deepfake, особенно в тех случаях, когда в них участвуют политические деятели. Он подчеркнул, что такие видеомонтажи имеют потенциал обмануть общественность и оказать влияние на результаты выборов.

В Китае власти приняли более жесткую позицию и объявили любое распространение явно ложной информации, включая дипфейки, уголовным преступлением. Согласно новым правилам, все дипфейки должны быть обязательно помечены специальной меткой, предупреждающей пользователей о том, что это не подлинная информация. Этот закон был принят Администрацией киберпространства Китая. Официально было заявлено, что использование технологий, связанных с дипфейками, может создать угрозу национальной безопасности, нарушить социальную стабильность и нарушить общественный порядок, а также причинить вред законным правам и интересам граждан.

Опасность, связанная с дипфейками, ощущается и по другим основаниям. Например, злоумышленники могут использовать дипфейки для распространения фальшивых видеообращений, включая угрозы начала новой мировой войны. Это может сбить с толку граждан и руководство других стран и привести к серьезным последствиям. Такие технологии, безусловно, представляют собой потенциальную угрозу и могут стать «ящиком Пандоры», способным вызвать катастрофические последствия. Именно поэтому ограничение на использование дипфейков оправданно.

Американский исследователь Дуглас Харрис подчеркивает, что необходимо обсуждать опасность и регулирование дипфейков уже сегодня, поскольку технологии развиваются быстро, и скоро будет легко создавать фальшивые видео, неотличимые от реальных. В данной ситуации возникает неотложная необходимость в установлении запрета на использование изображений политических лидеров государств в дипфейках и введении уголовной ответственности за их распространение, как это уже сделано в Китае.

Эксперты Республики Беларусь высказали свое мнение по поводу технологического и правового вопроса дипфейка.

Так, Александр Карлюкевич отметил: «Уже сегодня надо готовить проекты, где будут прописаны такие понятия, как fake и deepfake. Нам надо задуматься о радикальных скоростях в эволюции наших отечественных масс-медиа».

«Самое страшное – если вдруг роботы получат сознание – и тогда это будет процесс неконтролируемый... Чем меньше наши знания о чем-либо, тем более велика вероятность купиться на этот дипфейк. И поэтому самая большая группа риска – наши дети», – подчеркнула Ольга Агейко. Виталий Демиров сказал об этом: «Сейчас пока нет завершенных техрешений, которые бы помогли распознавать deepfakes. Когда они появятся, важно, чтобы распознавание таких роликов шло достаточно быстро. Если обличение будет запаздывать, то видео успеет вызвать эффект в соцсетях» [3].

Подводя итог, можно сказать, что сегодняшние вызовы, связанные с дипфейками, требуют разработки и внедрения нормативно-правовой базы, которая учитывала бы как технические аспекты, так и вопросы ответственности за использование и распространение технологий, основанных на искусственном интеллекте. Международные соглашения и национальное законодательство должны быть адаптированы к новой реальности, чтобы обеспечить общемировую безопасность и интегритет информационного пространства.

Список литературы

1. «Названы способы, позволяющие распознать deepfake». URL: https://soyuz.by/obshchestvo/nazvany-sposoby-pozvolyayushchie-raspoznat-deepfake

2. «Deepfake: краткая история появления и нюансы работы технологии». URL: https://habr.com/ru/companies/neuronet/articles/592119

3. «Deepfakes: новый вызов информационной безопасности». URL: https://expert.belta.by/03

4. Официальный сайт Академии Министерства внутренних дел Республики Беларусь. URL: https://www.amia.by/images/pages/activities/editorial-and-publishing-activity/electronic-versions/210609.pdf

Д. А. Нигматзянова,
магистрант,
Московский государственный университет
имени М. В. Ломоносова

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФРАСТРУКТУРЫ РЫНКА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Статья посвящена инфраструктуре рынка цифровых финансовых активов, правовой природе нового инструмента, а также проблемам законодательного регулирования общественных отношений, возникающих по поводу выпуска и обращения цифровых финансовых активов. Работа содержит анализ системы субъектов рынка цифровых финансовых активов, рассмотрение представленных в законе видов цифровых прав и их особенностей, описание законодательства в части эмиссии, учета и оборота цифровых финансовых активов.

Ключевые слова: цифровые финансовые активы, информационная система, ценные бумаги, решение о выпуске, оператор информационной системы, оператор обмена, цифровой актив

LEGAL SUPPORT FOR THE INFRASTRUCTURE OF THE DIGITAL FINANCIAL ASSETS MARKET IN THE RUSSIAN FEDERATION

Abstract. The article is devoted to the infrastructure of the digital financial assets market, the legal nature of a new instrument, as well as the problems of legislative regulation of social relations arising from the issuance and turnover of digital financial assets. The essay analyzes the system of subjects of the digital financial assets market, considers the types of digital rights presented in the law and their peculiarities, describes the legislation in terms of issuance, accounting and circulation of digital financial assets.

Keywords: digital financial assets; information system, securities, decision on issuance, operator of information system; operator of exchange, digital asset

Инновационные технологии начинают внедряться в самые разнообразные сферы жизни. Однако имплементация представленных технологий возможна только в случае глубокого исследования сущности и специфики новых институтов, в частности цифровых финансовых активов (далее – ЦФА). Вследствие этого перед правом встает вопрос регулирования новых отношений и выстраивания наиболее подходящей концепции, которая станет благоприятной почвой для дальнейшего развития этой сферы.

Российская Федерация обозначила четкий курс развития цифровой экономики: 4 июля 2019 г. была принята национальная программа «Цифровая экономика» [12], в состав которой в том числе входят проекты по созданию информационной инфраструктуры цифрового рынка и обеспечивающей ее нормативной базы. В рамках проекта был принят Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ о ЦФА) [27], который вступил в силу 1 января 2021 г.

Понятие инфраструктуры происходит из латинских слов infra – «ниже», «под» и structura – «строение», «расположение». При буквальном переводе инфраструктура – это некий фундамент, на котором стоит строение, обеспечивающий его стойкость и стабильность. Сам фундамент неразрывно связан со зданием, с его особенностями и спецификой, что приводит к логическому выводу: анализ инфраструктуры любого рынка, в том числе ЦФА, стоит начать с раскрытия правовой специфики структуры ЦФА.

«Совокупность объединяемых договорно-хозяйственными связями звеньев, участвующих в продвижении товаров от изготовителей к потребителям» [1. С. 3] – именно так обозначается структура товарного рынка в научной литературе. Безусловно, финансовые рынки, в частности цифровые, обрели свою специфику основных участников оборота актива: так, центральными субъектами рынка ЦФА, по аналогии с рынком ценных бумаг, являются эмитенты, инвесторы и профессиональные участники рынка.

В соответствии с ч. 3 ст. 2 ФЗ о ЦФА в качестве эмитентов могут выступать физические лица, зарегистрированные в установленном законом порядке в качестве индивидуальных предпринимателей, и юридические лица, как коммерческие, так и некоммерческие. При этом отсутствует прямой запрет на осуществление действий по внесению в ИС записи о зачислении ЦФА первому обладателю со стороны иностранных субъектов.

Однако в текущем законодательстве нормы, касающиеся особенностей взаимодействия с иностранными эмитентами, не представлены. Банк России в своем докладе [22] отмечает необходимость установления механизма взаимодействия российских и иностранных операторов обмена ЦФА и порядка допуска иностранных ЦФА к обращению, приводя перечень вопросов, которые планируются к обсуждению с участниками рынка. Вопросы посвящены квалификации иностранных цифровых активов в качестве ЦФА, требованиям к качеству иностранных ЦФА, выполнению требований к раскрытию информации иностранными эмитентами, порядку учета иностранных ЦФА и т. п. [22]. Реализация возможности осуществления сделок с иностранными ЦФА позволит расширить перечень доступных инвесторам финансовых инструментов, однако ввиду осложненной политической ситуации и явной переориентации на российских эмитентов ожидание регламентаций со стороны Банка России может затянуться.

Инвесторами (приобретателями или обладателями ЦФА) являются лица, которые указываются в решении о выпуске. При этом допускается указание как на конкретное лицо, круг лиц, либо на всех пользователей системы. Во втором случае квалификация в качестве публичной оферты является спорной (несмотря на то, что в ч. 7 ст. 3 ФЗ о ЦФА данная конструкция признается публичной офертой), так как в ФЗ о ЦФА любой обладатель ЦФА должен соответствовать критериям, указанным в ч. 7 ст. 4 ФЗ о ЦФА: лицо должно быть аутентифицировано/идентифицировано системой, а также быть включено в реестр пользователей. Следовательно, в рамках решения о выпуске ЦФА невозможно заключение сделки с каждым, кто отзовется на оферту в понимании п. 2 ст. 437 ГК РФ, так как круг субъектов изначально определен самой информационной системой, куда вносятся записи о выпуске, учете и обращении цифровых прав (далее – ИС).

В ФЗ о ЦФА присутствует еще одна фигура, которую можно отнести к субъекту структуры ЦФА – лицо, имеющее намерение приобрести ЦФА. Данный субъект указан в ч. 1 ст. 5.1 ФЗ о ЦФА, посвященной номинальным счетам операторов ИС, и относится к бенефициарам номинального счета. Это лицо, которое потенциально может стать приобретателем ЦФА и, соответственно, приравнивается к его статусу.

К профессиональным участникам рынка ЦФА относится фигура номинального держателя. Сам по себе субъект был заимствован из ФЗ о РЦБ: в соответствии со ст. 8.3 это депозитарий, на счете которого учитываются права на ценные бумаги, принадлежащие иным лицам. Другими словами, это зависимый посредник на рынке ценных бумаг, который может управлять активами по поручению депонента по счету депо.

Эта конструкция была включена и в ФЗ о ЦФА: ч. 4 ст. 2 закона указывается, что ЦФА могут быть зачислены номинальному держателю, учитывающему права на ЦФА, принадлежащие иным лицам. При этом номинальным держателем может быть только тот субъект, который может осуществлять депозитарную деятельность, за исключением оператора ИС – он не может выполнять данные функции ни в каком случае. В данной норме отсутствует ограничения для операторов обмена, так как номинальный держатель действует за свой счет и в интересах своих лиц, что совпадает с функционалом оператора обмена ЦФА в соответствии с ч. 1 ст. 10 ФЗ о ЦФА.

Под номинальным держателем скрываются известные рынку ценных бумаг посредники, преимущественно брокеры. Также спецификой брокерской деятельности обладает деятельность оператора ИС и оператора обмена ЦФА. Текущее законодательство не позволяет выявить существенные критерии для разграничения указанных фигур, однако ретроспективное осмысление регулирования ЦФА дает достаточные основания считать, что оператор обмена выступал ключевым субъектом инфраструктуры – юридическим лицом, правомочным совершать сделки по обмену токенов на рубли или иностранную валюту. Его деятельность должна была соответствовать или ФЗ о РЦБ, т. е. подпадать под регулирование брокерской или дилерской деятельности, деятельности по управлению ценными бумагами, или Федеральному закону «Об организованных торгах» [29]. Сделки предполагалось осуществлять исключительно через оператора обмена.

Изменение концепции привело к появлению еще одного субъекта – оператора ИС. Оператор ИС, в соответствии со ст. 5 ФЗ о ЦФА, – юридическое лицо, в том числе кредитная организация, лицо, имеющее право осуществлять депозитарную деятельность, либо лицо, имеющее право осуществлять деятельность организатора торговли. Одновременно с этим, личным законом оператора ИС должно быть российское право. Сейчас на рынке представлено десять операторов ИС и один оператор обмена.

Часть 2 ст. 2 ФЗ о ЦФА предусматривает возможность осуществления сделок, связанных с приобретением ЦФА при их выпуске, а также с прекращением обязательств, удостоверенных ЦФА, в ИС без привлечения оператора обмена. Выкуп ЦФА происходит при эмиссии инструмента, который полностью обеспечивается оператором ИС.

Для рассмотрения вторичного обращения необходимо обратить внимание на следующие положения ФЗ о ЦФА. Ч. 16 ст. 5 устанавливает, что при соблюдении обязанностей и запретов, предусмотренных в отношении деятельности операторов обмена, оператор ИС вправе обеспечивать заключение любых сделок без включения его в дополнительные реестры.

Данная возможность представлена и в правилах действующих операторов ИС. Так, в п. 8.1.1 правил Атомайза предусмотрено, что обращение цифровых прав, выпущенных на платформе, может осуществляться на платформе в соответствии с ч. 16 ст. 5 ФЗ о ЦФА, а также через операторов обмена; правила Сбербанка в пункте 11.13 регламентируют категорию иных сделок, связанных с ЦФА, заключение которых обеспечивается путем сопоставления разнонаправленных заявок на совершение; в правилах Лайтхауса подобным сделкам посвящена глава 14; схожая конструкция представлена в правилах Альфа-Банка и Мастерчейна.

Следовательно, осуществление сделок по купле-продаже ЦФА и иных сделок, связанных с ЦФА, включая обмен ЦФА на цифровые права других видов могут совершаться через оператора ИС, который обеспечивает их заключение путем сбора и сопоставления разнонаправленных заявок на совершение таких сделок.

Однако на текущий момент не разрешен вопрос о возможности обмена ЦФА между разными операторами ИС. Реализация принципа интероперабельности ложится на плечи оператора обмена в лице Московской биржи, которая обладает необходимой экспертизой для осуществления оборота разных финансовых инструментов. При этом остается открытым вопрос технического совмещения операторов ИС и возможности передачи ЦФА между пользователями разных платформ ввиду того, что все оператора ИС используют разные распределенные реестры и методологии выпуска, обращения и учета ЦФА.

Отдельной категорией участников являются майнеры или валидаторы распределенного реестра. Исключительность этой категории участников рынка связана с тем, что ЦФА не может существовать оторвано от ИС. Так, согласно ч. 1 ст. 1 ФЗ о ЦФА выпуск, учет и обращение инструментов возможны только путем внесения записей в ИС на основе распределенного реестра или в иные ИС.

ИС – понятие, закрепленное в федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В соответствии со ст. 2 указанного закона ИС – «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств». Соответственно, имеет смысл рассмотреть два аспекта понятия: совокупность информации в базе данных и информационные технологии.

Базой данных, в понимании п. 2 ст. 1260 Гражданского Кодекса Российской Федерации (далее – ГК РФ), является представленная в объективной форме совокупность самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ). Таким образом, ИС включает в себя совокупность баз данных, взаимодействовать с которыми возможно через информационные технологии, а именно через распределенный реестр.

Распределенный реестр преследует цель обеспечить публичную достоверность, открытость и определенность положения участников системы, однако благодаря информационным технологиям, данные цели достигаются эффективнее и в автоматизированном формате. Самым известным примером распределенного реестра является Blockchain, без которого невозможно представить первую криптовалюту в мире – Bitcoin. Это децентрализованная система, которая обеспечивает невозможность изменения информации, внесенной в систему, за счет того, что она записывается сразу в неограниченное количество блоков и для внесения изменений необходимо выполнить заново весь объем вычислений.

Публичный распределенный реестр может лежать в основе и корпоративных ИС, при этом создаются закрытые сети реестра. Данные системы обладают существенной долей приватности: они функционируют в определенной корпоративной структуре, их деятельность обеспечивается контролирующим лицом, а для пользователей устанавливаются финансовые и юридические критерии членства. Помимо этого, участники не могут свободно входить или выходить из сети, для этого необходимо предоставление участнику цифрового идентификатора и ключа.

ИС, используемая для операций с ЦФА, является корпоративной, так как оператор ИС осуществляет контроль за функционированием ИС и несет обязанность за ведение реестров пользователей. Контроль за деятельностью операторов ИС осуществляют органы государственной власти Российской Федерации, преимущественно Банк России, что обеспечивает законность и добросовестность операций в ИС.

Отметим, что в ФЗ о ЦФА перечислены не все возможные субъекты инфраструктуры. Так, Лайтхаус и Газпромбанк заключили меморандум о сотрудничестве, в рамках которого банк выступает андеррайтером, т. е. финансовым посредником, который обслуживает и обеспечивает размещение финансовых инструментов, в том числе ЦФА. Более того, оператор обмена в лице биржи может использовать свою инфраструктуру, т. е. клиринговые организации, брокеров, реестродержателей и т. д., для осуществления сделок с ЦФА. Также интересным является тот факт, что рейтинговое агентство АКРА разработало методологию присвоения рейтингов ЦФА.

Стоит также выделить регистратора (депозитария), представленного в ч. 4 ст. 12 ФЗ о ЦФА, который осуществляет функцию учета ЦФА, предусматривающих возможность осуществления прав по эмиссионным ценным бумагам. Таким образом, инфраструктура ЦФА и рынок ценных бумаг крайне сближены и связано это с особенностью ЦФА как финансового инструмента.

Таким образом, отмечается ярко выраженная аналогия с рынком ценных бумаг, что во многом обеспечивает возможность выстраивания более понятного для финансового рынка регулирования. Тем не менее выявляются специфические субъекты структуры и инфраструктуры ЦФА, свойственные исключительно рассматриваемому молодому рынку.

Еще одна особенность рассматриваемого рынка – специфический объект правоотношений. Федеральный закон № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» включил в статью 128 ГК РФ новый объект гражданского права и внес в закон

новую статью 141.1, посвященную цифровым правам. Заключение Правового управления аппарата Государственной Думы РФ подчеркнуло, что использование вместо нового понятия устоявшихся в мировой практике терминов «криптовалюта» и «токены» является более разумным решением.

Более того, упомянутое экспертное заключение содержит комментарий о том, что все перечисленные в законе права могут существовать в электронной форме, следовательно, норма о цифровых правах не создает новый объект гражданского права.

Фактическая подмена понятия объекта гражданского права и способа его фиксации приводит к «порочному удвоению сущностей», во многом вызвана многоаспектностью понятия digital asset («цифровой актив»), что влечет невозможность его отнесения к уже существующим объектам гражданских прав.

Цифровые активы – экономические блага, созданные и функционирующие с использованием цифровых технологий, являющиеся сущностной характеристикой отношений в цифровой экономике. Данные объекты обладают специфическими признаками: экономическою ценностью, информационной природой, цифровой формой, экстерриториальным характером.

Российская доктрина выбрала свой путь развития концепции, игнорируя международную практику определения цифровых активов, поэтому обозначить объем и содержание понятия без прямой законодательной регламентации не представляется возможным.

Закон дает понятие ЦФА, определяя актив как цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права на участие в капитале непубличных акционерных обществ, право требовать передачи эмиссионных ценных бумаг.

На сегодняшний день были токенизированы только денежные требования. Так, на практике операторов ИС встречаются ЦФА, закрепляющие дебиторскую задолженность, стоимость различных активов, в том числе металлов, иностранных валют, метров и т. д.

ЦФА, удостоверяющие права участия в капитале акционерного общества, наиболее приближены к традиционным акциям, поэтому в доктрине они иногда именуются как «цифровые акции». Они выступают средством фиксации прав, которые составляют содержание ценных бумаг, при этом самые ценные бумаги не эмитируются. Следовательно, этот вид ЦФА – это фактически ценные бумаги, существующие в распределенном реестре.

Другая конструкция ЦФА, представленная в ч. 1 и 2 ст. 12 ФЗ о ЦФА, использует иной подход. ЦФА, удостоверяющие возможность осуществления прав по эмиссионным ценным бумагам, прав требовать передачи эмиссионных ценных бумаг, закрепляют права, вытекающие из уже эмитированной ценной бумаги. То есть выпуск ЦФА состоит из двух этапов: эмиссии ценных бумаг, при этом исключительно непубличных акционерных обществ (далее – НАО), и токенизации активов, т. е. преобразования ценных бумаг в ЦФА. В данном случае ЦФА выступает как производный финансовый актив – эмиссия акций происходит по правилам ФЗ о РЦБ, а сам токен формируется на базе существующей ценной бумаги.

Отсутствие сделок с ЦФА, связанными с ценными бумагами, свидетельствует о том, что эти виды не являются перспективными для оборота. Распределенный реестр, безусловно, способен снизить операционные издержки, возникающие при эмиссии и обороте акций, облигаций и иных ценных бумаг, однако дублирование существующих финансовых инструментов не привлекает финансовый рынок и еще более сужает весь потенциал цифровых прав.

Несмотря на закрытый перечень видов ЦФА, законом предусматривается еще один вид цифрового актива. Согласно ч. 6 ст. 1 ФЗ о ЦФА, «в информационных системах, в которых осуществляется выпуск цифровых финансовых активов, также может осуществляться выпуск цифровых прав, включающих одновременно цифровые финансовые активы и иные цифровые права». Под «иными цифровыми правами» подразумеваются, прежде всего, утилитарные цифровые права, а также другие цифровые права, которые могут появиться в российском законодательстве в будущем. Цифровые права, включающие одновременно ЦФА и иные цифровые права, именуются Банком России «гибридными» (далее – гибриды).

Гибриды способны обеспечить появление более разнообразных финансовых инструментов и сделать цифровые права более привлекательными для инвесторов.

Примечательно, что в ФЗ о ЦФА отсутствуют особенности порядка выпуска и обращения гибридов, следовательно, должны использоваться те механизмы, которые заложены для классических видов ЦФА.

Выпуск ЦФА – восприятие российским законодательством модели STO (Security Token Offering). Поэтому механизм выпуска ЦФА во многом дублирует эмиссию ценных бумаг, которая регулируется ФЗ о РЦБ и Положением Банка России от 19.12.2019 № 706-П «О стандартах эмиссии ценных бумаг» и состоит из следующих стадий: принятие решения о размещении активов; утверждение решения о выпуске; регистрация выпуска (дополнительного выпуска) активов; размещение ценных бумаг; государственная регистрация отчета об итогах выпуска или представление уведомления об итогах выпуска (дополнительного выпуска) активов.

Наиболее приближенная к эмиссии ценных бумаг модель выпуска используется для ЦФА, удостоверяющих права участия в капитале акционерного общества. Ч. 3 ст. 13 ФЗ о ЦФА содержит положение о применении ФЗ о РЦБ с учетом некоторых особенностей:

Особые требования к уставу НАО: в уставе должна быть предусмотрена возможность выпуска акций в виде ЦФА. При этом данное положение вносится в устав в момент создания НАО, а изменить или исключить его нельзя. Также устав должен содержать сведения об учете ЦФА в ИС и способы созыва и проведения общего собрания, способы уведомления акционеров об осуществлении корпоративных действий, предусмотренных правилами ИС.

Выпуски ЦФА регистрируются оператором ИС, при этом государственная регистрация не осуществляется.

В решении о выпуске в обязательном порядке должны содержаться сведения о конкретной ИС, где хранятся ЦФА, о рисках, связанных с приобретением ЦФА.

Такое НАО не может быть преобразовано в ПАО.

Устанавливается запрет выпуска эмиссионных ценных бумаг, кроме ЦФА и акций, которые конвертируются в такие ЦФА. Также эти ЦФА нельзя конвертировать в акции-неЦФА при реорганизации и наоборот.

При анализе представленных положений закона напрашивается вывод, что законодатель предполагает создание специальный субъектов – НАО, которые специализируются на выпуске цифровых акций. Интересен также тот момент, что выпуск ЦФА, удостоверяющих права участия в капитале публичного акционерного общества, запрещается законом.

Свою специфику имеет и модель выпуска ЦФА, удостоверяющих возможность осуществления прав по эмиссионным ценным бумагам, прав требовать передачи эмиссионных ценных бумаг. Оператор ИС с даты выпуска этих видов ЦФА обязан обеспечить доступ к решению о выпуске ценных бумаг, лежащих «внутри» токена и к сведениям о наличии и порядке осуществления преимущественного права на их приобретение.

Отдельные нормы ФЗ о РЦБ устанавливают особенности участия в общем собрании НАО. Так, обладатели ЦФА дают указания голосовать определенным образом лицам, которым открывается лицевой счет ЦФА, при этом обществу представлена информация об обладателях ЦФА и количестве ценных бумаг, права которых удостоверяются ЦФА (п. 1 ст. 8.10 ФЗ о РЦБ). Определение особенностей осуществления прав по акциям, которые учитываются на лицевом счете ЦФА, отдается на усмотрение Банка России. На данный момент подзаконные акты в отношении этого вопроса отсутствуют.

Наиболее распространенный на рынке вид ЦФА, включающий денежные требования, использует самую типичную модель выпуска ЦФА. При этом эти ЦФА могут выпускаться не только НАО, или финансовыми активами НАО, но и другими субъектами – индивидуальными предпринимателями и юридическими лицами любой организационно-правовой формы.

Для этого вида ЦФА также в основу берется модель эмиссии, так как общая концепция регулирования ЦФА, как отмечалось, основывается на модели регулирования бездокументарных ценных бумаг, однако прямая отсылка к ФЗ о РЦБ отсутствует.

Проанализировав правила всех действующих операторов ИС, можно выделить наиболее характерные этапы выпуска ЦФА:

– Формирование эмитентом решения о выпуске. Так, в Лайтхаусе эмитент может сформировать документ с использованием функционала платформы.

Процедура допуска к выпуску ЦФА. Данная процедура заключается в предоставлении ряда документов для проверки платежеспособности эмитента и соответствия его действий законодательству Российской Федерации. Так, Атомайз требует заявление на допуск, решение о выпуске, протокол собрания, где принято решение о проведении выпуска, уведомление о рисках. Альфа-Банк проводит комплаенс-проверку эмитентов, порядок которой не раскрывается, и требует направления за 10 рабочих дней решения о выпуске для предварительной проверки на соответствие законодательству.

При положительном решении оператора ИС о допуске к выпуску оператор ИС присваивает выпуску идентификационный номер.

– Публикация решения на сайте оператора ИС и эмитента в исполнении требований ч. 6 ст. 3 ФЗ о ЦФА.

После этого приобретатели могут направить заявки на приобретение токенов, которые подписываются закрытым (приватным) ключом приобретателя.

– Уведомление эмитента о направлении приобретателями заявок.

– Перечисление ЦФА на кошелек приобретателей. С этого момента сделка считается исполненной.

– Признание выпуска состоявшимся, т. е. наступление условий, которые прописаны в решении о выпуске.

Для автоматизации процедуры выпуска ЦФА операторы ИС могут разработать смарт-контракты. Так, например, в правилах Сбербанка обязательства инвестора по оплате ЦФА, обязательства эмитента по передаче ЦФА и контроль выполнения условий решения о выпуске для признания выпуска состоявшимся обеспечиваются смарт-контрактом.

По своей сущности смарт-контракт – ключевой элемент блокчейн-системы, который необходим для облегчения, выполнения и обеспечения соблюдения обязательств между сторонами. Смарт-контракты выполняют две функции: хранят баланс токенов в кошельке и обеспечивают передачу токенов между пользователями. От реализации технологии смарт-контрактов, благодаря которым осуществляются транзакции, в конечном итоге зависит функционирование ЦФА и других цифровых прав. С другой стороны, интеграция смарт-контрактов в ИС требует большое количество ресурсов и дополнительную законодательную регламентацию, так как смарт-контракты меняют сущность исполнения обязательств (контрагенты не влияют на факт исполнения ввиду автоматизации) и договорной ответственности (проблема ошибки в функционировании самого смарт-контракте).

Криптозаписи – это совокупность электронных данных, которые содержат информацию о всем «цикле жизни» токена, начиная с его эмиссии и закрепления в кошельке его покупателя, заканчивая обращением и погашением. В публичном распределенном реестре криптозаписи начинают обладать имущественной значимостью только в результате взаимного интереса участников блокчейн-платформы.

Учет и обращение ЦФА в распределенном реестре происходят путем внесения или изменения криптозаписей в распределенный реестр. Эти записи вносятся оператором ИС по указанию эмитентов, обладателей ЦФА и других лиц, указанных в ФЗ о ЦФА, например, номинальных держателей. Согласно ст. 141.1 ГК РФ «осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу», поэтому перечень лиц, которые могут вносить эти записи, ограничен. Более того, записи о ЦФА могут вноситься оператором без указания на это со стороны пользователей системы в случаях, прямо предусмотренных законом. Речь идет о внесение записей на основании решения публичного органа власти или в рамках наследования по ч. 2 ст. 6 ФЗ о ЦФА.

При государственном регулировании ЦФА взаимно-доверительная составляющая преобразуется в общее правило, которому должны следовать все участники

рынка, при этом криптозаписи признаются государством как объект инвестирования только в случае своевременного и в полном объеме уведомления о факте владения ЦФА или совершения сделок с ними налоговые органы.

В соответствии с ч. 1 ст. 4 ФЗ О ЦФА учет ЦФА происходит в ИС, при этом способ учета устанавливается операторами самостоятельно в правилах. В правилах операторов ИС предусматривается компонент ИС, который обозначается как реестр (ЦФА/токенов/сделок) – централизованная база данных, которая содержит информацию обо всех сделках с ЦФА, а также другая информация, полный перечень которой представлен в правилах операторов ИС. Другим важным компонентном выступает кошелек пользователя, где содержится информация обо всех принадлежащих лицу токенах. Кошелек – программно-техническое средство, к которому закрепляется открытый и закрытый ключ, обеспечивающий доступ пользователей к ЦФА.

В ФЗ о ЦФА также устанавливаются особенности учета эмиссионных ценных бумаг: они учитываются на лицевом счете ЦФА, который открывается лицу, выпускающему ЦФА и осуществляющему права по этим ценным бумагам. При этом другие ценные бумаги зачислять на этот счет нельзя. Положение Банка России от 29.06.2022 № 799-П, вступившее в силу 1 апреля 2023 г., устанавливает дополнительные требования к деятельности реестродержателей ценных бумаг.

Обращение ЦФА, как было упомянуто ранее, может осуществляться через оператора ИС. Переход прав, которые удостоверяются ЦФА, происходит в момент внесения записи в ИС о совершении такого перехода. Более детальное регулирование содержится в правилах операторов ИС. Так, в правилах Лайтхауса, Сбербанка представлена модель «оферта-акцепт», а в правилах Мастерчейна, Атомайза и Альфа-Банка также показана возможность реализации модели сбора и сопоставления разнонаправленных сделок. Вторая модель по многом похожа на процедуру выпуска ЦФА, за исключением этапов составления решения о выпуске, прохождения процедуры допуска и присуждения идентификационного номера, так как все эти процедуры были уже пройдены на момент выпуска. Оферент составляет заявку на продажу ЦФА или на совершение другой сделки, а адресат оферты при желании приобретает токены путем направления заявки на приобретение.

Отличие второй от первой модели заключается в том, что при первой модели все заявки являются безадресными, т. е. применяется биржевая модель оборота финансовых инструментов, где факт заключения договора связан с совпадением двух безадресных заявок по цене, количеству и т. д.

Сделка, завершающая процесс обращения ЦФА, – погашение приводит к «погашению записи» о ЦФА. Данная формулировка встречает критику, запись нельзя погасить, так как она представляет из себя только набор цифр в базе данных ИС. Более того, само по себе погашение записи не влечет прекращения прав обладателя ЦФА по погашенным ЦФА и является скорее основанием для осуществления погашения ЦФА.

Выделяются следующие основания для погашения ЦФА:

Прекращение обязательства в силу их исполнения.

Речь идет о надлежащем исполнении обязательств со стороны эмитента. Детальный порядок погашения предусматривается в правилах операторов ИС.

Основания, предусмотренные в решении о выпуске.

Решение о выпуске предусматривает условия погашения ЦФА, в том числе, срок, дату, форму (как правило, в безналичной форме), способ (путем перечисления денежных средств на банковские счета обладателей или путем осуществления расчетов с использованием номинальных счетов), сумму и т. д. Также может быть предусмотрена модель досрочного погашения.

– Основания, предусмотренные законодательством Российской Федерации.

В главе 26 ГК РФ предусмотрены способы прекращения обязательств, которые также могут быть использованы в правоотношениях, связанных с ЦФА. Так, например, в решении о выпуске Атомайза № 1 от 01.08.2022 предусматривается прекращение обязательств путем зачета. Однако ФЗ о ЦФА есть специальная норма, в соответствии с которой ст. 413 ГК РФ не применяется в случае совпадения эмитента и обладателя ЦФА в одном лице в течение одного года.

Подводя итоги настоящего исследования, можно сделать вывод, что инфраструктуры рынка ЦФА находится на стадии становления, поэтому какие субъекты будут играть ключевые роли для функционирования рынка предстоит узнать в будущем. Так, несмотря на большое сходство с рынком ценных бумаг, инфраструктура ЦФА характеризуется особой технологической составляющей, которая добавляет к классической системе субъектов финансового рынка новых участников, а также создает новые требования и подходы к регулированию деятельности указанных субъектов. ФЗ о ЦФА особое внимание уделяет правовому регулированию деятельности операторов ИС и операторов обмена, так как эти фигуры обеспечивают функционирование ИС, допуск пользователей к платформе и законность при осуществлении сделок с ЦФА.

Система субъектов взаимосвязана с объектами, по поводу которых возникают правоотношения. По изменению ГК РФ в законе появился новый объект гражданского права – цифровые права, однако анализ определения, содержащего в ст. 141.1 ГК РФ, приводит к выводу, что речь идет о новом способе фиксации прав.

Более того, в законах представлен исчерпывающий перечень видов указанных цифровых прав, что становится преградой для развития рынка и предоставления возможности участникам рынка формировать эксклюзивные сделки по поводу новых финансовых активов. Чтобы решить данную проблему, ФЗ о ЦФА предусматривается конструкция гибридов, реализация которых ожидается в дальнейшем.

На сегодняшний день практическое воплощение получили исключительно ЦФА, включающие денежные требования. Выпуск представленного цифрового права происходит по модели STO, которая наиболее приближена к эмиссии ценных бумаг. Ключевым документом при выпуске ЦФА выступает решение о выпуске, и на данный момент практика содержит множество вариантов указанного документа, говорящих о желании участников рынка экспериментировать с новыми правовыми конструкциями.

Учет и обращение ЦФА осуществляется путем внесения записей в ИС, при этом для достижения юридической значимости указанных записей необходимо документарное закрепление имущественного права или его перехода.

Таким образом, бурное развитие сферы IT и финансов, на стыке которых и находятся ЦФА, приводит к появлению инновационных инструментов взаимодействия между участниками рынка, что усложняет работу законодателю, в частности в области выстраивания корректной модели регулирования новых общественных отношений. Поэтому научные исследования новых технологий крайне важны, поскольку вырабатывается необходимая теоретическая база для дальнейшего развития законодательства.

Список литературы

1. Абросимова Е. А. Организаторы торгового оборота: учебник для вузов. 2-е изд., перераб. и доп. М.: Юрайт, 2023. 183 с.

2. АКРА утвердило методологию присвоения рейтингов ЦФА. // АКРА. 2023. URL: https://www.acra-ratings.ru/company/news/100131

3. Гражданский кодекс от 30.11.1994 № 51-ФЗ Российской Федерации // Российская газета. 1994. № 238–239. 08 декабря.

4. Гражданский кодекс от 30.11.1994 № 51-ФЗ Российской Федерации // Российская газета. 1994. № 238–239. 08 декабря.

5. Захаркина А. В. Цифровые финансовые активы через призму учения о бездокументарных ценных бумагах // Ex jure. 2022. № 3. URL: https://cyberleninka.ru/article/n/tsifrovye-finansovye-aktivy-cherez-prizmu-ucheniya-o-bezdokumentarnyh-tsennyh-bumagah

6. Инвестбанки подписались на цифру // Коммерсантъ. 2022 г. URL: https://www.kommersant.ru/doc/5501983?from=top_main_2

7. Конобеевская И. М. Цифровые права как новый объект гражданских прав // Изв. Сарат. ун-та Нов. сер. Сер. Экономика. Управление. Право. 2019. № 3. URL: https://cyberleninka.ru/article/n/tsifrovye-prava-kak-novyi-obekt-grazhdanskih-prav

8. Матыцин Д. Е. Цифровые финансовые активы в дистанционных инвестиционных сделках //Банковское право. 2022. № 1. С. 39–47.

9. Минфин опередил ЦБ в дискуссии о торговле цифровыми активами // Ura.ru. 2023 г. URL: https://ura.news/articles/1036286162

10. Мурадян С. В. Цифровые активы: правовое регулирование и оценка рисков // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 123–151. EDN: RIZOKS.

11. Накамото С. Биткоин: система цифровой пиринговой наличности / С. Накамото // Bitcoin. URL: http:// bitcoinwhitepapers.com/bitcoin_ru.pdf

12. Новоселова Л. А., Полежаев О. А. Цифровые финансовые активы как объекты имущественных отношений: актуальные вопросы теории и практики // Власть закона. 2021. № 2. С. 75–91.

13. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам: протокол от 24.12.2018 № 16). URL: http://government.ru/info/35568

14 Перетолчин А. П. Генезис и перспективы развития правового регулирования цифровых финансовых активов в Российской Федерации // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 752–774. EDN: HLHZBU

15. Положение Банка России от 29.06.2022 № 799-П «Об открытии и ведении держателем реестра владельцев ценных бумаг лицевых счетов и счетов, не предназначенных для учета прав на ценные бумаги» // СПС «Консультант Плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_437842

16. Положении Банка России от 19.12.2019 № 706-П «О стандартах эмиссии ценных бумаг» (Зарегистрировано в Минюсте России 21.04.2020 № 58158) // Вестник Банка России, № 37–38, 26.05.2020.

17. Правила информационной системы АО Альфа-банк // Центральный банк Российской Федерации [Сайт]. [2000–2023]. URL: https://www.cbr.ru/vfs/finm_infrastructure/ois/rules/rules_alfa_02022023.pdf

18. Правила информационной системы ООО «Система распределенного реестра» // Центральный банк Российской Федерации [Сайт]. [2000–2023]. URL: https://www.cbr.ru/vfs/finm_infrastructure/ois/rules/rules_srr_09032023.pdf

19. Правила информационной системы ООО Атомайз // Центральный банк Российской Федерации [Сайт]. [2000–2023]. URL: https://www.cbr.ru/vfs/finm_infrastructure/ois/rules/rules_atomize_03022022.pdf

20. Правила информационной системы ООО Лайтхаус // Центральный банк Российской Федерации [Сайт]. [2000–2023]. URL: https://www.cbr.ru/vfs/finm_infrastructure/ois/rules/rules_litehaus_17032022.pdf

21. Правила информационной системы ПАО Сбербанк // Центральный банк Российской Федерации [Сайт]. [2000–2023]. URL: https://www.cbr.ru/vfs/finm_infrastructure/ois/rules/rules_sber_17032022.pdf

22. Проект федерального закона № 419059–7 «О цифровых финансовых активах». URL: http://sozd.parliament.gov.ru/ bill/419059-7

23. Проект Экспертного заключения Совета при Президенте РФ по кодификации и совершенствованию гражданского законодательства по проектуфедерального закона № 424632-7 «О внесении изменений в части первую, вторую ичетвертую Гражданского кодекса Российской Федерации», подготовленный в Исследовательском центре частного права имени С. С. Алексеева при Президенте РФ / Исследовательский центр частного права имени С. С. Алексеева при Президенте РФ. URL: http://privlaw.ru/wp-content/uploads/2018/04/meeting-190418-zakonoproekt-2-project-conclusion.pdf

24. Развитие рынка цифровых активов в Российской Федерации. Доклад для общественных консультаций // Банк России. 2022. URL: https://www.cbr.ru/press/event/?id=14281

25. Решение о выпуске цифровых финансовых активов № 1 от 01.08.2022 // ПАО «Горно-металлургическая компания «Норильский никель». ООО «Атомайз». 01.08.2022. URL: https://атомайз.рф/emission

26. Санниква Л. В., Харитонова Ю. С. Цифровые активы как объекты предпринимательского оборота // Право и экономика. 2018. № 4. С. 221–225.

27. Селин Ф. «Очередной прорыв — Закон о цифровых правах: на пути к вершинам юридической техники» // Журнал РШЧП. 2019. № 2. С. 60–69.

28. Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18.03.2019 № 34-ФЗ // Российская газета. № 124.

29. Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31.07.2020 № 259-ФЗ // Российская газета. 2020. № 173. 06 августа.

30. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // «Российская газета». 2006. № 165. 29 июля.

31. Федеральный закон РФ от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах» // Российская газета. 2011. № 266. 26 ноября.

32. Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 725–751. EDN: HGBQGL

А. А. Осташев,
студент,
Московский государственный технический университет
имени Н. Э. Баумана

ВНЕДРЕНИЕ НЕВИДИМЫХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ КАК СРЕДСТВО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ЦИФРОВЫЕ ФАЙЛЫ

Аннотация. В статье исследованы цифровые водяные знаки как средство обеспечения защиты авторских прав на цифровые файлы. Приведено понятие «цифровые водяные знаки», установлены его отличия от электронной подписи, определена правовая основа применения в рамках уголовного и гражданского судопроизводства. Отдельно проанализирован наиболее простой метод замены наименьшего значащего бита. Проведенный эксперимент в программе «OpenPuff» позволил прийти к выводу, что цифровые водяные знаки являются достаточно эффективным средством для маркировки видеопродукции для предотвращения ее дальнейшего контрафактного распространения. По итогам работы был составлен примерный перечень рекомендаций при работе с файлами, потенциально содержащими цифровые водяные знаки и указано на необходимость разработки алгоритма для их внедрения/извлечения в зависимости от конкретных задач.

Ключевые слова: цифровой водяной знак, наименьший значащий бит, право авторства, стегоключ, стегоконтейнер, хеш-значение

IMPLEMENTING INVISIBLE DIGITAL WATERMARKS AS A MEANS OF ENSURING COPYRIGHT PROTECTION TO DIGITAL FILES

Abstract. The present article explores digital watermarks (DWM) as a means of ensuring copyright protection for digital files. The article presents the concept of digital watermark, establishes the differences from the electronic signature

as a representative of technical means of protection, defines the legal basis for the use of digital watermarks in the framework of criminal and civil proceedings. The simplest method for replacing the least significant bit (LSB) is analyzed separately. The conducted experiment in the OpenPuff program led to the conclusion that the CEH is a fairly effective tool for marking video products to prevent its further counterfeit distribution. Based on the results of the work, an approximate list of recommendations was compiled for working with files potentially containing watermarks and it was indicated that it was necessary to develop an algorithm for introducing / extracting watermarks, depending on specific tasks.

Keywords: digital watermark (DWM), least significant bit (LSB), copyright, stegokey, stegocontainer, hash value

Цифровой водяной знак (digital watermark, ЦВЗ) – это некоторая информация, которая добавляется к исходному цифровому файлу, например, изображению, аудио или видео. Простейшим примером ЦВЗ являются видимые надписи и/или рисунки на картинке, позволяющие установить авторство. Всего посредством таких знаков-маркеров реализуются следующие цели:

обеспечение права авторства. Автор контента может разместить на изображении знак авторства, указать, например, свои ФИО или название компании, разместить логотип, позволяющий идентифицировать его как автора данного произведения. В России по общему правилу, в соответствии с п. 1 ст. 1300 ГК РФ информацией об авторском праве признается «любая информация, которая идентифицирует произведение, автора или иного правообладателя, либо информация об условиях использования произведения…» [1];

защита права авторства от неправомерного копирования и/или использования, поскольку удаление нанесенного водяного знака техническими средствами может представлять определенные сложности для потенциального правонарушителя.

Цифровые водяные знаки являются эффективным и правомерным средством охраны авторов цифрового контента, в частности, видеоизображений. Во-первых, эффективность обеспечивается широкой классификацией ЦВЗ по способам внедрения, встраивания и извлечения. Основными характеристиками являются надежность, незаметность, безопасность, емкость, прозрачность и т. д. Надежность обуславливает устойчивость к различным видам атак, незаметность характеризуется видимостью или невидимостью ЦВЗ человеческому глазу на изображении, безопасность обеспечивает защиту маркированного изображения от несанкционированного обнаружения, изменения или внедрения данных. Таким образом, наиболее защищенными будут являться те видеофайлы, в которых, помимо видимого ЦВЗ, присутствует еще и скрытый, обнаруживаемый только специализированным ПО, а также устойчивые при изменениях исходного файла, например при переконвертации видео из одного формата в другой и обратно.

Во-вторых, правомерность определяется как международным, так и национальным законодательством Российской Федерации в области охраны прав авторов видеоконтента. Понятие «технические средства защиты интеллектуальных продуктов» нашло отражение в таких основополагающих документах по охране

авторского права, как Договор ВОИС по авторскому праву и Договор ВОИС о правах исполнителей и производителей фонограмм [3] (оба Договора от 20 декабря 1996 г.). По п. 1 ст. 1299 ГК РФ в качестве технических средств защиты авторских прав «признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения» [1].

В США с конца 1998 г. действует Закон о защите авторских прав на цифровые документы DMCA (Digital Millennium Copyright Act). Положительная сторона этого закона обуславливается тем, что права владельцев электронных документов уравниваются с правами авторов «материальных» произведений. В Европе в 2001 г. была принята аналогичная американскому закону Директива об авторских правах EUCD (European Union Copyright Directive) Кроме того, существует возможность получить патент на программные продукты, предназначенные для защиты авторских прав, так, например, один из лидеров рынка программ ЦВЗ – компания Digimarc.

На данном этапе стоить обратить внимание на то, что определения ЦВЗ не содержится в отечественных ГОСТах, в отличие, например, от электронной подписи. По ст. 2 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», электронная подпись – это «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию» [8]. Данное определение представляется весьма схожим с определением, данным ЦВЗ, однако это разные понятия.

Во-первых, алгоритмы внедрения ЦВЗ основаны на стеганографических методах, ЭП – на методах криптографии (для работы с ними необходим специализированный софт – например, криптопровайдер «КриптоПро»).

Во-вторых, факт, удостоверяющий наличие ЦВЗ не является обязательным; выделяют как видимые ЦВЗ (например, знак копирайта с ФИО или псевдонимом автора, позволяющий однозначно того идентифицировать), так и невидимые, в то время как ЭП может встраиваться в электронный файл или располагается в отдельном документе с расширением .sig.

В-третьих, ЭП служит для идентификации лица (физического или юридического) при подаче им документов в электронном виде, т. е. используется для удостоверения различных юридически значимых событий, содержащихся в данных документах. ЦВЗ же имеет более узкую специализацию, он обеспечивает право авторства на результат интеллектуальной деятельности (РИД) и служит средством защиты от совершения несанкционированных действий с данным объектом без разрешения правообладателя.

В-четвертых, ЭП используется только для файлов текстовых форматов (для удостоверения документов), в то время как ЦВЗ наоборот, наименее пригодны для текстовых документов и применяются в графических, аудио- и видеофайлах.

Ввиду того, что ЦВЗ как совокупность информационных данных могут представлять криминалистически значимую информацию, например по делам о нарушении авторских и смежных прав, то их исследование целесообразно

рассматривать в рамках криминалистического учения о цифровой информации. В. Б. Вехов и С. В. Зуев в учебнике «Цифровая криминалистика» в криминалистическое учение о цифровой информации включают криминалистическое исследование документированной цифровой (компьютерной) информации – электронных документов, электронных образов бумажных документов, динамичной и статичной электронной подписи, а также следов их подделки или компрометации [9. С. 18]. С точки зрения цифровой криминалистики ЦВЗ и ЭП должны исследоваться как объекты одной группы.

Защита правообладателей гарантируется положениями статьи 1300 ГК РФ, в частности, пунктом 2, который запрещает удаление или изменение без разрешения автора или иного правообладателя информации об авторском праве [1]. Тем самым удаление с помощью сторонних программ встроенного ЦВЗ (как видимого, так и невидимого) будет являться нарушением. Хотя следует заметить, что, как правило, цифровой водяной знак, встроенный в изображение некоторой программой, не всегда можно обнаружить при помощи другого программного продукта. Это объясняется тем, что каждая программа является реализацией того или иного метода или методов внесения ЦВЗ. И если программы реализуют разные методы или даже разные алгоритмы одного метода, то показывать в качестве ЦВЗ они будут разную информацию.

Использование, в первую очередь скрытых цифровых водяных знаков, активно используется в киноиндустрии. ЦВЗ призваны защитить правообладателей от неправомерной перепродажи, когда, в случае если выпущенный фильм попадет в другой кинотеатр, студия сможет определить источник неправомерного распространения копии. При этом сам ЦВЗ зрителям остается невидим. Также это служит средством защиты правообладателей в сети «Интернет» от преждевременного распространения их фильмов. Если каждая копия контента защищена уникальным водяным знаком, то всплывшая в сети запись сразу выдаст источник утечки.

Эффективным средств защиты авторских прав в сети «Интернет» является цифровое управление правами Digital Rights Management (DRM), которое обеспечивает защиту цифрованных произведений от копирования и иных незаконных действий без согласия правообладателя. Одним из инструментов и являются цифровые водяные знаки. Каждый пользователь – автор видеоконтента – может защитить свой цифровой продукт в сети «Интернет». Для этого надо воспользоваться программой, которая поддерживает функцию WaterMarking.

Наиболее простым для понимания примером метода встраивания информации на уровне битовой плоскости является метод замены наименьшего значащего бита (LSB – Least Significant Bit, НЗБ). Суть метода заключается в замене последних значащих битов в контейнере (изображения, аудио- или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

Принцип основан на замене младших разрядов RGB-изображения на биты скрываемого файла, что не влечет существенного искажения изображения, поскольку каждый цвет может быть представлен комбинацией 255 × 255 × 255 оттенков. На рис. 1 представлен цвет #c32066 с характеристиками RGB 195, 32, 102.

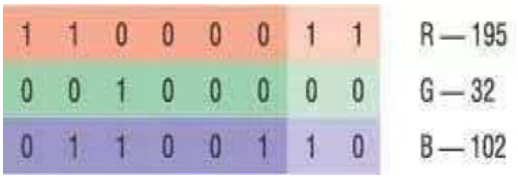

Рис. 1. Схема замены наименьших значащих битов в цвете #c32066

При внесении изменений в синий канал – значение 103 – получается новый оттенок, визуально не отличимый человеческим глазом (рис. 2).

Рис. 2. Цвета #c32066 и #c32067

Теоретически, исходя из полезного объема RGB-контейнера, имеется возможность спрятать три байта полезной информации на каждые четыре пиксела изображения, что соответствует 25 % объема картинки.

Достоинство данного метода заключается в небольшой сложности вычислений. Популярность обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации (пропускная способность создаваемого скрытого канала связи составляет при этом от 12,5 до 30 %).

Существенный недостаток такого метода – ЦВЗ может быть легко удален путем повторного наложения последовательности ЦВЗ. Сам по себе такой знак относится к категории хрупких, преобразование в сжатый формат или переконвертация уничтожает его полностью. В свою очередь, это может представлять сложности для выявления такого ЦВЗ, если в качестве такового использован файл с информацией, представляющей интерес для правоохранительных органов. Для обеспечения же безопасности созданного видеоконтента владелец файла внедряет водяной знак путем записи в него информации из определенного файла. Если возникла необходимость подтвердить авторство, владелец извлекает информацию из контейнера и доказывает тождество извлеченного и предъявленного файлов, что однозначно говорит об авторстве. Дополнительным средством защиты может служить хэш-функция. При встраивании секретной информации хэш-значение принимает переменный размер входных данных и на выходе возвращает фиксированный размер цифровой строки.

Дальнейшее развитие метод НЗБ получил в виде метода псевдослучайного интервала. В основе данного метода лежит использование набора псевдослучайных чисел (задаваемых секретным ключом), которые определяют псевдослучайный интервал между отдельными пикселями изображения, в которые методом НЗБ встраиваются информационные биты. Эта методика особенно эффективна в случае, когда битовая длина секретного сообщения существенно меньше количества пикселей изображения. Данный метод сохраняет преимущества и недостатки самого метода НЗБ.

Таким образом, метод НЗБ основан на том, что изменения, вносимые в исходный файл путем замены последних 2 или 3 битов исходного кадра на биты скрываемого изображения, не должны быть визуально заметны или восприниматься человеческим глазом. Несмотря на простоту метода и возможность сокрытия большого количества информации, он характеризуется хрупкостью внедряемых с его помощью ЦВЗ. Это накладывает ряд особенностей при работе специалиста с видеофайлом, потенциально содержащим скрытый ЦВЗ, внедренным методом НЗБ.

Существует большое разнообразие различных бесплатных программ и утилит с открытым исходным кодом, предназначенных для стеганографии (Anubis, DeEgger Embedder, DeepSound, Hallucinate, JHide, OpenPuff, OpenStego, Image Steganography, SilentEye), далеко не все из них подходят для решения задач безопасности. Наиболее часто встречаются программы, предназначенные для внедрения исходные файлы, таковыми чаще всего являются контейнеры формата .bmp, .png, .jpg, некоторые предназначены для внедрения ЦВЗ в аудиоконтейнеры (DeepSound), и лишь малое количество из предлагаемых программ имеют функцию добавления невидимых ЦВЗ в видеоконтейнеры, в частности это программы DeEgger Embedder (формат AVI) и OpenPuff (MP4). В данном исследовании будут подробно рассмотрены возможности и особенности работы последней.

В отличие от других утилит, поддерживающих парольную защиту скрываемого сообщения, OpenPuff умеет использовать для шифрования криптографически стойкий генератор псевдослучайных чисел (CSPRNG – Cryptographically secure pseudorandom number generator). В этом и заключается отличие – биты скрываемого изображения распределяются по всему контейнеру, тем самым данный генератор является усовершенствованным методом НЗБ – метод случайного интервала.

Программа OpenPuff предназначена для внедрения секретного файла (стегоключа), который может быть представлен текстовым, фото- или аудиофайлом. На основе паролей *A*, *B* или *C* длиной от 8 до 32 символов CSPRNG сгенерирует уникальный ключ, которым и будет зашифровано сообщение. OpenPuff поддерживает MP4, MPG, VOB и множество других форматов. Максимальный размер скрываемого файла – 256 Мбайт.

В качестве тестового видеофайла было выбрано 5-секундное видео с видом на парк и проезжающие автомобили с названием «пример.mp4» (рис. 3).

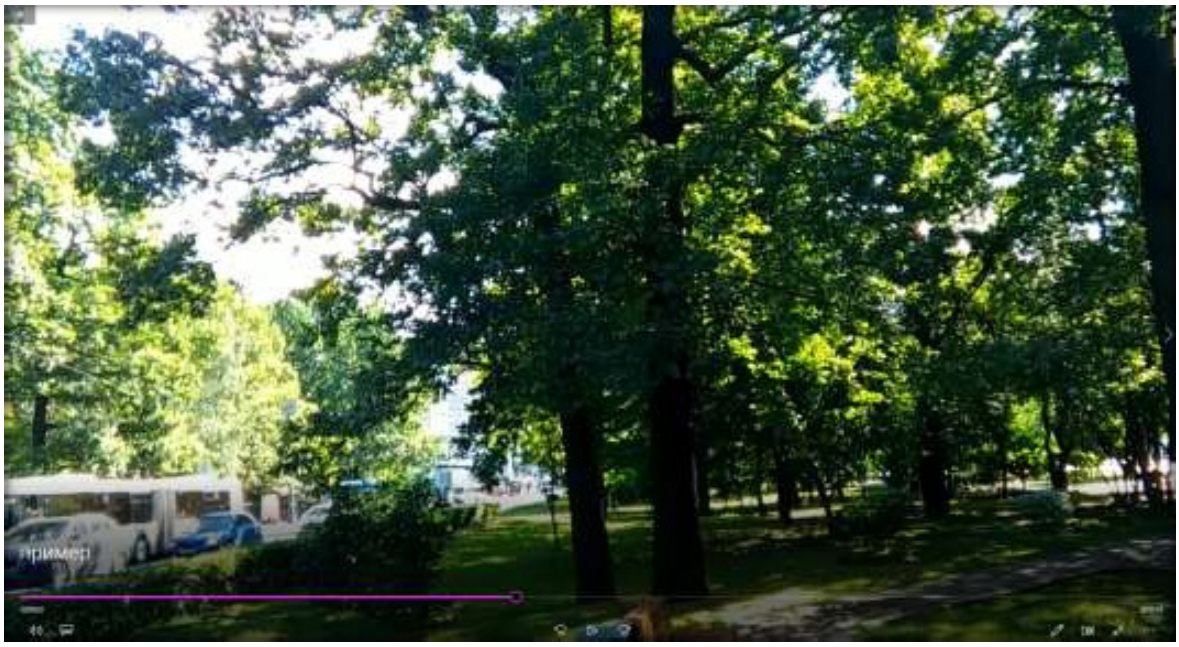

Рис. 3. Тестовое видео «пример.mp4»

На рис. 4 показан функционал программы OpenPuff, где в файл «пример.mp4» внедряется ЦВЗ, представленный тестовым файлом со словом «Проверка», дополнительно выбраны параметры вставки 20 % заполнения контейнера – такой показатель позволяет (в случае большого скрываемого файла) не ухудшать качество фотографии настолько, чтобы отличия были заметны человеческому глазу.

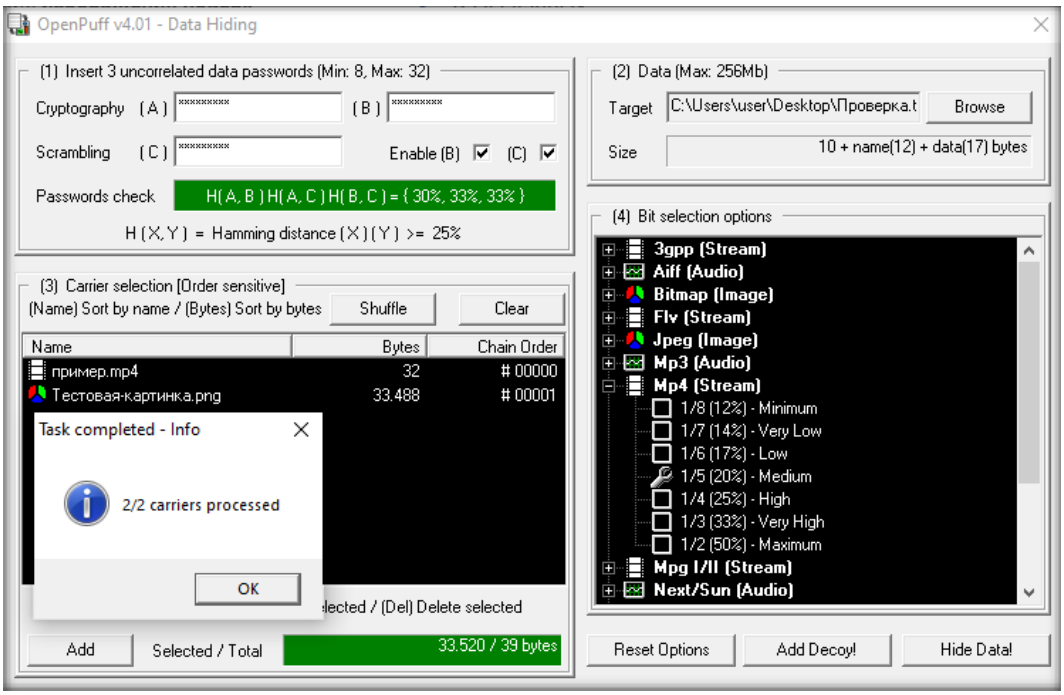

Рис. 4. Окно программы OpenPuff

Далее было проведено сравнение содержимого исходного и заполненного стегоконтейнеров – «пример.mp4» без ЦВЗ и «пример1.mp4» с внедренным ЦВЗ.

– в hex-редакторе WinHex. Визуальных различий в видео не наблюдалось. По результатам сравнения составлен отчет, представленный на рис. 5.

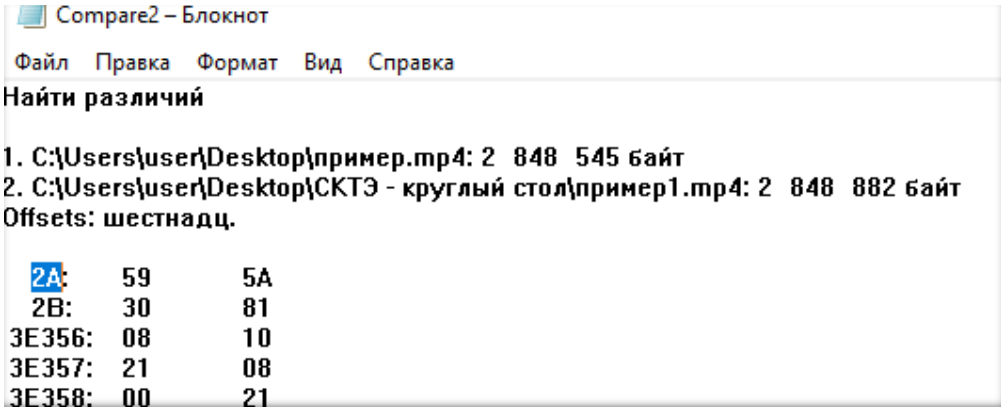

Рис. 5. Фрагмент программы «Блокнот» с результатом сравнения двух стегоконтейнеров

В данном случае был спрятан текстовый файл «Проверка2.txt» объемом 747 байт. Сравнение файлов в программе WinHex вывела объем пустого контейнера в 2.848.545 байт, стегокотейнера – в 2.848.882 байта. Анализ стегоконтейнера в hex-редакторе показал отсутствие зависимости между размером сообщения и числом измененных пикселей, что может усложнить его подробное исследование при отсутствии оригинала.

Тем не менее при кажущемся визуальном отсутствии изменений в файлах графических и аудиоформатов и в процессе сравнения исходного и предполагаемого измененного файла хеш-значения файлов будут различаться. Для определения MD5 хэш-значения была использована программа WinHex. С помощью инструмента «Вычислить хэш» были получены значения исходного и измененного файлов. Хэш-значения исходного файла – «CB85037A96851A72B9A013A81140 7A27» (рис. 6), хэш-значения измененного файла – «5DD06685339344748187CEE CA5F69F16» (рис. 7).

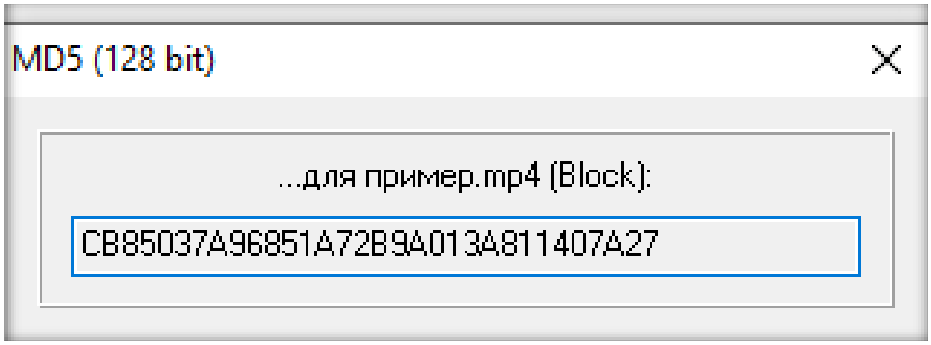

Рис. 6. Хэш-значение файла «пример.mp4»

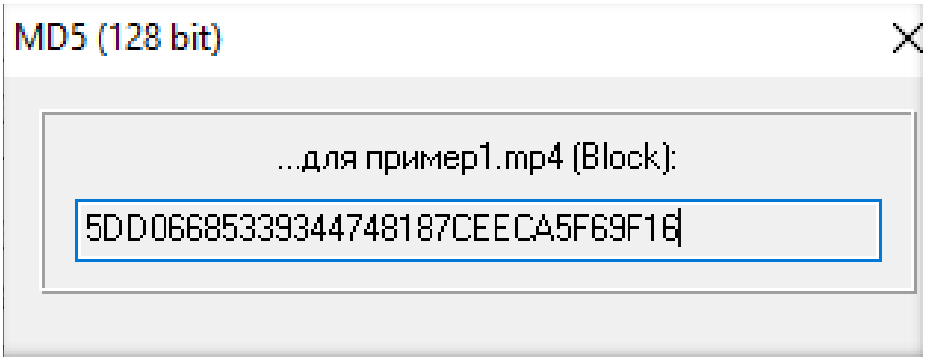

Рис. 7. Хэш-значение файла «пример1.mp4»

Далее был проведен аналогичный опыт – исходное видео было загружено в редактор. Программы, аналогичные Wondershare Filmora 12, позволяют пользователю ПК самостоятельно внедрить видимы ЦВЗ во весь видеоряд. Итоговым результатом стало 7-секундное видео с наложенным поверх изображения видимого ЦВЗ, которое было сохранено под новым названием «Мое видео.mp4» (рис. 8).

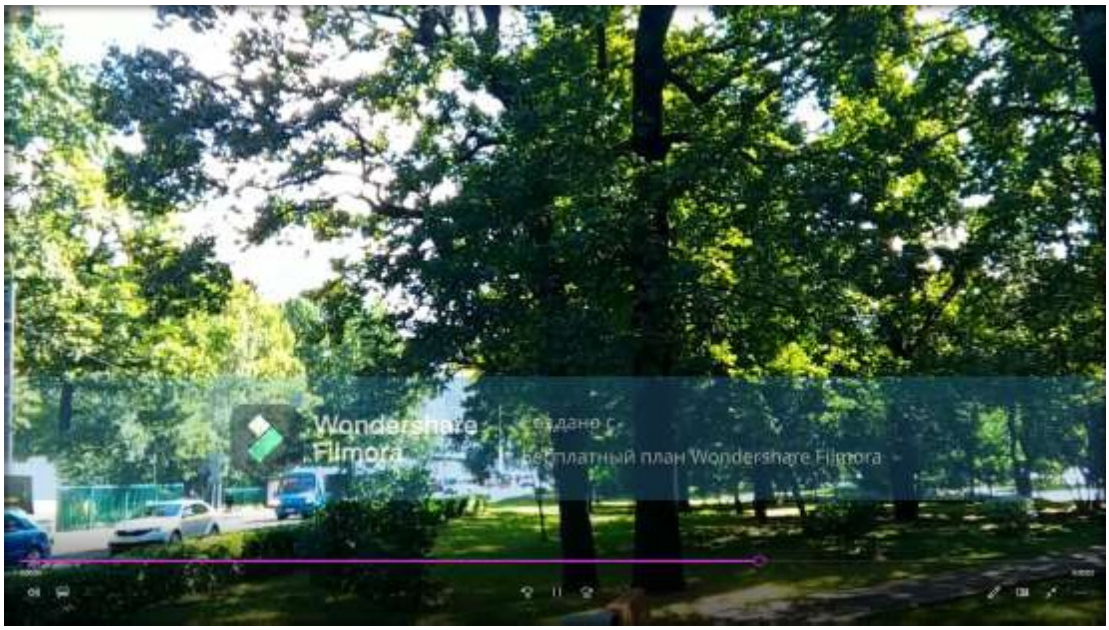

Рис. 8. Новый файл «Мое видео.mp4» после обработки в редакторе Wondershare Filmora 12

Структура содержимого файла отличается от предыдущего контейнера – биты информации, встречающейся в файле «пример.mp4», в данном контейнере расположены в каталоге mdat после всех иных каталогов коробки moov (рис. 9).

При сравнении метаданных исходного и заполненного контейнеров «Мое видео.mp4» и «Мое видео1.mp4» видно, что метаданные в части времени создания и изменения файла изменениям не подверглись – 7 мая 2023 года, 14:49.

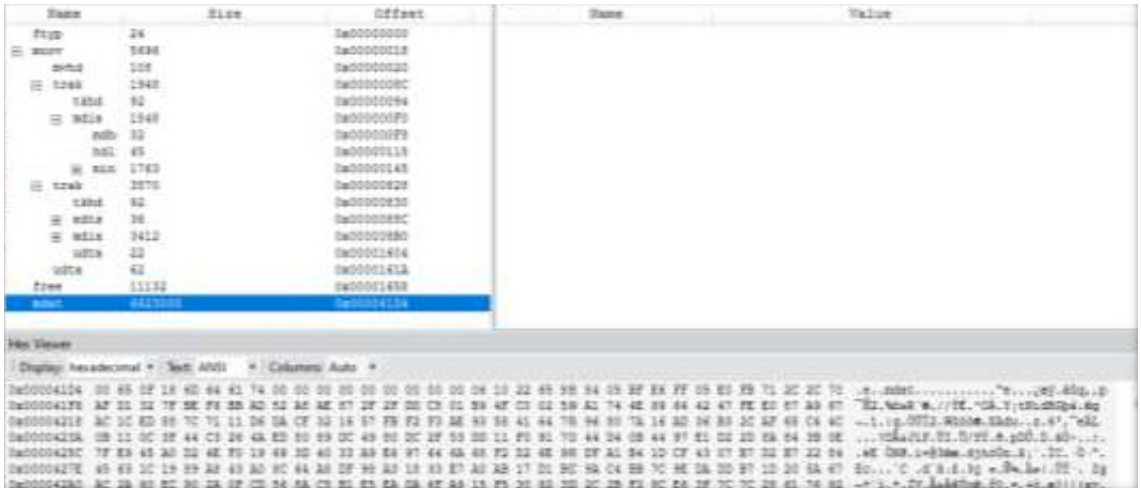

Рис. 9. Фрагмент программы «Elecard Video Format Analyzer» с открытым в ней файлом «Мое видео.mp4»

Стоит упомянуть о другом режиме работы программы – запись и чтение стегометок. Это скрытые строки длиной до 32 символов, которые можно использовать для защиты авторского права. Для работы в данном режиме необходимо написать про произвольную стегометку в верхней части окна и указать ниже файлы, в которые ее надо добавить. Исходные файлы останутся нетронутыми, а их копии с меткой сохранятся в указанном каталоге. Это является простым аналогом скрытого ЦВЗ с той лишь разницей, что скрывается не определенный файл, а только текст (метка). Соответственно, ее использование может быть необходимо только в случаях обеспечения права авторства. Так, в файл «пример.mp4» была внедрена стегометка «Осташев А. А. ЮР-83» (рис. 10). Тем не менее даже простое конвертирование в другой формат стирает стегометку, равно как и в случае, если файл был снова приведен к исходному формату. Стойкие стегометки, равно как и стойкие (робастые) ЦВЗ существуют, но их внедрение могут выполнять только отдельные программы, которые, как правило, встроены к какое-то конкретное оборудование (например, модели камеры).

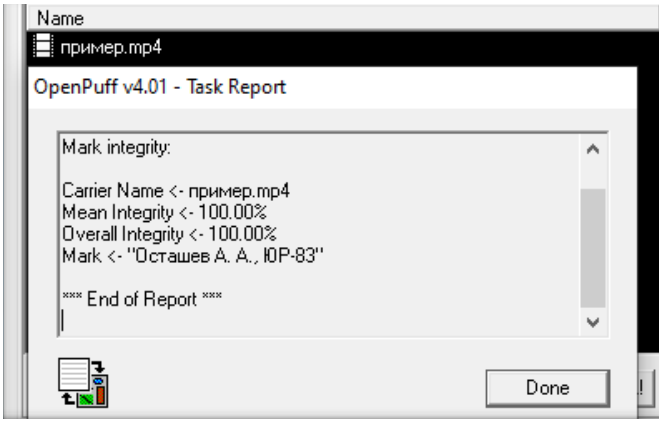

Рис. 10. Фрагмент программы «OpenPuff» со стегометкой в файле «пример.mp4»

Извлечение секретных файлов выполняется аналогичным образом указанными программными средствами.

Дополнительная защита ЦВЗ осуществляется с помощью генерации хэш-значения, что потенциально обеспечивает защиту авторских прав от незаконного использования в сети «Интернет» [7. С. 32]. Анализ изображений на наличие скрытых ЦВЗ может быть актуален в случаях проверки подлинности файла, если заранее известно, что он должен содержать секретный файл, а также в случаях обнаружения файлов и подозрений, что они содержат в себе скрытые файлы с важной информацией (например, криминального характера). Обнаружение ЦВЗ, скрытых методом замены наименьшего значащего бита, обладает рядом особенностей:

во-первых, анализ файла в hex-редакторе не дает ответа, какой программой был внедрен стегофайл;

во-вторых, метод LSB шифрует биты информации непосредственно в теле файла, а не дописывает код в конец файла, что усложняет обнаружение.

в-третьих, ЦВЗ могут быть как «хрупкими», т. е. повреждаться при различных манипуляциях с файлом – сжатии, переводе в другой формат и т. д., или «надежными», т. е. успешно противостоящими всем видам атак. Соответственно, дополнительно может потребоваться проверка по критериям надежности, незаметности и безопасности [5. С. 5]. Стоит обратить внимание на то, что установить факт внесения изменений в файл – в случае с ЦВЗ – может быть сложно, поскольку метаданные не меняются, что показала практика с программой OpenPuff и Elecard Video Format Analyzer.

Тем самым можно сформулировать ряд правил, способных помочь эксперту в определении файлов, потенциально содержащих скрытые ЦВЗ.

Работать с копией файла. Если конвертация файла из одного формата и обратно выявит расхождения в кодах файлов, то, возможно, при конвертации был потерян секретный файл.

По возможности, сравнить исследуемый файл с исходным – например, если это так называемая стоковая фотография – в hex-редакторе, или программе, аналогичной Beyond Compare 4.

Обратить внимание, что отсутствие отличий в hex-редакторе сравниваемых файлов не означает отсутствия стегосообщения, в то время как отличающиеся друг от друга хеш-фунции файлов могут свидетельствовать о данном факте [6. С. 41].

Тем самым можно сказать, что вопрос выявления скрытых ЦВЗ остается открытым, поскольку не всегда достаточным является наличие программ с открытым исходным кодом и поэтому может понадобиться разработка алгоритма по внедрению/извлечению ЦВЗ на одном из языков программирования для решения конкретных задач. Стеганографию эффективнее всего использовать не вместо криптографии, а вместе с ней. Такое сочетание позволяет скрыть как саму информацию, так и факт ее хранения или передачи.

Список литературы

1. Гражданский кодекс Российской Федерации (ГК РФ) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5142

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. М.: Солон-Пресс, 2009. 272 с.

3. Договор ВОИС по авторскому праву, Женева, 20 декабря 1996 г. // СПС «Гарант». URL: https://base.garant.ru/2561877

4. Договор ВОИС по исполнениям и фонограммам, Женева, 20 декабря 1996 г. // СПС «Гарант». URL: https://base.garant.ru/2561873

5. Муртазалиева И. А. Сравнение производительности различных методов нанесения водяных знаков // «StudNet». 2021. № 5. 15 с.

6. Осташев А. А. Исследование метода LSB для внедрения невидимых цифровых водяных знаков (ЦВЗ) в изображения // Сборник трудов конференции «Всероссийская студенческая конференция «Студенческая научная весна», посвященной 170-летию В. Г. Шухова. 2023. С. 40–42.

7. Серебрякова С. А., Филиппов М. В. Разработка алгоритма встраивания и извлечения цифровых водяных знаков для видеофайлов AVI-формата // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2021. № 1. С. 20–34.

8. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_112701

9. Цифровая криминалистика: учебник для вузов / В. Б. Вехов [и др.]; под редакцией В. Б. Вехова, С. В. Зуева. М.: Юрайт, 2023. 417 с.

М. И. Панкратьева,
магистрант,
Пермский государственный национальный
исследовательский университет

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Аннотация. В статье рассматриваются действующие и ранее существовавшие положения российского законодательства, регулирующие обработку персональных данных, раскрытых субъектами данных самостоятельно. Проанализированы актуальные изменения, внесенные в законодательство о персональных данных, определены их достоинства и недостатки. Изучено правовое регулирование персональных данных, раскрытых пользователем самостоятельно, в социальных сетях и условия законности их дальнейшей обработки. Определены основные способы защиты прав субъекта персональных данных, а также способы их защиты, применяемые в судебной практике. Предложены пути дальнейшего совершенствования законодательства в рассматриваемой области.

Ключевые слова: персональные данные, общедоступные персональные данные, разрешенные для распространения персональные данные, персональные данные, раскрытые субъектом персональных данных самостоятельно, социальные сети

PERSONAL DATA PROTECTION IN SOCIAL NETWORKS

Abstract. The article deals with the current and previously existing provisions of Russian legislation regulating the processing of personal data disclosed by data subjects independently. The changes to the Law on Personal Data introduced on 30.12.2020 are analyzed, their advantages and disadvantages are determined. The legal regulation of personal data disclosed by the user independently in social networks and the conditions for the legality of their further processing have been studied. The main ways of protecting the rights of the subject of personal data, as well as the ways of their protection used in judicial practice, are defined. The ways of further improvement of the legislation in this field are proposed.

Keywords: personal data, publicly available personal data, personal data authorized for distribution, personal data disclosed by the personal data subject independently

По статистике Global Digital, на начало 2023 г. в России насчитывалось 106 млн пользователей социальных сетей, что составляет более 70 % от общей численности населения [25]. Среднемесячная аудитория социальной сети «ВКонтакте» на конец 2022 г. составляла 79,5 млн российских пользователей [4]. Локальные нормативные акты социальных сетей (к примеру «ВКонтакте» [17. п. 5.3] и «Одноклассники» [6. п. 5.1]) обычно предусматривают обязанность пользователя указывать при регистрации актуальную и достоверную информацию о себе, такую как фамилия, имя, дата рождения и прочие. Это демонстрирует, насколько обширный массив личной информации граждан представлен сейчас в российском интернете. В связи с развитием современных технологий и путей их использования в противозаконных целях особо остро встает вопрос правового регулирования персональных данных, размещаемых гражданами самостоятельно в ходе своей интернет-деятельности.

С 2011 г. (когда в законе впервые появился этот термин) до 2020 г. персональные данные, доступ неограниченного круга лиц к которым был предоставлен самим субъектом данным либо по его просьбе, согласно Закону о персональных данных [11] считались «персональными данными, сделанными субъектом общедоступными». Подобные «общедоступные» данные можно было обрабатывать без согласия на обработку (даже если они относились к специальной категории данных); оператор был не обязан предоставлять информацию об обработке субъекту данных и уведомлять о ней Роскомнадзор (ст. 6, 10, 18, 22 Закона). До недавнего времени данные, размещенные гражданином в открытом доступе (например, в социальной сети), могли обрабатываться (собираться, использоваться, передаваться) любым лицом бесконтрольно.

В 2020 г. в Государственную Думу Российской Федерации был внесен законопроект, направленный, в первую очередь, на регулирование оборота персональных данных в социальных сетях, где, по словам автора проекта А. В. Горелкина, распространена ситуация использования общедоступных данных с нарушением принципа целеполагания [23. С. 7]. Согласно тексту законопроекта, «персональные данные, сделанные общедоступными» предлагалось заменить «общедоступными

персональными данными», обработка которых допускалась лишь при наличии согласия субъекта на это [8].

Законопроект был доработан в ходе рассмотрения, и, в итоге, 30.12.2020 в Закон о персональных данных были внесены следующие изменения [9]:

1) термин «общедоступные персональные данные», представленный в первоначальном законопроекте, был заменен на «персональные данные, разрешенные субъектом для распространения», основные же положения законопроекта в большей части остались неизменны;

2) термин «персональные данные, сделанные общедоступными» исчез из текста Закона, но упоминание о них осталось в пункте 2 статьи 10.1, о чем будет упомянуто далее.

Говоря о персональных данных, разрешенных субъектом для распространения (п. 1.1 ст. 3 Закона о персональных данных [10]), нельзя не отметить ряд недостатков.

Начнем с определения: разрешенными для распространения данными являются такие персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом данных путем дачи согласия на их обработку.

В названии данной категории данных используется термин «распространение», который относится к действиям по обработке данных. Обработка персональных данных – это любые действия с данными, включая передачу данных (распространение, предоставление и доступ (п. 3 ст. 3). В Законе приводится определение терминов «распределение» и «предоставление». Распространение – это действия, направленные на раскрытие данных неопределенному кругу лиц. Предоставление – действия, направленные на раскрытие данных определенному кругу лиц или лицу (пункты 5, 6 ст. 3). Определение «доступа» законодателем не приводится. В п. 6 ст. 2 Закона об информации [12] «доступ к информации» определяется как возможность получения информации и ее использования. Это определение противоречит определению «обработки персональных данных», потому его использование по аналогии с данным законом в нашем случае невозможно.

При рассмотрении определений «разрешенных для распространения персональных данных» и непосредственно операции по «распространению» встает вопрос о том, намеренно ли законодатель использовал различные характеристики адресата, которому будет предоставлен доступ к данным; в одном случае это неограниченный круг лиц, в другом – неопределенный. Имеет ли значение эта разница или нет, сказать затруднительно, как минимум в виду отсутствия в российском законодательстве однозначного определения каждого из использованных понятий.

Также затруднительно сказать, в каком смысле законодатель использует в определении «разрешенных для распространения данных» термин «доступ», – подразумевается ли при этом одно из действий по передаче данных, определение из Закона об информации или словарное значение.

Не добавляют ясности положения об особенностях обработки новой категории данных (ст. 10.1 Закона о персональных данных), где устанавливаются требования к согласию на их обработку. Исходя из этих положений, при оформлении согласия субъект данных вправе как разрешить, так и запретить действия

по передаче своих данных не только по распространению, но и по передаче и доступу. То есть изначально названные «разрешенными для распространения» персональные данные по своему содержанию, могут «разрешаться» для всех операций по передаче данных.

Однако главный вопрос заключается в том, выполнены ли были задачи, на решение которых был направлен первоначальный законопроект? К сожалению, нет, ибо введенная категория данных не только не заменила ранее существующие «общедоступные» персональные данные, но и усложнила и без того непроработанный понятийный аппарат Закона о персональных данных. Эти изменения также усложняют документооборот организаций, так как для каждого случая распространения персональных данных клиента либо работника теперь требуется получение отдельного от них согласия на обработку.

Второе интересующее нас изменение Закона о персональных данных от 30.12.2020 содержится в п. 2 ст. 10.1: при раскрытии персональных данных неопределенному кругу лиц самим субъектом данных без предоставления оператору соответствующего согласия; каждое лицо, осуществившее их последующую обработку, обязано предоставить доказательства законности такой обработки. Здесь конструкция «персональных данных, сделанных общедоступными» фактически сохранена, хотя формально и не поименована. Помимо этого, законодателем был закреплен механизм их защиты путем установления запрета неограниченному кругу лиц на неправомерную обработку таких данных.

Стоит отметить, что именно к этому положению апеллирует социальная сеть «ВКонтакте». Так, в п. 6.4 Правил защиты информации о пользователях сайта VK.com [16] установлено, что ООО «Вконтакте» не имеет цели получить от пользователя разрешения на распространение персональных данных; пользователь самостоятельно предоставляет доступ к ним неограниченному кругу лиц.

Интереснее позиция социальной сети «Одноклассники». В п. п. 2.1 и 4.1 Политики конфиденциальности OK.ru [14] говорится: ООО «Мейл.Ру» считает, что пользователь понимает, что при размещении своей личной информации, он явно делает ее общедоступной, а в дальнейшем доступной для копирования и распространения другими пользователями. Вероятно, под этим подразумевается отсылка к ст. 7 Закона об информации об «общедоступной информации», которая фактически охватывает любую информацию, размещенную в открытом доступе в Интернете и вводит презумпцию ее свободного использования (за рядом законных ограничений в отношении распространения). Однако «личная информация» (что по сути является перефразированием определения персональных данных – любой информации, относящейся к физическому лицу) попадает под регулирование не Закона об информации, а специального законодательства – Закона о персональных данных [22]. В связи с чем подобная отсылка в Политике конфиденциальности OK.ru видится некорректной.

Необходимо определить границы «законности» обработки персональных данных, раскрытых неопределенному кругу лиц (например, в Интернете) самостоятельно. Изначальное «раскрытие» обыкновенно происходит на том или ином интернет-сайте, т. е. первоначальным оператором данных выступает администратор

этого сайта. В случае с социальными сетями персональные данные пользователей обрабатываются в силу необходимости для исполнения/заключения договора по инициативе пользователя (пп. 5 п. 1 ст. 6 Закона о персональных данных), которые заключается непосредственно при регистрации (обычно путем проставления «галочек» или нажатием кнопки, под которой указано «Нажимая «Продолжить», вы принимаете пользовательское соглашение...»). При этом собираются такие персональные данные, как имя, дата рождения, номер телефона, – без их предоставления регистрация невозможна.

Прочие персональные данные пользователь размещает по своему усмотрению, а также он может «защитить» свой аккаунт настройками приватности/конфиденциальности, ограничив доступ к ней прочих пользователей сети. Но и при этом часть персональных данных будет доступна сторонним пользователям, такие как имя, дата рождения, фотография профиля, город проживания/рождения, посещаемые/оконченные учебные заведения и др.

Будучи размещенными в социальной сети, персональные данные становятся доступны неограниченному кругу лиц, как зарегистрированным, так и незарегистрированным пользователям этой сети и Интернета в целом.

Случаи обработки этих данных физическим лицом исключительно для личных и семейных нужд при соблюдении прав субъекта данных не попадают под действие Закона о персональных данных (п. 2 ст. 1). При этом действует п. 1 ст. 152.2 Гражданского кодекса Российской Федерации (далее ГК РФ) [3], согласно которому сбор, хранение, распространение и использование любой информации о частной жизни гражданина допускается без его согласия в случае, если она была раскрыта самим гражданином или по его воле. Законодатель не раскрывает использованное в Законе о персональных данных понятие «личные и семейные нужды» (как, например, раскрывается аналогичное понятие [13] в Законе об информации, что, однако, неприменимо к рассматриваемому вопросу).

Очевидно, относимость конкретного случая обработки персональных данных к категории «для личных и семейных» определяет правоприменитель. Так, к подобным нуждам может относится использование родительского чата учеников школы в мессенджере [21], распространение листовок среди членов СНТ [2], а также высказывание оценочных мнений о человеке с использованием его данных в открытых группах в социальной сети [18].

Другие возможные случаи законной обработки персональных данных (помимо того, когда присутствует согласие субъекта данных) перечислены в ст. 6 Закона о персональных данных. К подобным относятся, в частности: необходимость осуществления деятельности органов судебной или исполнительной власти; достижение целей, предусмотренных международным договором России; исполнение договора, выгодоприобретателем, поручителем или инициатором заключения которого является субъект данных; обработка обезличенных данных и т. д.

Если действия лица по обработке чужих персональных данных не подходят под определение «личных и семейных нужд» и не отвечают перечисленным в ст. 6 Закона о персональных данных условиям обработки, возможно привлечение его к административной (ст. 13.11 Кодекса об административных правонарушениях

Российской Федерации – далее КоАП РФ) [5] или уголовной (ст. 137 Уголовного кодекса Российской Федерации) [24] ответственности.

Гражданско-правовыми способами защиты прав в случаях нарушения правил обработки персональных данных являются возмещение убытков (если они причинены) и компенсация морального вреда. Стоит отметить, что значительная часть судебных дел подобной направленности сопряжена с защитой чести, достоинства и деловой репутации (ст. 152 ГК РФ).

Рассмотрим несколько примеров привлечения к ответственности за нарушение законодательства о защите персональных данных. Так, за создание страницы в сети «ВКонтакте» с использованием полученных из открытых источников персональных данных и размещением объявлений интимного содержания с содержанием этих данных правонарушителя привлекли к ответственности по ч. 1 ст. 13.11 КоАП РФ и назначили наказание в виде предупреждения [15].

Размещение фотографии и персональных данных бывшего работника (продублированных с его же страницы) в социальных сетях вместе с порочащими комментариями повлекло обязание судом ответчика удалить опубликованную информацию и возместить потерпевшей компенсацию морального вреда в размере 10 000 рублей (при изначально запрошенных 100 000 рублей) [1].

За публикование фамилии и имени истца вместе с обвинениями в неуплате алиментов в «городской» группе «ВКонтакте» с ответчицы взыскали компенсацию морального вреда в пользу истца в размере 5 000 рублей (именно за распространение персональных данных без согласия, но не за порочащие сведения) [20].

Примечательно гражданское дело к сетевому изданию, которое в многочисленных источниках в Интернете (социальных сетях, видео-хостинги) размещало персональные данные истца, взятые из открытых источников, включая имя, адрес, фотографии, в том числе измененные с помощью фотомонтажа, вместе с недостоверными и порочащими его сведениями. Суд признал нарушающимися личные неимущественные права истца, его права как субъекта персональных данных, обязал ответчика удалить все содержащие сведения об истце данные, опубликовать опровержение, запретил ответчику дальнейшую обработку персональных данных истца, взыскал в пользу ответчика компенсацию морального вреда в размере 50 000 рублей (при запрошенных истцом 150 000 рублей), расходы на нотариуса, адвоката, представителя и государственную пошлину в размере 293 000 рублей, а также неустойку в случае неисполнения судебного решения [19].

В представленной судебной практике прослеживается применение таких способов защиты гражданских прав, как удаление незаконно распространенных персональных данных и запрет их дальнейшей обработки, которые прямо не перечислены в ст. 12 ГК РФ. Прослеживается и уменьшение судами изначально заявленного истцами размера компенсации морального вреда.

Резюмируя изложенное, можно сделать ряд выводов. В Интернете размещен огромный массив персональных данных, размещенных субъектами данных самостоятельно. Развитие современных цифровых технологий и программного обеспечения открывает все новые возможности неправомерного использования этих данных, а их защита сопряжена с судебными тяжбами и усмотрением

правоприменителей. Существующие методы защиты прав субъектов персональных данных применимы, но недостаточно эффективны. К сожалению, изменения Закона о персональных данных 30.12.2020, несмотря на изначальные намерения защитить данные граждан в социальных сетях, хоть и исключили возможность бесконтрольной обработки распространенных самими пользователями персональных данных, но эффективного механизма защиты их не внесли. В связи с чем перспективными направлениями совершенствования Закона о персональных данных являются:

1) раскрытие задействованного понятийного аппарата – закрепление определений «доступа» и «личных и семейных нужд», обоснование добавления термина «неопределенный круг лиц» в термине «разрешенных для распространения персональных данных» при уже существующем «неограниченном»;

2) развитие положений о «персональных данных, раскрытых субъектом данных самостоятельно», наделение субъекта данных эффективным механизмом защиты своих прав.

Список литературы

1. Апелляционное определение Пермского краевого суда по делу №33-9092/2018 от 27.08.2018 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbDq

2. Апелляционное определение Архангельского областного суда по делу №33-4528/2022 от 17.08.2022 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbQf

3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5142

4. Итоги четвертого квартала 2022 г. ВКонтакте. Пресс-служба ВКонтакте. 24.03.2023. URL: https://vk.com/press/q4-2022-results

5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661

6. О внесении изменений в Федеральный закон «О персональных данных» в части установления особенностей обработки общедоступных персональных данных: пояснительная записка к законопроекту от 17.11.2020. URL: https://sozd.duma.gov.ru/bill/1057337-7

7. О внесении изменений в Федеральный закон «О персональных данных» в части установления особенностей обработки общедоступных персональных данных: проект федерального закона от 17.11.2020. URL: https://sozd.duma.gov.ru/bill/1057337-7

8. О внесении изменений в Федеральный закон «О персональных данных»: федеральный закон от 30.12.2020 № 519-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_372682

9. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_439201

10. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс». URL: https://student2.consultant.ru/cgi/online.cgi?req=doc&n=117587&base=LAW&from=439201-0&rnd=v9XmKA#WxNY6pT6plLJ0rBN1

11. Об информации, информационных технологиях и защите информации: федеральный закон от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798

12. Лицензионное соглашение ООО «Одноклассники». URL: https://ok.ru/res/default/docs/odkl/agreement13_4.html

13. Правила пользования Сайтом ВКонтакте. URL: https://vk.com/terms

14. Утеген Д., Рахметов Б. Ж. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 825-844. EDN: DRGDDJ

15. Перечень личных, семейных и домашних нужд, удовлетворение которых не влечет исполнения обязанностей, предусмотренныз частями 2-4 статьи 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации»: Постановление Правительства РФ от 31.07.2014 № 747 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_166887

16. Постановление по делу об административном правонарушении Мирового судьи судебного участка № 60 Фроловского судебного района Волгоградской области по делу № 5-60-195/2021 от 29.04.2021 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbCA

17. Правила защиты информации о пользователях сайта VK.com. URL: https://vk.com/privacy

18. Решение Железногорского городского суда Красноярского края по делу № 2-644/2019 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbCr

19. Решение Новокуйбышевского городского суда Самарской области по делу № 2-22/2022 от 24.03.2022 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbqX

20. Решение Орджоникидзевского районного суда г. Магнитогорска Челябинской области по делу № 2-896/2021 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZcBt

21. Решение Сормовского районного суда г. Нижнего Новгорода по делу № 12-16-2021 от 27.01.2021 // ГАС РФ «Правосудие». URL: https://clck.ru/35ZbEP

22. Рожкова М. А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? 13.01.2021 // Закон.ру. URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_personalnye_dannye_razreshennye_subektom_dlya_raspros

23. Стенограмма обсуждения проекта федерального закона № 1057337-7 «О внесении изменений в Федеральный закон «О персональных данных» в части установления особенностей обработки общедоступных персональных данных» от 09.12.2020. URL: https://sozd.duma.gov.ru/bill/1057337-7

24. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_453968/

25. Simon Kemp. Digital 2023: The Russian Federation. 13.01.2023. URL: https://datareportal.com/reports/digital-2023-russian-federation

Е. О. Пащук,
студент,
Уральский государственный экономический университет

РЕАЛИЗАЦИЯ КОНЦЕПЦИИ УСТОЙЧИВОГО РАЗВИТИЯ В УСЛОВИЯХ ВНЕДРЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРАВОВЫЕ АСПЕКТЫ И ВЫЗОВЫ

Аннотация. В статье проанализированы негативные аспекты внедрения искусственного интеллекта в контексте реализации концепции по устойчивому развитию. Изучены цели устойчивого развития и проанализирована их взаимосвязь. Детально рассмотрены негативные последствия внедрения цифровых технологий как для общества, так и для государства. Выявлены пробелы в законодательстве в части регулирования вопросов, связанных с информационно-коммуникационными технологиями и предложены варианты их восполнения.

Ключевые слова: право, цифровые технологии, устойчивое развитие, концепция устойчивого развития, цели устойчивого развития, цифровое право, технологии, искусственный интеллект

IMPLEMENTATION OF THE CONCEPT OF SUSTAINABLE DEVELOPMENT IN THE CONDITIONS OF IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE: LEGAL ASPECTS AND CHALLENGES

Abstract. The article analyzes the negative aspects of the introduction of new technologies, and in particular artificial intelligence, in the context of the implementation of the concept of sustainable development. The Sustainable Development Goals are studied and their interrelation is analyzed. The negative consequences of the introduction of technologies, both for society and for the state as a whole, are considered in detail. Gaps in legislation regarding the regulation of issues related to information and communication technologies have been studied and solutions have been proposed.

Keywords: law, digital technologies, sustainable development, sustainable development concept, sustainable development goals, digital law, technologies, artificial intelligence

Концепция устойчивого развития – это комплекс мероприятий по успешному изменению государства с учетом экономических, социальных и экологических факторов. Данная программа включает в себя 17 целей, достижение которых имеет огромное значения в реализации рассматриваемой концепции и в решении глобальных проблем [6. С. 386–394]. Одной из целей устойчивого развития является интеграция инновационных технологий. Данная цель является действительно глобальной и определяет результат в части достижения остальных целей устойчивого развития. Информационно-коммуникационные технологии стали неотъемлемой частью каждого человека и охватили все сферы общественной жизни. Технологии используются для автоматизации различных процессов и повышения

эффективности производства [3. С. 520–522]. Однако развитие новых технологий, как и любое другое явление, не может быть исключительно положительным со всех точек зрения. В дискуссионном поле все чаще фигурирует вопрос угрозы искусственного интеллекта для безопасности государства и защиты прав человека и гражданина [2. С. 75–78]. Рассмотрим негативные последствия внедрения новых технологий более подробно.

Перед тем как непосредственно перейти к рассматриваемой теме необходимо отметить, что Российская Федерация выступает одной из стран, присоединившихся к реализации концепции устойчивого развития. Весной 1996 г. Указом президента РФ был утвержден последовательных переход России к устойчивому развитию.

Технологии развиваются стремительными темпами [4]. В качестве примера, подтверждающего данное положение, можно привести нейросеть. Еще несколько лет назад большая часть граждан не имела представления о данной системе. Сейчас нейросеть может создавать изображения, музыкальные произведения, тексты, которые неотличимы от созданных руками человека. Данный факт действительно вызывает волнения среди специалистов. Так как объекты, сгенерированные посредством искусственного интеллекта, могут выдаваться за «реальные» с целью подрыва авторитета государства на международной арене и возникновению негативных волнений в обществе. Дезинформация, как явление и сейчас присутствует в СМИ, однако по мере расширения возможностей искусственного интеллекта такой показатель может существенно возрасти [7].

Кроме того, с появлением технологий возникло и другое масштабное, но негативное явление – киберпреступность. В соответствии со статистической информацией отечественной компании InfoWatch только за 2022 г. в России утекло более 600 млн записей персональных данных. Кибератаки и акты хищения конфиденциальной информации могут нанести серьезный вред не только отдельным личностям, но и всему государству в целом. С теоретической точки зрения можно предположить, если разработки в сфере искусственного интеллекта продолжатся, и он будет становиться более «самостоятельным», то будет существовать существенная вероятность выхода технологий из-под контроля человека, что может привести к необратимым последствиям.

Нельзя не упомянуть о том, что процесс интеграции новых технологий ведет к оптимизации различных процессов и, как следствие, к сокращению рабочих мест [1]. Соответственно такое последствие внедрения инноваций препятствует осуществлению цели по ликвидации безработицы. Привычные для нас профессии с каждым годом все больше становятся менее востребованными и на их место приходят новые, как правило, непосредственно связанные с информационно-коммуникационными технологиями. Однако не все граждане имеют необходимые компетенции в области технологий. В связи с чем остро стоит вопрос об обучении необходимым навыкам в сфере программирования и технологий различных категорий граждан.

Одним из основных факторов, определяющих успешность реализации той или иной поставленной цели, выступает процесс правового регулирования.

Однако в настоящее время законодательство России и других зарубежных государств не регламентирует вопросы, связанные с интеграцией и использованием технологий, в достаточной мере. Особенно остро стоит вопрос о принятии отдельного кодифицированного акта в полной мере, регулирующего вопросы, связанные с разработкой, внедрением и распространением инновационных технологий [5]. В качестве положительного аспекта представляется возможным отметить разработку Цифрового кодекса Российской Федерации. Данный законодательный акт будет направлен на комплексное устранение правовых лакун в части регулирования новых технологий и цифровых прав. Также на стадии обсуждения находится мера по обязательной маркировке контента, созданного с помощью искусственного интеллекта. Кроме того, необходимо урегулировать деятельность и ответственность самих разработчиков новых технологий. Представляется возможным введение дополнительных мер по обучению населения навыкам в информационном пространстве.

Подведем итоги: концепция устойчивого развития – это путь к обеспечению сбалансированного развития государства и общества во всех сферах. Развитие и внедрение технологий выступает одним из важных критериев для реализации всех целей концепции, но в то же время создает новые вызовы для законодателя. Необходима адаптация права по цифровым реалиям с учетом всех особенностей развития общества на конкретном этапе. Несмотря на то что развитие инновационных технологий в любом случае будет опережать процесс адаптации законодательства, именно право выступает инструментом для эффективного развития общества и государства.

Список литературы

1. Денисова Я. В., Петрова А. С. , Сопин В. Ф. Оптимизация производственного процесса путем внедрения методов бережливого производства // Вестник Воронежского государственного университета инженерных технологий. 2022. Т. 84, № 2(92). С. 315–323.

2. Интересы в механизме публичной власти: проблемы теории и практики: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2023. С. 77–78.

3. Лоос Д. С. Автоматизация технологических процессов как основное направление в повышении производительности труда // Актуальные проблемы авиации и космонавтики: Сборник материалов VI Международной научно-практической конференции, посвященной Дню космонавтики. Красноярск, 13–17 апреля 2020 г. / под общей редакцией Ю. Ю. Логинова. В 3-х томах. Т. 1. Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева», 2020. С. 520–522.

4. Харитонова Ю. С. Правовые средства обеспечения принципа прозрачности искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 337–358. EDN: DXNWHV

5. Хомякова С. С. Информационный кодекс Российской Федерации: необходимость разработки и принятия // Актуальные проблемы права: материалы

VIII Междунар. науч. конф. (г. Казань, декабрь 2019 г.). Казань: Молодой ученый, 2019. С. 13–15.

6. Чепусов А. Г. Цели устойчивого развития в 2020 г. // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2021. Т. 8, № 4. С. 386–394.

7. AI training in school – approaches, results and conclusions / V. V. Tabakova-Komsalova, S. N. Stoyanov, T. A. Glushkova, S. I. Grozdev // Информатизация образования и методика электронного обучения: цифровые технологии в образовании: материалы VI Международной научной конференции: в трех частях, Красноярск, 20–23 сентября 2022 года. Vol. Часть 3. Красноярск: Красноярский государственный педагогический университет им. В. П. Астафьева, 2022. P. 464–468.

А. К. Рябов,
студент
Национальный исследовательский университет
«Высшая школа экономики»,
Санкт-Петербургский филиал

ГРАЖДАНСКО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ МАССОВЫХ МНОГОПОЛЬЗОВАТЕЛЬСКИХ ОНЛАЙН-ИГР В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Развитие индустрии массовых многопользовательских онлайн-игр ставит перед юриспруденцией новые вопросы, касающиеся их гражданско-правового режима. Российское законодательство и судебная практика на данном этапе склонны классифицировать отношения по поводу онлайн-игр как отношения из игр и пари. Указанный подход представляется спорным в современных условиях. В статье рассматриваются существующие в правовой доктрине и практике российские и зарубежные концепции гражданско-правового регулирования различных отношений, возникающих по поводу онлайн-игр. Делается вывод о необходимости совершенствования существующего гражданско-правового регулирования в сфере цифровых развлечений в целях повышения защиты прав и законных интересов субъектов данных отношений.

Ключевые слова: право, цифровые технологии, онлайн-игры, правовое регулирование онлайн-игр, виртуальный мир, виртуальная собственность

CIVIL LAW REGULATION OF MASSIVELY MULTIPLAYER ONLINE GAMES IN THE RUSSIAN FEDERATION

Abstract. The development of the industry of massively multiplayer online games poses new questions for the jurisprudence regarding their civil law regime. Russian legislation and judicial practice, at this stage, tend to classify relations regarding online games as legal relations regulated as games and bets. This approach seems to be controversial in modern conditions. This paper examines and analyzes the existing

Russian and foreign concepts of civil law regulation of various relations arising from online games, both within the framework of doctrine and practice. The author concludes that it is necessary to improve the existing civil law regulation in the field of digital entertainment in order to increase the protection of the rights and legitimate interests of the subjects of these relations.

Keywords: law, digital technologies, online games, legal regulation of online games, virtual world, virtual property

Введение. Технологический прогресс, выражающийся в появлении и крайне активном развитии сети «Интернет», ставит как перед мировой, так и российской юриспруденцией новые вызовы. Причем потребность в приведении существующих отношений в правовую плоскость возникает не только в традиционных областях, наподобие финансового сектора, переходящего в цифровую среду, но и в индустрии развлечений. Вероятно, наиболее ярким примером в данном контексте выступают онлайн-игры.

Существующая судебная практика склонна относить весь массив гражданско-правовых отношений, возникающих в связи с онлайн-играми, к предмету регулирования главы 58 Гражданского кодекса Российской Федерации (далее – ГК РФ), что фактически лишает пользователя возможности эффективно защищать свои интересы в судебном порядке.

В то же время данная сфера притягивает к себе огромный исследовательский интерес, вызванный тем, что массовые многопользовательские онлайн-игры ставят перед юридической наукой ряд острых вопросов, применимых и к другим областям человеческой деятельности. Данные проблемы связаны как с определением правового статуса «виртуальной собственности», присутствующей буквально в каждой онлайн-игре, так и с квалификацией содержания правоотношений, возникающих между различными субъектами по поводу онлайн-игр. При этом остается не решенным вопрос о том, должны ли вообще онлайн-игры и присущие им отношения становится объектом гражданско-правового регулирования и, если да, то насколько глубокой должна быть степень правовой интервенции.

Виртуальное пространство. В качестве первого шага необходимо определить ряд понятий, являющихся ключевыми в рамках данной темы. В первую очередь, к таковым относятся: онлайн-игры, виртуальное пространство и виртуальное имущество. Стоит отметить, что законодательного закрепления в российском праве данные термины не имеют и, как следствие, применяются преимущественно в научной литературе, хоть и встречаются в текстах как нормативных актов [38], так судебных решений [25], однако без раскрытия содержания.

Начать стоит с наиболее абстрактного понятия в данном ряду. В настоящее время с развитием технологий дополненной (AR) или виртуальной реальности (VR) возникает необходимость разграничения данных понятий. Так, согласно М. А. Рожковой, виртуальная реальность представляет собой: «иной, несуществующий мир» с собственными субъектами и объектами, «реальность» которого передается пользователю через ощущения – зрение, слух, обоняние, осязание и др.» [32], что, как показано ниже, позволяет выделить виртуальную реальность

в качестве частного случая виртуального мира, отличающегося более высокой степенью моделирования.

В. В. Архипов отмечает, что применимо к информационным технологиям виртуальный мир означает «моделируемую компьютерными средствами относительно постоянную среду, предназначенную для взаимодействия между пользователями посредством цифровых образов» [11]. Исследователь выделяет следующие характеристики виртуального мира: относительное постоянство среды, искусственную сущность, моделируемую посредством компьютерных технологий, и создание для цели взаимодействия между пользователями, посредством цифровых образов. Ю. М. Батурин определяет виртуальный мир как «комплекс общественных отношений, формирующихся в процессе выхода пользователя в сеть Интернет или локальные сети, создающиеся по поводу данных, обработка которых осуществляется посредством ЭВМ» [31]. Данное определение является крайне широким, целиком и полностью поглощающим все общественные отношения, возникающие в связи с деятельностью субъекта в сети Интернет, что, в свою очередь, не позволяет с достаточной степенью точности отразить специфику объекта.

Иную характеристику приводит Е. Ю. Мартьянова, не создавая четкой дефиниции, она указывает на следующие особенности виртуальной реальности: неполное отражение реального мира, производный характер (в значении связанности с миром реальным), «уникальное ощущение дали, как бы близко предмет не был» (прим.: автором используется одна из характеристик «ауры» в терминологии В. Беньямина, как недоступность или невозможность присвоения, или утилитарного использования созерцаемого объекта, несмотря на близость в пространстве), наличие собственных атрибутов, отличных от реального мира, таких как время и пространство [18]. Таким образом, Е. Ю. Мартьянова акцентирует внимание именно на отражении, хоть и с особенностями, реального мира в мире виртуальном, что концептуально позволяет переносить внутриигровые отношения в правовую плоскость.

В зарубежной научной литературе в отношении данного понятия выработался схожий подход. Так, Орин Керр указывает на такие свойства виртуальных миров, как искусственная моделлируемость и в то же время неразрывная связь с реальным миром [5]. Кристофер Кифрино же дает определение виртуального мира как онлайн среды, включающей социальное взаимодействие посредством графического интерфейса [2].

Также искусственную моделируемость посредством компьютерных технологий и широкую возможность для социального взаимодействия пользователей посредством «аватаров» выделяют основоположники правового исследования виртуальных миров и онлайн-игр Бенджамин Дюранске [16] и Грег Ластовка и др. [6], причем первый указывает в качестве признаков также наличие виртуальной экономической системы и возможность создания пользовательского контента, доступного для использования в рамках виртуального мира [3].

Таким образом, хоть единого и общепринятого определения виртуального мира в юридической науке не существует, можно выделить ряд свойств,

определяющих содержание данного понятия. Представляется, что применительно к данной работе, будет наиболее разумным использовать дефиницию, предложенную В. В. Архиповым как, с одной стороны, достаточно полно отражающую содержание данного понятия, с другой же, позволяющей исключить чрезмерно широкое толкование, ввиду выделяемых различными исследователями особенностей виртуального мира, характерных непосредственно для онлайн-игр, но отсутствующих в иных отношениях, определяемых как виртуальные.

Онлайн-игры. Понятие «онлайн-игры» также не имеет нормативного закрепления, по крайней мере в рамках российского законодательства. Стоит отметить, что в статье речь идет лишь о многопользовательских онлайн-играх, преимущественно ролевых, характеризующихся активным социальным взаимодействием игроков, обуславливающим возникновение в процессе игры отношений, имеющих природу, доступную и, согласно некоторым концепциям, желательную для правового регулирования.

Также онлайн-игры тесно связаны с видеоиграми, представляя, несомненно, их разновидность. Стоит отметить, что понятие «видеоигра» отсутствует в российском законодательстве, однако данный объект интеллектуальной собственности определяется в рамках существующей судебной практики как программа для ЭВМ [21, 27]. Данная позиция прослеживается и в подзаконных актах, к примеру, в письме Федеральной налоговой службы от 23 января 2017 г. № СД-4-3/988@ «О рассмотрении обращения», согласно которому: «Игра является программой для ЭВМ и представляет собой совокупность данных, команд и порождаемых ею аудиовизуальных отображений (далее – данные и команды), активируемых последовательно для получения Лицензиатом определенного результата, предусмотренного сценарием Игры…» [23]. Тем не менее данный подход критикуется целым рядом авторов ввиду включения в видеоигру значительного количества иных объектов интеллектуальной собственности (аудиовизуальных произведений, сценария, изображений и т. д.), обладающих самостоятельной охраноспособностью, что указывает на правовую природу видеоигры как сложного объекта интеллектуальной собственности [17], из чего следует вывод о том, что на данный объект распространяются не только общие положения авторского права, но и специальные, предусмотренные ст. 1240 ГК РФ. Сторонники данной концепции склонны рассматривать видеоигру как мультимедийный продукт, что хоть, с позиции автора, несомненно, ближе к его правовой природе, вскрывает, однако, пробел в правовом регулировании, требующий заполнения.

При этом учитывая стремительное совершенствование и усложнение структуры видеоигр, некоторые исследователи, в частности, М. А. Рожкова, приходят к выводу о том, что данный пробел не может восполняться за счет положений гражданского кодекса о программах для ЭВМ, ввиду того, что «программа, хотя и является основой для создания видеоигры с технической точки зрения, в правовом ключе представляет собой лишь одну из составляющих видеоигры, что не позволяет признавать за программой приоритет перед другими элементами этого сложного объекта» [34].

А. И. Савельев утверждает, что онлайн-игры представляют собой разновидность видеоигр (видеоигры исследователь определяет как сложный объект,

включающий в себя программу для ЭВМ [36]), в которых пользователь посредством «аватара» взаимодействует как с компьютерными персонажами, так и иными пользователями, при этом данные отношения могут иметь экономический характер в отношении оборота внутриигрового имущества и внутриигровой валюты.

В зарубежной научной литературе выделяются два качества многопользовательских онлайн-игр, отличающие их от однопользовательских видеоигр: динамичность и стабильность. Динамичность заключается в постоянных изменениях «виртуального мира» онлайн-игры, а стабильность – в его автономности от каждого отдельного пользователя [7]. Кроме того, отношения игроков в рамках онлайн-игры могут моделировать взаимоотношения, характерные для реального мира, что наполняет действия игроков экономическим и, потенциально, правовым содержанием (к примеру, игрок «зарабатывает» виртуальную валюту или ценные внутриигровые предметы с целью продажи их другим игрокам уже за реальные деньги) [16].

Таким образом, онлайн-игры возможно определить как разновидность видеоигр, использующих постоянное соединение с сетью Интернет и функционирующих независимо от воли каждого отдельного игрока, осуществляющего внутриигровое взаимодействие посредством аватара с другими игроками, в рамках которого возникают взаимоотношения, носящие экономический характер, при этом данные отношения могут возникать как с иными пользователями, так и с издателем игры. Применительно же к российской правовой системе представляется обоснованным рассматривать видеоигры в целом и онлайн-игры в частности как мультимедийные продукты, в смысле пункта 1 статьи 1240 ГК РФ, ввиду сложной природы данных объектов. Безусловно, данный подход хоть и широко поддерживается в юридическом сообществе, о чем сказано выше, тем не менее противоречит устоявшейся судебной практике. Однако представляется, что в условиях отсутствия проработки законодателем вопросов, связанных с гражданско-правовым режимом онлайн-игр в целом, указанный взгляд на проблему представляется автору обоснованным и требующим в будущем неизбежного разрешения путем внесения соответствующих положений в часть 4 Гражданского кодекса Российской Федерации.

В этой связи логично было бы с целью исключения разночтений как в отношении видеоигр, так и иных мультимедийных продуктов закрепить в Гражданском кодексе определение данного понятия, включающее открытый перечень объектов интеллектуальной собственности, обладающих указанными характеристиками.

Виртуальная собственность. Еще одним понятием, крайне важным в рамках данной проблематики является «виртуальная собственность». Примеры ее регулирования можно обнаружить в иностранном законодательстве. Так, в Республике Китай, согласно Постановлению Министерства юстиции от 23.11.2011, в отношении виртуальной собственности распространены вещные права [14], при этом данный объект считается электромагнитной записью, размещенной на сервере, и рассматривается законодателем как движимая вещь [9], что, хоть и позволило дать «собственникам» определенную защиту от преступных посягательств (в настоящее время Тайваньская правоприменительная практика насчитывает сотни дел,

касающихся, преимущественно, краж виртуальной собственности [1]), но вряд ли точно отразило правовую природу виртуальной собственности. Сходные по содержанию правовые акты, существуют также в Республике Корея, однако и там законодатель ограничился лишь признанием существования права собственности в отношении виртуального имущества [37]. Часть третья Payment Services Act, принятого 20.02.2019 в Сингапуре, содержит определение непосредственно внутриигровых активов (in-game asset), представляющих собой любую цифровую репрезентацию стоимости (any digital representation of value),

А) купленной либо иным способом приобретенной лицом (игроком);

Б) не деноминированной ни в какой валюте;

В) представляющей собой часть онлайн-игры;

Г) используемой игроком для оплаты или обмена на виртуальные услуги или объекты в онлайн-игре.

При этом внутриигровые активы, согласно данному закону, считаются «цифровым платежным токеном ограниченного назначения» (limited purpose digital payment token), который, в свою очередь, не может быть возвращен издателю или продан за деньги и может использоваться только для оплаты или обмена на виртуальные объекты или виртуальные услуги в рамках онлайн-игры или в рамках отношений, являющихся ее частью либо находящихся в связи с ней [8].

Таким образом, Сингапур является на данный момент единственной страной, законодательно закрепившей данное понятие и, более того, установившей специфический правовой режим.

В рамках данной статьи понятие «виртуальное имущество» равнозначно «игровому имуществу». Стоит заметить, что границы данных понятий трактуются различными исследователями неоднородно. Так, В. В. Архипов дает узкое определение данного термина как «объектов, которыми игроки посредством своих персонажей могут владеть, пользоваться и распоряжаться в виртуальном пространстве» [10].

М. И. Рожкова же, напротив, определяет виртуальное имущество как «нематериальные объекты, которые имеют экономическую ценность, но полезны или могут быть использованы исключительно в виртуальном пространстве», причем состав виртуального имущества таков:

1) игровое имущество;

2) криптовалюты;

3) виртуальные токены;

4) доменные имена;

5) виртуальное имущество в социальных сетях, включающее в себя как аккаунты пользователей, так и различные объекты, наподобие стикеров и поздравительных картинок [35]. Н. В. Гаразовская не соглашается с М. И. Рожковой в отношении релевантности данного определения, ввиду отсутствия законодательного закрепления понятия «виртуальное пространство», что, учитывая вышеописанное, обоснованно. Исследовательница указывает на следующие признаки «игрового имущества» как компоненты имущества виртуального:

а) игровое имущество должно быть связано с онлайн-играми;

б) игровое имущество не может существовать помимо них;

в) игровое имущество выступает нематериальным объектом, по поводу которого возникают отношения внутри онлайн-игры и взаимосвязанные с ними отношения.

На данной основе выводится следующее определение игрового имущества: «нематериальные объекты, которыми игроки посредством своих персонажей могут владеть, пользоваться и распоряжаться в MMORPG, по поводу которых возникают отношения в компьютерной игре и взаимосвязанные с ними отношения. К игровому имуществу относятся игровые аккаунты, персонажи и все те объекты, которые были куплены или иным образом приобретены в MMORPG [13]». С точки зрения автора, данное определение является достаточно точным, но упускающим из поля зрения то обстоятельство, что оборот данных объектов, вне зависимости от условий пользовательского соглашения (о чем ниже), может происходить и вне самих онлайн-игр, на сторонних интернет-площадках [19], при этом данные отношения будут связаны с игрой весьма опосредованно.

При этом правовая природа данных объектов вызывает достаточно большое количество споров. Данное обстоятельство, в совокупности с тем, что внутриигровые объекты тем или иным образом фигурируют во всем массиве отношений, связанных с гражданско-правовым содержанием онлайн-игр, вновь приводят к вопросу о необходимости соответствующей легальной дефиниции данного термина.

Таким образом, все основные понятия, применяемые в рамках данной статьи, остаются неопределенными в нормативно-правовых актах. Причем данная ситуация характерна не только для Российской Федерации, но и для большинства стран в мире.

Тем не менее как российская, так и зарубежная судебная практика уже не первое десятилетие полнится делами, связанными с отношениями, вытекающими из онлайн-игр, в пределах виртуальных миров которых происходит оборот виртуальной собственности. Данное обстоятельство указывает на то, что правовое регулирование в рамках данной сферы необходимо, пусть даже в упрощенной форме, по примеру Кореи и Тайваня.

Существующие подходы к регулированию отношений, возникающих в связи с онлайн-играми. Однозначного ответа на вопрос о границе действия правовых норм в отношениях, порождаемых онлайн-играми, нет. Тем не менее за годы, прошедшие с постановки вопроса о соотношении права и цифровых виртуальных миров, выработалось несколько подходов. Как правило, расхождения касаются оборота виртуальной собственности, в данном случае игрового имущества. Наличие правового содержания в отношениях, касающихся, к примеру, заключения лицензионного соглашения между игроком и правообладателем, для судебной практики очевидно. Но стоит лишь возникнуть спору о прекращении доступа к игровому аккаунту, который, в свою очередь, может иметь весьма немалую цену за счет приобретенных пользователем виртуальных объектов, как данные отношения оказываются в некой «серой зоне», из которой есть ряд выходов.

Отрицание правового содержания в отношениях, возникающих из онлайн-игр. Первый заключается в отрицании правового содержания у внутриигровых

отношений. Данного подхода, безусловно, придерживаются российские суды, стабильно классифицирующие отношения, вытекающие из онлайн-игр как отношения из игр и пари, в смысле ст. 1062 Гражданского кодекса Российской Федерации, что закрывает доступ к судебной защите для сторон данных отношений, за исключением предусмотренных законом случаев. Несмотря на то, что идея внеправового содержания игр является классической для отечественной (и не только) юриспруденции, представляется, что онлайн-игра имеет ряд существенных отличий от игр и пари, в смысле ст. 1062 ГК РФ и тем более азартных игр, определяемых пунктом 1 статьи 4 Федерального закона от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» как «основанное на риске соглашение о выигрыше, заключенное двумя или несколькими участниками такого соглашения между собой либо с организатором азартной игры по правилам, установленным организатором азартной игры» [39].

Тем не менее, основываясь на Определении Конституционного суда РФ от 26 мая 2011 г. № 684-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Шевченко Евгения Игоревича на нарушение его конституционных прав статьями 1062 и 1063 Гражданского кодекса Российской Федерации» [22], в котором Конституционный суд признал понятие «игра» формально определенным, можно сделать вывод о том, что с точки зрения действующего законодательства никаких различий между данными явлениями попросту нет. Ярким примером такого подхода является достаточно широко известное в рамках исследуемой проблематики определение № 11–115/2009 11-43/2011 от 1 июня 2011 г. по делу № 11-115/2009 Басманного районного суда города Москвы [20]. Основанием для иска против ООО «Иннова Системс» послужила блокировка учетной записи истца, приведшая к тому, что пользователь, приобретший за определенную сумму виртуальный предмет на срок 28 дней, пользовался им на 3 дня меньше, кроме того, истец приобретал платную подписку на игровой сервис, срок которой истекал лишь через 7 дней после блокировки. Блокировка аккаунта произошла, исходя из условий пользовательского соглашения, таким образом, суд пришел к выводу о том, что данные правоотношения относятся к организации игрового процесса, а значит должны регулироваться нормами главы 58 ГК РФ, что исключает возможность их судебной защиты. Указанная позиция прослеживается почти во всех (что будет раскрыто ниже) делах, рассматриваемых российскими судами [29, 30]. Выбор данного подхода судами объясним: с одной стороны, отсутствие правового вмешательства разгружает судебную систему, ввиду потенциально огромного количества споров подобного рода, как, например, происходило в Южной Корее [14]. С другой, учитывая отсутствие законодательного разграничения между многопользовательскими онлайн-играми и азартными играми, суды следуют традиционному для континентальной правовой семьи подходу, не допускающему вмешательства права в данные отношения [40].

Тем не менее данный подход подвергается обоснованной критике: соглашения, предусмотренные ст. 1062 ГК, носят алеаторный характер, что никаким образом не связано с онлайн-играми. К примеру, покупая виртуальный предмет

в ММО, пользователь имеет четкое представление о том, что он получит, равно как и оператор онлайн-игры, выставляющий данный предмет на продажу. Отсутствует как таковое и соглашение о выигрыше, победа или поражение могут являться составными частями действий игрока, но никак не конечным результатом или конечной целью его деятельности.

Таким образом, данный подход, несмотря на его позитивное восприятие, российской судебной системой не может считаться верным. Так как он, с одной стороны, не отражает реально существующих отношений в рамках онлайн-игр, с другой же, приводит к дискриминации пользователей, несущих вполне реальные убытки вследствие виртуальных правоотношений, но при этом лишающихся права на судебную защиту.

Всецелое распространение норм права на отношения, возникающие из онлайн-игр. Полярной по отношению к вышеописанному подходу является идея о необходимости распространения действия норм права на все внутриигровые отношения. Не удивительно, что данный подход крайне широко критикуется в юридической литературе.

В данном случае будет уместным привести уже ставший хрестоматийным пример из некогда популярной MMORPG «Ultima Online», игровой процесс которой допускает кражу игрового имущества одного игрока другим, причем жертва кражи теряет предмет без возможности восстановления. Учитывая наличие в игре экономической компоненты, позволяющей через ряд сделок продать предмет за вполне реальные деньги, можно говорить об экономическом ущербе. Однако данные действия предусмотрены правилами игры, и распространение правовых норм на данные отношения выглядят совершенно излишними, представляется, что средний игрок ни при каких обстоятельствах не воспримет «хищение», пусть даже купленного за значительную для него сумму виртуального предмета из виртуального сундука в виртуальном доме, находящегося в не менее виртуальном мире, как покушение на его реальное право собственности. Вместе с тем в реальном мире данное деяние образовывало бы состав, предусмотренный ч. 3 ст. 158 УК РФ, стоит отметить, что подобные конструкции в подавляющем большинстве случаев носят лишь умозрительный характер [12].

Тем не менее в российской судебной практике встречается как минимум один случай, в котором суд дал правовую квалификацию сугубо внутриигровой ситуации: в решении мирового судьи судебного участка № 48 Черемушкинского судебного района от 18 июня 2012 г. по делу № 02-0095/48/2012 [28] судья указал следующее: «Суд полагает, что истец денежных средств «Золото» для приобретения CET+15 не вносил, данный CET+15 им был найден и подобран на игровой карте. Впоследствии игроком, потерявшим CET+15, была предъявлена соответствующая претензия, и администрацией игры принято решение об изъятии у истца CET+15 и возвращении его потерявшему игроку. В силу ст. 227 ГК РФ, нашедший потерянную вещь обязан немедленно уведомить об этом лицо, потерявшее ее, или собственника вещи или кого-либо другого из известных ему лиц, имеющих право получить ее, и возвратить найденную вещь этому лицу, в связи с чем суд приходит к выводу об отказе истцу в удовлетворении его исковых требований в данной

части», впрочем, следующие инстанции отнесли данные правоотношения к предмету главы 58 ГК РФ [24]. В целом, можно констатировать, что в юридической литературе по данному вопросу указанный подход встречает достаточно резкую критику [33]. Причина указанной неприязни коренится в том, что объектом «интервенции» права является игра, в рамках которой, как указывал в своей работе Б. Дюранске, и предполагается, что игроки будут совершать действия, не воспроизведенные ими в реальном мире, именно в этом заключается сама суть игры [3].

Учитывая вышеописанное, данный подход представляется крайне сомнительным как с точки зрения судов, так и самих игроков, рискующих, к примеру, стать субъектами деликтной ответственности за действия, совершенные внутри игры, при том, что их поведение не предполагало наличия какого-либо отражения в реальном мире. Однако это вовсе не значит, что виртуальные правоотношения все же должны быть выведены из правового поля.

Концепция «магического круга». Для проведения демаркационной линии между отношениями, не имеющими правового содержания и подлежащими правовой охране, была выдвинута идея теста «Магического круга» (The Magic circle test) [3, p 75]. Данное понятие впервые появилось в труде Й. Хейзинги «Человек играющий» («Homo ludens»), и означает отделение реального мира от виртуального своеобразной границей – тем самым «магическим кругом». Согласно Б. Дюранске, разделение проходит в зависимости от того, осознает ли разумно пользователь то обстоятельство, что его действия в виртуальном пространстве будут иметь выражение в реальном мире. Так, описанная выше «кража» предмета не будет являться предметом правового регулирования, но несанкционированное получение доступа к игровому аккаунту с целью, к примеру, передачи игрового имущества на аккаунт правонарушителя с целью последующей перепродажи будут преступны.

Однако данная модель «магического круга» также подвергается критике. В качестве примера можно привести работу А. Т. Фэйрфилда «The Magic circle», согласно которой любые действия игроков в виртуальном мире, если они имеют правовое содержание (например, купля-продажа игрового имущества), порождают вполне реальные последствия, следовательно, должны признаваться таковыми. Отличие от идеи о тотальном признании всех внутриигровых отношений реальными заключается в том, что применение права все же должно базироваться на согласии сторон. При этом исследователь имеет в виду не только пользовательское соглашение (EULA), подразумевая то, что все действия игрока в рамках правил не порождают правовых последствий, но и правила, создаваемые самим сообществом как способ определить границы действия права [4].

Представляется, что данный подход верен и реализуем как таковой лишь отчасти, принятие пользовательского соглашения действительно представляется простым и понятным способом выразить согласие игрока и очертить границы дозволенного (не говоря уже о том, что зачастую нарушение данных правил ведет к исключению игрока из виртуального мира, вследствие блокировки доступа к аккаунту), но, по крайней мере, в условиях современной российской судебной системы, восприятие судом норм какого-либо игрового сообщества как квазиправовых маловероятно и даже вредно, ввиду их принципиальной неопределенности.

Представляется, что теория «магического круга» в ее изначальном варианте предлагает наиболее адекватное решение существующей проблемы ввиду того, что, с одной стороны, обеспечивается защита интересов игроков, в том числе имеющих достаточно явный экономический характер, не позволяющий отнести возникающие отношения исключительно к игровому процессу, не подлежащему регулированию, в силу описанной выше природы игры как таковой. С другой же, применение указанного теста позволяет избегать как излишней интервенции права в конвенционально неправовые отношения, так и неизбежной загрузки судов потоком дел, разрешение которых требует чрезмерных трудозатрат со стороны судебной системы, учитывая нетривиальность подходов, необходимых для разрешения споров, при достаточно ограниченной сфере их применения. Возможно, в странах англо-американской правовой семьи применение модифицированного теста «магического круга», предложенного А. Т. Фэйрфилдом, учитывая ее прецедентный характер, все же допустимо, но, применительно как ко всей континентальной правовой системе в целом, так и к российской в частности, данный подход выглядит избыточным и потенциально неэффективным.

Заключение. Подводя итог, можно сказать, на данный момент законодательное регулирование отношений в сфере цифровых развлечений является крайне фрагментированным, тем не менее сложившаяся ситуация позволяет при будущей правовой квалификации выбрать подходы, наиболее точно отражающие реальную картину и позволяющие обеспечить наибольшую защиту интересов всех сторон соответствующих правоотношений.

Представляется, что при определении возможности применения гражданско-правового регулирования стоит опираться на концепцию «магического круга». Таким образом, регулированию будут подлежать лишь отношения, имеющие выражение в реальном мире. За некоторыми исключениями данные отношения представляют собой взаимодействие между игроком и оператором онлайн-игры, возникающее на основе лицензионного соглашения. Отношения же между игроками в рамках отдельно взятой игры представляют собой часть игрового процесса, и, следовательно, вмешательство «извне» в большей части случаев будет противно целям, для которых пользователи и играют в игры. Применение расширенной концепции «магического круга» А. Т. Фэйрфилда, предлагавшего учитывать при правовом регулировании внутриигровых отношений обычаи, сложившиеся внутри самого игрового сообщества, хоть и является более «демократичным», ввиду лучшего отражения интересов игроков, но вряд ли может быть воспринято судебной системой, кроме того, представляется, что признание споров между игроками основанием для судебного иска создаст нагрузку на суды в размере совершенно не пропорциональном защищаемому интересу. Таким образом, существующая на данный момент квалификация подавляющего большинства отношений по поводу онлайн-игр как отношений из игр и пари, в смысле главы 58 Гражданского кодекса Российской Федерации, должна применяться лишь к отношениям между игроками, предусмотренным игровым процессом и не связанным с оборотом внутриигровых предметов, имеющих экономическую ценность в реальном мире.

Обобщая вышесказанное, онлайн-игры представляют собой пример предмета, глубоко проникшего в жизнь миллионов людей, вызывающего огромное количество спорных ситуаций, но при этом по большей части находящегося вне правового поля. Неудивительно, что данное явление привлекло столь широкий интерес исследователей, обращенный к различным его аспектам, что дает огромный теоретический материал для конструирования моделей правового регулирования. Тем не менее, представляется, что без должного нормативно-правового отражения или по крайней мере формирования непротиворечивой судебной практики гражданско-правовые отношения по поводу онлайн-игр в рамках российской юриспруденции останутся в «серой зоне», создавая пространство и возможности для различного рода злоупотреблений.

Список литературы

1. Bekker L. Defining virtual property in terms of the constitutional property clause. URL: http://repository.nwu.ac.za/bitstream/handle/10394/11009/Bekker_L.pdf?sequence=1&isAllowed=y

2. Cifrino C. J. Virtual property, virtual rights: Why contract law, not property law, must be the governing paradigm in the law of virtual worlds – BCL Rev., 2014 // HeinOnline. URL: https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=3354&context=bclr

3. Duranske B. T. Virtual Law. Navigating the Legal Landscape of Virtual Worlds. Chicago, Illinois, 2008.

4. Joshua A. T. Fairfield The Magic Circle (November 19, 2008). Vanderbilt Journal of Entertainment and Technology Law, 2009, Washington & Lee Legal Studies Paper No. 2008-45,. URL: https://ssrn.com/abstract=1304234

5. Kerr O. S. Criminal law in virtual worlds – U. Chi. Legal F., 2008 – HeinOnline. URL: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1432&context=uclf

6. Lastowka, Greg and Hunter, Dan, The Laws of the Virtual Worlds. California Law Review. 2004. Vol. 92, No. 1. URL: https://ssrn.com/abstract=402860 or http://dx.doi.org/10.2139/ssrn.402860

7. Lipson A. S., Brain R. D. Computer and Video Game Law: Cases, Statutes, Forms, Problems & Materials. Carolina Academic Press, 2009.

8. Payment services act 2019. URL: https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220

9. Sarah Xuan Virtual Property in Greater China. URL: https://www.hg.org/legal-articles/virtual-property-in-greater-china-5538

10. Архипов В. В. Виртуальная собственность: системные правовые проблемы в контексте развития индустрии компьютерных игр // Закон. 2014. № 9. С. 70.

11. Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Правоведение. 2013. № 2(307). URL: https://cyberleninka.ru/article/n/virtualnoe-pravo-osnovnye-problemy-novogo-napravleniya-yuridicheskih-issledovaniy

12. Архипов В. В. Компьютерные игры, «магический круг» и смысловые пределы права // Международный журнал исследований культуры. 2019. № 1(34). URL: https://cyberleninka.ru/article/n/kompyuternye-igry-magicheskiy-krug-i-smyslovye-predely-prava

13. Гаразовская Н. В. Виртуальное имущество в играх: перспективы правового регулирования // E-Scio. 2020. № 4(43). URL: https://cyberleninka.ru/article/n/virtualnoe-imuschestvo-v-igrah-perspektivy-pravovogo-regulirovaniya

14. Горохова, О. Н. «игровое имущество» как разновидность «виртуального имущества» // E-commerce и взаимосвязанные области (правовое регулирование): сборник статей / под ред. М. А. Рожковой. М.: Статут, 2019. С. 378–392.

15. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // Российская газета. 2006. 22 декабря.

16. Дюранске Бенджамин Т., Кейн Шон Ф. Виртуальные миры, реальные проблемы // Правоведение. 2013. № 2 (307). URL: https://cyberleninka.ru/article/n/virtualnye-miry-realnye-problemy

17. Ивашов, В. С. Право виртуальных миров: проблемы определения правовой природы внутри игровых объектов и применения законодательства РФ к правоотношениям с их участием // Вестник молодых ученых и специалистов Самарского государственного университета. 2016. № 2(9). С. 73–77.

18. Мартьянова Е. Ю. Договоры, опосредующие использование объектов онлайн-игр // Право цифровой экономики. 2020 (16): Ежегодник-антология / под ред. М. А. Рожковой. М.: Статут, 2020. С. 164–184.

19. Механизм и объемы оборота внутриигровых предметов иллюстрирует, например, данный материал. Неизвестный рынок. Как торговля внутриигровыми предметами стала сферой с многомиллионным оборотом. URL: https://habr.com/ru/company/wirex/blog/400719

20. Определение Басманного районного суда города Москвы № 11-115/2009 11-43/2011 от 1 июня 2011 г. по делу № 11-115/2009 URL: //sudact.ru/regular/doc/64Gc17ps4Hgx

21. Определение Высшего Арбитражного суда Российской Федерации от 21 марта 2011 г. № ВАС-2706/11 по делу № А40-41186/10-143-352 // СПС «КонсультантПлюс».

22. Определение Конституционного Суда РФ от 26 мая 2011 г. № 684-О-О «Об отказе в принятии к рассмотрению жалобы гражданина Шевченко Евгения Игоревича на нарушение его конституционных прав статьями 1062 и 1063 Гражданского кодекса Российской Федерации» // СПС «Гарант».

23. Письмо Федеральной налоговой службы от 23 января 2017 г. № СД-4-3/988@ «О рассмотрении обращения»// СПС «КонсультантПлюс».

24. Постановление Президиума Московского городского суда по делу № 44г-45 от 24.05.2013. URL: https://mos-gorsud.ru/mgs/services/cases/presidium-civil/details/c5ae3ecd-bd64-4b41-bb5a-f123e8801c18?participants=%D0%9F%D1%83%D1%82%D0%B8%D0%BB%D0%BE%D0%B2+%D0%98.%D0%90

25. Постановление ФАС Западно-Сибирского округа от 25.05.2012 по делу № А03-10143/2011 // СПС «Консультант Плюс».

26. Приказ Росстата от 30.07.2021 № 459 «Об утверждении форм федерального статистического наблюдения для организации федерального статистического наблюдения за уровнем жизни и обследованиями домашних хозяйств» // СПС «Консультант Плюс».

27. Решение Арбитражного суд Московской области от 23 июня 2011 года по делу № А41-9246/2011 // СПС «КонсультантПлюс».

28. Решение мирового судьи судебного участка № 48 Черемушкинского судебного района от 18 июня 2012 г. по делу № 02-0095/48/2012 URL: //sudact.ru/magistrate/doc/4OobUeH4PW5a

29. Решение Невского районного суда г. Санкт-Петербург № 2-1008/2017 2-1008/2017(2-8898/2016;)~М-9977/2016 2-8898/2016 М-9977/2016 от 28 марта 2017 г. по делу № 2-1008/2017. URL: //sudact.ru/regular/doc/EzyPTMaFVOdt

30. Решение Петродворцового районного суда г. Санкт-Петербург № 2-989/2016 2-989/2017 2-989/2017~М-288/2017 М-288/2017 от 25 сентября 2017 г. по делу № 2-989/2016. URL: //sudact.ru/regular/doc/ZXOff4CokLZd

31. Решетов К. Ю., Николаев М. А. Правовой статус виртуальных объектов в России // Вестник НИБ. 2019. № 37. URL: https://cyberleninka.ru/article/n/pravovoy-status-virtualnyh-obektov-v-rossii

32. Рожкова М. А. Виртуальная реальность и Метавселенная: предмет правового исследования // Virtual reality and Metaverse: subject of legal research // Закон.ру. 2022. 12 января URL: https://zakon.ru/blog/2022/1/12/virtualnaya_realnost_i_metavselennaya_predmet_pravovogo_issledovaniya

33. Рожкова М. А. О применении ст. 1062 ГК РФ к отношениям по поводу многопользовательских онлайн-игр // Хозяйство и право. 2021. № 1. С. 99–108.

34. Рожкова М. А. Современная компьютерная игра – это не программа для ЭВМ // A modern computer game is not a computer program // Закон.ру. 2021. 15 ноября. URL: https://zakon.ru/blog/2021/11/15/sovremennaya_kompyuternaya_igra__eto_ne_programma problemy

35. Рожкова М. А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // Закон.ру. 2018. 13 июня. URL: https://zakon.ru/blog/2018/06/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym

36. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. М.: Статут, 2014.

37. Смирнова, Т. С. Игровые объекты MMORPG как вещи и объекты гражданских прав // Государство и право: теория и практика: материалы VI Междунар. науч. конф. (г. Санкт-Петербург, апрель 2020 г.). Санкт-Петербург: Свое издательство, 2020. С. 8–16. URL: https://moluch.ru/conf/law/archive/366/15757

38. Федеральный закон от 08.12.2020 № 385-ФЗ «О федеральном бюджете на 2021 год и на плановый период 2022 и 2023 годов» // Российская газета. 2020. 11 декабря.

39. Федеральный закон от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» // Российская газета. 2006. 31 декабря.

40. Федотов А. Г. Игры и пари в гражданском праве // Вестник гражданского права. 2011. Т. 11, № 2 // СПС «КонсультантПлюс».

Э. Р. Сабирзянова,
студент,
Казанский федеральный университет

К ВОПРОСУ О ПОНЯТИИ И КЛАССИФИКАЦИИ КИБЕРПРЕСТУПЛЕНИЙ КАК УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Современный этап социально-экономического развития характеризуется информатизацией всех сфер общественной жизни, повышением роли информации, информационных технологий и ресурсов. Активное развитие компьютерных и информационных технологий привело к зарождению новых видов киберпреступлений преступлений, а также их качественному изменению. Рассматриваются подходы к определению понятий «киберпреступление» и «преступление в сфере компьютерной информации». Делается попытка дать определение понятию «киберпреступлние». Анализируются виды киберпреступлений. Определяется влияние киберпреступлений на экономическую безопасность Российской Федерации.

Ключевые слова: киберпреступление, компьютерное преступление, преступление в сфере компьютерной информации, угроза экономической безопасности

TO THE QUESTION OF THE CONCEPT AND CLASSIFICATION OF CYBERCRIMES AS A THREAT TO ECONOMIC SAFETY OF THE RUSSIAN FEDERATION

Abstract. The modern stage of socio-economic development is characterized by informatization of all spheres of public life, an increase in the role of information, information technologies and resources. The active development of computer and information technologies led to the emergence of new types of cybercrime crimes, as well as their qualitative change. The article examines approaches to defining the concepts of “cybercrime” and “crime in the field of computer information.” An attempt is being made to define the concept of “cybercrime,” the types of cybercrime are being analyzed. The impact of cybercrimes on the economic safety of the Russian Federation is determined.

Keywords: cybercrime, computer crime, computer information crime, economic safety threat

В современных реалиях прогрессивной тенденцией развития общества являются внедрение и использование компьютерных технологий. Их расширенное применение приходится на различные области: экономику, социальную сферу, оборону, управление и т. д. Таким образом, процесс цифровизации ускоряет и упрощает многие процессы в современном обществе, однако помимо позитивных сторон этого процесса имеются и негативные. Стремительное развитие электронной коммерции вызвал повышенный интерес со стороны представителей криминальной среды. В руки криминальных структур все чаще начинает попадать

информация по личным данным физических и юридических лиц, кредитных организаций, нанося при этом значительный ущерб экономике государства и его экономической безопасности.

Под киберпреступлениями в общем виде следует понимать любые преступления, связанные с неправомерным использованием компьютера, компьютерной информации.

В юридической литературе ведутся активные дискуссии о соотношении понятий «киберпреступление», «компьютерное преступление», «преступление в сфере компьютерной информации» и т. д. Многие авторы используют термины «киберпреступления» и «компьютерные преступления» в качестве синонимов.

Так, Т. Л. Тропина считает, что киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству [5].

Киберпреступность, на наш взгляд, – это преступная деятельность с использованием киберпространства в незаконных целях. Большинство киберпреступлений происходит на основе кибератак в сети Интернет и других сетях связи для получения финансовой выгоды.

Проанализировав мнения различных ученых, мы пришли к выводы, что существуют широкий и узкий подходы к пониманию киберпреступлений. По широкому подходу киберпреступление – это любое преступление, совершаемое с использованием компьютерных технологий или сети Интернет: кража личных данных, мошенничество, нарушение авторских прав, хакерство и др. Например, достаточно актуальным способом совершения преступления, предусмотренного ст. 135 Уголовного кодекса Российской Федерации (далее – УК РФ) [1] «Развратные действия», является распространение интимных фотографий в социальных сетях с целью развращения другого лица и получения собственной выгоды. По узкому подходу киберпреступление – это только те преступления, которые совершаются исключительно в сфере информационных технологий, такие как хакерство, вирусы и др. При этом преступления, совершаемые с использованием компьютерных технологий в других сферах жизни (например, финансовые мошенничества через Интернет), не рассматриваются как киберпреступления. К данному виду можно отнести все составы преступлений, которые закреплены в главе 28 УК РФ.

На наш взгляд, первый подход является более предпочтительным. При этом понятие «киберпреступления» является более широким, чем понятие «преступления в сфере компьютерной информации», используемое в главе 28 УК РФ.

Т. А. Далгалы отмечает, что «отнюдь не все деяния, под которыми в литературе подразумевают преступления в киберпространстве, входят в понятие «преступления в сфере компьютерной информации». Ими признаются лишь те деяния, что посягают на общественные отношения, касающиеся безопасности компьютерной информации» [3].

В. И. Кожевникова определяет преступления в сфере компьютерной информации как опасные общественные деяния, которые совершаются общеопасным способом и посягают на неприкосновенность конфиденциальной компьютерной

информации [4]. Н. С. Бабкова отмечает, что преступления, предусмотренные главой 28 УК РФ, посягают на компьютерную информацию, на сведения, содержащиеся в электронных носителях, программные средства [2].

Понятие «компьютерное преступление», или «киберпреступление», не используется в Уголовном кодексе РФ, но при этом имеет криминологическое значение. Выделяют следующие виды киберпреступлений: компьютерные преступления против конституционных прав и свобод человека и гражданина, компьютерные преступления в сфере экономики, в сфере общественной безопасности; против государственной безопасности.

Ответственность за преступления в сфере компьютерной информации предусмотрена гл. 28 Уголовного кодекса РФ (далее УК РФ), а именно ст. 272 «Неправомерный доступ к компьютерной информации»; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»; ст. 274^1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»; ст. 274^2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

Таким образом, под преступлениями в сфере компьютерной информации как разновидности киберпреступлений следует понимать, на наш взгляд, посягательства на информационную безопасность Российской Федерации с использованием информационных и компьютерных технологий, которые создают угрозу и могут причинять вред общественной безопасности.

Если использовать функциональный поход, то можно выделить следующие виды киберпреступлений:

1. Несанкционированный доступ к компьютерной информации: такие преступления включают хакерские атаки, взломы, использование недокументированных функций программного обеспечения и другие способы получения доступа к защищенной информации.

2. Распространение вредоносного программного обеспечения: к данному виду деяний относятся действия, направленные на создание, распространение и использование вредоносных программ, таких как вирусы, черви, трояны и шпионское программное обеспечение.

3. Мошенничество – это различные виды мошенничества, осуществляемого через сеть, например, кража финансовых данных, онлайн-мошенничество, фишинг и фарминг.

4. Кибертерроризм: такие преступления связаны с использованием компьютерной информации и сетей для создания паники, причинения вреда жизни и здоровью людей, уничтожения или повреждения важных объектов или на создание пропаганды терроризма.

5. Кибершпионаж – это действия, направленные на несанкционированное получение информации, коммерческих секретов, государственных секретов и другой конфиденциальной информации путем вторжения в компьютерные системы.

6. Кибернападение: подобные преступления включают блокировку, отказ в обслуживании (DDoS-атаки) и нанесение ущерба компьютерным системам, сетям или веб-ресурсам.

Преступления, связанные с компьютерной информацией, имеют серьезное влияние на экономическую безопасность Российской Федерации. В современном информационном обществе, где компьютеры и Интернет являются неотъемлемой частью деловых процессов и коммуникаций, киберугрозы представляют собой значительную опасность для национальной экономики.

Одним из основных аспектов влияния преступлений в сфере компьютерной информации на экономическую безопасность является угроза для бизнеса и коммерческих организаций. Киберпреступники могут получить несанкционированный доступ к конфиденциальным данным, включая банковские счета, клиентскую информацию, интеллектуальную собственность и коммерческие секреты. Это может привести к финансовым потерям, утечке важной информации и нарушению доверия клиентов. Крупные преступления в сфере компьютерной информации на компании могут нанести значительный ущерб экономике страны, особенно если они направлены на критическую инфраструктуру или ключевые отрасли.

Таким образом, рассматривая киберпреступления и их виды, необходимо отметить, что существуют узкий и широкий подходы. В соответствии с «узким» подходом к киберпреступлениям относятся только те преступления, для которых общественные отношения, связанные с компьютерной информацией, являются основным объектом преступного посягательства и которые закрепленные в главе 28 УК РФ.

В соответствии с «широким» подходом к киберпреступлениям относят преступления, в которых общественные отношения, связанные с компьютерной информацией, выступают как основным объектом посягательства, так и дополнительным: кража с банковского счета, а равно в отношении электронных денежных средств мошенничество с использованием электронных средств платежей, мошенничество в сфере компьютерной информации, неправомерный оборот средств платежей и т. д.

Список литературы

1. Уголовный кодекс Российской Федерации: [федер. закон от 13.06.1996 № 63-ФЗ] // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

2. Бабкова Н. С. Особенности совершения преступлений в сфере компьютерной информации // Интеллектуальные ресурсы – региональному развитию. 2021. № 1. С. 660–664.

3. Далгалы Т. А. Киберкриминология: вызовы XXI века // Российская юстиция. 2020. № 10. URL: https://www.consultant.ru/law/podborki/sootnoshenie_ponyatij_kiberprestuplenie_i_prestuplenie_v_sfere_kompyuternoj_informacii/?ysclid=lmayfwsiac513630517

4. Кожевникова В. И. Преступления в сфере компьютерной информации: актуальность и вопросы правоприменения // Правовая реформа. 2022. № 2. С. 48–50.

5. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук: 12.00.08 / Дальневост. гос. ун-т. – Владивосток, 2005. 26 с.

А. С. Смирнова,
студент,
Нижегородский институт управления – филиал
Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации

ВЕБ-САЙТ: СПЕЦИФИКА ЗАЩИТЫ ИНТЕЛЛЕКТУАЛЬНЫХ ПРАВ В УСЛОВИЯХ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье рассмотрены вопросы, связанные с определением правового режима веб-сайта как объекта интеллектуальных прав, а также проанализирована его специфика в части отнесения к числу сложных объектов. Целью исследования является анализ проблемных аспектов в части защиты веб-сайта, в том числе результатов интеллектуальной деятельности, используемых при его составлении, созданных посредством применения искусственного интеллекта. Предлагается несколько подходов к определению субъекта интеллектуальных прав на объекты веб-дизайна, созданные нейросетью, основываясь на оценке которых выбран наиболее целесообразный вариант. Формулируются положения, закрепление которых в нормах гражданского законодательства позволит урегулировать имеющиеся на сегодняшний день пробелы в сфере права интеллектуальной собственности.

Ключевые слова: веб-сайт, авторское право, искусственный интеллект, субъект интеллектуальных прав, нейросеть, веб-дизайн, творческий критерий

WEBSITE: THE SPECIFICS OF INTELLECTUAL PROPERTY RIGHTS PROTECTION IN THE CONDITIONS OF ARTIFICIAL INTELLIGENCE DEVELOPMENT

Abstract. The article deals with issues related to the definition of the legal regime of a website as an object of intellectual rights, and also analyzes its specificity in terms of attribution to the number of complex objects. The purpose of this study is to analyze problematic aspects in terms of website protection, including the results of intellectual activity used in its compilation, created through the use of artificial intelligence. In the text of the scientific work, several approaches are proposed to determine the subject of intellectual rights to web design objects created by a neural network, based on the assessment of which the most appropriate option is selected and the formulation of provisions is proposed, the consolidation of which in the norms of civil legislation will allow to some extent to resolve the gaps in the field of intellectual property law that exist today.

Keywords: website, copyright, artificial intelligence, subject of intellectual rights, neural network, web design, creative criterion

В рамках современных реалий общественное развитие характеризуется постоянным совершенствованием цифровых технологий, в том числе развитием информационно-телекоммуникационной сети Интернет. Однако наряду со всеми

преимуществами виртуальных возможностей меняющиеся реалии ставят ряд вопросов правового характера, в частности в сфере права интеллектуальной собственности. Так, одним из актуальных проблемных аспектов указанной подотрасли гражданского права является вопрос охраны авторским правом веб-сайта (его компонентов), созданного при помощи искусственного интеллекта. При этом начать исследование указанного аспекта представляется целесообразным с определения правового режима веб-сайта, а также его специфики как объекта интеллектуальных прав.

Прежде чем перейти к анализу правовой природы веб-сайта, следует обратиться к определению данного понятия, легальная вариация которого закреплена в пункте 13 части 1 статьи 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – ФЗ № 149-ФЗ): «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” по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети “Интернет”» [2].

Представленная дефиниция, по мнению некоторых ученых, направлена на определение «публично-правового статуса интернет-сайта и позволяет определить его место в системе законодательства об информации» [11. С. 324], но при этом не позволяет в полной мере определить статус сайта как объекта гражданских прав. В связи с изложенным представляется целесообразным обратиться к положениям гражданского законодательства, а именно к пункту 2 статьи 1260 Гражданского кодекса РФ (далее – ГК РФ), содержание которого определяет интернет-сайт как составное произведение. Стоит отметить, что отнесение законодателем веб-сайта к числу составных произведений тем не менее не сократило поле для дискуссий среди ученых, исследования которых направлены на определение правовой природы веб-сайтов, что подчеркивает актуальность анализируемого вопроса.

На сегодняшний день дискуссионными являются вопросы о наличии оснований придания веб-сайту режима особого объекта интеллектуальных прав и их достаточности при отнесении сайта к числу составных произведений. Кроме того, анализ правовой доктрины свидетельствует о необходимости исследования вопроса об обоснованности квалификации интернет-сайта как сложного объекта интеллектуальных прав. В рамках анализа указанных аспектов представляется целесообразным рассмотреть изучаемый объект с технической точки зрения.

Так, обращаясь к научному труду А. И. Савельева, можно выделить следующие компоненты веб-сайта: «система управления содержимым сайта; дизайн; текст веб-страниц, изложенный с использованием специальных языков HTML (отвечающий за логическую структуру страницы) и CSS (отвечающий за ее внешний вид и иные функции); контент (информационное наполнение веб-сайта)» [11. С. 325]. Представленный перечень элементов свидетельствует о сложной структуре интернет-сайта, условно состоящей из трех слоев: презентационного (дизайна), бизнес-логики (характерен для сложных сайтов, например, интернет-магазинов)

и слоя базы данных. Можно сделать вывод о комплексном характере веб-сайта, раскрыть специфику которого как объекта гражданских прав можно посредством следующей формулировки дефиниции анализируемого объекта, предложенной Е. С. Басмановой: «Интернет-сайт – это предназначенный для размещения в сети Интернет результат интеллектуальной деятельности, состоящий из статичной основы, представляющей собой программный код и порождаемые им визуальные отображения (дизайн сайта), и динамичного содержания (контента), представляющего собой совокупность разнородных объектов исключительных прав и иных материалов, системно расположенных в пределах базового (статичного) элемента сайта» [6. С. 93].

Таким образом, обращаясь к содержанию вышеупомянутой ст. 1260 ГК РФ, можно заключить, что авторским правом охраняется именно контентная составляющая сайта, т. е. совокупность результатов интеллектуальной деятельности, квалифицируемых как самостоятельные объекты авторского права, а именно их творческий подбор или расположение (составительство). Однако в правовой доктрине имеет место мнение, согласно которому такое регулирование веб-сайтов видится весьма фрагментарным: встает вопрос, кого следует признавать автором сайта в целом и каков точный перечень результатов интеллектуальной деятельности, однозначно входящих в состав сайта.

Для того чтобы выяснить, следует ли наделить веб-сайт особым правовым режимом и рассматривать его в качестве самостоятельного объекта интеллектуальных прав, обоснованным видится обратиться к зарубежной практике. Так, анализ положений законодательства иностранных государств позволяет сделать вывод о схожем с отечественным подходе в части регулирования исследуемого вопроса: охране подлежит творческий подбор контента на сайте, а о возможности охраны авторским правом веб-сайта в целом, как самостоятельного объекта, не упоминается. Внимания при этом заслуживает подход, применяемый бюро авторских прав США [14. С. 1], согласно которому интернет-сайт выступает некой формой выражения, носителем результатов интеллектуальной деятельности, однако сам по себе сайт в качестве объекта авторских прав американская практика также не признает.

Таким образом, при определении правовой природы веб-сайта как объекта интеллектуальных прав нормы отечественного и зарубежного законодательства указывают на два аспекта: 1) охрану отдельных элементов сайта как самостоятельных объектов авторского права и 2) охрану подбора или расположения его компонентов, осуществляемых творческим трудом (составительство). Здесь важно отметить, что сайту как составному произведению должен быть присущ творческий характер (п. 2 ч. 2 ст. 1259 ГК РФ): например, максимально простой одностраничный интернет-сайт, содержащий какой-либо один результат интеллектуальной деятельности (стихотворение), не будет подлежать охране авторским правом, а будет, скорее, выступать как раз формой выражения содержащегося на нем произведения.

Помимо проанализированных аспектов, одним из дискуссионных вопросов в части характеристики веб-сайта как результата интеллектуальной деятельности

является проблема обоснованности отнесения исследуемого объекта к числу сложных. Аргументируя позицию ученых, квалифицирующих сайт как сложный объект, видится необходимым обратиться к положениям статьи 1240 ГК РФ [1], регламентирующей перечень таких объектов (кинофильм, иное аудиовизуальное произведение, театрально-зрелищное представление, мультимедийный продукт, база данных), который является закрытым. Однако закрытость такого перечня – вопрос весьма дискуссионный: в правовой доктрине превалирует мнение о целесообразности включения в него и веб-сайта. Обоснованность данной позиции можно подтвердить, опираясь на дефиницию понятия «сложный объект», под которым согласно теоретическим исследованиям понимается объект гражданских прав, «созданный организатором такого объекта, включающий в себя несколько принадлежащих различным правообладателям охраняемых результатов интеллектуальной деятельности, объединенных структурными связями, предназначенных для их использования по единому назначению» [9. С. 85]. Исходя из предложенной формулировки и опираясь на законодательные положения, можно выделить следующие критерии сложного объекта интеллектуальных прав: наличие лица, организовавшего создание такого объекта; совокупность нескольких охраняемых результатов интеллектуальной деятельности, составляющих сложный объект; структурная взаимосвязь и единая цель включенных в состав сайта объектов интеллектуальных прав. В силу того, что сайт включает в себя созданные авторами в сотрудничестве структурно связанные результаты интеллектуальной деятельности (объекты дизайна, графики, литературные произведения, программы для ЭВМ и иные элементы), рассмотрение интернет-сайта в качестве сложного объекта представляется аргументированным.

Таким образом, анализируемый объект интеллектуальных прав следует рассматривать не только как составное произведение, но и как сложный объект, в связи с чем целесообразно внести изменения в действующее законодательство, а именно в статью 1240 ГК РФ, в части включения его в перечень сложных объектов. Представленная редакция указанной нормы видится перспективной с точки зрения приобретения лицом, организовавшим создание сайта, прав на результаты интеллектуальной деятельности, входящие в его состав. Таким образом, можно сделать вывод, что оснований для признания сайта в качестве особого объекта авторских прав на сегодняшний день не имеется, веб-сайт следует квалифицировать и как составное произведение, и как сложный объект.

Особого внимания заслуживает вопрос об определении авторства и творческого критерия веб-сайта, созданного с помощью искусственного интеллекта (конструктора сайтов). Так, на сегодняшний день пользуются популярностью такие сервисы, как Tilda Publishing (блочный конструктор сайтов, не требующий умений и навыков в области программирования) и Taplink (платформа для создания сайтов, адаптированных под мобильные устройства и предназначенных, как правило, для таргета в социальных сетях). Указанные платформы выполняют функции верстальщика и программиста, в связи с чем встает вопрос, кого признавать автором сайта: его создателя, который осуществлял верстку посредством «собирания» блоков, составляющих сайт, или же в таком случае авторскими правами его

наделить нельзя ввиду отсутствия творческого подхода к созданию интернет-сайта. Центральным элементом в рамках анализа данного вопроса является наличие творческого критерия в деятельности создателя сайта.

Так, если веб-сайт является максимально простым (состоит из одной страницы, представляет собой хаотичную (либо хронологическую) сборку размещенных в библиотеке платформы блоков) и его верстка не требует вклада действий творческого характера (в части дизайнерских решений, построения композиционных связок, применения анимаций, в том числе разработки и использования при их создании HTML-кодов, и тому подобное), то такой объект авторским правом охраняться не будет. Таким образом, наличие творческого критерия – признак, позволяющий отграничить сайт, не являющийся объектом авторского права, от сайта, который авторским правом охраняется; т. е. только потому, что создатель веб-сайта использует при его верстке специальные сервисы, творцом он от этого быть не перестает.

Более подробно представленный аспект следует рассмотреть в рамках специфики регулирования прав на объекты веб-дизайна как одной из составляющих веб-сайта. С учетом изложенного можно заключить, что творческой деятельности на современном этапе общественного развития присуще слияние искусства и технологий, в связи с чем популярностью пользуется такая ниша, как digital-искусство. В частности, как ранее было отмечено, на сегодняшний день все большей популярностью пользуются различные системы искусственного интеллекта: активно используются нейросетки-генераторы, что позволяет автоматизировать работу, существенно ее упростив и ускорив. Так, известными на сегодняшний день нейросетями, применяемыми в сфере веб-дизайна, являются Midjourney, Kandinsky 2.2, Magician, Craiyon и многие другие (используются для генерации графики), а также ChatGPT, AI-ассистент, Gerwin AI (применяются для разработки контента). Однако наряду с преимуществами цифровых возможностей меняющиеся реалии ставят ряд вопросов правового характера. Так, одним из актуальных проблемных аспектов права интеллектуальной собственности является неопределенность субъекта интеллектуальных прав на объекты, созданные нейросетями, к использованию которых чаще всего прибегают при создании результатов интеллектуальной деятельности в сфере веб-дизайна. Решение указанного вопроса позволит определить, каким образом и чьи именно права на результат, сгенерированный нейросетью, следует охранять.

Прежде всего, необходимо определить, что понимается под искусственным интеллектом (далее – ИИ), легальное определение которого закреплено в Национальной стратегии развития искусственного интеллекта на период до 2030 г. (указ Президента РФ от 10.10.2019 № 490): «Искусственный интеллект – 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» [3].

Говоря о субъекте интеллектуальных прав, представляется целесообразным обратиться к нормам гражданского законодательства: анализ статей 1228 и 1347

Гражданского кодекса РФ [1] позволяет выявить ключевые критерии указанного понятия: (1) творческий характер результата интеллектуальной деятельности, который должен быть создан (2) физическим лицом.

Таким образом, указанные положения свидетельствуют о неправомерности наделения ИИ статусом субъекта интеллектуальных (авторских) прав. Однако исследователи неоднозначно подходят к данному вопросу. Так, согласно предложенной американским философом Д. Ж. Серлом теории «сильного и слабого искусственного интеллекта» «слабый» ИИ способен решать какую-либо задачу, основываясь на заданных человеком параметрах, «при этом сам искусственный интеллект не может понимать смысл тех объектов, с которым он работает» [12. С. 33].

«Сильный» же ИИ обладает таким уровнем развития, при котором его способности сопоставимы (или даже превосходят) возможности человеческого разума. В связи с этим некоторые авторы придерживаются мнения о целесообразности наделения ИИ статусом субъекта интеллектуальных прав. В частности, В. В. Архипов и В. Б. Наумов в своем исследовании, анализируя правовое положение ИИ, приходят к выводу о необходимости включения главы 5.1 «Роботы-агенты» в подраздел 2 «Лица» части 1 ГК РФ [12. С. 33]. Схожий подход к решению данного вопроса рассматривает Т. Н. Михалева, которая указывает при этом на необходимость разработки определенной методологии, «которая позволит выделять определенные виды искусственного интеллекта, которые могли бы стать полноценными участниками правоотношений» [8. С. 127], и определяет ИИ как «электронное лицо». Обращаясь к зарубежной правоприменительной практике, можно отметить, что в 2019 г. в Китае в одном из постановлений Окружной суд указал, что статья, созданная с помощью алгоритма, не может быть скопирована без разрешения [8. С. 126] (примечательно, что до этого законодатели и правоприменители указанного государства придерживались позиции о невозможности защиты авторским правом объекта, созданного ИИ).

Кроме того, ярким примером, подтверждающим анализируемую позицию, может служить продажа «одного из произведений ИИ в серии работ, сгенерированных в стиле Рембрандта, «Портрет Эдмонда де Белами», на аукционе Christie`s в 2018 г. в Нью-Йорке за 432,5 тыс. дол.; в углу картины стоит подпись алгоритма» [8. С. 119]. Однако представленные точки зрения видятся некорректными в части несоблюдения признаков субъекта интеллектуальных прав, закрепленных в указанных ранее статьях 1228 и 1347 ГК РФ. Несмотря на то, что в правовой доктрине высказывается мнение о дальнейшей автоматизации и самообучении ИИ, в том числе нейросетей, которые позволили бы им генерировать произведения без человеческого вмешательства, тем не менее существование роботов с подобным функционалом на сегодняшний день не доказано, и предполагается, что в обозримом будущем ИИ вряд ли будет обладать критериями, наделяющими его правосубъектностью. При этом если говорить о наделении технологий ИИ правосубъектностью, то возникает ряд закономерных вопросов: какие права и обязанности будут присущи алгоритму? Каким образом он будет нести ответственность?

По справедливому замечанию А. С. Антонян, ИИ (нейросеть), «не обладая имуществом, не имея осознанной воли для владения, пользования и распоряжения им, не способна нести ни имущественную, никакую-либо иную ответственность» [5. С. 515], что подтверждает необоснованность признания нейросети автором созданного ею произведения. В связи с этим более обоснованной представляется позиция об отнесении данного явления к объектам, а не субъектам интеллектуальных прав, аргументируя ее тем, что технологиями ИИ можно владеть, пользоваться и распоряжаться.

С учетом изложенного целесообразно рассмотреть иные подходы к определению субъекта на результаты, сгенерированные нейросетью. Прежде чем перейти к их исследованию, следует разобраться с тем, будет ли обладать творческим характером результат, сгенерированный нейросетью? Представляется, что для ответа следует разобраться непосредственно со спецификой выполняемых нейросеткой функций и созданных ею объектов.

Роль нейросетей на примере веб-дизайна характеризуется самым разнообразным спектром возможностей ИИ: благодаря нейросеткам представители данной профессии могут путем ввода определенной команды (промта) генерировать различные изображения, работать с типографикой, создавая неповторимые виды шрифтов, и применять полученные результаты в том числе при создании сайтов. Помимо этого, у представителей рассматриваемой профессии есть возможность с помощью ИИ «регулировать контраст создаваемых объектов, их цветовую насыщенность, а также использовать высокую вариативность параметров» [10. С. 9]. Как мы видим, с одной стороны, сущность выполняемых ИИ функций сводится к воспроизведению нейросетью той программы (запроса), которую задаст человек, однако, с другой стороны, при вводе одной и той же команды компьютерный алгоритм будет генерировать постоянно новый, уникальный результат. Но опять же, можно ли охарактеризовать такой процесс как деятельность творческую?

Целесообразным представляется рассмотреть понятие творческой деятельности с точки зрения двух аспектов. С субъективной стороны, как исходит из названия подхода, «создание произведения в результате творческой деятельности присуще только человеку» [13. С. 507] в силу неразрывной связи между человеческой личностью и результатом творческого труда.

Кроме того, при генерации задаваемых значений ИИ не способен воспроизводить мыслительную деятельность человека, что опять же подтверждает отсутствие в создаваемом нейросетью объекте творческого начала. С точки зрения же объективного подхода творческим характером наделяется не деятельность, т. е. не процесс создания объекта, а сам объект, произведение, ценность которого определяется в зависимости от его вклада в культуру. Однако, как ранее нами было отмечено, на сегодняшний день системы ИИ находятся пока на том уровне развития, когда генерация произведения посредством компьютерных алгоритмов возможна лишь с помощью человека, который предварительно загружает необходимые данные и осуществляет контроль за выдаваемыми результатами, которые субъект может также изменять. В связи с изложенным объективный подход тоже не позволяет отнести объект, созданный нейросетью, к результатам творческой деятельности.

Вместе с этим важно обратить внимание на то, что использование веб-дизайнером систем ИИ указанным способом (путем ввода простейшего запроса) не будет квалифицировано как творческая деятельность, а значит, получаемые результаты не будут являться объектами авторского права, подтверждением чему служит анализ судебной практики [4]. Так, если веб-дизайнер не осуществляет творческого вклада при генерации графических элементов, т. е. вводит в строку поиска наименование объекта, который необходимо создать нейросети, то в таком случае и получаемый результат также не приобретет творческое начало. Однако обратной ситуация видится в случае модификации со стороны веб-дизайнера созданного нейросетью объекта, например, путем удаления каких-либо элементов и добавления уже созданных им конструкций, в результате чего у субъекта получается оригинальное произведение, сочетающее в себе результаты деятельности как человека, так и ИИ. Вышеизложенное опять же позволяет заключить, что субъектом прав на созданные нейросетями объекты может выступать только физическое лицо – веб-дизайнер. Тем не менее в правовой регламентации нуждается вопрос о справедливом распределении прав и доходов между разработчиком программного кода ИИ и конечным пользователем (веб-дизайнером). Правовая доктрина предлагает несколько подходов к решению указанного вопроса.

Если говорить о признании автором цифрового произведения разработчика ИИ, то данный подход будет весьма эффективен с точки зрения развития сферы цифровых технологий, компьютерных программ. Но, с другой стороны, в силу того что дизайнер не обладает правом авторства на результаты, сгенерированные нейросетью, соответственно, он не будет заинтересован в регулярном использовании соответствующих программ. Такая ситуация чревата сдвигом акцента на создание не новых уникальных произведений, а программных кодов, что, в свою очередь, замедлит темпы развития сферы как веб-дизайна, так и разработок систем ИИ вследствие упадка спроса на них со стороны пользователей. К тому же изложенная позиция противоречит существующим положениям гражданского законодательства в части указания признаков субъекта интеллектуальных прав: при разработке кода ИИ замысел лица не направлен на создание соответствующего произведения, что свидетельствует об отсутствии творческой составляющей в его деятельности [8. С. 114].

Что касается следующего подхода, то роль автора уже предлагается отвести веб-дизайнеру. Однако здесь тоже следует учитывать ряд ключевых моментов: как ранее отмечалось, субъекту недостаточно совершить комбинацию элементарных действий (ввод запроса в поисковой строке, нажатие кнопки поиска), необходимо в процессе формирования какого-либо объекта применять навыки творческого характера, осуществлять мыслительную деятельность, а также осознавать, каким он хочет видеть конечный результат. При этом алгоритм ИИ в данном случае фактически выступает неким инструментом, посредством которого веб-дизайнер создает результат интеллектуальной деятельности. Представленный подход видится наиболее корректным и соответствующим положениям ГК РФ, поскольку ИИ на сегодняшний день не развит на таком уровне,

чтобы генерировать произведения обособленно от лица, предпринимающего меры творческого характера для разработки объекта интеллектуальных прав. Причем подобное регулирование данного вопроса не должно лишать разработчика ИИ возможности получения вознаграждения за использование соответствующей технологии. Таким образом, в целях предотвращения возникновения правовой неопределенности и формирования четкой позиции в части определения правового положения создателя объекта веб-дизайна как составного компонента интернет-сайта посредством ИИ (нейросети) предлагается осуществить реформу Части IV ГК РФ. Совершенствование действующего законодательства возможно путем включения в указанную часть анализируемого закона примерный перечень следующих новелл: права на сами технологии ИИ (нейросети) и применяемые алгоритмы должны принадлежать их разработчику, а результаты, создаваемые посредством применения данных генераторов, – пользователям ИИ (веб-дизайнерам) при условии наличия в деятельности лица творческого начала. При этом в силу того, что творческая составляющая является центральным элементом при квалификации произведения в качестве объекта авторских прав, необходимым шагом на пути усовершенствования механизма правового регулирования общественных отношений, осложненных применением при создании объекта интеллектуальных прав алгоритмов ИИ, по мнению А. С. Антонян, видится необходимым ввести трактовку понятия «творческий критерий» [5. С. 516]. В случае отсутствия творческого вклада со стороны веб-дизайнера, создающего объект с помощью нейросетки, «полученный результат не должен подлежать какой-либо правовой охране» [5. С. 516].

Таким образом, в рамках активного развития цифровых технологий законодателю важно успевать адаптировать нормы законодательства под те условия, которые диктует меняющаяся реальность. В частности, на основе изложенных в юридической литературе позиций и опыта зарубежных стран можно заключить, что в дальнейших научных изысканиях нуждаются вопросы, связанные с характеристикой правового режима веб-сайта как объекта авторских прав и определением правовой природы кибертворческого начала в лице нейросетей, используемых веб-дизайнерами при генерировании объектов веб-дизайна, являющихся составным элементом интернет-сайта.

Список литературы

1. Российская Федерация. Законы. Гражданский кодекс РФ (часть четвертая): Федеральный закон от 18.12.2006 № 230-ФЗ // Собрание законодательства РФ. 2006. № 52 (ч. I). Ст. 5496.

2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ. 2006. № 31 (ч. I). Ст. 3448.

3. О развитии искусственного интеллекта в Российской Федерации: указ Президента РФ от 10.10.2019 № 490 (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_335184

4. О применении части четвертой Гражданского кодекса Российской Федерации: постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_323470

5. Антонян А. С. Право на результат интеллектуальной деятельности, созданный с применением нейросетей // Скиф. 2023. № 6 (82). С. 512-516. URL: https://cyberleninka.ru/article/n/pravo-na-rezultat-intellektualnoy-deyatelnosti-sozdannyy-s-primeneniem-neyrosetey

6. Басманова Е. С. Интернет-сайт как объект имущественных прав: дисс. … канд. юрид. наук. М., 2010. 175 с.

7. Воскресенская Е. В., Ворона-Сливинская Л. Г., Лойко А. Н. К вопросу о правовой природе результатов деятельности искусственного интеллекта // Colloquium-journal. 2019. №5 (29). С. 114–116. URL: https://cyberleninka.ru/article/n/k-voprosu-o-pravovoy-prirode-rezultatov-deyatelnosti-iskusstvennogo-intellekta

8. Михалева Т. Н. Правовое обеспечение цифровизации искусства // Вестник РУДН. Серия: Юридические науки. 2023. № 1. С. 117–134. URL: https://cyberleninka.ru/article/n/pravovoe-obespechenie-tsifrovizatsii-iskusstva

9. Новоселова Л. А. Право интеллектуальной собственности. Т. 1. Общие положения: учебник / под общ. ред. д.ю.н., проф. Л. А. Новоселовой. М.: Статут, 2017. 512 с.

10. Петрухина О. В. Генеративная графика: вчера, сегодня, завтра // НАУ. 2023. № 88-2. С. 9–11. URL: https://cyberleninka.ru/article/n/generativnaya-grafika-vchera-segodnya-zavtra

11. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. 2-е изд., перераб. и доп. М.: Статут, 2016. 640 с.

12. Трохов М. С., Колоскова О. А. , Глазов И. Д. Гражданско-правовое регулирование искусственного интеллекта в Российской Федерации // Юридические исследования. 2023. № 3. С. 24–39. URL: https://cyberleninka.ru/article/n/grazhdansko-pravovoe-regulirovanie-iskusstvennogo-intellekta-v-rossiyskoy-federatsii

13. Чернышов М. С. Субъект интеллектуальных прав на результаты интеллектуальной деятельности, созданные искусственным интеллектом // Скиф. 2023. №1 (77). С. 506–511. URL: https://cyberleninka.ru/article/n/subekt-intellektualnyh-prav-na-rezultaty-intellektualnoy-deyatelnosti-sozdannye-iskusstvennym-intellektom

14. U.S. Copyright Office. Compendium of U.S. Copyright Office Practices §101 (3d ed. 2019). Guidance regarding the copyrightability and registrability of websites and website content (Chapter 1000). 8 p.

Л. А. Смирнова,
студент,
Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского

ДИСТАНЦИОННОЕ ЭЛЕКТРОННОЕ ГОЛОСОВАНИЕ КАК ПЕРСПЕКТИВНАЯ ФОРМА РЕАЛИЗАЦИИ АКТИВНОГО ИЗБИРАТЕЛЬНОГО ПРАВА

Аннотация. Статья посвящена исследованию дистанционного электронного голосования: сущности, появления, преимуществ и недостатков данной формы реализации активного избирательного права. Проанализированы подходы к пониманию дистанционного электронного голосования иностранными государствами. Дана оценка инновационной форме в условиях российской действительности. В целях повышения уровня нормативно-правового регулирования данной области предложено введение ряда новых терминов.

Ключевые слова: дистанционное электронное голосование, избирательный процесс, выборы, интернет-голосование, избиратель, избирательное право

INTRERNET-VOTING AS A PROMISING FORM OF REALIZATION AN ACTIVE SUFFRAGE

Abstract. The article is devoted to the study of remote electronic voting: the essence, emergence, advantages and disadvantages of this form of realization of active electoral right. The author analyzes approaches to the understanding of remote electronic voting by foreign states, gives an assessment of the innovative form in the conditions of the Russian reality. Moreover, in order to improve the level of normative-legal regulation of this area, the introduction of a number of new terms is proposed.

Keywords: remote electronic voting, electoral process, elections, internet voting, voter, electoral law

Развитие информационно-коммуникационных технологий (далее – ИКТ), компьютеризация и роботизация качественно влияют на современную жизнь каждого человека. Активное внедрение ИКТ в государственное управление стало причиной зарождения феномена электронной демократии и стремления построить цифровое государство [10. С. 191]. Важным направлением взятого курса является цифровизация электоральных процедур, иллюстрацией которого является внедрение в российскую действительность дистанционного электронного голосования (далее – ДЭГ).

Дистанционное электронное голосование представляет собой голосование без использования бумажного бюллетеня, с применением специального программного обеспечения [1]. Несмотря на то, что апробация ДЭГ произошла в 2019 г., законодательно термин был введен лишь в 2020 г. Федеральным законом от 23.05.2020 № 154-ФЗ.

Как было отмечено, технология интернет-голосования является сравнительно молодой. Эксперимент по внедрению в избирательный процесс ДЭГ начался с выборов, проводимых в Москве в 2019 году. Реализация активного избирательного права граждан осуществлялась с использованием регионального портала государственных и муниципальных услуг.

Продемонстрировавшее свою эффективность ДЭГ было применено уже на выборах 2021 года. Теперь апробация интернет-голосования затронула уже семь субъектов Российской Федерации – Москву, Севастополь, Нижегородскую, Ярославскую, Курскую, Мурманскую и Ростовскую области. Примечательно, что процедура дистанционного голосования различалась организационно и нормативно. Так, у москвичей была возможность вносить изменения в избирательный бюллетень в течение периода для голосования, а в других субъектах России электронный бюллетень можно было заполнить лишь единожды [3. С. 25]. Кроме того, жители Москвы реализовывали активное избирательное право с помощью регионального портала государственных и муниципальных услуг, а остальные субъекты Российской Федерации, участвующие в эксперименте, – посредством федеральной платформы.

Примечательно, что уже в 2023 г. в Единый день голосования дистанционно смогут проголосовать жители 24 регионов нашего государства. Важно отметить, что несмотря на неоднозначность восприятия процедуры в общественном сознании и ее новизну по состоянию на 7 августа гражданами уже подано свыше 400 тысяч заявлений. Регионами-лидерами стали: Алтайский край, Московская, Псковская, Воронежская и Нижегородская области [5].

Дистанционное электронное голосование было введено в российскую политическую и правовую систему с целью решения ряда проблем, к которым мы относим:

– преодоление человеческого фактора при подсчете голосов на избирательном участке,

– снижение нагрузки на избирательные комиссии,

– уменьшение финансовых затрат,

– оптимизация избирательного процесса.

В зарубежной литературе существует подход, в соответствии с которым интернет-голосование выступает способом обеспечения гендерного равенства в политической среде – преодоления искажения в сторону определенной демографической группы. По мнению авторов, снижение расходов на участие в выборах может изменить демографический состав избирателей и тем самым повлиять на результаты [4. С. 76].

Несмотря на значительные преимущества «цифровой» формы реализации активного избирательного права, отмечаются значительные риски: кража персональных данных избирателей, возможность влияния на избирательный процесс и национальную политику. Кроме того, дистанционное электронное голосование вызывает сомнение и в части проведения процедуры аутенфикации избирателей, анонимизации избирательных бюллетеней и законности итогов выборов в целом. Так, по данным американского «Центра демократии и технологий», применение

дистанционной формы голосования оказывает влияние на безопасность, справедливость и доступность выборов [6].

Тренд на оспаривание результатов интернет-голосования оппозицией отмечается как в национальной, так и в международной правовой действительности. С подобным административным исковым заявлением в Мосгорсуд в 2019 г. обратился кандидат в депутаты Иван Ульянченко. По его мнению, предусмотренное порядком проведения шифрование в достаточной мере не обеспечивает защиту персональных данных и нарушает тайну голосования. Иваном Ульянченко также было указано на нарушение принципа равенства избирателей: в 2019 г. ДЭГ было запланировано лишь в трех избирательных округах Москвы [2]. Затрагивая международную практику, после подобного иска в 2009 г. в Германии Конституционный суд ФРГ признал неконституционным использование электронных систем при проведении выборов или голосования в стране [7].

Примечательно, что большинство государств Европы, Соединенные Штаты Америки не признают интернет-голосование альтернативой традиционной форме реализации активного избирательного права. Показательна практика США: в некоторых штатах голосовать посредством сети Интернет могут лишь определенные категории избирателей: военнослужащие, иностранные граждане, избиратели с инвалидностью [2]. В Эстонии и Швейцарии, где интернет-голосование было испытано или полностью реализовано, процент людей, использующих эту форму, колеблется от 20 до 40: едва ли превышает 40 % на национальных выборах в Эстонии, 20 % – в Женеве. Это обстоятельство наглядно демонстрирует недоверие избирателей к инновационной форме голосования.

В Великобритании, напротив, интернет-голосование воспринимается как средство, способное повысить электоральную явку среди молодежи, аналогично тому, как введение возможности голосовать по почте оказало позитивное влияние на увеличение количества избирателей старшего поколения [8].

Говоря о ситуации, складывающейся в России, отмечается неуклонный рост количества избирателей, предпочитающих дистанционное электронное голосование традиционной форме, а также формирование доверия к такому формату реализации активного избирательного права. По заявлению заместителя председателя ТИК ДЭГ, «число партий, не признающих процедуру ДЭГ, неуклонно сокращается, и даже самые рьяные ее критики постепенно пересматривают свою позицию» [9].

По нашему мнению, дистанционное электронное голосование полностью соответствует критериям информационного общества, совершенствует избирательный процесс и направлено на качественное построение цифрового государства. В каждой демократической и правовой стране проведение свободных и честных выборов и голосований выступает в качестве одного из наиболее важных направлений политики. Мобильность, прозрачность, безопасность и эффективность – те принципы, на которых базируется процедура ДЭГ, не первый год доказывая это успешной практикой применения.

Ввиду активного развития этой технологии нами предлагается усовершенствование нормативно-правовой базы путем введения новых понятий в российское

законодательство, таких как система шифрования, электронный список избирателей, нода блокчейн, ключ расшифрования.

Кроме того, представляется важным развивать образовательно-просветительское направление и проводить тематические мероприятия среди школьников и студентов высших учебных заведений. Взаимодействие с молодыми людьми может осуществляться в различных форматах: в виде лекций, семинаров, круглых столов, творческих и научных конкурсов. Молодежь должна быть знакома с процедурой дистанционного электронного голосования, знать об основных преимуществах такой формы и понимать принцип его функционирования. На наш взгляд, интерес к ДЭГ и его популярность могут быть достигнуты лишь при ведении в данной области активной информационной кампании избирательными комиссиями разных уровней и общественными организациями.

Список литературы

1. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 23.05.2020 № 154-ФЗ // Собрание законодательства РФ. 2020. № 21. Ст. 3233.

2. Апелляционное определение Верховного суда Российской Федерации от 06.08.2019 № 5-АПА19-93. URL: https://vsrf.ru/stor_pdf.php?id=1798064

3. Гриценко Е. В. Право на хорошее управление в условиях цифровой трансформации // Сравнительное конституционное обозрение. 2022. № 4. С. 15–36.

4. Wigginton M., Stockemer D. Does the Introduction of Online Voting Create Divesity in Representation? // Political Studies ReviewVolume. 2021. P. 172–182.

5. Более 400 тысяч россиян подали заявки на участие в электронном голосовании // РИА Новости. URL: https://ria.ru/20230807/golosovanie-1888590532.html

6. How Many Disabled People Vote Over the Internet? We Need Better Data.// Center for Democracy and Technology. URL: https://cdt.org/insights/how-many-disabled-people-vote-over-the-internet-we-need-better-data

7. Конституционный суд Германии предложил голосовать по старинке // Право.Ru. URL: https://pravo.ru/interpravo/news/view/8571

8. Will New Technology Boost Turnout? Evaluating Experiments in E-Voting v. All-Postal Voting Facilities in UK Local Elections. // HarvardKennedySchool. URL: https://www.hks.harvard.edu/publications/will-new-technology-boost-turnout-evaluating-experiments-e-voting-v-all-postal-voting

9. Качественное наблюдение: ДЭГ требует серьезной подготовки – эксперт // Российское агентство правовой и судебной информации. URL: https://rapsinews.ru/election_right_news/20220823/308226273.html

10. Интересы в механизме публичной власти: проблемы теории и практики: монография / отв. ред. Ю. А. Тихомиров. М.: Проспект, 2023.

В. А. Гагарина,
студент,
Институт законодательства и сравнительного правоведения
при Правительстве Российской Федерации

ЦИФРОВАЯ ПЕРСПЕКТИВА СУДА ПРИСЯЖНЫХ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. В настоящее время цифровые технологии активно развиваются и внедряются во все сферы человеческой жизнедеятельности. Большинство органов власти уже прошли процесс цифровизации, за счет которого удалось существенно повысить производительность труда сотрудников, а также сократить время обращения в государственные и муниципальные органы власти со стороны граждан. Суды РФ также широко внедряют процессы цифровизации. Электронные повестки уже прочно вошли в жизнь судов и граждан. Также суды старательно внедряют дистанционные технологии допроса свидетелей в судах, в том числе в тех судах, которые рассматриваю уголовные дела с участием присяжных заседателей. В рамках настоящей статьи предпринята попытка научного анализа и критического осмысления цифровой перспективы суда присяжных заседателей в Российской Федерации.

Ключевые слова: развитие права, суд присяжных, внедрение цифровых технологии, инновации в судебном заседании

DIGITAL PERSPECTIVE OF JURIES IN THE RUSSIAN FEDERATION

Abstract. At present, digital technologies are actively developing and being introduced into all spheres of human life. Most authorities have already gone through the process of digitalization, due to which it was possible to significantly increase the productivity of employees, as well as reduce the time for citizens to contact state and municipal authorities. The courts of the Russian Federation are also widely implementing digitalization processes. Electronic subpoenas have already firmly entered the life of courts and citizens. The courts are also diligently introducing remote technologies for interrogating witnesses in courts, as well as in those courts that consider criminal cases with the participation of jurors. Within the framework of this article, the author made an attempt to scientific analysis and critical understanding of the digital perspective of the jury trial in the Russian Federation.

Keywords: development of law, jury trial, introduction of digital technologies, innovations in the court session

Введение. Беспроводные технологии и мобильные устройства меняют то, как суды отправляют правосудие, благодаря все более широкому использованию средств цифровизации, например, таких как смартфоны и планшеты в практике судов, судей и присяжных заседателей. В совещательной комнате мобильные устройства могут упростить предоставление и использование информации и способствовать более эффективному обсуждению и общему принятию решений.

Но прежде чем такие технологии станут обычным явлением в зале присяжных, судам было бы полезно получить эмпирические данные о влиянии – положительном и/или отрицательном – их предоставления присяжным как с точки зрения эффективности, так и с точки зрения сохранения фундаментальных предпосылок права обвиняемого на справедливый суд.

В настоящее время в суде обычное дело видеть ряд визуальных технологий в действии в процессе судебного разбирательства. Удаленные видеотехнологии используются для привлечения в зал суда свидетелей, обвиняемых и, иногда, судей [11. С. 242].

Также используются записанные видеодоказательства, которые могут включать кадры с камер видеонаблюдения, кадры с носимых на теле полицейских камер, криминалистические анимации или преступления, снятые свидетелями на их мобильные телефоны. Этот «визуальный поворот» в праве привел к бурно развивающейся юриспруденции в области использования цифровых технологий [13].

В результате в настоящее время имеется значительный объем работ по восприятию присяжными визуальных доказательств и дистанционных показаний.

В дополнение ко все более наглядному характеру доказательств изменился и способ представления. Ноутбуки и планшеты теперь часто используются в российских судах. Имеющиеся приложения для представления доказательств, такие, позволяют прокурорам и адвокатам использовать свои планшеты для «вывода» изображений на экраны, расположенные в зале суда. Это включает в себя стационарные экраны, которые отображают доказательства для присяжных, свидетелей или присутствующих лиц. Присяжные по большей части просматривают доказательства либо на больших экранах, установленных на стенах зала суда, либо на экранах меньшего размера, расположенных в ложе присяжных [4. С. 61].

Некоторые из этих доказательств также могут быть переданы присяжным, чтобы они взяли их с собой в совещательную комнату, либо на бумаге (обычно для письменных документов, таких как стенограммы или записи телефонных разговоров), либо, что чаще, на DVD (для видеодоказательств). В некоторых юрисдикциях планшеты были введены в совещательную комнату.

Действительно, по мере того как наша жизнь становится все более насыщенной технологиями, мы можем ожидать появления таких устройств в системе правосудия так же, как присяжные могут ожидать использования передовых технологий при представлении доказательств.

Внедрение новых технологий в процесс отправления правосудия может способствовать повышению эффективности и понимания в ходе судебного разбирательства, между этими принципами и принципом справедливости может сохраняться постоянное противоречие.

Неудивительно, что предоставление планшетов присяжным в уголовных делах вызывает аналогичные опасения. Например, в то время как присяжные заседателей могут отзывать доказательства или сокращать время обсуждения, некоторые присяжные заседатели могут оказаться в невыгодном положении, если они не знакомы с такой технологией, и, следовательно, могут отказаться от участия в обсуждениях.

Кроме того, использование технологий может привести к тому, что одним доказательствам будет придан чрезмерный вес по сравнению с другими. Если электронные доказательства исходят в основном от обвинения, эти проблемы могут поставить под угрозу право на справедливое судебное разбирательство. Перед тем как российским присяжным будут предоставлены планшеты для обсуждения, важно определить любые возможные предвзятые последствия с помощью тщательного эмпирического исследования [1. С. 75].

В этой статье описывается эксперимент, проведенный для изучения противоречия между продуктивностью и справедливостью, а также для проверки того, каким образом планшеты в зале присяжных формируют взаимодействие присяжных с доказательствами и их обсуждение. Это было достигнуто путем изучения методов, которые присяжные используют – как индивидуально, так и в составе коллективной группы – для допроса и обсуждения с использованием доказательств, представленных либо в цифровой, либо в печатной форме.

Влияние использования планшетов как на вердикты, так и на совещательный процесс было ключевым результатом, представляющим интерес на данном этапе. Мы также представляем предварительные выводы о том, как использование планшетов может повлиять на качество обсуждения.

Наглядные материалы в совещательной комнате. Право на справедливое судебное разбирательство считается одним из основных прав человека. Справедливость, или надлежащая правовая процедура, включает право на своевременное слушание дела беспристрастным судьей с возможностью противостоять своим обвинителям.

Несмотря на большое доверие к институту суда присяжных, информация, предоставляемая присяжным, тщательно регулируется для защиты прав обвиняемых и обеспечения того, чтобы присяжные выносили решение по делу только на основе доказательств, представленных в зале суда. Это означает, что присяжные не могут проводить независимые исследования с использованием внешних источников – это проблема, с которой сталкиваются современные присяжные заседатели, которые все больше привыкли к мгновенному доступу к Интернету и социальным сетям [6. С. 118].

Хотя традиционно присяжным запрещалось делать записи, если это отвлекало их от судебного разбирательства, исследования показали, что это эффективный метод, помогающий присяжным вспоминать события в совещательной комнате. По мере того, как доказательства, представляемые на судебных процессах, становятся все более сложными, опасения по поводу возможностей присяжных требуют дальнейшего изучения новаторских способов содействия принятию ими решений.

Для борьбы с проблемами и поощрения более информированных решений присяжных российские судьи, а также судьи в других странах общего права предоставляют присяжным дополнительную информацию, которую они могут взять с собой при обсуждении, включая стенограммы интервью и вещественные доказательства (такие как свидетельские показания, фотографии и видеоматериалы).

Для отдельных присяжных такие технологические средства могут активизировать их память и улучшить понимание и участие; для присяжных в целом они могут улучшить тщательность обсуждения; можно стимулировать хорошо

информированные и критические обсуждения и дебаты среди присяжных, избегать когнитивных упрощений и достигать более справедливых результатов.

Предоставление присяжным дополнительного общего цифрового дисплея, подключенного к отдельным планшетам, могло бы смягчить опасения по поводу ограниченного взаимодействия присяжных и позволить присяжным как коллективу стать «информационным процессором» или смыслообразующей единицей.

В такой конфигурации планшеты могли бы служить «площадкой для действий», позволяя отдельным присяжным извлекать необходимую информацию из предоставленных доказательств, а общий экран мог бы стать «пространством для размышлений», позволяя коллективу выявлять закономерности и проверять заявления. Действительно, нет недостатка в других типах «сред с несколькими поверхностями», от доски, управляемой одним пользователем до нескольких, или интерактивных многопользовательских столешниц, и каждый из них может предлагать разные возможности или поддерживать разные уровни доступности и сотрудничество для тех, кто не знаком с технологиями, и тех, у кого больше опыта [9. С. 57].

Тем не менее аргументы против передачи определенных цифровых доказательств в руки присяжных остаются убедительными. Например, если мощные или графические образы могут повлиять на вердикт, то легкодоступные цифровые изображения, позволяющие быстро увеличивать и уменьшать масштаб, могут усугубить эту проблему. Даже с внедрением технологий в совещательную комнату судья по-прежнему будет играть роль привратника в отношении эмоциональных образов.

Кроме того, по сравнению с использованием бумажной информации и доказательств табличка может отвлекать внимание присяжных от группы. Это, в свою очередь, может подорвать качество принимаемых коллективом решений из-за уменьшения учета альтернативных точек зрения, выдвинутых другими членами суда присяжных.

Введение планшетов в совещательную комнату может также более тонким образом изменить динамику совещаний присяжных. Некоторые исследования, проведенные в учебных заведениях и на деловых встречах, показывают, что мы умеем справляться с несколькими задачами, умеем пользоваться мобильными устройствами и одновременно с легкостью участвовать в других беседах. Другие исследования показывают, что использование учащимися портативных устройств может привести к менее активному вовлечению и участию. Можно утверждать, что эту проблему можно было бы смягчить путем введения общего показа, требующего от присяжных сотрудничества и совместного участия в предоставленном им материале.

Это поднимает вопросы о том, как изображения, распространяемые с помощью цифровых технологий, повлияют на ритуальную динамику обсуждения присяжных. Изображения, представленные в суде, «не говорят сами за себя. Скорее, они связаны со словами, с историей, которая строится свидетелями, обвиняемыми и адвокатами через повествование о судебном процессе. Хотя присяжные также принимают участие в процессе повествования, способы, которыми

образы и размышления объединяются, когда присяжные совместно конструируют нарративы, еще глубоко не исследованы» [15. С. 172].

Например, предположим, что визуальные дисплеи в зале суда дают нам ощущение общности и общей цели, поскольку они: обеспечивают общую перцептивную и концептуальную основу между исследователями фактов и свидетелями, а также между самими исследователями. Это осязаемые и общедоступные репрезентации реальности, которые позволяют лицам, принимающим решения, иметь единую основу для суждения и уверенность в том, что суждение исходит из этого визуально заметного, общедоступного объекта.

Хотя за этим общим восприятием может скрываться «феноменологическая изменчивость восприятия людьми того, что они видят на экране, а также то, как они по-разному используют увиденное для принятия решений», это феноменологическое расхождение может быть выявлено после просмотра экранов. Далее необходимо переместиться в комнату для совещаний, где изображения можно оспаривать, подвергать сомнению и переосмысливать в ходе обсуждения.

В конечном счете, конфигурация технологий, скорее всего, сформирует и изменит то, как присяжные думают об уликах и обсуждают их. Будут ли эти изменения означать, что групповые процессы пострадают, когда отдельные присяжные уткнутся в собственные планшеты? Будут ли присяжные «соблазнены» их экранами? Нарушит ли использование планшетов право обвиняемых на справедливое судебное разбирательство?

Участниками исследования были 152 члена сообщества, выбранные из пула присяжных, которые были освобождены от службы в день исследования или иным образом вызвались участвовать (75 женщин, 77 мужчин). Средний возраст составлял 44,7 года (SD = 15,1 года), а возраст колебался от от 18 до 80 лет. Подавляющее большинство (92,1 %) выборки ранее не входили в состав присяжных. Две трети выборки имели высшее образование в той или иной форме: 40,8 % участников имели степень бакалавра, а 23 % – аспирантура. Еще 30,3 % имели среднюю школу как высший уровень образования, а 5,9 % выборки закончили формальное образование после начальной школы. Характеристики выборки в целом соответствовали характеристикам населения России: 50,2 % женщин, 24,7 % с университетским образованием и 20 % закончившие среднюю школу, хотя фиктивная выборка присяжных имела несколько более высокий уровень образования [2. С. 19].

План представлял собой смешанный план 2 (условие доказательства) на 2 (обсуждение), участники распределялись для получения доказательств через iPad или на бумаге (условие доказательства) и выносили свои вердикты до и после группового обсуждения (обсуждение). Последний фактор был внутрисубъектным. Все участники одной и той же сессии тестирования были отнесены к одному и тому же условию доказательства, и каждая группа присяжных состояла из восьми-двенадцати участников.

Пробное моделирование. Участники просмотрели 60-минутное видео имитации уголовного процесса, на котором подсудимому было предъявлено обвинение в сговоре с целью совершения террористического акта. Судебный процесс, хотя и гипотетический и разыгрывался актерами, был очень тесно связан с двумя реальными уголовными процессами и подтвержден в процессе консультаций

с судьями и адвокатами, чтобы сценарий был максимально реалистичным. По сценарию террористического заговора обвиняемым было предъявлено обвинение в получении материалов для бомбы, которая должна была быть взорвана в кинотеатре. Как и в реальных судебных процессах, на которых основывался сценарий, версия обвинения основывалась на косвенных доказательствах. Чтобы стимулировать обсуждение, представленные доказательства были разработаны на этапе предварительной проверки, чтобы обеспечить 50-процентный уровень обвинительных приговоров [7. С. 232].

Основные элементы доказательств. Доказательства обвинения были представлены либо на бумаге, либо на iPad. Доказательства были предоставлены по каждому из основных элементов обвинения, таких как хранение подсудимым большого количества различных химических веществ и его антизападная идеология. Изображения взяты из общедоступных архивов. Примеры используемых изображений включали политические листовки, написанные на арабском и английском языках, скриншоты обезглавливания, изображения различных химикатов, предположительно найденных в гараже ответчика, и отмеченные карты кинотеатров, которые предположительно были целями предполагаемой террористической атаки. Также были включены стенограммы предполагаемых телефонных разговоров и стенограмма некоторых показаний одного свидетеля обвинения. Всего присяжным было предоставлено для рассмотрения 50 доказательств [12. С. 31].

Анкета для предварительного обсуждения. После просмотра видео присяжные прошли первичный опрос, чтобы зафиксировать свой индивидуальный вердикт: виновен или невиновен. Участников также спрашивали, насколько они уверены в своем решении, по шкале от 0 % – совсем не уверен, до 100 % – полностью уверен. Их также спрашивали, насколько вероятно, что подсудимый совершил каждый из аспектов предполагаемого преступления, от 1 (совсем маловероятно) до 7 (весьма вероятно). Эти аспекты включали в себя, заключал ли ответчик соглашение с другими лицами для осуществления незаконной деятельности, заключал ли он соглашение о закладке бомбы, предпринимал ли какие-либо действия для выполнения плана и имел ли план террористическую цель (a = . 94). Вместе эти три меры вердикта были разработаны не только для оценки результатов судебного разбирательства на основе вердикта, но и для выявления тонких различий в восприятии участниками дела.

Групповое обсуждение. Затем группам присяжных были предоставлены 50 изображений, которые представляли доказательства обвинения. Каждой группе было предложено обсудить одно из двух условий: традиционное бумажное условие, включающее доказательства на печатных копиях в отдельных папках с оглавлением (повторяя текущую процедуру в Виктории), или планшетное условие, включающее просмотр тех же доказательств на отдельном iPad (экран стандартного размера со складной подставкой) с изображениями, отображаемыми через Dropbox, включая список всех изображений на полях в левой части экрана и выбранное изображение на остальной части экрана. У этого второго условия было дополнительное измерение: все iPad были связаны через Apple iOS интерфейс

совместного использования экрана через Apple TV на общий 42-дюймовый экран, расположенный на одной стороне комнаты [3. С. 258].

Цель технологии совместного использования состояла в том, чтобы позволить участникам отразить определенное изображение, которое они просматривали на своем индивидуальном iPad, на большом экране, чтобы группа могла видеть и использовать в своем обсуждении. Он был задуман как дополнительная технология, которая могла бы повысить сплоченность группы и свести к минимуму вероятность того, что люди потеряют себя в своих индивидуальных экранах и пренебрегут необходимым групповым процессом.

Анкета после обсуждения. Окончательная анкета включала те же три показателя оценки индивидуальных взглядов присяжных на вердикт, что и анкета до обсуждения. Мера из пяти пунктов, оценивающая вероятность того, что различные элементы правонарушения имели место, сформировала надежную шкалу. Эта анкета также оценивала вердикт группы по дихотомическому пункту: виновен, не виновен [10. С. 35].

Полученные результаты. Предварительные анализы. Мы также оценили возможное влияние предпочтений при просмотре телепередач на вердикты участников из-за различий в ожиданиях в отношении цифровых доказательств.

Участники не тратили много времени на просмотр программ, посвященных исследованию места преступления, общих криминальных программ или других реалити-шоу, при этом около половины выборки вообще не смотрели ни одну из этих программ.

Динамика обсуждения. Хотя детальный качественный анализ качества взаимодействия присяжных еще предстоит провести, можно сделать некоторые первоначальные комментарии относительно последствий для политики о том, как участники в различных условиях связаны друг с другом. В обоих случаях присяжные поддерживали хороший зрительный контакт друг с другом и участвовали в оживленных дебатах. Обе группы тратили от одной до десяти минут в начале каждого обсуждения, тихо погрузившись в свои книги доказательств/ iPad [14. С. 63].

Группа использовавшая планшеты, быстрее перешла к обсуждению, в то время как группа, работавшая с бумагой, дольше перелистывала страницы. Однако, как только они начинали говорить, те, у кого были доказательства на бумаге, проводили больше времени, глядя друг на друга, и меньше времени, перемещаясь взад и вперед по своим папкам. Это может быть связано с трудностью перемещения по громоздкой папке. Имея список всех изображений слева от экрана iPad – каждое пронумерованное и с названием – присяжные в этом состоянии могли легко найти изображение, которое они хотели просмотреть. Вполне вероятно, что из-за этого легко, присяжные в состоянии планшета продолжали пролистывать свои изображения, в то время как сложность перемещения по бумажным папкам делала присяжных более привлекательными, чтобы смотреть прямо друг на друга и не просматривать свои изображения. В отзывах в конце каждой сессии присяжные в бумажном состоянии предположили, что перемещение по папкам было медленным и что иногда они не могли найти изображения, которые искали. Напротив,

присяжные заседатели в условиях планшета постоянно отмечали скорость и легкость перемещения по изображениям [5. С. 119].

Казалось, не было различий между условиями «цивилизованности» совещательного процесса. В обоих случаях участники относились друг к другу с уважением и прислушивались к тому, что говорили другие (характер взаимодействия измерялся; результаты выходят за рамки этой статьи). Присяжные заседатели, работавшие с iPad, как правило, просматривали изображения на своих устройствах и редко использовали предоставленный «экран для совместного использования». На сеансах обратной связи некоторые участники отметили, что совместное использование экрана было «пустой тратой времени», когда все они могли легко вывести изображение на свои собственные экраны. Однако в большинстве случаев один или два присяжных в iPad условие использовало бы экран, чтобы привлечь внимание других присяжных к конкретному доказательству. В целом обсуждение было успешным проектом по укреплению солидарности для обеих групп, что согласуется с другими исследованиями динамики обсуждения. Далее в процессе обсуждения обе группы меньше смотрели на доказательства и больше друг на друга, предполагая, что они быстро перешли от пассивных получателей к активным создателям общей истории [8. С. 434].

Обсуждение. С точки зрения как результата обсуждения (вынесенного вердикта), так и качества обсуждения (характера самих взаимодействий) существенных различий между условиями бумаги и планшета, по-видимому, нет. То есть использование планшетов для просмотра цифровых доказательств не отвлекает от совещательного процесса, не наносит ущерба присяжным и не ставит под угрозу право обвиняемого на справедливое судебное разбирательство.

Учитывая возможную экономию времени и ресурсов, связанных с использованием доказательств в цифровой форме, ожидается, что мобильные устройства станут обычным элементом среды зала суда не только для юристов, но и для присяжных. Исследование, представленное в этой статье, предполагает, что мобильные технологии также могут быть надлежащим образом распространены на совещательную комнату. В качестве ключевых лиц, принимающих решения в уголовных процессах (по крайней мере, в гражданских процессах), присяжным все чаще будут давать планшеты как для просмотра доказательств в суде, так и для последующего ознакомления с ними в совещательной комнате. Это исследование показало, что iPad прост в использовании и упрощает задачу поиска информации даже для тех присяжных заседателей с ограниченным опытом использования компьютера или без него. Необходимо проверить, относится ли этот вывод в равной степени к другим планшетам.

С точки зрения затрат, экономия, достигнутая с помощью iPad, включает в себя отсутствие необходимости размещать маленькие экраны в ложе присяжных в каждом зале суда присяжных, часы рабочего времени сотрудников, копирующие документы, и потенциальное сокращение времени обсуждения. Однако, хотя из этого исследования может показаться, что нет никаких препятствий для массового использования iPad для совещаний присяжных, следует отметить ряд предостережений.

Во-первых, в исследовании есть предположение, что iPad может побудить присяжных уделять больше внимания доказательствам, которые они получают в цифровой форме, а не устным доказательствам, которые можно получить только с помощью протоколов судебных заседаний.

Второй, и, тесно связанный с этим, такой легкий доступ к досье может помочь присяжным отказаться от интерпретации, которая возникает в результате обмена мнениями в зале суда на главном допросе и перекрестном допросе, чтобы сформировать свою собственную интерпретацию научных диаграмм и других компьютерные представления, а не интерпретация, возникающая в результате словесного обмена во время допроса и перекрестного допроса.

Например, присяжные могли бы, таким образом, взять на себя роль арбитра научных доказательств, решая, действительно ли отпечаток пальца принадлежал этому человеку или образец крови на полу был взят из этого конкретного оружия. С легким доступом к изображениям на iPad, существует реальная опасность того, что присяжных даст свою интерпретацию не только фотографий, но и научных диаграмм. Это, однако, оценочная задача, которая открыта для всех присяжных, независимо от формы, в которой представлены доказательства. Наконец, есть более практичные аспекты наличия большого количества доступных планшетов, что может быть непомерно дорогим, а также время и усилия, необходимые для их обновления по мере выпуска нового программного обеспечения.

Ободренные удобством использования iPad вместо громоздких папок, присяжные могут все чаще запрашивать больше доказательств в цифровой форме. Судьи, не желающие сдерживать энтузиазм присяжных, могут согласиться. Это могло бы позволить присяжным провести то, что можно было бы считать формой второго судебного разбирательства, (по-видимому) полностью оснащенного всей информацией в цифровой форме. В той мере, в какой этот подход отражает обычные процессы взвешивания доказательств в совещательной группе, такая процедура вполне уместна. Но также возможно, что присяжные по общему праву, которым поручено проверить силу обвинения, постепенно перейдут к своему коллеге по гражданскому праву, ответственному за установление истины. Хотя это только предположения, возможности и опасности, связанные с более широким использованием iPad, требуют дальнейших исследований.

Следует отметить, что это исследование было ограничено одним типом дел, связанных с террористическим заговором, с косвенными уликами. Другие типы случаев могут привести к другим результатам. Например, дела, основанные на (заведомо ненадежных) показаниях свидетелей, могут решаться присяжными, которые «решают для себя», соответствует ли нечеткое изображение с камер наблюдения человеку на скамье подсудимых. Кроме того, это исследование было ограничено одним (правда, большим) составом присяжных. Вполне возможно, что присяжные в этом исследовании были более космополитичными или более скептичными, чем аналогичные присяжные заседатели в других юрисдикциях или в региональных или сельских районах.

Экспериментальный метод из соображений экономии не имел полностью сбалансированной схемы, при этом одна экспериментальная группа не подвергалась

предварительному опросу. Используемый здесь упрощенный план не учитывает возможные эффекты обучения между двумя опросами.

Российские суды уже быстро переходят к более широкому использованию цифровых доказательств, поэтому кажется неизбежным, что большие, громоздкие папки будут заменены тонкими планшетами как за барным столом, так и в зале заседаний присяжных. Хотя это предварительные выводы, и будет проведен дальнейший анализ, чтобы понять нюансы, лежащие в основе этих заголовков, они должны дать определенный уровень уверенности тем в судах, которые хотят расширить использование мобильных технологий за пределы зала суда в зал присяжных. Исследование подтверждает, что технология работает (при правильном управлении), проходит порог удовлетворенности пользователей и не имеет явных недостатков.

Следующим этапом после завершения всех анализов является разработка рекомендаций, которые помогут судам внедрить планшетные технологии. Есть надежда, что это исследование поможет максимально облегчить этот переход.

Список литературы

1. Арнаут Д. А. Цифровизация правосудия и эффективность новых судов // М.: Общество с ограниченной ответственностью «Интернаука», 2020. С. 73–78.

2. Бурдина Е. В. Новые организационные формы работы судов в условиях их цифровизации // Российское правосудие. 2020. № 10. С. 15–25.

3. Бурдина Е. В. Цифровизация судов и справедливость судебного разбирательства: в поисках баланса. Екатеринбург: Уральский государственный юридический университет, 2021. С. 253–260.

4. Гришина Е. Б. Проблемы осуществления правосудия судом присяжных и тенденции развития суда присяжных в России // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2020. № 3(84). С. 59–64.

5. Гусейнова Г. М. Актуальные проблемы суда присяжных в России // Закон и право. 2019. № 4. С. 115–126.

6. Лаврентьев А. Р., Леваневская Е. А. , Сохоян А. Р. Цифровизация в деятельности судов в современной России. Н. Новгород: Издательство «Автор», 2022. С. 113–121.

7. Рясов А. А. Вопросы деятельности суда присяжных с учетом последних изменений законодательства. Пермь: Пермский институт Федеральной службы исполнения наказаний, 2019. С. 231–233.

8. Сабиров Д. Р. Суд присяжных в районных судах: анализ и первые итоги // Ижевск: Удмуртский государственный университет, 2021. С. 431–435.

9. Салихова М. А., Ерин М. А. Проблемы и перспективы внедрения цифровизации в деятельность судов общей юрисдикции в рамках уголовного судопроизводства. Донецк: Цифровая типография, 2022. С. 53–61.

10. Сарсембаев М. А. Национальные суды и суд ЕАЭС: проблемы цифровизации. М.: Проспект, 2019. С. 32–36.

11. Середа О. В. К вопросу о цифровизации уголовного судопроизводства районных судов. Красноярск: Красноярский государственный аграрный университет, 2022. С. 241–243.

12. Филимонов А. Д. Модернизированный суд присяжных: перспективы, проблемы и пути решения // ExLegis: правовые исследования. 2022. № 3. С. 28–34.
13. Цифровизация правоприменения: поиск новых решений: монография / отв. ред. Д. А. Пашенцев. М.: Инфотропик Медиа, 2022.
14. Юлдашев Ш. Приоритетные направления цифровизации деятельности судов // Гражданское общество. 2020. Т. 19, № 3(63). С. 62–64.
15. Ягибекова З. А. К вопросу о роли суда в условиях цифровизации правосудия // Закон и право. 2023. № 5. С. 171–173.

О. М. Стешина,
магистрант,
Национальный исследовательский Нижегородский государственный университет имени Н. И. Лобачевского

БЕЗУСЛОВНЫЙ БАЗОВЫЙ ДОХОД: КОНЦЕПЦИЯ И ЕЕ РЕАЛИЗАЦИЯ

Аннотация. Современный этап развития технологий и цифровизации выявил проблемы в сфере занятости и социального обеспечения, позволяющие обратиться к теме безусловного базового дохода, которая ранее поднималась в XX веке. В настоящее время получают развитие различные направления этой концепции, как классические, так и экспериментальные. В статье обобщаются представления о безусловном базовом доходе и выясняется применимость этого института к российской правовой системе.

Ключевые слова: право, цифровизация, безусловный базовый доход, система социального обеспечения, пилотный проект, трансформация занятости, безработица

UNCONDITIONAL BASIC INCOME: THE CONCEPT AND ITS IMPLEMENTATION

Abstract. The current stage of technology development and digitalization has revealed problems in the field of employment and social welfare, allowing us to address the topic of unconditional basic income, which was previously raised in the XX century. Currently, various directions of this concept are being developed, both classical and experimental. This work is aimed at generalizing the idea of unconditional basic income and clarifying the applicability of this institution to the Russian legal system.

Keywords: law, digitalization, unconditional basic income, welfare system, pilot project, transformation of employment, unemployment

Введение. Развитие трудовых отношений, а вместе с ними и трудового права создало основу для формирования права социального обеспечения, и в настоящее время на основе конструкции трудовых отношений формируются системы социальной защиты. Вместе в тем в связи с трансформацией занятости происходит отход

от традиционной модели трудовых отношений, основанных на преимущественно бессрочном трудовом договоре, организации работодателем процесса трудовой деятельности в соответствии с трудовым законодательством, локальными актами, трудовым договором, а также четко установленной системе социальных гарантий, предоставляемых работникам. Эти отношения заменяются неустойчивыми формами взаимодействия, которые не могут быть отнесены к гражданско-правовым, и в то же время не создают для работника полный комплекс трудо-правовых гарантий. Ярким примером такого рода отношений является платформенная занятость, обусловленная возможностями по поиску исполнителей с помощью цифровых платформ-агрегаторов и их дальнейшим взаимодействием с заказчиком в виде получения заданий и оплаты по мере их исполнения.

В связи с неустойчивым характером и слабой социальной гарантированностью нетипичных форм занятости, возникает потребность в трансформации системы социального обеспечения. В качестве одного из способов ее преобразования может быть рассмотрен безусловный базовый доход (далее – ББД), который должен выступить как одно из средств обеспечения достойного существования (поскольку не предполагает отказа от социальных услуг или бесплатной медицинской помощи), своеобразной страховкой каждого члена общества от безработицы, риск которой значительно увеличился с развитием технологий.

Основная часть. В настоящее время сформировалось классическое определение безусловного базового дохода, предложенное в рамках «Всемирной сети базового дохода». Многими исследователями оно используется в качестве основного, когда речь идет о практических аспектах его реализации. Формулируется определение следующим образом: «безусловным базовым доходом являются периодические денежные выплаты, предоставляемые всем на индивидуальной основе без каких-либо условий» [9]. В данной работе определение, данное «Всемирной сетью базового дохода», использовано в качестве основного.

Исходя из предложенного определения, можно выделить следующие признаки ББД:

1. **Периодичность (регулярность) выплаты.** Выплаты, которые составят базовый доход, предполагаются не разовыми, а разбитыми на части и выплачиваемыми в течение определенного периода времени (предположительно, продолжительности жизни получателя). Поскольку классическое определение не содержит требования постоянного размера выплат, их периодический характер позволит производить своевременную индексацию, а также корректировать размеры выплат в зависимости от размера государственных доходов, из которых должно осуществляться финансирование этой программы. Кроме того, регулярные выплаты направлены на обеспечение базовых потребностей любого гражданина, независимо от его собственной экономической грамотности. Период выплат, как правило, определяется как один месяц, однако само определение такого указания не содержит. Так, в американском штате Аляска выплаты производятся ежегодно, что не мешает считать эту систему единственным случаем действительной реализации принципов ББД [8].

2. **Денежный характер.** Выплаты должны производиться в форме, позволяющей получателю самостоятельно распоряжаться ими для приобретения

необходимых материальных благ в индивидуальном порядке. Такое положение может обеспечить денежная форма в отличие от натуральной формы или обеспечения правами на набор товаров или услуг.

3. **Индивидуальная основа.** Данный признак указывает на то, что выплаты предоставляются каждому лицу в отдельности, а не в составе домохозяйства или иного объединения граждан. Задача введения ББД заключается в том, чтобы обеспечить каждого минимальным уровнем ресурсов, необходимых для сглаживания социальных противоречий и обеспечения личной свободы дееспособных граждан. Вместе с тем распределение дохода через объединения создают риски концентрации ресурсов в руках их руководителей и укреплению зависимого положения их членов.

4. **Универсальность.** Поскольку понятия универсального базового дохода и безусловного базового дохода обычно не разделяются, ББД при описании характеризуется универсальностью. Однако данный термин в различных интерпретациях имеет разное содержание. Так, в изложении Е. С. Садовой [6. С. 68] универсальность означает предоставление выплат независимо от размера иных доходов. С точки зрения В. Н. Бобкова и Е. В. Одинцовой [7. С. 9], данный признак рассматривается как предназначенность для всех членов сообщества. Ю. Д. Квашнин [2. С. 174] представляет универсальность как равенство размера дохода для всех получателей. В целом на основании изложенного можно обозначить критерий универсальности комплексно – как совокупность всеохватности и равномерности распределения.

Критерий универсальности не является однозначным. Так, при анализе существующей практики авторы используют термин «безусловный базовый доход» в том числе применительно к программам, охватывающим только отдельные группы населения. Следует учитывать, что данные обстоятельства порождаются в первую очередь экспериментальным характером большинства реально существующих на практике систем ББД и отсутствием материальных ресурсов для его полномасштабной реализации. Вместе с тем и в данной ситуации сохраняют свое значение отдельные аспекты универсальности, такие как выплаты независимо от размера иных доходов или одинаковый размер дохода для всех получателей. В экспериментальных условиях эти критерии – важный показатель, позволяющий отследить эффект, оказываемый на поведение конкретного человека, которому выплаты предназначены, и позиции группы получателей в целом по сравнению с лицами аналогичного социального положения, таких выплат не получающих.

5. **Безусловность.** Получение соответствующих выплат предписывается не связывать с занятостью, уровнем доходов или иными обстоятельствами. Этот критерий выступает гарантией критерия универсальности, наиболее расширяя круг субъектов, имеющих доступ к базовому доходу. С другой стороны, безусловность можно рассматривать и в административно-правовом аспекте. Возникновение права на ББД не должно требовать соблюдения получателем каких-либо специально для этого предназначенных административных процедур, порядок их назначения должен быть автоматическим [4. С. 82].

Вместе с тем классическое определение не содержит критерия, позволяющего ограничить круг получателей ББД на территории конкретной страны,

т. е. не установлены пределы универсальности по кругу лиц. Поскольку в настоящее время еще не сформировалась жизнеспособная модель базового дохода, действующая на всей территории определенного государства, можно говорить о том, что соответствующий критерий оставлен на усмотрение конкретного государства. Вместе с тем в связи с активными современными миграционными процессами требуется четко ограничить круг управомоченных субъектов. В данном случае требуется комплексный критерий, например, такой как одновременное наличие гражданства государства, в котором производятся выплаты, и определенное время проживания на соответствующей территории.

Кроме того, следует отметить, что одной из задач, которая преследуется введением ББД, является сокращение числа иных денежных мер социального обеспечения (вплоть до сведения всех таких мер к одному базовому доходу), и, соответственно, сокращение расходов на их администрирование.

Таким образом, безусловный базовый доход вместо адресной поддержки уязвимых категорий населения, осуществляемой на основе свободы реализации своих прав, предполагает автоматические выплаты денежных средств всем членам общества, в том числе и тем его категориям, которые в трудовых отношениях традиционного типа не считаются уязвимыми. Эта концепция отходит от принципов связи обеспечения с трудовой деятельностью, приоритета в обеспечении некоторых категорий граждан [5. С. 47], характерных для существующей модели социального обеспечения. Взамен ББД позволяет его получателям в полной мере свободно распоряжаться своими способностями к труду и реализовывать свободу предпринимательской деятельности, не будучи стесненными необходимостью финансово обеспечивать свое выживание.

С другой стороны, доход, который предназначен для каждого гражданина вне зависимости от каких-либо условий, должен являться гарантией принципа свободы труда, а также гарантией права работника на самозащиту рудовых прав, наиболее актуальную для нетипичных форм занятости. Этот институт, в том виде, в котором разрабатывается теоретически, предполагает покрытие за счет выплат базовых потребностей человека, что снижает для него риски, связанные с безработицей, и тем самым предоставляет большую фактическую свободу в защите своих трудовых прав.

Оценить актуальность концепции ББД можно, рассмотрев популярные в реализации модели, в каждую из которых в целом вписывается данное выше определение и выводимые из него признаки базового дохода.

Исходя из мировой практики, существует реальная необходимость первоначального введения экспериментальной модели ББД, которая позволила бы на основе исследования экспериментальных и контрольных групп оценить соотношение затрат и экономически полезных изменений и в конечном итоге определить целесообразность установления базового дохода. Для этого можно рассмотреть существующую практику экспериментов в данной сфере. Отметим, что оценить модели экспериментов можно по следующим критериям:

1) с точки зрения охвата получателей во времени, пространстве и по кругу лиц;

2) с точки зрения источника формирования;

3) с точки зрения взаимодействия с другими схемами социальной помощи, действующими в государстве.

Можно выделить модели, основанные на различных принципах:

1. **Универсальный базовый доход (принцип универсальности).** Такая модель реализована в штате Аляска в США и имеет следующие характеристики: 1) получателями выплаты являются лица, прожившие в штате не менее 6 месяцев и имеющие намерение проживать там и далее; 2) источником финансирования программы является роялти от государственных нефтяных доходов, а средством распределения – Постоянный фонд Аляски, аккумулирующий не менее 25 % соответствующих доходов и ежегодно распределяющий определенную их часть в виде выплат населению; 3) выплаты осуществляются ежегодно; 4) ББД не заменяет существующие социальные гарантии, 5) хотя и имеет более социально ориентированную направленность. Эффектом введения такого дохода является снижение неравенства в обществе и сокращение оттока населения. Данная модель основана на ресурсной экономике, которая хотя и по-прежнему актуальна, но зависит от невозобновляемого источника. Кроме того, доход от ресурса распределяется среди жителей территории, на которой происходит его добыча. Таким образом, данная модель позволяет организовать базовый доход в достаточно небольшом и относительно обособленном обществе. Однако отсутствие реально существующих примеров реализации подобной модели на общегосударственном уровне не позволяет считать эту модель актуальной для построения модели базового дохода в России, поскольку состав общегосударственных доходов и расходов по составу не совпадают с доходами и расходами отдельного штата.

Это подтверждает и практика реализации концепции ББД в Монголии в период с 2010 по 2012 гг. Первоначально предполагалось, что финансирование программы будет осуществляться за счет доходов от природных ресурсов. Вместе с тем, исходя из практики его реализации, недостаточность финансов послужила основным условием прекращения программы. Это подтверждает ограниченность возможности применения ресурсных доходов как основы базового дохода в государстве в целом. Вместе с тем на территории Монголии действует и другая программа – населению переданы акции горнодобывающей компании, которые могут находиться во владении гражданина для получения дивидендов или могут быть проданы обратно государству. Отличие от предыдущего варианта состоит в том, что перераспределение осуществляется неравномерно, в том числе за счет неравных доходов лиц, осуществивших продажу акций и лиц, имеющих право на дивиденды, а также такой вариант предполагает возможность акционеров получать информацию о результатах деятельности соответствующей компании, делая ее более прозрачной.

Таким образом, для эксперимента, предусматривающего большой охват получателей ББД в России, целесообразно обратить внимание на возможность перераспределения доходов от продажи полезных ископаемых путем создания фонда для распределения или всеобщего распространения акций. Однако, как показывает практика, следует предусмотреть дополнительный источник финансирования.

2. **Модель, основанная на принципах социальной справедливости и социальной защиты.** Эта модель предполагает ограничение круга адресатов выплат только лицами, которых государство считает наиболее нуждающимися в дополнительной помощи. В строгом смысле слова такие выплаты не являются ББД, но позволяют экспериментально смоделировать последствия его введения для социальных групп, чье положение в случае внедрения базового дохода изменится (предположительно, улучшится) наиболее значительно.

Примером такого рода может служить практика Финляндии, на территории которой проводился эксперимент по реализации концепции ББД в период с 2017 по 2018 год в виде выплаты гарантированного дохода в размере 560 евро [1. С. 50]. Данный эксперимент имеет следующие характеристики: 1) круг получателей ограничен отобранными с помощью жеребьевки 2 000 человек, имеющих статус безработных и малоимущих в возрасте от 25 до 58 лет; 2) базовый доход заменяет пособие по безработице; 3) финансирование осуществлялось за счет бюджетных ассигнований. Показательны результаты эксперимента – вместо стимулирования занятости имело место повышение требований получателей пособия к предлагаемым рабочим местам за счет повышения уверенности этих лиц. Таким образом, данные могут быть использованы при разработке новой модели социальных гарантий работникам, которая будет рассмотрена ниже.

Оригинальная модель предложена в Ирландии под названием «Базовый доход для искусства» [10]. Она содержит сразу несколько особенностей: 1) получатели определяются по признаку принадлежности к творческим профессиям, предполагающим проектную организацию деятельности, и, как следствие, непостоянную занятость и непостоянный заработок; 2) заявительный порядок получения выплат; 3) получение выплат влияет на доступ к иным мерам социальной поддержки, кроме того 4) выплаты учитываются для целей подоходного налога, а их назначение предполагает необходимость получения статуса самозанятого. Несмотря на специфическую сферу применения, принципиальная основа данной модели может послужить исходной точкой моделирования базового дохода для иных лиц с неустойчивой занятостью. В данном случае целесообразно рассмотреть такие положения, как учет выплат для получения иных мер социальной поддержки и корректировки системы налогообложения, применяемой в отношении получателя. Очевидно, развитие данного института следует развивать на стыке права социального обеспечения как средства социальной защиты уязвимой группы населения и трудового права, т. е. особенности базового дохода должны учитываться при установлении правового регулирования нетипичных форм занятости.

Можно отметить и еще одну возможную разновидность базового дохода, появившуюся в результате пандемии COVID-19: **доход, который можно назвать «экстренным»** [3. С. 17]. В строгом смысле эта модель не является ББД, поскольку имеет временный характер и приведение ее в действие обусловлено возникновением ситуации пандемии. Особенностью этой модели является ограниченный во времени характер выплат – они осуществляются в период тяжелой экономической ситуации, вызванной пандемией, в результате которой имела место объективная невозможность работников осуществлять свои трудовые функции и, как следствие,

самостоятельно себя обеспечивать. Такой характер выплат позволяет достичь универсальности как критерия ББД. Кроме того, называются и такие моменты, как направленность на поддержку человека вместо поддержки бизнеса, неспособного к самоокупаемости, способствующую формированию более устойчивой экономики по окончании кризисных явлений. Конкретные способы практической реализации могут быть различными: предоставление всем получателям равных сумм (Япония), различный размер выплат в зависимости от размера домохозяйств (Республика Корея) или в зависимости от материального положения получателя (Сингапур).

Вместе с тем, в литературе отмечается, что такая модель может спровоцировать отказ получателей от труда при наличии соответствующих выплат на период проблемной ситуации. Также возможны осложнения при прекращении выплат по окончании ситуации, потребовавшей введения дополнительных мер защиты [3. С. 17]. Однако, представляется, что четко определенные законом условия применения базового дохода и однозначно установленный его временный характер могли бы способствовать преодолению этого недостатка. Несмотря на то, что подобная схема вызвана конкретной ситуацией распространения COVID-19 [12], данная модель может получить отражение в законодательстве о чрезвычайном положении в конкретно определенных случаях. В связи с этим целесообразно рассмотреть возможность введения ББД в число мер, применяемых при введении чрезвычайного положения. Условиями его приведения в действие могут быть объективная невозможность исполнения трудовой функции определенной долей населения на соответствующей территории и отсутствие у этой группы населения в связи с этим средств к существованию. Исключение могут составлять группы работников, заработная плата которых выплачивается за счет средств соответствующего бюджета. Следует отметить, что для применения такой меры целесообразным было бы формирование специального фонда. В качестве источника его формирования может быть рассмотрена рента от добычи полезных ископаемых, поскольку размер фондов может быть постоянным во времени, а приведение его в действие не предполагается регулярным.

Кроме моделей, уже реализованных на практике, можно отметить еще несколько концепций, которые еще не получили практической реализации. Среди них можно выделить следующие:

1. **ББД как средство смягчения технологической безработицы, создания системы социальных гарантий работнику в новых условиях труда.** В частности, формирующаяся в настоящее время платформенная экономика не предоставляет гражданам ни постоянных рабочих мест, ни социальных гарантий, свойственных традиционной модели занятости [6. С. 63]. Владельцы платформ, по своему статусу приближенные к агрегаторам, не всегда осуществляют социальное страхование работника, а отсутствие постоянного коллектива негативно сказывается на профсоюзном объединении. В этом случае базовый доход призван обеспечить страховку работника от социальных рисков и, с другой стороны, позволить ему выбирать из предложенных условий труда наиболее приемлемые (что подтверждается результатами рассмотренного выше финляндского эксперимента). Кроме того, характер ББД позволяет обеспечить нормальное существование

человека на период приспособления к изменившемуся характеру трудовых отношений: переподготовки, организации предпринимательской деятельности и др.

Если принять во внимание указанные характеристики, данная концепция близка к ирландскому эксперименту. В качестве характеристики экспериментальной модели можно предложить следующие положения: 1) получателями могут быть определены граждане, имеющие нестандартную форму занятости (не урегулированную ТК РФ либо прямо определенную как платформенная занятость); 2) заявительный порядок получения выплат, поскольку самостоятельное отслеживание данной категории потребует сложных процедур; 3) выплаты могут заменить иные меры социальной поддержки денежного характера, направленные на поддержку безработных и малоимущих.

Конституция РФ имеет положения, которые можно рассматривать как основу для введения базового дохода различных объемов. Так, для ББД в собственном смысле основой может служить ч. 1 ст. 7, определяющая РФ как социальное государство, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека, а также ч. 1 ст. 37, согласно которой труд свободен и каждый имеет право свободно распоряжаться своими способностями к труду, выбирать род деятельности и профессию. Таким образом, Конституция РФ имеет правовую основу для введения ББД как средства преодоления последствий технологической безработицы и новых социальных гарантий в условиях информатизации производства.

Представляется правильным развивать нормативное регулирование ББД данной модели вместе с правовым регулированием занятости и защиты от безработицы, поскольку для данной модели эти институты являются взаимсвязанными. Нормативный акт (закон) в данной сфере должен соответствовать принципам закона о занятости.

2. **ББД как обобществленная заработная плата.** Можно отметить позицию Ж.-М. Монье и К. Верчеллона [11], которые указывают на то, что в условиях «когнитивного капитализма» концепция труда и концепция занятости перестают быть тождественными, возникают новые формы труда, которые авторы относят к коллективным и фактически не оплачиваемым (в первую очередь в сфере создания интеллектуальной собственности на интернет-площадках), поскольку они не вписываются в существующую модель производства. В этой ситуации ББД выступает как «обобществленная заработная плата», перераспределяемая на каждого члена общества как вознаграждение за добровольное и самостоятельное участие в таком труде. Универсальный характер дохода в данном случае обеспечивал бы стабильность такой экономики свободного коллективного труда и саму возможность граждан свободно в ней участвовать, ориентируясь на достижение своей индивидуальной цели.

В качестве основы такой модели можно рассматривать положения ч. 2 ст. 7 Конституции РФ, согласно которой в Российской Федерации охраняются труд и здоровье людей, а также ч. 3 ст. 37 Конституции Российской Федерации, которая устанавливает право на вознаграждение за труд без какой бы то ни было дискриминации, обеспечивая таким образом оплату деятельности людей, создающих продукт, имеющий экономическую ценность, но не состоящих в трудовых

отношениях с владельцем интернет-площадки, получающим выгоды от полезной деятельности пользователей соответствующего ресурса.

В отличие от предыдущей модели, данная разновидность требует собственно всеобщего характера, поскольку представляется затруднительным без значительных затрат дополнительных финансовых и административных ресурсов выделить экспериментальную группу для установления «обобществленной заработной платы». Как модель, предназначенная для более абстрактных целей, она может быть реализована при наличии положительных результатов экспериментов с ББД и устойчивой экономики.

Заключение. Таким образом, базовый доход может стать одним из элементов новой модели социального обеспечения, основанной на неустойчивом характере трудовых отношений. Этот институт, который может быть межотраслевым в рамках трудового права и права социального обеспечения, отходит от принципа адресности и индивидуального характера поддержки, предоставляя социальную защиту одновременно всем членам общества, большинство из которых, предположительно, в ближайшем будущем будет находиться в ситуации повышенного социального риска безработицы. Однако испытание применимости ББД целесообразно начать с адресных пилотных проектов в отношении наиболее уязвимых в новых экономических условиях категорий населения.

В качестве моделей ББД, актуальных для России, можно отметить «экстренный базовый доход» в рамках законодательства о чрезвычайном положении и экспериментальная модель защиты от технологической безработицы и создания новой гарантии соблюдения трудовых прав работника в рамках законодательства о занятости. В качестве наиболее перспективной экспериментальной группы можно рассматривать граждан, имеющих нестабильную занятость без иных социальных гарантий.

Вместе с тем отмечается, что ББД не является общепризнанным средством смягчения неравенства и последствий безработицы из-за необходимости перестройки. В качестве недостатков этой формы перераспределения доходов выделяют, как правило, необходимость значительных изменений налоговой системы, предназначенность выплат в том числе и тем лицам, которые в них не нуждаются, а также предполагаемый эффект дестимуляции занятости.

Список литературы

1. Волков А. М. Теория и практика базового дохода в ряде северных стран // Мировая экономика и международные отношения. 2020. Т. 64, № 9. С. 48–52.

2. Квашнин Ю. Д. Базовый доход для европейских стран: от теории к практике // Современная Европа. 2019. № 3. С. 171–181.

3. Квашнин Ю. Д. Базовый доход как ответ на новые экономические вызовы. Анализ и прогноз // Журнал ИМЭМО РАН. 2020. № 3. С. 13–23.

4. Кузнецов Ю. В. Безусловный базовый доход и проблема асимметрии информации // Экономическая политика. 2019. Т. 14, № 3. С. 80–95.

5. Григорьев И. В., Шайхатдинов В. Ш. Право социального обеспечения: учебник и практикум для вузов. 9-е изд., перераб. и доп. М.: Юрайт, 2023. 432 с.

6. Садовая Е. С. Концепция и реализация идеи безусловного базового дохода в контексте трансформации социально-трудовой сферы // Социально-трудовые исследования. 2020. № 38 (1). С. 59–72.

7. Универсальный базовый доход: шанс для России?: [монография] / В. Н. Бобков, [и др.]; под ред. В. Н. Бобкова (отв. ред.), Е. В. Одинцовой. Ижевск: Шелест, 2022. 360 с.

8. A short history of the Basic Income idea // Basic Income Earth Network. URL: https://basicincome.org/history

9. Basic Income Earth Network. URL: https://basicincome.org

10. Basic Income for the Arts Pilot Scheme: Reports. URL: https://www.gov.ie/en/publication/29337-basic-income-for-the-arts-pilot-scheme-guidelines-for-applicants

11. Monnier J.-M., Vercellone C. Le revenu de base comme revenu primaire// Guillaume Allègre et Henri Sterdyniak. Faut-il un revenu universel? L'état du débat, OFCE. 2017. URL: https://hal.archives-ouvertes.fr/hal-01486202/document

12. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

К. С. Суслин,
магистрант,
Международный юридический институт

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВИЗАЦИИ СИСТЕМЫ ЗАКУПОК ДЛЯ ОБЕСПЕЧЕНИЯ ГОСУДАРСТВЕННЫХ (МУНИЦИПАЛЬНЫХ) НУЖД

Аннотация. В статье рассматривается вопрос автоматизации государственных закупок. Отмечается практически полный переход к электронным процедурам: внедряются технологии блокчейн, искусственный интеллект, однако многие вопросы не разрешены: не определены основные термины; не закреплены мероприятия по обучению сотрудников, ответственных за проведение закупок. Наряду с этим отмечается увеличение недобросовестного использования участниками закупок технологий, которым необходимо противодействие.

Ключевые слова: система закупок, цифровизация системы закупок, автоматизация системы закупок, цифровые картели, искусственный интеллект в закупках

LEGAL REGULATION OF DIGITALIZATION OF THE PROCUREMENT SYSTEM TO ENSURE STATE (MUNICIPAL) NEEDS

Abstract. The article deals with the issue of automation of public procurement. The author draws attention to the fact that there has been an almost complete transition to electronic procedures: blockchain technologies and artificial intelligence are being introduced, but many issues have not been resolved. Thus, the basic terms are not

defined; measures for training employees responsible for procurement are not fixed. The author notes an increase in unfair use by procurement participants of technologies that need to be countered.

Keywords: procurement system, digitalization of the procurement system, automation of the procurement system, digital cartels, artificial intelligence in procurement

В настоящее время информационные технологии стали одним из главных факторов развития государственной политики во всех ее сферах. Также данный вектор развития находит свое отражение в отдельных нормативно-правовых документах, например,в Программе «Цифровая экономика», утвержденной распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р [1], Указе Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации до 2030 года» (далее – Указ) [2]. В вышеуказанных документах в одной из первоочередных целей говорится о необходимости цифровизации и автоматизации закупок.

Следует отметить, что государственные закупки – одна из первых сфер, куда активно стали внедряться информационные технологии. Уже с 1 июля 2018 г. вместо одной электронной процедуры в электронной форме их стало уже десять, а с 1 января 2019 г. проведение закупок в электронной форме – обязанность заказчика. С 2021 г. на большинстве этапов госзакупок стороны начали применять системы электронного документооборота.

Внесение изменений в законодательство в части цифровизации продолжается и по сей день. Например, в 2022 г. получило закрепление обязательное электронное актирование: предоставление счетов-фактур через ЕИС; акта о приемке в новом формате.

По мнению Л. М. Пахомовой, такая быстрота обусловлена колоссальным объемом информации, который существует в системе закупок, необходимостью ее систематизации, упорядочивания и контроля [3, 7].

Инвестиции в цифровую инфраструктуру увеличиваются во всех развитых странах. Особенно по мере того, как все больше государственных услуг переходят в онлайн-режим. Пандемия COVID-19 только усилила этот спрос [10].

Цифровизация закупок позволяет государству повышать их прозрачность, а также осуществлять сбор, хранение и анализ информации о проведенной закупке. Также переход на электронные способы определения подрядчиков, поставщиков, исполнителей значительно упрощает закупочный процесс и обеспечивает экономию времени сотрудников за счет автоматизации отдельных процессов.

Отметим, однако, что возникшая электронная система закупок не смогла полностью искоренить коррупционные проявления, как это изначально и планировалось.

Согласно данным, представленным Федеральной антимонопольной службой Российской Федерации, чаще всего со стороны заказчиков можно наблюдать нарушения законодательства, связанные:

– с порядком определения поставщиков (подрядчиков, исполнителей);

– требованиями в закупочной документации, наличие которых ограничивает число участников закупки;

– заключением контракта с нарушением объявленных условий закупок [4].

Более того, участники закупок стали использовать информационные технологии в недобросовестных целях. Примерами могут выступить автоматизированные программы, позволяющие блокировать других участников закупки; специальные учетные записи, созданные для автоматической отправки сообщений для переговоров участников, стремящихся заключить антиконкурентное соглашение и другие.

Например, 19 апреля 2023 г. Арбитражный суд Челябинской области подтвердил законность решения Челябинского УФАС по делу о нарушении запрета на картель в отношении шести местных поставщиков металлопродукции. Как сообщалось, УФАС установило, что компании в период с августа 2018 г. по сентябрь 2021 г. приняли совместное участие в 54 закупках. Общая сумма начальных цен контрактов составила 290 млн рублей. При этом участники картеля по итогам торгов заключили контракты на сумму более 70 млн рублей [5].

Не так давно для предотвращения вышеописанных злоупотреблений участниками закупки стали использовать технологию распределенного реестра (блокчейн). С 1 января 2020 г. начала свою работу система «Независимый регистратор». Она позволяет фиксировать действия всех субъектов контрактных отношений в Единой информационной системе в сфере закупок (далее – ЕИС) и на электронных площадках (далее – ЭТП), осуществлять видеофиксацию действий и отслеживать работоспособность ЕИС и ЭТП.

В последние годы все чаще можно услышать об использовании еще одной технологии – искусственного интеллекта. Ее повсеместное изучение и развитие начало набирать обороты после издания Указа Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» [6].

Применительно к использованию технологии в системе государственных и муниципальных закупок, можно выделить следующие направления, где будет целесообразно и полезно ее применение [7, 218]:

– проверка участников закупки на соответствие требованиям законодательства;

– отслеживание и контроль системой всех этапов подписания и выполнения контрактных обязательств;

– мониторинг цен на закупаемые товары, работы, услуги;

– моделирование и прогнозирование планируемых результатов деятельности;

– актуализация баз данных для сотрудников по вопросам применения законодательства в сфере осуществления закупок.

Несмотря на то что цифровизация закупок происходит быстрыми темпами, многие дискуссионные вопросы так и остаются без нормативного закрепления. Например, за пределами правового регулирования остался большой пласт разграничения и определения правовых категорий и технических норм, таких как цифровой контракт, цифровой реестр и другие. Отсутствие понимания у участников закупки ключевых определений может повлечь за собой принятие неверных решений и привлечение к ответственности.

В качестве еще одного проблемного момента в научной литературе отмечается отсутствие знаний у государственных служащих в сфере современных

информационных технологий [8], автоматизации и цифровизации. Государство только сейчас активно стало принимать меры для того, чтобы не только программисты и разработчики были технически грамотными (например, в программы вузов включаются дисциплины, которые дают общее понимание информационных технологий). Однако те специалисты в сфере закупок, которые работают уже долгое время, достаточно сложно адаптируются к новым цифровым реалиям [9, 376].

Таким образом, технический прогресс и экономические стимулы способствуют быстрому развитию и цифровизации всех сфер государственной деятельности, включая государственные закупки. С учетом изложенного, следует говорить о том, что присутствует необходимость выстраивать управленческую стратегию в сфере закупок в условиях ускорения цифровой трансформации, основой которой выступит прежде всего, отечественная и зарубежная практика. Важнейшие действия в данном процессе должны быть направлены на совершенствование процессов правового регулирования.

Список литературы

1. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Собрание законодательства РФ. 2017. № 32. Ст. 5138.

2. Указ Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации до 2030 года» // Собрание законодательства РФ. 2020. № 30. Ст. 4884.

3. Пахомова Л. М. Цифровизация контрактных отношений: первые итоги и правовые пробелы // Право и цифровая экономика. 2022. № 4. С. 5–15.

4. Разъяснение ФАС России контрольной практики 44-ФЗ и 223-ФЗ. URL: https://fas.gov.ru/ckeditor_assets/attachments/1252/raz_yasneniya_fas_rossii_44_fz_i_223_fz_v11_compressed_1.pdf

5. Суд подтвердил решение Челябинского УФАС о картельном сговоре на торгах группы металлотрейдеров. URL: https://www.interfax-russia.ru/ural/news/sud-podtverdil-reshenie-chelyabinskogo-ufas-o-kartelnom-sgovore-na-torgah-gruppy-metallotreyderov

6. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства РФ. 14.10.2019. № 41. Ст. 5700.

7. Сергеева С. А. Искусственный интеллект в сфере закупок: возможности и перспективы // Инновации и инвестиции. 2022. № 12. С 216–219.

8. Минич С. А. Совершенствование системы обязательных требований, предъявляемых к бизнесу в условиях цифрового преобразования экономики // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 775–802. EDN: IBFBAQ

9. Вакуленко А. Н., Белокрылова О. С. Цифровизация управления публичными закупками // Россия: тенденции и перспективы развития. 2022. С. 374–378.

10. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

А. А. Ткалина,
студент,
Санкт-Петербургский государственный университет

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ТЕХНОЛОГИИ «ДИПФЕЙК»

Аннотация. Все больше людей сталкиваются с возможностью использования технологии «дипфейк», которая позволяет создавать и изменять видео-, фото- или аудиозаписи. С одной стороны, эта технология является полезным инструментом в медиапространстве и медицине, однако, «дипфейк» может быть использован для создания фальшивых видео-, фото- и аудиоматериалов, которые могут нанести вред лицам, персональные данные которых были использованы в качестве введенной информации. Правовое регулирование технологии «дипфейк» становится все более актуальной проблемой и вызовом для современных юристов. В статье рассмотрены различные аспекты правового регулирования использования технологии «дипфейк». Поскольку «дипфейк» – не юридическое, а техническое понятие, целью статьи является рассмотрение правовых режимов, применимых к «дипфейкам» в нескольких плоскостях, а именно в отношении к «классическим» правовым институтам, таким как персональные данные, авторское право, нематериальные блага и информации.

Ключевые слова: право, цифровые технологии, информация, дипфейки, нематериальные блага, интеллектуальная собственность, искусственный интеллект, персональные данные, авторское право

LEGAL REGULATION OF DEEPFAKE TECHNOLOGY

Abstract. More and more people are encountering the possibility of using “deepfake” technology, which allows for the creation and modification of video, photo, or audio recordings. On one hand, this technology serves as a valuable tool in the media space and medicine. However, “deepfake” can be used to produce counterfeit video, photo, and audio materials that can harm individuals whose personal data has been used as input information. As a result, the legal regulation of “deepfake” technology is becoming an increasingly relevant issue and challenge for contemporary legal professionals. This article will explore various aspects of the legal regulation of the use of “deepfake” technology. Since “deepfake” is not a legal but a conditional technical concept, the aim is to examine the legal frameworks applicable to “deepfakes” on multiple parallel fronts, in relation to “classic” legal institutions such as personal data, copyright, nonmaterial values, and information.

Keywords: law, digital technologies, information, deepfakes, nonmaterial values, intellectual property, artificial intelligence, personal data, copyright

Использование искусственного интеллекта (далее – «ИИ») в некоторых сферах общественной жизни стало обыденным явлением. Мир наполнен

технологическими системами и инструментами, приводимыми в движение технологиями искусственного интеллекта, которые все больше овладевают нашей повседневной жизнью. Современные технологии ИИ имеют ряд преимуществ, которые выражаются в повышении экономической производительности, снижении издержек, эффективности государственного управления и оптимизации административно-распорядительных функций [8. С. 91–104]. Однако, несмотря на эти преимущества, существуют и опасности. Высокая распространенность технологий ИИ среди широкой публики, а также простота их применения открывают возможности для использования достижений технологического прогресса не только во благо, но и в неправомерных и преступных целях.

Дипфейки – это одна из таких инноваций, основанных на ИИ, которая вызывает огромные опасения среди юридических и научных экспертов. Поскольку создание этих синтетических материалов, называемых дипфейками, становится все более общедоступным, и каждый человек, даже не имеющий специальных навыков, способен создать некую «глубокую подделку», растут опасения, связанные с недобросовестным использованием технологии, требующие немедленного внимания и реагирования. Дипфейки могут иметь серьезные последствия для общества. Обман и манипуляция, нарушение конфиденциальности и авторских прав, провоцирование ненависти, угроза национальной безопасности – только некоторые из проблем, которые может вызвать технология дипфейк. В связи с этим необходимо не только развивать технологии, которые могут помочь в борьбе с дипфейками, но и обеспечить данную технологию правовым регулированиям, чтобы избежать негативных последствий для общества.

Дипфейки – это технология искусственного интеллекта, которая использует нейронные сети для создания ложных видео, аудио или изображений. Эти технологии могут создавать очень реалистичные «подделки», которые могут быть использованы, в том числе, для обмана и манипуляции. В самом широком смысле под «дипфейком» обычно понимают создание фото-, видео- или аудиозаписей, имитирующих реальность. Технически это осуществляется путем наложения существующих изображений и видео на исходные изображения или видеоролики с помощью так называемой генеративно-состязательной сети [5. С. 87–103]. Проще говоря, технология «дипфейк» позволяет создавать поддельные видео и фото, на которых лица одних людей подменяются лицами других. Это делается при помощи алгоритмов машинного обучения, которые обрабатывают огромные объемы данных, чтобы создать подобные «фейки». Дипфейки имеют тесную связь с исследованиями в области криминалистики цифровых изображений. Оригинальные лица, выражения и даже голоса копируются, изменяются и заменяются «фейковыми», нарушая тем самым социальное доверие и создавая проблемы с конфиденциальностью и другие правовые проблемы. Генеративно-состязательные сети (далее – GAN) используется для морфинга оригинального контента. Роль GAN заключается в том, чтобы обучать две архитектуры нейронных сетей – генератор (декодер) и дискриминатор – в адверсариальных отношениях. Как только кодировщик извлекает латентные характеристики оригинальных изображений лиц, генератор (декодер) восстанавливает изображения, а дискриминатор определяет, насколько реалистично изображение, созданное генератором [18. С. 25].

Как упоминалось ранее, существует несколько видов дипфейков. Видео-дипфейки – это наиболее известный тип дипфейков. С их помощью можно создавать ложные видеозаписи, в которых лица людей могут быть заменены на другие. Аудио-дипфейки могут быть использованы для создания ложных аудиозаписей, в которых голоса людей могут быть скомпонованы из разных фрагментов речи. Фото-дипфейки могут быть использованы для создания ложных фотографий, которые могут быть изменены таким образом, чтобы лица людей выглядели иначе, чем на самом деле. Текстовые дипфейки могут быть использованы для создания ложных новостей, комментариев, сообщений в социальных сетях и других текстовых сообщений.

Согласно исследованию, проведенному компанией Sentinel, которая разрабатывает платформу, оснащенную ИИ для защиты от дипфейков, количество таких видео выросло с 14 678 в 2019 г. до 145 277 в 2021 [19. С. 1].

Технология синтезированных видео нельзя назвать новыми. Они начинают свой путь с конца девяностых годов двадцатого века. Так, в 1997 г. компания Video Rewrite представила технологию, которая позволяла сформировать видео, где артикуляция лица совпадала с синтезированной аудиодорожкой. В 1997 г. три исследователя Google – Кристоф Бреглер, Мишель Коувелл и Малколм Слейни – создали инновационную программу Video Rewrite Program [17. С. 1]. Специалисты впервые использовали технологию лицевой анимации. Но это было только начало, уже через десять лет подобная технология использовалась в кинокартине Джеймса Кэмерона «Аватар», тем самым продемонстрировав специалистам киноиндустрии возможность искусственно заменять с помощью современных технологий лица актеров. Он стал одним из первых фильмов, где большая часть персонажей была создана с помощью компьютерной графики и технологии захвата движений актеров. История же технологии дипфейк в современном виде началась в 2014 г. с появления нескольких исследовательских групп, которые занимались разработкой алгоритмов машинного обучения и нейронных сетей. Эти группы начали работу над новыми методами для создания фальшивых изображений и видео. Затем в 2017 г. компания NVIDIA представила новый тип алгоритма машинного обучения, основанный на глубинном обучении. Этот алгоритм был назван GAN (Generative Adversarial Networks), и он начал использоваться для создания дипфейка. Он позволяет создавать реалистичные фотографии людей, которых на самом деле не существует. Также в 2017 г. на GitHub появился открытый исходный код программы FakeApp, которая позволяет создавать дипфейки изображений и видео. Эта программа была создана на основе библиотеки TensorFlow, которую разработала компания Google. Вскоре после выпуска FakeApp, другие разработчики начали создавать свои собственные программы для генерирования дипфейков [8. С. 1]. В этом же году появился термин «дипфейк». Одноименный пользователь платформы Reddit заполнил сайт-агрегатор онлайн-новостей видеороликами порнографического содержания, в которых применялась технология замены лица (англ. face-swap) с открытым исходным кодом. Этот метод он и назвал deepfake. Также в 2017 г. были запущены проекты «Face2Face» (Мюнхенский университет) и «Synthesizing Obama» (Вашингтонский университет). Однако в 2018 году

технология «дипфейк» стала гораздо более сложной и утонченной благодаря появлению системы Deep Voice 2. Эта система создана компанией Baidu Research, и она представляет собой набор алгоритмов для создания легко узнаваемых голосов с помощью машинного обучения.

Сейчас существуют три поколения программ «дипфейк». Первое поколение основывалось на большой базе данных тестовых изображений и обучалось благодаря им. Второе поколение преодолело барьер публичности путем внедрения нейронной сети «GAN». Третье поколение является усовершенствованной и немного дополненной версией второго поколения. Именно в нем несколько нейронных сетей объединяются в одну модель, что позволяет работать непосредственно с лицом, а не в пространстве 2D-кадра.

Так в чем же заключается основная проблема пробела законодательства относительно дипфейков. Вопрос заключается в том, насколько необходимо защищать общество от возможных вредоносных последствий создания фальшивых изображений. Хотя искусство и литература часто создают вымышленные миры, авторы произведений всегда стараются убедить зрителей или читателей в реальности описываемых событий. Даже если произведение заведомо является вымыслом, оно может восприниматься публикой как изображение реальности. Так, например, И. Левитан изобразил в своей картине «Над вечным покоем» пейзаж около озера Удомля, а церковь – из окрестностей города Плес. В литературе отмечалось, что эта картина – «перенесение мотива, увиденного на одном озере, на изображение другого, сходного». Но для зрителей реальность изображенного не вызывает сомнений, пусть даже они и понимают, что изображенное на картине место в действительности нигде не существует [5. С. 87-103]. Как писал Федор Шаляпин в своей книге «Маска и душа»: «Убедить публику – значит, в сущности, хорошо ее обмануть, вернее, создать в ней такое настроение, при котором она сама охотно поддается обману, сживается с вымыслом и переживает его как некую высшую правду» [18. С. 117]. Так что проблема связана скорее не с самим фактом «подделывания» данных и введения потребителя информации в заблуждение, так как «фальшивки» известны правовой среде уже достаточно давно, с ними боролись, но колоссальной правовой проблемой они не являлись.

Проблема же заключается в тех возможностях, которые создает технология, оснащенная генеративно-состязательной сетью, для лица, использующего ее. Ведь создание дипфейков не всегда сопряжено с противоправными мотивами. Важно понимать, что создание искусственной реальности возможно и вовсе не связано с недобросовестными намерениями лица и преследует цель реализации творческих намерений автора. Однако, так или иначе, это создает серьезные угрозы для общественных интересов, а значит и для интересов государства. В таких обстоятельствах право не может оставаться безразличным к расширению использования ИИ при создании результатов интеллектуальной деятельности. Поэтому, считаю необходимым сделать акцент на противодействие недобросовестному использованию такого инструмента, рассмотрев его в призме различных «архаичных» правовых институтов, таких как персональные данные, авторское право, нематериальные блага и информация.

Как было сказано ранее, дипфейки позволяют синтезировать видео, аудио и изображения, в которых реальные люди появляются в контексте, не связанном с их действительной деятельностью и сферой занятости. Подобные продукты совместной деятельности человека и ИИ вызывают серьезную обеспокоенность в связи с возможными нарушениями в том числе прав на защиту персональных данных.

В контексте персональных данных применительно к дипфейкам, в Российской Федерации возможно рассмотреть в рамках существующего законодательства, в частности, Федерального закона «О персональных данных» № 152-ФЗ и Гражданского кодекса Российской Федерации косвенно связанные с ними вопросы.

Согласно Закону «О персональных данных», голос и внешность человека относятся к его биометрическим данным, которые представляют собой сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность. В соответствии с разъяснениями Роскомнадзора, к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и другие), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта [11. С. 7].

Согласно пункту 3 статьи 3 Федерального закона № 152-ФЗ, под обработкой персональных данных понимается «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» [15. С. 4]. Дипфейки, в которых используются изображения или другие идентифицирующие признаки реальных лиц, могут рассматриваться как обработка персональных данных. Это означает, что для их создания и распространения необходимо получить согласие субъектов персональных данных (лиц, чьи данные используются) или их законных представителей. Это вытекает из п. 1 ч. 1 ст. 6 вышеуказанного Закона «О персональных данных». Данный закон также предусматривает случаи, когда согласие субъекта не требуется, среди которых: реализация международных договоров Российской Федерации, в связи с осуществлением правосудия и исполнением судебных актов, проведение обязательной дактилоскопической регистрации и иные, среди которых, естественно, не прописано использование персональных данных для создания дипфейка. Соответственно при создании подобного рода материалов, необходимо заручиться согласием субъекта персональных данных. В противном случае, ответственность может возникнуть в соответствии со статьей 13.11 КоАП РФ, предусматривающей административную ответственность за нарушение правил обработки персональных данных [6. С. 193].

Важно отметить, что существует точка зрения, согласно которой используемые в дипфейке данные нельзя считать персональными. Приверженцы данной

теории оперируют тем, что поддельные изображения или видео не могут рассматриваться как личные (персональные) данные, поскольку после изменения их нельзя больше отождествлять с исходными данными субъекта, лицо, тело, голос, действия или имитация на самом деле ему не принадлежат. Таким образом, содержимое в некотором смысле является искусственной анимацией или графикой, созданной разработчиком [7. С. 396–400]. Однако я исхожу из того, что сам дипфейк является искусственно созданной информацией, содержащей изображение личности, ее или сходный с ней голос. Таким образом, получается, что в любом случае имеет место биометрика субъекта персональных данных. Как было указано ранее, под обработкой персональных данных понимается не только изменение, но и сбор данных для обучения ИИ. Таким образом, вывод напрашивается сам, изготовление дипфейков без согласия субъекта персональных данных – грубое нарушение действующего законодательства «О персональных данных», ответственность за которое предусмотрена административным законодательством.

Также важно отметить, что Гражданский кодекс РФ предоставляет каждому гражданину право на неприкосновенность частной жизни, включая неприкосновенность его изображения. Статья 152.1 ГК РФ устанавливает, что использование изображения гражданина без его согласия влечет за собой ответственность. В случае дипфейков, где используются изображения без разрешения, возможна гражданско-правовая ответственность, в том числе возмещение морального вреда. Но этот подход будет детально раскрыт далее.

Однако стоит учитывать, что законодательство по-прежнему не является исчерпывающим в регулировании «дипфейков» и связанных с ними вопросов. Текущее законодательство не содержит специфических положений, касающихся дипфейков, и в некоторых случаях может оказаться недостаточным для решения возникающих проблем и споров. В связи с этим, возможно, потребуется принятие специализированных нормативных актов или дополнений к существующим законам для более четкого определения правовых рамок, касающихся создания и распространения дипфейков.

В целом, дипфейки и персональные данные по российскому законодательству находятся в поле зрения правовых регуляторов. Несмотря на то, что текущее законодательство Российской Федерации уже обеспечивает определенный уровень защиты персональных данных и прав на неприкосновенность частной жизни, существует потребность в более точном и всестороннем регулировании дипфейков для предотвращения их негативного воздействия на права и свободы граждан.

Важным аспектом, связанным с дипфейками, является вопрос авторских прав и охраны интеллектуальной собственности. Создание «дипфейков» может затрагивать как права авторов оригинальных произведений, так и права лиц, чьи изображения и материалы используются для синтеза «дипфейков».

В Российской Федерации авторские права и интеллектуальная собственность регулируются Гражданским кодексом РФ (часть IV), который определяет правила и условия использования произведений и охраняемых объектов. Согласно статье 1257 Гражданского кодекса РФ автором произведения признается гражданин,

творческим трудом которого оно создано [2. С. 48]. В соответствии с законодательством, автор произведения обладает исключительными правами на свое творение, что включает право на использование и распространение произведения, а также право на авторство и интегритет (целостность) произведения.

Создание дипфейков может нарушать авторские права различными способами.

Во-первых, использование оригинальных произведений (например, видео, фотографий или аудиозаписей) без согласия автора или законных правообладателей может рассматриваться как нарушение авторских прав. Согласно п. 1 ст. 1229 ГК РФ, использование результата интеллектуальной деятельности или средства индивидуализации (в том числе их использование способами, предусмотренными указанным кодексом), если такое использование осуществляется без согласия правообладателя, является незаконным и влечет ответственность, за исключением случаев, когда использование результата интеллектуальной деятельности или средства индивидуализации лицами иными, чем правообладатель, без его согласия допускается ГК РФ [2. С. 5]. А допускается оно в случаях свободного использования в целях, указанных в ст. 1274 ГК РФ, а именно в целях информационных, научных, учебных или культурных.

Во-вторых, в ряде случаев «дипфейки» могут рассматриваться как произведения, созданные на основе оригинальных материалов, и в качестве таковых могут пользоваться авторским правом. Однако для признания дипфейка произведением, оно должно обладать необходимой степенью творческого вклада и оригинальности, что в каждом конкретном случае определяется судебной практикой. Однако, даже при условии того, что переработка произведения предполагает создание нового (производного) произведения на основе уже существующего, право на переработку произведения является одним из способов использования результата интеллектуальной деятельности и как таковое принадлежит правообладателю, в том числе не являющемуся автором первоначального произведения, который вправе перерабатывать произведение [10. С. 33]. При этом необходимо заручиться согласием правообладателя исходного произведения.

Важно отметить, что существующее законодательство предусматривает исключения и ограничения авторского права, такие как цитирование, пародия и сатира, которые могут быть применимы к дипфейкам в определенных обстоятельствах. Однако использование этих исключений требует строгого соблюдения условий и ограничений, установленных законом, и не должно приводить к необоснованному ущемлению законных интересов авторов и правообладателей оригинальных произведений.

В целом, если рассматривать право авторства на дипфейк как результат интеллектуальной деятельности, созданной программой, то по российскому законодательству автором может быть только гражданин, творческим трудом которого создан этот результат (ст. 1228 ГК РФ). А правообладателем может быть лишь физическое или юридическое лицо, обладающее исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (ст. 1229 ГК РФ). Так что за любой машиной должно стоять физическое или юридическое лицо, в противном случае не будет создан объект авторского права [3. С. 1].

В целом, вопрос дипфейков и авторских прав в России находится в зоне активного правового дискурса. Существующее законодательство охраняет интересы авторов и правообладателей, однако не является полностью адаптированным для регулирования специфических особенностей дипфейков. В связи с этим потребуется дополнительное законодательное развитие и судебная практика для более четкого определения правовых рамок, касающихся создания и использования «дипфейков» в контексте авторских прав и интеллектуальной собственности. Возможно, потребуется разработка новых норм и подходов, специально направленных на решение вопросов, связанных с дипфейками и охраной авторских прав.

Нематериальные блага представляют собой ценности, не имеющие физической формы, но оказывающие значительное влияние на жизнь и благосостояние людей. В контексте дипфейков стоит рассмотреть взаимосвязь между этими технологиями и нематериальными благами, такими как репутация, честь, достоинство, личная жизнь и авторские права.

Очевидно, что дипфейки могут негативно сказываться на нематериальных благах как отдельных личностей, так и общества в целом. Использование технологии дипфейк может привести к нарушению права на неприкосновенность частной жизни, доброго имени, чести и достоинства личности, деловой репутации и других. Создание и распространение поддельных изображений и видео может нанести серьезный моральный вред, дискредитировать людей и повредить их репутации. Также дипфейки могут стать средством манипуляции общественным мнением и искажением фактов, что подрывает доверие к информации и массмедийным источникам. В особенности это касается политической сферы. Неоднократно технология «дипфейк» использовалась как метод «грязной игры» на политической арене. Жертвами «дипфейков» становились такие мировые личности, как Дональд Трамп, Владимир Путин, Барак Обама, Нэнси Пелоси, Ким Чен Ын и другие [4. С. 1].

В России защита нематериальных благ осуществляется на основе Гражданского кодекса РФ, законов «О СМИ» и «О персональных данных», а также Конституции РФ и международных договоров. Например, статья 23 Конституции РФ гарантирует право на неприкосновенность частной жизни, а статья 152.1 ГК РФ устанавливает право на неприкосновенность изображения.

Однако в контексте дипфейков существующее законодательство может оказаться недостаточным для обеспечения полноценной защиты нематериальных благ. В частности, может возникать сложность в определении и доказывании морального вреда, причиненного дипфейками, а также в определении степени ответственности за их создание и распространение.

В связи с этим для эффективной защиты нематериальных благ в условиях распространения дипфейков потребуется развитие правовых механизмов и законодательства. Потребуется введение специальных норм, учитывающих особенности дипфейков и устанавливающих четкие критерии ответственности за их создание и использование. Также важным направлением является развитие судебной практики по делам, связанным с дипфейками, которая поможет определить рамки применения существующих норм и выработать новые подходы к регулированию этой проблематики.

Кроме того, для минимизации негативных последствий дипфейков на нематериальные блага необходимо привлечение усилий всех заинтересованных сторон: государства, общества, компаний-разработчиков технологий и пользователей. Важными мерами могут стать просветительская деятельность, информирование общественности о рисках и последствиях использования дипфейков, а также разработка и применение технических средств для обнаружения и блокирования поддельных медиаматериалов. Так, к примеру 17 августа 2022 г. компания «Сбер» получила два патента Федеральной службы по интеллектуальной собственности на технологии, созданные в рамках исследования по выявлению дипфейков. Результатом работы является повышение точности и эффективности обнаружения синтетического изменения изображений лиц людей в видео. Основу технологий составляет ряд ансамблей нейросетевых моделей класса EfficientNet (патент № 2768797) и метод амплификации и анализа средствами ИИ микроизменений в цветах объектов на кадрах (патент № 2774624). Объединенные в одну систему, они позволяют с высокой точностью определить синтетически измененные изображения лиц на видео [11. С. 1].

В целом, дипфейки и нематериальные блага представляют сложную проблематику, требующую комплексного подхода и учета многочисленных факторов. Развитие законодательства и правоприменительной практики, совместные усилия всех участников и использование инновационных технологий могут способствовать обеспечению защиты нематериальных благ в эпоху «дипфейков».

Дипфейки оказывают значительное воздействие на сферу информации, поскольку они могут искажать и манипулировать данными, приводя к распространению ложных сведений и подрывая доверие к источникам информации. В связи с этим важно разобраться в том, как дипфейки взаимодействуют с информацией, и какие меры могут быть предприняты для минимизации негативных последствий.

Проблема дипфейков актуальна не только для личной жизни и деловых отношений, но и для общественного дискурса и политического процесса. Создание поддельных видео- и аудиозаписей с участием политических деятелей, знаменитостей и других общественных персон может стать инструментом дезинформации, манипуляции общественным мнением и дестабилизации мировой обстановки. Такие случаи могут приводить к недоверию к официальным источникам информации, массмедийным компаниям и представителям власти.

В России вопросам дипфейков и информации уделяется повышенное внимание на различных уровнях. Законодательство в сфере информации включает такие акты, как Федеральный закон «О СМИ», «О связи», «О персональных данных», конечно же «Об информации, информационных технологиях и о защите информации» и другие, определяющие правила обработки и распространения информации, ответственность за нарушения и ограничения. Однако специфика дипфейков требует дополнительного регулирования и разработки новых, эффективных механизмов контроля и противодействия.

Действующие законы РФ неэффективны в борьбе с распространением ложной информации, по сравнению с законами Китая или США, но о них мы поговорим далее. В законодательстве Российской Федерации в ст. 15.3 ФЗ № 149-ФЗ

запрещается распространение в Интернете недостоверной общественно значимой информации [14. С. 13], что, конечно, может относиться к дипфейкам. Но ведь недостоверность информации еще нужно установить, к тому же данная норма в любом случае применяется только в ограниченной сфере [4. С. 87–103]. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия, наказываются согласно ст. 207.1-2 УК РФ [13. С. 152–153].

Важным направлением в борьбе с негативным влиянием дипфейков на информацию является разработка и применение технологий, позволяющих обнаруживать и блокировать поддельные изображения и видео. Исследовательские группы и IT-компании активно работают над созданием таких инструментов, которые могут быть интегрированы в социальные сети, мессенджеры и другие платформы для автоматического выявления и фильтрации дипфейков.

Кроме того, для обеспечения информационной безопасности и противодействия «дипфейкам» необходимо проводить просветительскую работу среди населения и развивать культуру медиаграмотности [1]. Люди должны быть информированы о рисках, связанных с дипфейками, и уметь распознавать их при встрече с подозрительными материалами. Государству необходимо помочь обществу сформировать критический подход к информации и снизить уровень восприимчивости к манипуляциям и дезинформации.

Сотрудничество между государством, медиа, IT-компаниями и гражданским обществом также является ключевым фактором в борьбе с «дипфейками» и их влиянием на информацию. Вместе эти стороны могут разрабатывать стратегии, направленные на предотвращение распространения поддельных материалов, обеспечение информационной прозрачности и поддержание доверия к источникам информации.

В целом, дипфейки и информация представляют сложную и актуальную проблему, требующую комплексного подхода и применения инновационных решений. Анализ показал, что данная область является самой незащищенной с правовой точки зрения. Развитие законодательства, использование технологий обнаружения дипфейков, просветительская деятельность и сотрудничество всех заинтересованных сторон могут сыграть решающую роль в борьбе с негативными последствиями дипфейков и обеспечении информационной безопасности.

Безусловно, правовое регулирование дипфейков в зарубежных странах различается в зависимости от конкретной страны и ее законодательства. Однако некоторые страны уже приняли и активно пользуются законами, направленными на борьбу с использованием дипфейков, в то время как в других странах законодательство менее развито или отсутствует вовсе.

По моему мнению, наибольшую эффективность в части правового регулирования дипфейков показала Китайская Народная Республика. Согласно анализу, китайский законодатель отказался от полного запрета дипфейков, однако установил ряд специальных правил для их использования. Одними из таких правил являются обязательная маркировка сгенерированных искусственным интеллектом материалов, а также дополнительные обязанности для операторов и поставщиков

информационных услуг. Целью данных положений является предотвращение использования дипфейков в неправомерных целях, таких как подрыв общественного порядка и государственного строя, а также нарушение прав граждан на изображение, честь и достоинство, а также на неприкосновенность частной жизни. Китайский законодатель также установил ответственность за неправомерное создание и распространение поддельных аудиовизуальных материалов, включая гражданско-правовую и уголовную ответственность. Такой подход к регулированию «дипфейков» является наиболее оптимальным и соответствует требованиям современности, что может стать примером для других стран при разработке национального правового регулирования в этой области [9. С. 91–104]. Также в Китае полностью запрещена публикация ложных новостей, созданных с использованием искусственного интеллекта и виртуальной реальности.

В США существует законодательство, которое запрещает использование дипфейков в целях нарушения избирательных прав, мошенничества и других преступлений. Также в США действует Digital Millennium Copyright Act (DMCA), который регулирует использование технологий для защиты авторских прав и пресекает нарушения в этой области (как пример, законы штатов Калифорния и Техас о признании незаконными определенных дипфейков в политических целях). В Калифорнии запрещается создавать и распространять дипфейки в пределах 60 дней до выборов. Также в некоторых штатах приняты законы, запрещающие «реалистичные фейковые видео и фото, включая сгенерированные на компьютере дипфейки в целях распространения видео сексуального характера [5. С. 87–103].

В Европейском союзе (ЕС) существует Общая регламентация по защите персональных данных (GDPR), которая может быть использована для пресечения распространения дипфейков, если они содержат персональные данные людей без их согласия. В ЕС также действует Директива о некоторых аспектах авторских прав и смежных прав в цифровом рынке, которая регулирует использование авторских прав на цифровые контент.

Важно отметить, что некоторые компании, такие как Facebook (признана экстремистской, ее деятельность запрещена на территории Российской Федерации), Google и Twitter (социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации), также разработали свои политики по борьбе с дипфейками и проводят работу по выявлению и удалению дезинформации, в том числе созданной с помощью ИИ.

В целом, правовое регулирование дипфейков в зарубежных странах продолжает развиваться вместе с появлением новых технологий и применением дипфейков в различных сферах жизни.

Подытожив, хотелось бы указать на недостаточность правового регулирования технологии дипфейк в Российской Федерации. Однако, многие страны, в том числе и «дружественный» для нас Китай, уже успешно применяют на практике специализированное законодательство относительно данной технологии. Хотя в РФ уже обсуждалось внесение на законодательном уровне регуляции подмены в роликах голоса и внешности человека, на практике на сегодняшний день данный закон отсутствует. Так 2 февраля 2022 г. заместитель главы комитета Госдумы по

информационной политике, информационным технологиям и связи Антон Горелкин заявил о необходимости регулирования обсуждаемой индустрии. Он подчеркнул, что в этом вопросе стоит ориентироваться на китайский опыт. Т. е., вполне возможно, что в ближайшее время мы получим законопроект, содержащий норму об обязательстве маркировать весь материал, который производится при помощи искусственного интеллекта. Данный законопроект будет касаться не только технологии «замены лица», но и произведений, созданных с помощью уже многим известных нейронных сетей. Однако вопрос правообладателей таких произведений до сих пор является актуальной проблемой современной юридической науки.

Подводя итоги, с точки зрения законодательства, регулирование дипфейков может включать несколько аспектов. Первый из них – защита частной жизни. Законы о защите частной жизни должны быть усилены, чтобы предотвратить использование дипфейков для нарушения частной жизни людей. Это может включать запрет на создание и распространение дипфейков без согласия всех участников, чьи лица используются. Второй – защита от мошенничества. Законы о мошенничестве должны быть обновлены, чтобы включить дипфейки как форму мошенничества. Это подведет недобросовестных лиц к уголовной ответственности за создание и распространение дипфейков с целью обмана. Третий – авторские права. Законы об авторском праве должны быть обновлены, чтобы включить дипфейки и определить, кому принадлежат права на создание и распространение таких материалов. Четвертый аспект – образование и информирование. Вероятно, наиболее важным является информирование общественности о дипфейках и их потенциальных последствиях, чтобы предотвратить риски нарушения прав граждан.

В целом, регулирование дипфейков должно быть сбалансированным, чтобы предотвратить их злоупотребление, но при этом не ограничивать свободу выражения и творчества.

Список литературы

1. Анненкова И. В., Залоило М. В. Новая культура коммуникаций в условиях цифровой и социокультурной глобализации: право, медиа и национальная идентичность // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 140–155.

2. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СПС «КонсультантПлюс.

3. Дипфейки: как трансформируется авторское право на контент // РБК URL: https://trends.rbc.ru/trends/industry/5fc688fe9a79473e6ff9b82a

4. Как создаются дипфейки и почему они опасны // Dev.BY. URL: https://devby.io/news

5. Калятин, В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87-103. DOI: 10.37239/0869-4400-2022-19-7-87-103. EDN: FENGGS

6. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // СПС «КонсультантПлюс.

7. Масликова Я. А. Дипфейки как угроза персональным данным // Грядущим поколениям завещаем: творить добро в защиту права: материалы Всероссийской

научно-практической конференции с международным участием, Оренбург, 29 марта 2021 года. Ногинск: Аналитика родис, 2021. С. 396-400. EDN: FHUXMS

8. Научно-технический центр ФГУП «ГРЧЦ» // Обзор технологий создания Deepfake и методов его выявлениям: Татьяна Корешкова. URL: https://rdc.grfc.ru/2020/06/research-deepfake

9. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая / Р. И. Дремлюга, В. В. Моисейцев, Д. В. Парин, Л. И. Романова // Азиатско-тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 4. С. 91-104. DOI: 10.24866/1813-3274/2022-4/91-104. EDN: WYXDSB

10. Постановление Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // СПС «КонсультантПлюс.

11. Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео-изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» // «Экономика и жизнь» (Бухгалтерское приложение). № 36, 13.09.2013.

12. Сбер запатентовал технологии по распознаванию дипфейков // Роспатент. URL: https://rospatent.gov.ru/ru/news/sber-dipfeyk-17082022.

13. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс.

14. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СПС «КонсультантПлюс.

15. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс.

16. Шаляпин Ф. И. Маска и душа. СПб., 2017. С. 117.

17. Laba // Эволюция технологии deepfake: почему она опасна, автор: Яна Ягори. URL: https://l-a-b-a.com/blog/2579-evolyuciya-tehnologii-deepfake-pochemu-ona-opasna

18. Purva Kaushik Privacy and Other Legal Concerns in the Wake of Deepfake Technology: Comparative Study of India, US, and China // Handbook of Research on Cyber Law, Data Protection, and Privacy. New York: IGI Global, 2022. С. 25.

19. Sentinel // Defending Against Deepfakes and Information Warfare. URL: https://thesentinel.ai

Д. С. Федоров,
студент,
Московский государственный университет
имени М. В. Ломоносова

ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье предпринята попытка выявить правовую сущность преступлений в сфере информационных технологий, установить особенности в ходе их совершения, проанализировать акты высших судебных инстанций и судебных

решений, лежащих в основе правоприменительной практики по данному вопросу, выработать эффективные средства и способы для предупреждения данного вида преступлений.

Ключевые слова: информационные технологии, киберпреступность, IT-преступления, информационная безопасность, Интернет, аудит информационной безопасности, информационная инфраструктура

CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Abstract. The article identifies the essence of crimes in the field of information technology, to establish features during their commission, to analyse the acts of the highest courts and judicial decisions, who have developed law enforcement practice on the issue and the views of scholars whose writings have affected the issue, as well as the development of the most effective means to prevent this type of crime.

Keywords: information technology, cyber-crime, IT-crimes, information security, internet, audit of information security, information infrastructure

В условиях постиндустриального общества сеть «Интернет» приобрела колоссальное значение как в духовной сфере, так и в сфере экономической. В условиях развития цифровой экономики важное значение для функционирования экономических процессов приобретает управление на основе данных и расширение информационной инфраструктуры бизнеса. Для поддержания функционирования российской цифровой экономики важное значение в деятельности контрольных органов и хозяйствующих субъектов приобретает обеспечение безопасности данных.

По данным ТАСС, в России 124 миллиона человек пользуется Интернетом [8]. По состоянию на март 2022-го объем интернет-торговли составил 4.1 трлн рублей [7]. Это создает значительную угрозу распространения преступлений в этой сфере [5. С. 73]. Преступники активно пользуются новыми возможностями для совершения различных противоправных деяний.

Актуальность темы исследования обусловлена стремительным ростом значения обеспечения информационной безопасности в жизни общества. Исследователи отмечают двадцатикратный рост киберпреступности с 2013 по 2020 г. [9. С. 214]. Объектом таких преступлений будут в том числе и экономические отношения, и отношения в сфере государственной безопасности. Фактором, объединяющим все эти преступления в единую группу, будет именно использование при их совершении информационных технологий в том или ином виде.

В этой связи беспокойство вызывает низкая проработанность данной темы законодателем, кроме того, необходимо выявить особенности совершения преступлений в сфере компьютерной информации и определить специфику противодействия совершению компьютерного преступления.

Особенность состава преступления, предусмотренном в ст. 159.6 УК РФ является специфический способ совершения преступления, который не характерен как для общего состава мошенничества, так и для квалифицированных составов

[1]. Способ совершения мошенничества в сфере компьютерной информации не связан с обманом или злоупотреблением доверия, а выражается в виде ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование информационных технологий.

Рассматривая вопрос квалификации преступления, предусмотренного статьей 159.6 УК РФ, мы обращаемся к Постановлению Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», в котором Пленум Верховного Суда дает толкование понятия «вмешательство в функционирование средств хранения обработки или передачи компьютерной информации или информационно телекоммуникационных сетей» и в нем он подразумевает, что это воздействие программных и программно-аппаратных средств на серверы, средства вычислительной техники – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него [2].

Еще одной особенностью квалификации данного деяния является дополнительная квалификации по статье 272, 273 или 274.1 УК РФ. Верховный Суд приводит разграничение по вопросам квалификации данного преступления, исходя из которого мы можем увидеть, что основа разграничения мошенничества в сфере компьютерной информации с другими составами – это особый объект – информация, чаще всего интерпретируемая как данные. В итоге мы можем сделать вывод, что преступление, предусмотренное ст. 159.6 УК РФ, направлено на защиту данных от неправомерного воздействия со стороны неуправомоченных на это пользователей.

Говоря об особенностях преступлений, совершаемых в сфере компьютерной информации, стоит отметить, что в доктрине нет единого мнения об отнесении данных преступлений к какой-то конкретной классификации, однако мы можем выявить общие характеристики данных преступлений. Первая особенность – латентность, т. е. их обнаружение крайне затруднено, а все следы остаются долгое время не установленными [6. С. 54]. Это делает киберпреступность колоссальной проблемой для правоприменителей: большое количество нераскрытых преступлений дополнительно нагружает аппарат правоохранительных органов и затрудняет их функционирование.

Вторая особенность – трансграничность. Это означает, что субъект, объект и потерпевший от преступления могут находиться, где угодно и на любом расстоянии друг от друга, но при этом факт совершения преступления независим от любых территориальных особенностей. На наш взгляд, это усиливает роль международной кооперации в деле противодействия преступности.

Отметим роль Российской Федерации в потенциальном развитии совместных институтов контроля и расследования. Так, в 2021 г. в ООН начато рассмотрение резолюции, посвященной борьбе с киберпреступностью, инициатором принятия которой была Россия [4].

Третья особенность киберпреступлений – они могут быть автоматизированы. То есть в данных преступлениях не обязательно активное участие субъекта преступления: оно может совершаться, когда сам субъект непосредственно не вовлечен в этот процесс. Это дополнительно усложняет расследование и делает доказывание виновности конкретного лица еще более трудным. Следующей особенностью является новизна киберпреступлений. Традиционные способы расследования таких преступлений, на наш взгляд, не вполне эффективны. Государство должно постепенно внедрять новые способы пресечения киберпреступлений. Что в очередной раз подтверждает практическую значимость работы ученых-правоведов в рамках данной проблематики.

Подводя итог, мы можем сделать вывод, что данный вид преступлений имеет особую специфику и сложность, а оперативное воздействие, направленное на их устранение, – затруднительно. Также видно, что отсутствие специальных подходов к их расследованию со стороны правоохранительных органов и специальных обзоров практики со стороны судов не позволяет сформировать методологическую базу для организации эффективного противодействия и расследования IT- преступлений.

Опираясь на доктрину, а также практику обеспечения информационной безопасности в частном секторе, можно выявить ряд способов, которые минимизируют риск совершения преступлений в сфере компьютерной информации. Во-первых, создание системы управления информационной безопасностью, которая ограничивает доступ к самой информации от третьих лиц и направлена на предотвращение негативных последствий от «утечки» данной информации и аудит данной системы.

Подобные системы не раз предотвращали совершение преступления, что мы можем увидеть и на уровне судебных решений. Так, сотрудника компании признали виновным в покушении на мошенничество в сфере компьютерной информации (ч. 3 ст. 30, п. «б» ч. 3 ст. 159.6 УК РФ), когда он под своей учетной записью в корпоративной информационной системе осуществлял модификацию данных реестра корпоративных SIM-карт на другие номера с их последующим переоформлением [3]. Однако его преступный умысел не был доведен до конца, так как специалистами подразделения поддержки продаж и сервисного обслуживания клиентов корпорации были выявлены незаконные действия лица, а сим-карты с указанными абонентскими номерами были заблокированы после подтверждения его незаконных действий.

Также для достижения необходимого уровня безопасности информации осуществляются мероприятия по аудиту текущего состояния защиты информационной инфраструктуры. Существуют международные стандарты, определяющие требования к аудиту информационной безопасности, например, COBIT, рекомендации которого могут быть внедрены в бизнес-процессы компании. Однако осуществление подобного аудита не регламентировано на уровне федеральных стандартов или иных актов, из-за чего создание СУИБ и их аудит не являются обязательными, что создает риск преступного воздействия на данные компаний.

В итоге видно, что применение специальных средств защиты данных способствует предотвращению или выявлению преступлений в сфере компьютерной

информации. Однако отсутствует нормативно-правовая база, регулирующая внедрение данных способов, международные стандарты, в свою очередь, носят лишь рекомендательный характер, из-за чего целесообразно на уровне РФ сформировать стандарты обеспечения информационной безопасности [10].

Таким образом, можно сделать вывод, что, исходя из специфики преступлений в сфере компьютерных технологий в виде особого нематериального предмета посягательств, требуется применение особых способов как их расследования, так и предотвращения с обязательным применением информационных технологий. Следует также сделать вывод о том, что отсутствие необходимого методического и нормативного обеспечения на национальном уровне является причиной возникновения угроз информационной безопасности и безопасности критической информационной инфраструктуры Российской Федерации.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс».

2. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс».

3. Приговор № 1-243/2020 от 29 июля 2020 г. по делу № 1-243/2020 // СПС «КонсультантПлюс».

4. Резолюции 73-й сессии (2018–2019 гг.) Третьего комитета по социальным, гуманитарным вопросам и вопросам культуры Генеральной Ассамблеи ООН. URL: https://undocs.org/ru/A/73/590

5. Бегишев И. Р. Ответственность за нарушение работы информационно-телекоммуникационных устройств, их систем и сетей // Безопасность информационных технологий. 2011. Т. 18, № 1. С. 73–75.

6. Лакомов А. С. Киберпреступность: современные тенденции. Академическая мысль, 2019. № 2 (7). С. 53–56.

7. Рынок интернет-торговли в России за год вырос более чем на 50 % // Ведомости. URL:https://www.vedomosti.ru/business/news/2022/03/22/914638-rinok-internet-torgovli-v-rossii-za-2021-god-viros-v-poltora-raza

8. Число пользователей интернета в России достигло 124 млн // ТАСС. URL: https://tass.ru/obschestvo/12698757

9. Приходько А. А., Керопян Г. Б. Потери банков от киберпреступности. StudNet, 2020. Т. 3, № 12. С. 212–217.

10. Русскевич Е. А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 650-672. DOI: 10.21202/jdtl.2023.28. EDN: FISEET

Т. Д. Хамдеева,
магистрант,
Российский государственный университет правосудия
(Северо-Кавказский филиал)

КОНЦЕПТУАЛЬНЫЕ АСПЕКТЫ ЦИФРОВИЗАЦИИ УГОЛОВНОГО ПРОИЗВОДСТВА В КОНТЕКСТЕ УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ОТНОШЕНИЙ

Аннотация. Статья посвящена определению отдельных аспектов концептуализации исследования цифровизации уголовного производства в контексте уголовно-процессуальных отношений. Выделены факторы, обусловливающие актуальность комплексного исследования вопросов использования цифровых технологий в уголовном производстве: социально-политический, нормативно-правовой, криминогенный, праксеологический. Определены основные перспективные направления дальнейшего исследования цифровизации уголовного производства. Сделан вывод, что неотложной является необходимость концептуальной разработки основных стратегических аспектов цифровизации уголовного производства. Одной из первых задач на этом пути является разработка понятийного аппарата и определение основных стратегических направлений и границ цифровизации с последующей разработкой соответствующих теоретико-правовых основ реализации цифровизации уголовного производства по каждому из направлений.

Ключевые слова: цифровизация, уголовное дело, электронное уголовное производство, цифровизация уголовного судопроизводства, электронное правосудие, электронные доказательства, электронные документы

CONCEPTUAL ASPECTS OF DIGITALIZATION OF CRIMINAL PROCEEDINGS IN THE CONTEXT OF CRIMINAL PROCEDURE RELATIONS

Abstract. The article is devoted to the definition of certain aspects of the conceptualization of the study of digitalization of criminal proceedings. The author identify the factors that determine the relevance of a comprehensive study of the use of digital technologies in criminal proceedings. Such factors include: socio-political, legal, criminogenic, praxeological. The main perspective directions of further research of digitalization of criminal proceedings are determined. It is concluded that there is an urgent need for conceptual development of the main strategic aspects of digitalization of criminal proceedings. One of the first tasks on this path is to develop the conceptual framework and determine the main strategic directions and boundaries of digitalization, with further development of appropriate theoretical and legal bases for the implementation of digitalization of criminal proceedings in each of the areas.

Keywords: digitalization, criminal case, electronic criminal proceedings, digitalization of criminal proceedings, electronic justice, electronic evidence, electronic documents

Стремительное внедрение информационных технологий во все сферы социальной жизни, наблюдающееся в последние годы, запустило глобальный процесс информатизации общества, всеобъемлющий переход к процессу создания, фиксирования и передачи информации в электронном пространстве. Автоматизация, оцифровка данных и диджитализация стали ключевыми лозунгами в разных социальных сферах, в основном в бизнесе и государственном управлении. Мировой современный тренд развития общества предполагает повсеместное использование информационных технологий во всех сферах и по всем направлениям человеческой жизнедеятельности. Среди принятых нормативных документов в последние годы немало таких, которые призваны закрепить отечественное направление общественного развития, коррелирующее с мировыми тенденциями. Среди примеров государственных правовых цифровых решений следует отметить, в частности, создание портала государственных услуг.

Учитывая такие тенденции развития нашего государства, вполне логично, что информатизация и цифровизация общества не обошли стороной и уголовное судопроизводство, которое поддается перманентному изменению и реформированию, находится в поиске оптимального баланса интересов государства, общества и отдельных участников уголовного процесса, стремится идти в ногу с научно-техническим прогрессом.

Цифровизацию обоснованно можно признать одной из основных тенденций развития российского уголовного производства. С одной стороны, внедрение новейших цифровых технологий в этой области весьма востребовано с учетом перспективы существенного повышения эффективности деятельности субъектов уголовного производства при решении его задач, в частности, в способе предоставления органам досудебного расследования новых возможностей по раскрытию преступления, установлению виновного лица и его местонахождения, ускорению производства через применение режима видеоконференции и т.п.

С другой стороны, автоматизация и перевод уголовного производства в электронный формат (создание электронного уголовного производства) значительно упростит взаимодействие субъектов уголовного производства вследствие внедрения электронной формы процессуальной коммуникации, уменьшит время согласования определенных разновидностей процессуальных решений, а следовательно, будет способствовать реализации принципа разумных сроков.

Проблематика цифровизации в области уголовного производства была предметом исследований таких представителей уголовно-процессуальной науки, как А. А. Аубакирова [1], Р. Я. Мамедов [2], В. И. Пржиленский [3], О. И. Андреева, В. В. Иванов, А. Ю. Нестеров, Т. В. Трубникова [4], А. А. Усачев [5], М. С. Спиридонов [6], А. А. Дмитриева, П. С. Пастухов [7], А. Р. Шарипова [8] и других ученых.

При этом примечательно то, что проблематика цифровизации уголовного производства нередко связывается исследователями с внедрением информационных технологий и переводом отдельных процессуальных отношений в систему электронного документооборота. Однако цифровизация уголовного производства не ограничивается исключительным использованием технологий; она характеризуется изменением культуры и способа мышления правоприменителей, обретением

ими цифровой компетентности; формированием новых способов и принципов цифрового взаимодействия участников правоотношений и т. д. Следует также отметить, что, несмотря на численность научных публикаций по заявленной тематике, сегодня отсутствует как единое понимание целей и границ цифровизации уголовного производства, так и комплексной ее стратегии, а следовательно, отсутствует интегрированный научно-прикладной взгляд на проблему, связанную с такой цифровизацией.

Такой уровень научной разработки этого направления нельзя признать достаточным для существующего запроса по концептуализации цифровой трансформации уголовного производства и создания доктринального основания будущим законодательным инициативам.

Поэтому представляется необходимым проведение фундаментального исследования по цифровой трансформации уголовного судопроизводства России с учетом лучших международных практик использования информационных технологий в уголовном производстве. Разработка ключевых положений (теоретико-прикладного и нормативного характера) цифровизации уголовного производства будет способствовать систематизации и алгоритмизации государственной деятельности в этой сфере. При этом первоочередными вопросами в данном контексте являются правовая и теоретическая диагностика ситуации в сфере цифровизации уголовного производства, формулировка понятийного аппарата и определение ее перспективных направлений.

Целью этого научного исследования является определение отдельных аспектов цифровизации уголовного производства, которые являются неотъемлемыми составляющими концептуализации такого процесса, а именно: определение различных факторов актуализации цифровой трансформации уголовного производства, осуществление правовой и теоретической диагностики цифровизации уголовного производства; обозначение актуальных направлений исследование в данной сфере.

Относительно факторов актуализации цифровой трансформации уголовного производства на современном этапе уголовно-процессуальная деятельность характеризуется наличием электронного сегмента, который в разных формах присутствует на всех ее этапах. В то же время процесс цифровизации этой области находится на стадии развития, что отмечается в ряде политических документов, и постоянной модификации уголовно-процессуального законодательства посредством внесения соответствующих изменений и дополнений, сопровождающих процесс постепенного перехода на электронный документооборот, внедрения «электронного правосудия» и расширения использования различных цифровых инструментов при реализации уголовно-процессуальной деятельности. Ускорение этого процесса определяется совокупностью разноплановых обстоятельств, в частности, социально-политического, нормативно-правового, криминогенного, праксеологического характера. Рассмотрим их более подробно.

В части **социально-политических факторов** в данном сегменте нашего исследования мы не ставим своей целью рассмотреть весь перечень таких факторов, актуализирующих цифровизацию уголовного производства. Нами будут

освещаться только наглядные факторы. Одними из них, подчеркнувшими необходимость цифровизации уголовного производства, особенно в векторе процессуальной коммуникации, стали карантинные ограничения, введенные во время пандемии COVID-19. Граждане впервые столкнулись с беспрецедентными до этого времени запретами, направленными на предотвращение распространения инфекционной болезни. Соответствующие ограничительные мероприятия активизировали поиск путей использования инновационных технологий для обеспечения деятельности судебной системы без угрозы доступности правосудия.

И в этом смысле пандемия COVID-19 [9] уже доказала важность и потребность цифровых технологий для обеспечения функционирования уголовного производства в дистанционных условиях и создала стимул для реформирования системы правосудия в этом направлении, реалии же военного положения в ряде российских регионов стали дополнительным толчком к ее ускорению. Следовательно, необходимость дальнейшей цифровой трансформации уголовного производства в России с существенной модификацией уголовно-процессуальной формы путем внедрения цифровых технологий перехода на полный электронный документооборот уже не вызывает сомнения и является делом времени.

Нормативно-правовой фактор актуализации цифровизации уголовного производства связан с состоянием ее законодательного обеспечения, значительно отстающего от объективных потребностей современности по более масштабному использованию цифровых технологий в уголовном процессе России.

Анализ действующего уголовно-процессуального законодательства свидетельствуют о хаотическом нормировании тех или иных вопросов внедрения цифровых технологий в область уголовного производства, в частности, относительно осуществления и фиксации электронных процедур, создания электронного уголовного производства и других направлений цифровизации. Такой уровень нормативной регламентации по большей части неудовлетворителен ввиду определенной правовой неопределенности, порождающей и расхождения в правоприменительной практике. К тому же, как уже отмечалось, цифровизация уголовного производства находится только на начальной стадии, соответственно предметом нормативного урегулирования должны стать и другие перспективные для уголовного судопроизводства цифровые решения.

Следовательно, очевидна потребность концептуальной разработки проблематики цифровизации уголовного производства, включающей в себя исследование как процесса цифровой трансформации уголовного производства, так и качества действующего уголовно-процессуального законодательства в данной сфере. Результаты такого исследования будут служить основой для взвешенных соответствующих законодательных решений по регламентации уголовно-процессуальных отношений.

Сущность **криминогенного фактора** актуализации комплексной цифровизации уголовного производства составляет объективный рост киберпреступности в нашей стране. Мощный процесс развития цифровой эры влечет за собой и существенную трансформацию преступной деятельности, использование новейших технологий в преступных целях, существенный рост кибератак. Соответственно,

одним из приоритетных направлений дальнейшего реформирования российского уголовно-процессуального законодательства является нормативное сопровождение противодействия киберпреступности.

Недостаточный уровень правового регулирования, его неопределенность порождают неоднородность правоприменительной практики, обуславливающей существование тесно связанного с нормативно-правовым праксеологического аспекта актуальности концептуальной разработки вопросов цифровизации уголовного производства. Последний продиктован, в частности, востребованностью на практике доктринальных разработок в аспекте использования электронной информации в доказывании, решении ряда дискуссионных проблем по нормативной регламентации отдельных аспектов процессуального порядка применения режима видеоконференции (определение понятий технических средств и технологий, используемых при применении режима видеоконференции; допустимости информации, полученной с применением режима видеоконференции и др.); определение «цифровых особенностей» применения отдельных мер обеспечения уголовного производства и проведения следственных (розыскных) и негласных следственных (розыскных) действий. Соответственно «отсутствие последовательной «цифровой политики» уголовно-процессуального закона влечет за собой появление противоположных по содержанию позиции судебных органов.

Указанные и другие обстоятельства являются элементами многоаспектной системы факторов, не только способствующих ускорению процесса цифровой трансформации национального уголовного судопроизводства, но и актуализирующих проведение концептуального исследования цифровизации уголовного производства.

Нами определены лишь основные направления цифровизации уголовного производства вне их детального раскрытия. Представляется, что актуальными для научного поиска в области цифровизации уголовного производства являются следующие направления:

1. Исследование методологических вопросов цифровизации уголовного производства. К таким относятся: теоретико-правовые аспекты обеспечения прав и свобод человека в условиях цифровизации уголовного производства; формулировка понятийного аппарата; определение границ цифровизации; разработка стандартов, основ и гарантий и др.

2. Разработка теоретико-правовых основ использования цифровых технологий для оптимизации уголовно-процессуальной деятельности:

– перевод документооборота в области уголовного производства в электронную форму (настоятельная необходимость перевода документирования уголовного производства в электронный сегмент является базовой предпосылкой разработки электронного уголовного производства);

– введение единой интегрированной электронной системы органов уголовной юстиции, соединенной с общегосударственными электронными реестрами и базами данных электронного уголовного производства;

– использование информационно-аналитических систем и интеллектуальных алгоритмов для повышения эффективности расследования уголовных правонарушений;

– расширение цифрового сегмента при проведении следственных (розыскных), негласных следственных (розыскных) и других процессуальных действий;

– совершенствование судебного контроля в условиях цифровизации уголовного производства;

– обеспечение выполнения координационных функций в области цифровизации уголовного производства.

3. Создание теоретической основы для дальнейшего внедрения электронного правосудия в России.

4. Исследование границ и возможностей использования технологий искусственного интеллекта в уголовном производстве.

5. Определение механизма электронной процессуальной коммуникации участников уголовного производства (создание единой цифровой платформы для коммуникации) и особенностей электронного взаимодействия населения с государственными органами на начальном этапе досудебного расследования (создание online серверов для подачи заявлений, сообщений о совершенном правонарушении).

6. Внедрение электронных механизмов предотвращения нарушения прав и свобод участников уголовного производства.

7. Разработка теоретико-правовых основ использования электронных доказательств в уголовном производстве (определение специфики доказывания в условиях цифровизации уголовного производства).

8. Исследование процессуальных особенностей расследования киберпреступлений.

9. Использование цифровых технологий при международном сотрудничестве в уголовном производстве.

10. Определение путей формирования цифровой компетентности правоприменителей.

Определенные направления, безусловно, тесно связаны друг с другом. Однако отдельное их выделение в качестве самостоятельных векторов научного исследования необходимо для всестороннего и полного анализа соответствующей проблематики и получения научных результатов, которые в совокупности будут создавать концепцию цифровой трансформации уголовного производства в России.

Проведенное научное исследование закладывает фундамент концептуализации в условиях цифровизации уголовного производства и определяет стратегию дальнейшей разработки этой проблематики. Можно констатировать, что на сегодняшний день цифровизация уголовного производства находится на начальной стадии. Законодательные же инициативы по внедрению цифровых технологий в сферу уголовного производства не носят системный характер, а цифровые новации действующего уголовно-процессуального законодательства нуждаются в оценке с точки зрения соответствия их стандартам качества закона. В этой связи можно утверждать, что необходима концептуальная разработка основных стратегических аспектов условий цифровизации уголовного производства. Одной из первых задач на этом пути является определение основных стратегических направлений научного поиска в данной сфере.

Ближайшей перспективой концептуализации в условиях цифровизации уголовного производства является определение понятийного аппарата и границ такой цифровизации, разработка теоретико-правовых основ ее реализации по каждому из выделенных направлений. В этом аспекте не вызывает сомнений важность осуществления научного поиска в рассматриваемой сфере.

Список литературы

1. Аубакирова А. А. Цифровизация уголовного процесса // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 41–43.

2. Мамедов Р. Я. Цифровизация ведения уголовного процесса // Юридический вестник Кубанского государственного университета. 2019. № 1. С. 67–71.

3. Пржиленский В. И. Теоретико-познавательные основы уголовного судопроизводства в контексте возможностей его цифровизации // Журнал российского права. 2019. № 7. С. 17–29.

4. Андреева О. И., Иванов В. В., Нестеров А. Ю., Трубникова Т. В. Технологии распознавания лиц в уголовном судопроизводстве: проблема оснований правового регулирования использования искусственного интеллекта // Вестник Томского государственного университета. 2019. № 449. С. 201–212.

5. Усачев А. А. Цифровизация начального этапа досудебного производства и правовая определенность российского уголовного процесса // Вестник Университета имени О. Е. Кутафина (МГЮА). 2019. № 8 (60). С. 100–111.

6. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481–497.

7. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270–295.

8. Шарипова А. Р. Направления цифровизации уголовного судопроизводства: применимый опыт арбитражного процесса // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 131–135.

9. Пандемия и самоизоляция: криминальные угрозы и правовые последствия / А. А. Шутова, З. И. Хисамова, М. А. Ефремова, А. А. Никифорова. М.: Проспект, 2021. 112 с. EDN: ABIDXJ

Р. Р. Хафизова,
магистрант,
Казанский (Приволжский) федеральный университет

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ РОЛИ ПРЕПОДАВАТЕЛЯ В ОБРАЗОВАТЕЛЬНОЙ СРЕДЕ

Аннотация. Статья посвящена особенностям и изменениям современного образования в условиях перехода общества к цифровой экономике. Современный образовательный процесс требует от преподавателя умения адаптироваться

к новым технологиям и использовать цифровые инструменты для облегчения обучения и повышения эффективности учебного процесса. Цифровая трансформация роли преподавателя включает в себя использование компьютеров, Интернета, программного обеспечения и электронных учебных материалов для обогащения учебного процесса и создания интерактивной и увлекательной среды для обучения.

Ключевые слова: право, цифровые технологии, образование, преподавание, дистанционное обучение, цифровое поколение, новая экосистема

DIGITAL TRANSFORMATION OF THE ROLE OF THE TEACHER IN THE EDUCATIONAL ENVIRONMENT

Abstract. The article is devoted to the features and changes of modern education in the context of the transition of society to the digital economy. The modern educational process requires the teacher to be able to adapt to new technologies and use digital tools to facilitate learning and increase the efficiency of the educational process. Digital transformation of the role of the teacher involves the use of computers, the Internet, software and electronic learning materials to enrich the learning process and create an interactive and engaging learning environment.

Keywords: law, digital technologies, education, teaching, distance learning, digital generation, new ecosystem

В условиях перехода общества к цифровой экономике, глобализации, развития информационных технологий трансформируется и современное образование. Вызовы цифровой эпохи, воздействуя на образование, меняют его содержание и структуру, цели и методы, характер взаимодействия участников образовательного процесса. В результате формируется новая образовательная экосистема, включающая новые технологические платформы, новую роль преподавателя и образовательный дизайн. Происходит переход от концепции классического образования к «lifelong learning», т. е. непрерывному обучению в течение жизни, а также к смешанному обучению, предусматривающему применение дистанционных технологий обучения [2. С. 95].

Такие изменения требуют пересмотра традиционных подходов к обучению и оценке знаний. Это вызывает необходимость разработки новых учебных программ, которые бы отвечали потребностям цифровой экономики и современным технологиям.

Одним из главных достоинств цифровой экосистемы в образовании является доступность к образованию для всех групп населения. Возможность изучать материалы онлайн и получать знания удаленно открывает границы для тех, кто ранее был исключен из образовательного процесса по различным причинам.

Технологические платформы, такие как онлайн-курсы, видеолекции, вебинары и т. д., позволяют получать знания в любое время и любом месте. Это дает возможность гибкого распределения времени и ресурсов, что особенно важно для работающих людей, желающих получить дополнительное образование или прокачать свои навыки.

В данной новой эпохе роль преподавателя также меняется. Если раньше преподаватель был центром знаний, то сейчас его роль больше сопровождающая и ориентирующая сторона. Преподаватель помогает студентам освоить материалы, но больше акцент делается на самостоятельное изучение и решение задач.

Образовательное содержание также должно быть адаптировано к изменяющемуся миру. Важно учитывать современные требования рынка труда и развивать навыки, которые будут востребованы в будущем. Кроме того, формирование критического мышления, навыков самоорганизации и саморазвития, коммуникации и сотрудничества становятся все более важными в новой образовательной экосистеме.

Таким образом, цифровая эпоха изменяет образование, делая его более доступным и гибким, и требует пересмотра традиционных подходов и создания новых образовательных экосистем. Для успешной адаптации к этим изменениям необходимо постоянно обновлять знания и развивать навыки в течение всей жизни.

Цифровизация образования – значимая составляющая процесса формирования «нового человека», причем человека во всех его личностных аспектах – от гражданина до специалиста-профессионала. При этом в обществе – и в педагогическом сообществе, и среди родителей, и у работодателей присутствует недоверие к цифровизации образования и связанным с ним переменам. Возникает вопрос: будет ли такое образование качественным, обеспечит ли появление в различных профессиональных областях профессионалов личностный карьерный рост и благополучие человека. Плюсы у цифрового образования появляются, если студент мотивирован, знает, чего хочет от образования, способен к самоорганизации и самообразованию, умеет адекватно оценивать себя, дифференцировать ресурсы и информацию (это должно быть сформировано в школе и далее поддерживаться в вузе), если он не «замкнут» на сеть [1. С. 26].

Другой вопрос о преподавателях в условиях цифровизации. Цифровая трансформация преподавателя в образовательной среде означает использование цифровых технологий и инструментов для улучшения процесса обучения и повышения качества образования. Эта трансформация включает в себя изменение подхода к преподаванию, интеграцию цифровых ресурсов и инструментов в учебный процесс, а также развитие цифровых навыков у преподавателей.

Одним из основных аспектов цифровой трансформации преподавателя является использование электронных учебных материалов и онлайн-платформ. Преподаватели могут создавать и делиться цифровыми учебными материалами, такими как презентации, видеоуроки, интерактивные задания и тесты. Это помогает студентам получить доступ к актуальной информации и позволяет преподавателям эффективно представлять материалы.

Другим аспектом цифровой трансформации преподавателя является использование онлайн-инструментов и приложений для коммуникации и совместной работы. Преподаватели могут использовать такие инструменты, как видеоконференции, чаты, форумы и облачные хранилища, чтобы поддерживать коммуникацию с учащимися и сотрудничество между студентами. Это создает возможность для более гибкого и интерактивного обучения.

Цифровая трансформация преподавателя также включает развитие цифровых навыков и компетенций. Преподаватели должны быть готовы использовать новые технологии и уметь эффективно с помощью них обучать. Это может включать обучение в области цифровой грамотности, а также использование профессиональных разработок и образовательных ресурсов.

Цифровая трансформация преподавателя в образовательной среде имеет большие преимущества. Она помогает улучшить доступность образования и предоставляет студентам новые возможности для самостоятельного обучения. Также она может повысить эффективность преподавания и позволит преподавателям индивидуализировать образовательный процесс в соответствии с потребностями каждого студента.

Одной из основных проблем цифровой трансформации преподавателя является недостаточная компетентность и уверенность в использовании цифровых технологий. Многие преподаватели не получили достаточного обучения в этой области и не имеют достаточного опыта работы с цифровыми инструментами и ресурсами.

Другой проблемой является ограниченный доступ к необходимым ресурсам и инфраструктуре. Некоторые школы и университеты могут не обладать достаточными средствами для создания цифровых учебных материалов или не иметь доступа к высокоскоростному Интернету.

Также преподавателям может быть сложно адаптироваться к изменениям в образовательном процессе, связанным с цифровой трансформацией. Возможно, они не знают, как интегрировать цифровые инструменты в свою учебную программу или как оценивать эффективность этих инструментов.

Один из путей решения этих проблем – обеспечение преподавателей необходимыми знаниями и навыками в области цифровой трансформации. Преподавателям следует предлагать обучение и поддержку в использовании цифровых инструментов и ресурсов. Это может быть в форме специальных курсов, тренингов или менторской поддержки.

Также необходимо обеспечить доступ к соответствующей инфраструктуре и ресурсам. Школы и университеты должны обеспечить наличие высокоскоростного Интернета, компьютеров и других необходимых технических средств для работы с цифровыми инструментами. Можно также сотрудничать с внешними организациями или компаниями, чтобы получить дополнительную поддержку и ресурсы.

Важно также обеспечить преподавателям поддержку и руководство в процессе адаптации к изменениям, связанным с цифровой трансформацией. Это может быть предложено в виде консультаций, обратной связи или обмена опытом с другими преподавателями.

Кроме того, педагоги должны быть готовы к использованию новых информационных технологий и электронных образовательных ресурсов. Они должны уметь эффективно работать с компьютерами, интернетом, программным обеспечением и другими цифровыми инструментами. Также, в условиях цифровой экономики особое внимание должно уделяться развитию навыков цифровой грамотности.

Педагоги должны уметь эффективно находить, анализировать и использовать информацию из различных цифровых источников. Они должны уметь критически оценивать информацию и использовать ее в образовательном процессе.

Таким образом, сам педагог становится ключевым элементом в реализации дистанционного обучения в цифровой экономике. Он должен иметь не только традиционные педагогические знания и навыки, но и быть готовым к использованию новых технологий и методов обучения. Только тогда будет возможно создание эффективной и качественной системы дистанционного образования.

Список литературы

1. Дьякова Е. А., Сечкарева Г. Г. Цифровизация образования как основа подготовки учителя XXI века: проблемы и решения // Вестник Армавирского государственного педагогического университета. 2019. № 2. С. 24–36.

2. Стеблецова И. С., Гейцман Л. Э. Цифровая трансформация преподавателя в условиях современного образовательного процесса // Технологии в образовании. 2021. № 4. С. 95–100.

А. Д. Цветкова,
студент,
Уральский государственный юридический университет
имени В. Ф. Яковлева

ПРОБЛЕМА РАССОГЛАСОВАННОСТИ ПРИ ЦИФРОВИЗАЦИИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. В работе рассматриваются аспекты единой комплексной проблемы: согласования научных юридических исследований, в которых предлагается внедрение какой-либо цифровой технологии, с действительными потребностями практических работников, для которых данная технология предназначена, и программно-техническими возможностями ее реализации. Решение проблемы видится в создании условий для общения представителей юридической науки с практическим работниками и специалистами в сфере цифровых технологий. В качестве таких условий предлагаются дополнительное рецензирование юридических научных работ по смежной тематики специалистом в сфере современных технологий; обязательное для ученых прохождение ежегодной стажировки в правоохранительном органе; кооперация юридических и технических вузов; организация междисциплинарных научно-практических конференций и т. д.

Ключевые слова: интеграция науки и практики, суд, следственный комитет, компьютерный (клавиатурный) почерк, цифровизация юридической деятельности, проблемы цифровизации, научно-образовательные центры

Финансирование: Исследование выполнено за счет гранта Российского научного фонда № 23-78-10011, https://rscf.ru/project/23-78-10011

THE PROBLEM OF INCONSISTENCY IN THE DIGITALISATION OF LAW ENFORCEMENT ACTIVITIES

Abstract. The paper deals with the aspects of a single complex problem: reconciliation of scientific legal research, which proposes the introduction of any digital technology, with the actual needs of practitioners, for whom this technology is intended, and the software and hardware capabilities of its implementation. The solution to the problem is seen in the creation of conditions for communication between representatives of legal science and practitioners and specialists in the field of digital technologies. As such conditions are proposed additional reviewing of legal scientific works on related topics by a specialist in the field of modern technologies; compulsory for scientists to undergo annual internship in a law enforcement agency; cooperation of law and technical universities; organisation of interdisciplinary scientific-practical conferences, etc.

Keywords: integration of science and practice, court, investigative committee, computer (keyboard) handwriting, digitalisation of legal activity, problems of digitalisation, scientific and educational centers

Трендом современной эпохи является всеобщая цифровизация: она обсуждается в научной и научно-популярной среде во всех направлениях человеческого знания: гуманитарных, естественных и технических науках; становится важной темой в искусстве; с различных сторон оценивается политическими группами и т. д. Сегодня цифровые технологии в целом уже никого не удивляют, новые разработки воспринимаются как обыденное и закономерное движение прогресса.

Однако, несмотря на такую радужность картины, детальное ее рассмотрение позволяет выявить множество проблем. Причем мы не говорим о тех проблемах, которые порождают и поддерживают дискуссию о благотворных или разрушительных последствиях стремительного развития современных технологий как в ближайшем будущем, так и в далекой перспективе, хотя они безусловно играют не последнюю роль [22, 23]. В настоящей работе внимание будет уделено, по существу, одной комплексной проблеме, которая не столь заметна, как противостояние сторонников и противников цифровизации [11], но при этом не менее значима. Постулируя как аксиому, что прогресс и совершенствование технологий неизбежный процесс, который будет только наращивать свои темпы [14. С. 118], остановим свое внимание на проблеме согласования между собой научных юридических рекомендаций, технических возможностей и потребностей юридической практики.

Большое число юридических научных конференций сегодня посвящено цифровой трансформации права и отдельных его отраслей. Множество научных статей, диссертаций и иных работ написано на аналогичную тематику [1, 25, 5, 18]. При этом в исследованиях, особенно диссертационных, встречаются результаты опросов практических работников, которые подтверждают актуальность труда ученого и позволяют судить о востребованности в профессиональном сообществе технико-технологических нововведений, предлагаемых автором [4, 6, 10, 12].

Одновременно с этим в большинстве случаев прикладные технологические системы не могут быть воплощены в жизнь юристом без специальных знаний. Для этого требуется или наличие соответствующих компетенций в компьютерно-технической сфере знаний, или помощь профессиональных программистов. Последние в свою очередь могут помочь неспециалисту в определении границ возможного: исследовательская мысль может быть подвержена излишнему оптимизму, не позволяющему ученому-юристу оценить все риски и ограничения, в связи с которыми реализация технологии, несмотря на всю привлекательность, невозможна при современном уровне технологического развития [18. С. 215].

Безусловно, не все ученые-юристы в силу каких-либо причин согласуют свои работы с целевой аудиторией или представителями других наук. Это может быть связано со следующими обстоятельствами.

Низкий уровень научной компетенции. Это актуально для студентов (начинающих исследователей), которых в некоторых учебных заведениях обязуют публиковать научные статьи. В итоге возникает ситуация, когда юношеский романтизм, отсутствие системных знаний об особенностях научно-исследовательской работы, а также объективная сложность получения эмпирического материала и формирования деловых контактов с представителями неюридических профессий, действуя в совокупности, приводят к переполнению информационного пространства неточными, когда, например, отождествляются понятия «цифровой личности» и «робота» [24. С. 130], и оторванными от реальных нужд работами. Далее данные идеи имеют риск мультиплицироваться в результате цитирования и самоцитирования, а также привести к появлению прикладных проектов, в которых исходное понятие наполняется иными смыслами. Последнее характерно, например, для концепции «нейронета», под которой сегодня реализуются коммерческие проекты, основанные на простой технологии искусственного интеллекта, не предполагающей интеграции мозга человека с машиной [15. С. 86–87].

Первостепенно для решения этой проблемы следует отказаться от политики обязательной научной деятельности студентов, а для тех, кто имеет интерес и способности к ней – на ранних стадиях проводить обучающие мероприятия, которые, следует отметить, практикуются в вузах. Далее, считаем небесполезным уже не только для студентов, но и для ученых любого уровня внедрить систему двойного рецензирования научных публикаций (внутреннего для студентов в ситуациях, где требуется рецензия научного руководителя; внешнего – в редакциях журналов), а также добавления дополнительного консультанта в диссертационных исследованиях [20]. В итоге должно получаться следующее: основной рецензент (научный руководитель, консультант) является специалистом в области юриспруденции, а дополнительный рецензент (консультант) – в компьютерно-технической сфере. Это позволит исключить практику опубликования работ, которые объективно не согласуются с современным уровнем цифровых технологий.

Объективная сложность получения эмпирического материала. Так, нередко можно встретить нежелание практических работников (например, судей, следователей, дознавателей и т. д.) тратить собственное время на заполнение каких-либо анкет, даже если их результаты могут впоследствии помочь

в профессиональной деятельности. Кроме того, отдельной трудностью может являться доставление опросников и иных материалов для сбора статистики до конкретных представителей правоохранительной сферы: на объектах службы действует пропускной режим; руководитель отдела (председатель суда) может не давать своего согласия для проведения опроса и т. д.

Следует также отметить, что указанная проблема может возникнуть у любого исследователя, поскольку авторитет в научной среде не обязательно влияет на статус в сообществе практических работников. Однако, если у кандидатов и докторов наук есть возможность задействовать профессиональные контакты и административные ресурсы: провести анкетирование практикующих магистрантов или обучающихся на курсах повышения квалификации либо получить гарантийное письмо ректора образовательной организации, то для студента или даже аспиранта, хотя и в меньшей степени, данные пути ограничены. Основное, на что можно рассчитывать начинающим исследователям, – помощь научного руководителя. Но если каждый студент будет для своей статьи опрашивать работников следственных органов, суда и т. д., то последние все время будут вынуждены посвятить заполнению анкет, а не выполнению действительных рабочих обязанностей.

К сожалению, простых рекомендаций для решения указанной проблемы сформулировать нельзя: в каждом конкретном случае нужно обращаться за помощью к старшим коллегам, знакомым, занятым в практической деятельности, индивидуально разговаривать с потенциальными респондентами, обосновывая важность проводимого анкетирования.

Разобщенность науки и практики. Описанная в предыдущем пункте проблема возникает, когда у исследователя уже есть как минимум общее представление будущей работы, а значит он примерно представляет, что намеревается предложить профессиональному сообществу для оптимизации рабочих процессов. Однако прежде может возникнуть проблема принципиальной неосведомленности теоретиков о потребностях практиков.

Во многом на решение данной проблемы направлены совместные научно-практические конференции, однако если представителей коммерческого сектора можно встретить на подобных мероприятиях, то работников правоохранительных органов, особенно рядовых служащих – почти нереально. Даже если не учитывать, что практические работники в целом предпочитают ведомственные конференции, ограниченные узкими рамками сотрудников полиции, следственного комитета, суда и т. д., их посещают преимущественно лица, занимающие руководящие должности, или те, кто сочетает практическую и научную деятельность. Такая выборка существенно ограничивает круг проблем, которые будут затронуты в ходе обсуждения, поскольку проблемы начальствующего и рядовых звеньев разнятся. Например, в центральном аппарате следственного комитета Российской Федерации функционируют модули АИС «Надзор», тогда как районные следственные отделы подчас даже не имеют полного доступа к справочно-правовым системам, а весь документооборот обязаны вести в бумажной форме.

Для получения информации о реальных потребностях практики оптимальным является совмещение научной и практической деятельности. Однако это

невозможно в связи с тем, что глубокая наука и качественное выполнение служебных обязанностей требуют больших затрат времени и сил. Поэтому считаем перспективным возродить советскую практику «ознакомления», в рамках которой обязать всех научных работников раз в год проходить недельную стажировку в том органе, к деятельности которого относится сфера его научных интересов: например, для криминалистов таковыми будут следственные отделы следственного комитета и полиции, а также экспертно-криминалистические центры.

Игнорирование «несущественных» потребностей. Данная проблема является прямым продолжением описанной выше, поскольку может быть связана с «объективным игнорированием», когда о таких проблемах, затрагивающих интересы низшего звена служащих, просто не знают. Однако незнание или, порой, нежелание знать может быть связано с погоней за новаторством, стремлением «быть в тренде», разрабатывать то, о чем раньше никто не слышал, и т. д. В этой технологической гонке, безусловно, появляются весьма интересные и востребованные, как показывают опросы, технологические решения, способные не только облегчить работу сотрудников правоохранительных органов, помочь им в принятии решений, но и продвинуть прогресс [3. С. 5–6; 7. С. 16–17]. Однако из внимания выпадают менее уникальные трудности, с которыми сталкиваются эти же работники. Так, например, внедрив в деятельность правоохранительных органов автоматизированные системы электронного документооборота, их развитие и совершенствование вышло из сферы интереса ученых и разработчиков, тогда как на практике осталось большое число проблем, связанных в первую очередь с дублированием документации, несовершенством алгоритмов распознавания в системе обезличивания судебных решений и т. п. Другой иллюстрацией данной проблемы является отсутствие системы-транскрайбера для автоматизированного перевода записи судебного заседания в письменный формат протокола в то время, как юристы обсуждают потенциальную возможность замены судьи искусственным интеллектом, принимающим решение в споре [13]. Вместе с тем укажем, что проблема автоматизированного транскрибирования весьма широко обсуждается в рамках оптимизации работы следователя [9, 2], что позволяет выделить еще один аспект рассматриваемой проблемы: отсутствие кооперации ученых даже в смежных отраслях науки: криминалистике, ориентированной на предварительное расследование, и уголовном процессе, сосредоточенном на судебных стадиях разбирательства по делу.

Эта проблема решается аналогично описанной выше с тем лишь уточнением, что в рамках «ознакомления» должно обязательно предусматриваться в том числе знакомство с обыденными задачами представителей всех должностей, а не только руководящего звена.

Излишняя самоуверенность в собственной компьютерно-технической грамотности. Всеобщая распространенность цифровых технологий дает иллюзию их постижимости специалистом в любой области знаний, в связи с чем некоторые юристы, не имея специальной подготовки, берутся разрабатывать темы, связанные, например, с искусственным интеллектом или криптовалютой и т. д., в итоге предлагая модели интеграции или ограничения, которые не достижимы из-за специфики самой технологии. Так, например, на одной конференции была

озвучена позиция, что использование системы «Честный знак» позволит идентифицировать конкретного покупателя, когда на деле ее возможности ограничиваются локализацией точки розничной торговли, но никак не предполагают сбор персонализирующих сведений, в частности о банковских реквизитах карты, которой производилась оплата продукции с кодом марки.

Другие, осознавая недостаточность популярных знаний по отдельным вопросам цифровизации, считают, что теоретическое погружение в конкретную проблему позволит преодолеть техническую неграмотность, создаст полное представление о том, как технология работает, какие у нее существуют ограничения, риски широкого распространения и т. д. Несмотря на обоснованность такой позиции, изучение научных работ по техническим специальностям в конкретно выбранной области является лишь первым шагом, который бессмысленен без консультации с практикующим программистом. Это связано с тем, что детально проработанный проект, по которому находятся развернутые научные публикации с описанием формул, лежащих в основе функционирования системы, вполне может ограничиваться лабораторными условиями, и нет гарантии, что подобная технологическая система будет реально функциональной.

Так, в научных библиотеках содержится большое число статей, в которых описываются модели распознания пользователя компьютерной системы по его клавиатурному почерку [17, 16, 8], однако непосредственно программы в свободном доступе обнаружить почти нереально, а те, что находятся, анализируют слишком узкий перечень идентификационно-значимых признаков.

Таким образом, после изучения темы на теоретическом уровне требуется обсудить реальную возможность технической реализации задуманного проекта с профессионалами в соответствующей области, а еще лучше непосредственно присутствовать при создании технологической системы, ее обучении (если говорить про технологию нейронных сетей), так как именно это позволит понять, как функционируют система, что она может и, главное, почему.

Разобщенность разных сфер научного знания. Данная проблема является существенной преградой для решения трудности, описанной в предыдущем пункте. Так, юристы представляют собой сравнительно замкнутое сообщество, а если в их кругу имеются представители иных профессий, то неформальное общение очень быстро сводится к обсуждению правовых вопросов, так они в той или иной мере затрагивают всех, а сами юристы к тому же имеют профессионально поставленную речь. Вместе с тем специалисты в области компьютерных технологий – часто замкнутые и необщительные люди, живущие в виртуальной среде. В результате, потенциальная возможность случайного знакомства юриста с программистом очень мала, а после знакомства еще необходимо «найти общий язык» с тем, чтобы достичь взаимопонимания и согласованности между желаемым итоговым видом технологии и техническими возможностями ее разработки.

Для решения этой проблемы весьма перспективным является кооперация университетов различного профиля либо университетов с различными компаниями. Этого можно достичь с помощью научно-образовательных центров, которые объединяют в рамках перспективных направлений национальной политики различные организации: вузы, научно-исследовательские институты, промышленные

корпорации, цифровые компании и т. д. [21]. Другая модель: коллаборация университетов, например, на уровне совместных магистерских программ юридического и технического университетов, либо по модели взаимообучения. Последняя, на наш взгляд, должна заключаться в том, что неделю в семестре преподаватели из одного университета будут проводить пары по основам своей дисциплины в вузе, с которым заключено соглашение, и наоборот. Также видится весьма перспективным проведение совместных научно-практических конференций для ученых (в том числе начинающих исследователей) в юридических и компьютерно-технической областях знания. Эти меры позволят объединить исследователей в различных сферах, дать возможность сформировать профессиональные контакты.

Всеобщая цифровизация предъявляет новые требования к научным исследованиям: их актуальность и достоверность должны подтверждаться запросом со стороны профессионального сообщества и технической возможностью реализации предлагаемых технологических систем. Для этого важно получать обратную связь от практических работников, выяснять действительные пробелы в цифровой трансформации правоохранительной деятельности, детально изучать техническую сторону вопроса конкретной технологии, взаимодействовать с представителями компьютерно-технической области знания с тем, чтобы удостовериться в реализуемости проекта и лучше понять особенности функционирования цифровой системы. Однако воплощение указанных рекомендаций в жизнь может быть затруднительно, в связи с чем преодоление большинства проблем возможно следующими методами:

1. Введение обязательного двойного рецензирования (научного консультирования) по работам, соединяющим в себе юридические и компьютерно-технические идеи.

2. Введение практики ежегодного «ознакомления» ученых в течение недели с работой органа, на сотрудников которого ориентированы их исследования.

3. Активизация взаимодействий работников и обучающихся организаций – членов научно-исследовательских центров.

4. Кооперация университетов, занятых подготовкой юристов и специалистов в области цифровых технологий, в формате совместных учебных программ, обмена учебными курсами на неделю в семестре.

5. Организация совместных научно-практических конференций для юристов и программистов.

Помимо перечисленного, следует активизировать и поддерживать практику дополнительного обучения заинтересованных студентов основам научно-исследовательской деятельности, проведения научно-практических конференций, объединяющих среди участников ученых и практиков. Таким образом, удастся достичь реальной востребованности цифровых проектов у непосредственной целевой аудитории, а также их технологической адекватности и реализуемости.

Список литературы

1. Аржанникова М. И. Цифровизация в праве // Актуальные научные исследования в современном мире. 2020. № 5–3(61). С. 21–26.

2. Балалаева М. В. Технология использования программ-транскрайберов при проведении допроса: оценка эффективности // Современное уголовно-процессуальное

право – уроки истории и проблемы дальнейшего реформирования. 2020. Т. 1, № 1(2). С. 22–28.

3. Бахтеев Д. В. Искусственный интеллект в следственной деятельности: задачи и проблемы // Российский следователь. 2020. № 9. С. 3–6. DOI: 10.18572/1812-3783-2020-9-3-6

4. Бахтеев Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: дис. … д-ра юрид. наук. Екатеринбург, 2022. 504 с.

5. Бессонов А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография. М.: Проспект, 2021. 816 с.

6. Бессонов А. А. Современные информационные технологии на службе следствия // Сибирские уголовно-процессуальные и криминалистические чтения. 2022. № 1(35). С. 94–100. DOI: 10.17150/2411-6122.2022.1.94-100.

7. Бессонов А. А. Цифровые технологии в криминалистическом обеспечении расследования серийных убийств // Советская и российская криминалистика: традиции и перспективы: материалы Всероссийской научно-практической конференции с международным участием, Москва, 02 февраля 2023 года. М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 14–19.

8. Варламова С. А., Вавилина Е. А. Идентификация пользователя на основе клавиатурного почерка // Инновационное приборостроение. 2023. Т. 2, № 3. С. 67–71. DOI: 10.31799/2949-0693-2023-3-67-71

9. Вахмянина Н. Б., Иванов Э. А. Возможности использования программ-транскрайберов при производстве следственных действий // Российский следователь. 2019. № 2. С. 6–9.

10. Вехов В. Б. Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. … д-ра юрид. наук. Волгоград, 2008. 561 с.

11. Готчина Л. В. Цифровизация наркопреступлений и противодействия им // Криминология: вчера, сегодня, завтра. 2019. № 4(55). С. 32–36.

12. Замараева Н. А. Правовые и организационно-методические проблемы использования компьютерных технологий при производстве судебных экспертиз: дис. … канд. юрид. наук. М., 2001. 202 с.

13. Казиханова С. С. О проблеме использования искусственного интеллекта в качестве судьи // Высокотехнологичное право: современные вызовы: материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Часть 1. Красноярск: Красноярский государственный аграрный университет, 2023. С. 146–152.

14. Колесов М. В. О некоторых вопросах межведомственного электронного взаимодействия // Горизонты гуманитарного знания. 2018. № 3. С. 116–122. DOI: 10.17805/ggz.2018.3.9

15. Лаптев В. А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2. С. 79–102.

16. Ложников П. С., Сулавко А. Е. Технология идентификации пользователей компьютерных систем по динамике подсознательных движений // Автоматизация. Современные технологии. 2015. № 5. С. 31–36.

17. Мазниченко Н. И. Подход к повышению надежности идентификации пользователей компьютерных систем по клавиатурному почерку // The Progressive Researches Science & Genesis. 2014. № 1. С. 66–71.

18. Марковичева Е. В. Цифровизация уголовного процесса: мифы и реальность // Судебная реформа в современной России: результаты, проблемы и перспективы: материалы Международной научно-практической конференции, посвященной 100-летию Кубанского государственного университета, Краснодар, 27 марта 2020 г. / отв. ред. В. А. Семенцов. Краснодар: Кубанский государственный университет, 2020. С. 213–217.

19. Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. Воронеж, 2001. 386 с.

20. Морозова А. Л. Криминалистическое исследование потожировых следов рук человека с целью установления их давности: дис. … канд. юрид. наук. М., 2000. 120 с.

21. Научно-образовательные центры мирового уровня: официальный сайт. URL: https://ноц.рф/

22. Порываева О. В. Некоторые аспекты влияния цифровизации на гражданское право // Электронное приложение к Российскому юридическому журналу. 2020. № 3. С. 60–62. DOI: 10.34076/2219-6838-2020-3-60-62.

23. Саркисян А. А. Профессия судебного эксперта в условиях цифровизации // Союз криминалистов и криминологов. 2020. № 1. С. 87–93. DOI 10.31085/2310-8681-2020-1-207-87-93

24. Хачатрян С. А. Право и цифровизация: проблемы взаимодействия // Интеллектуальные ресурсы – региональному развитию. 2020. № 1. С. 429–434.

25. Электронные доказательства в уголовном судопроизводстве: учебное пособие / С. В. Зуев, Д. В. Бахтеев, В. Б. Вехов [и др.]. 1-е изд. М.: Юрайт, 2021. 193 с.

А. М. Чечурин,
студент,
Елецкий государственный университет
имени И. А. Бунина
А. С. Сикач,
студент,
Дальневосточный федеральный университет

НОРМАТИВИЗМ VS ТОТАЛЬНАЯ АВТОНОМИЯ: ЕСТЬ ЛИ МЕСТО ПРАВОВОЙ РЕГУЛЯЦИИ В КОНТЕКСТЕ МЕТАМИРОВ?

Аннотация. В статье предпринимается попытка комплексного осмысления сущностного содержания категории метавселенных и действительного состояния механизма нормативной правовой регуляции отношений, опосредованных цифровой формой, с целью выработки качественного баланса между их саморегуляцией и неизбежным проникновением в таковые элементы нормативных предписаний.

На основе предпосылок, обнаруживаемых в действующем национальном и международном праве, формулируется и обосновывается предмет и объект нового правового явления – права метавселенных, ее содержательного и институционального деления.

Ключевые слова: право, этика, виртуальная реальность, метавселенная, нормативизм, правовая автономия

NORMATIVISM VS TOTAL AUTONOMY: IS THERE A PLACE FOR RIGHT REGULATION IN THE CONTEXT OF METAWORLDS? (PROBLEM STATEMENT)

Abstract. Within the framework of this article, the authors attempt to comprehensively comprehend the essential content of the category of metaverses, as well as the actual state of the mechanism of normative legal regulation of relations mediated by digital form, in order to develop a qualitative balance between their self-regulation and the inevitable penetration of elements of normative prescriptions into such. Based on the prerequisites found in the current national and international law, an effective attempt has been made to formulate and substantiate the subject and object of a new legal phenomenon – the law of the metaverses, its substantive and institutional division.

Keywords: law, ethics, virtual reality, metaverse, normativism, legal autonomy

В основе непрерывного течения истории, ее неумолимого движения вперед лежит технический прогресс. Именно такое значение придает ему Карл Маркс в своем учении о научно-техническом прогрессе [приводится по 15. С. 847].

Действительно, ускоряясь, приобретая новые формы и качества, изменяя внешний облик, без изменения сущности, научно-технический прогресс стал мощным фактором изменений, происходящих в социуме. Это обуславливает справедливость тезиса: на различных этапах своего развития общество, помещенное в сферу негативных явлений, вызванных им самим или объективными процессами, вынуждено считаться с той инновационно-технологической средой, которое им же и создано. Впоследствии эта среда становится некой «лакмусовой бумажкой» эпохи, тем спектром, в котором указанное общество пребывает в данное время.

Как известно, у каждой медали две стороны. Думается, что указанное положение справедливо для любого технологического «новшества». Очевидно, не оспорим тот факт, что так или иначе даже самая безобидная технологическая инновация может быть применена как во благо, так и во зло для социального мироустройства. Лекарство отличается от яда только количественной характеристикой. Так и здесь: явное перенасыщение действительности различными технологиями несет собой риск превращения таковых из дара в такое нечто, что может быть использовано с вредоносными для общества целями, особенно в ситуации отсутствия адекватных и релевантных как времени, так и самой технологии регуляторных и предиктивных мер.

В рамках настоящей статьи наше внимание будет сконцентрировано на вопросе нормативной правовой регуляции отношений, опосредованных тенденцией

неумолимого развития феномена виртуальной метафизической реальности (так называемых метавселенных). Актуальность темы не вызывает сомнений, ведь на сегодняшний день, несмотря на уже довольно длительный промежуток своего существования, ни одна из действующих правовых систем не предоставила действенного механизма регуляции указанной, относительно инновационной сферы общественной жизни, а в научной среде до сих пор не утвердилось однозначного мнения о том, какую позицию должно занять в этом вопросе право: приспособиться и, активно вмешавшись, облачить исследуемые социальные связи в правовую форму или отстраниться, уйти в стороны, уступив место саморегуляции.

Здесь, на наш взгляд, важно отметить: развитие глобальной сети Интернет, обусловившее возникновение механизма, обеспечивающего возможность одновременного взаимодействия множества пользователей в рамках единого пространства, созданного на основе специального цифрового алгоритма, в совокупности с усовершенствованием самой компьютерной технологии, создало благоприятную почву для проникновения идей и механизмов виртуальной реальности в больший спектр социальных связей и общественных отношений.

Фактически указанное на сегодняшний день привело к тому, что человечество находится в той красной точке, когда цифровой мир, являясь трехмерной копией реальной нормальности, которой уже не уместиться в узких рамках, имеющихся у человечества высокотехнологичных устройств, вырывается за эти узкие рамки и начинает свое активное смешение с миром физическим, стирая имеющиеся раньше между ними границы, что не может не сказываться на развитии важнейших социальных институтов: семьи, государства, права, экономики, образования и ряда других. Вследствие этого, то, что еще недавно рядом экспертов скептически именовалось очередной финансовой пирамидой, с развитием блокчейн-технологий, криптовалют, NFT, больших данных, технологий VR и других, вплоть до интеграции нейросетей мозга и микропроцессоров, вживления микрочипов для прямого подключения человека, сегодня становится все более незаменимым и дефицитным, выступая релевантной времени формой опосредования разнообразных экономических процессов.

Так, в цифровую реальность уже перенесены следующие возможности: получение образования, бесконтактная доставка товаров, оказание юридических и иных услуг, многие финансово-экономические процессы и операции, заключение договоров и сделок и многое другое. Активно обсуждаются проекты сохранения и развития объектов культурного наследия сквозь призму создания цифровой платформы – супер сервиса, позволяющей осуществлять инвестирование и добровольные пожертвования на содержание и реставрацию таких объектов с использованием NFT-технологий и цифрового рубля, выстраивать туристические маршруты на основе цифровой карты России с размещенными на ней объемными моделями объектов культурного наследия как существующих, так и утраченных, что позволит осуществлять сохранение культурного кода в масштабах всей страны.

Виртуальная вселенная как воплощение слияния физического (physical) и цифрового (digital) (так называемая вселенная фиджитал) на сегодняшний день с точки зрения экономического анализа является одной из самых динамично

развивающихся сегментов цифрового мира. Во многом это обуславливается тем высоким уровнем дохода, который она приносит как самим организаторам, так и самим пользователям. Так, например, стоимость отдельных внутриигровых объектов в рамках отдельной многопользовательской компьютерной игры, которую часто именуют прототипом или уменьшенной копией метавселенных, равно как и самих виртуальных персонажей при их продаже с использованием различных стриминговых сервисов (в частности, таковым является Steam) может варьироваться от нескольких сотен рублей до десятков тысяч долларов США.

Указанное, как кажется, опосредует тот бурный рост внимания к виртуальным мирам вследствие их экономической привлекательности, что фактически, как справедливо отмечается в том числе рядом аналитиков, приведет к росту объема оборота капиталов в рамках рынка метавселенных до 5–5,5 трлн долларов США к 2030 году.

И указанные процессы, как видится, не могут быть, скажем так, бесцветны для права, которое уже сегодня начало постепенно обращать свое внимание на новый формирующийся тип отношений, которые могут быть охарактеризованы как виртуальные, возникающие, изменяющиеся и прекращающиеся по поводу обладания объектами, которым, во-первых, присущи потребительские качества либо же они обладают действительной или потенциальной коммерческой ценностью из-за готовности пользователей платить за них реальные деньги, а во-вторых, они существуют лишь в рамках определенной виртуальной среды, например, конкретной многопользовательской игры, что обуславливает возможность владения, пользования и распоряжения указанными объектами (т. е. фактического господства, извлечения из них какой-либо выгоды и определения дальнейшей судьбы таких объектов путем совершения юридически значимых действий) возможно только в данном виртуальном пространстве, а за очерченными им границами они становятся экономически бесполезными для их «собственников».

Указанное выше дополнительно обуславливает актуальность рассмотрения вопросов, связанных с правовой природой виртуальных метафизических миров, места и роли права в механизме регуляции опосредованных ею общественных отношений, защиты нарушенных прав в виртуальном пространстве.

На данном этапе наших рассуждений отметим, что метавселенная должна быть определена как формально-определенный двусоставный конструкт, базисом которого является та самая (1) digital-environment (среда цифры), представленная в виде всеобъемлющей интероперабельной сети трехмерных виртуальных (цифровых) миров, визуализируемых в реальном времени, позволяющая (2) так называемой physical-environment (средой физической) в лице неограниченного числа лиц одновременно получать синхронный опыт с ощущением личного присутствия и с непрерывностью данных, таких как идентичность, история, права, объекты, коммуникации и платежи.

Есть ли место праву в системе регулирования отношений, возникающих в рамках исследуемой нами формы, а равно отношений, находящихся за ее рамками, но сохраняющих с ней тесную взаимосвязь, близкую по своей природе к зависимости. Фактически для разрешения последнего необходимо разобраться в том, (1) обладает

ли исследуемый нами конструкт виртуальной метафизической реальности неким аналогом суверенитета (его некой «оцифрованной» версией), который необходимо учитывать при построении вообще любого механизма регулирования отношений, образующихся внутри образуемого виртуальным миром контура, (2) а если все же место нормативной правовой составляющей в системе регуляторных механизмов исследуемых отношений все-таки есть, то какова модель его воздействия и роль в регулировании отношений в рамках виртуальных (внутриигровых) миров?

Монетизация отношений, складывающихся внутри виртуальных миров, а равно и вокруг них, отражаясь во вне, о чем достаточно подробно было написано выше, по справедливому замечанию А. М. Чечурина, оставляет все меньше сомнений полагать, что само по себе пространство виртуальных метафизических миров не заслуживает внимания представителей юридического сообщества, а применение к исследуемой группе отношений норм права не имеет всякого смысла [13].

Виртуальные миры без всякого сомнения уже сегодня обладают высокой экономической ценностью, а также способностью выступать формализующей формой цифровых рынков, на которых возможен оборот различных экономически и социально значимых благ, что обуславливается прежде различными запросами со стороны заинтересованных лиц.

Существующий на сегодняшний день пробел в нормативном правовом регулировании отношений, существующих в рамках таких метамиров, фактически образует ситуацию, способствующую порождать ситуации нарушения законных интересов различных субъектов. Например, если рассматривать многопользовательскую компьютерную игру как некую уменьшенную копию исследуемого нами контура, то среди таких субъектов можно справедливо назвать пользователей и организаторов многопользовательских онлайн-игр.

Кроме того, события, происходящие в рамках конкретного виртуального метафизического пространства, способны порождать реальные последствия, являющиеся значимыми в том числе и для права как системы и действенного механизма регуляции. В частности, примером таких значимых для права последствий, являющихся следствием действий в виртуальном пространстве, выступает, например, по смыслу правовой позиции, выраженной в постановлении Девятого арбитражного апелляционного суда от 15 мая 2018 г. № 09АП-16416/2018 по делу № А40-124668/2017, сокрытие в таком пространстве определенных видов имущества, которые должны быть учтены, например, при производстве по делам о банкротстве и ряде других случаев.

До недавнего времени виртуальные миры могли быть охарактеризованы как некое формально единое пространство, свободное от публично-правового воздействия. Основой регулирования отношений в рамках такого пространства выступала саморегуляция, основанная на специфических сводах норм и правилах, действие которых обеспечивалось различными техническими средствами [1].

В указанных обстоятельствах Е. А. Войниканис отмечает, что подобный механизм регулирования существования виртуальных миров воплощал интересы небольшого круга лиц, именуемых «цифровой элитой», в связи с чем обладает существенным демократическим дефицитом [3]. Указанное фактически стало тем

существенным обстоятельством, поспособствовавшим скорейшему вмешательству в регулирование указанной категории отношений со стороны государства. Весь публично-правовой инструментарий регулирования исследуемой области отношений исчерпывается тремя основными подходами.

Прежде всего, это подход, который был описан нами в самом начале приведенных рассуждений. Согласно данному подходу виртуальные миры полностью свободны от действия правовых норм. Регулирование отношений, лежащих в плоскости виртуальных миров, отводится на своеобразный откуп усмотрения участников таких отношений.

В противовес указанному подходу Б. Дюранске было сформулировано и детально описано правило некоего круга, согласно которому обращение к нормам и правилам, установленным реальным правом, происходит точечно и лишь в ситуациях, когда последствия охватывают в своем действии не только само виртуальное пространство, но и пространство реальное [приводится по 10].

Третий подход основывается на введении виртуального (внутриигрового) пространства в сферу действия права, что позволяет оправдывать существенное государственное вмешательство, в частности, необходимостью защиты интересов конкретного пользователя от злоупотреблений со стороны разработчика.

Признание истинности именно третьего (как видится, нормативного) подхода к регулированию метамиров на сегодняшний день, кажется, подтверждается все большей приверженностью ему со стороны судов, что следует из анализа судебной статистики дел, рассмотренных федеральными судами общей юрисдикции и арбитражными судами с 2017 по 2022 год. Судами, в частности, апелляционного и кассационного звена, сегодня особо подчеркивается, что отношения, возникающие в рамках виртуального, в том числе и внутриигрового пространства, обладают экономической ценностью и существенным экономическим потенциалом, что указывает на невозможность их игнорирования со стороны права как традиционного социального регулятора. Именно указанное, связанное с существенными ожиданиями лиц, участвующих в отношениях в рамках виртуального пространства, оправдывает присутствие правовой регуляторики в рамках метавселенной как таковой, в которой существует экономическая составляющая, затрагивающая среди прочего и материальное положение лица в реальном пространстве.

Несмотря на указанное соображение, рядом судов все еще высказывается мысль о том, что право не должно (а равным образом и не обязано) вмешиваться в регулирование отношений, возникающих как внутри, так и вокруг виртуального пространства. С указанным подходом трудно согласиться, так как он прежде всего неверен логически и основывается на не совсем точном применении и толковании норм материального права без поправки на специфику рассматриваемой области отношений [13. С. 52-56].

Однако существующий на сегодняшний день механизм нормативного правового регулирования нельзя признать удовлетворительным, что подчеркивается и профессиональным сообществом разработчиков, а также и пользователей, которые до сих пор лишены в силу правовой неопределенности эффективных и экономически оправданных способов защиты своих прав и законных интересов.

Конечно, право в условиях метавселенных должно быть ориентировано на защиту прав и интересов всех участников таких правоотношений. В то же время, это регулирование должно учитывать особенности метавселенных, которые могут включать в себя как физические, так и интеллектуальные аспекты. В этой связи у любого из существующих на сегодняшний день государств есть выбор между как минимум двумя моделями развития правового регулирования метавселенных, а именно (1) консервативной и (2) либеральной [10. С. 31]. Первый подход позволит сохранить такой признак государства и государственности, как государственный суверенитет, а вслед за ним и надлежащим образом обеспечить равенство граждан и защиту принадлежащих им прав и свобод. Противоположный подход, по мнению отдельных представителей научного сообщества, может породить к образованию квазигосударственных структур, которые возьмут под свой контроль государственные функции в виртуальном пространстве, ведь у них нет необходимости детальной, длительной проработки и согласования изменений в законы в масштабах страны [2]. Так, представители крупных поисковых систем уже отмечают, что, если отменить любое государственное регулирование, они способны существовать, основываясь на своих локальных регламентах [4. С. 119]. Но и консерватизм разрешительной модели регулирования не сможет быть эффективным в новых условиях, поскольку лишь увеличит дистанцию между новой действительностью и правом в его нормативистском понимании.

Одним из ключевых аспектов регулирования прав в метавселенных является определение прав и обязанностей участников таких правоотношений. Это могут быть права и обязанности, связанные с использованием ресурсов и технологий, с доступом к информации и результатам интеллектуальной деятельности, а также права и обязанности, связанные с участием в различных видах общественной деятельности и участии в образовании и научных исследованиях.

Представляется, что в данных условиях, наиболее допустимым с точки зрения задач нормативной правовой регуляции метавселенной, является диспозитивно-императивный подход.

Так, существуют принципы, универсальные и применимые почти повсеместно, в том числе в виртуальном мире. Вот только какие принципы будут превалировать при установлении правового регулирования в цифровом мире [9]? Следует предположить, что в метавселенных будет применяться старый и универсальный принцип права – равенство всех перед законом, следовательно, каждому правомочию будет соответствовать некая обязанность. Действовать будут те же нормы, что и на сегодняшний день в сети Интернет, но с большей адаптацией правового регулирования реального мира к цифровому: право собственности, особенно интеллектуальной, право пользования, защита аккаунтов в сети и персональных данных.

Например, есть два признанных права – на жизнь и на самовыражение. В реальном мире право на жизнь приоритетнее самовыражения, за его нарушение полагается строгое наказание. Но в метавселенной для аватаров оно не так важно, как для людей в обычном мире – виртуального аватара всего можно восстановить и загрузить заново. Право на самовыражение без дискриминации, наоборот, становится более значимо. Принципы права сохранятся, но их приоритет и особенности применения изменятся.

Насчет защиты от оскорблений, то здесь можно предположить два варианта развития событий. Если метавселенные пойдут по пути онлайн-игр, где аватар не будет связан с реальным человеком, оскорбления не будут считаться правонарушением и отвечать за них, например, платить штраф, не будет необходимости. Если же метавселенные будут развиваться как социальные сети и аватары будут верифицированы, за оскорбления придется нести ответственность в реальном мире.

Если взять в расчет сущность децентрализации технологий Web 3.0 и метавселенных, следует предположить, что они будут саморегулируемыми с правовой точки зрения. В них будут действовать собственные правовые политики корпораций – создателей. Создатели метавселенных будут соблюдать законы стран, в которых они работают, как сегодня это делают владельцы социальных сетей. Иначе государство будет блокировать и штрафовать их.

Так, в условиях метавселенной пользователи будут обладать теми же правами, что и в реальном мире, особенно правом собственности. Пользователи могут покупать разные вещи – от персонажей и скинов к ним до территорий в метавселенных. В реальной жизни право собственности подтверждается документами, например, свидетельством или договором купли продажи. Для этого аналогом аналогичных документов может стать NFT. К примеру, пользователь пожелает купить виртуальный дом в метавселенной. Чтобы подтвердить оплату и права собственника можно использовать NFT – уникальный токен зафиксирует, что человек законно владеет виртуальным объектом. Преимущество NFT для подтверждения права собственности в том, что нельзя подменить, уничтожить, украсть и фальсифицировать, а еще невозможно потерять, потому что он хранится на тысячах компьютеров одновременно. Но здесь возникает вопрос, окажет ли помощь NFT во время судебного заседания, который касается каждой юрисдикции. Но если большинство стран признают виртутальные активы в метавселенных цифровыми активами, использование NFT станет хорошим вариантом подтверждения прав собственности.

Активные рассуждения на сегодняшний день складываются вокруг вопроса о возможном формировании в связи с вышеназванными обстоятельствами некой совершенной новой правовой субстанции, именуемой правом метавселенных.

В общей теории права принято осуществлять деление системы права на различные по своему содержанию, предопределенному предметом и методом правового регулирования, отрасли права. В свою очередь нормы права распадаются на подотрасли (более крупные структурные образования, объединяющие в себе формально определенную совокупность правовых норм, регулирующую наиболее крупную общность общественных отношений, составляющих элемент, содержание предмета родовой отрасли права). Последние в свою очередь подразделяются на институты, которые представляют собой группу норм права, связанных между собой предметно-функциональными связями, регулирующих конкретный вид общественных отношений и приобретающих в силу этого относительную устойчивость и самостоятельность функционирования.

Употребление термина «отрасль права» в таком контексте в отношении механизма правового регулирования метавселенных вряд ли уместно; например, кажется, что было бы неоправданно (с точки зрения классических подходов к использованию термина «отрасль права») говорить о праве метавселенных. Поэтому

в определении права метавселенных нами осознанно используется (и кажется должно использоваться далее) выражение «регуляторная конструкция», как термин, обозначающий самые разнообразные юридические инструменты, позволяющие наиболее эффективным образом осуществлять нормативное правовое опосредование и регулирование отношений, возникающих вокруг и внутри феномена виртуальной, метавселенной реальности.

Таким образом, с определенной долей уверенности на сегодняшний день можно заключить, что метамиры являются не какой-то выдумкой фантастов, а скорее наше настоящее и наше будущее. В рамках последнего традиционное государство будет вынуждено уступить государству цифровому, являющемуся, как кажется, следующей эволюционной формой данного общественно-политического института. Указанное опосредует возникновение электронных (оцифрованных) правительств, а равно виртуализацию всего того, что принято именовать повседневностью, что непременно должно сопровождаться постановкой “во главу угла” защиты государственной безопасности и прав человека. В связи с этим оптимальным видится нормативный подход регуляции отношений, возникающих как в рамках очерченного метамирами контура, так хоть и за его пределами, но тесно связанными с метавселенными, с оправданным преобладанием норм императивного характера.

Список литературы

1. Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Правоведение. 2013. № 2. С. 93–114.

2. Болл М. Метавселенная: как она меняет наш мир. М.: Альпина Паблишер, 2023. С. 362.

3. Войниканис Е. А. Право интеллектуальной собственности в цифровую эпоху: парадигма баланса и гибкости. М.: Юриспруденция. 2014. С. 552.

4. Жевняк О. В. Гражданско-правовое регулирование отношений по оказанию услуг в цифровой экономике: соотношение императивных и диспозитивных начал // Вестник ННГУ. 2020. № 3. С. 117–125.

5. Жуков В. Право и этика метавселенной // Закон. 2022. № 7.

6. Измайлова А. А. Метавселенная как новая экономическая система // Modern Economy Success. 2021. № 6. С. 175–179.

7. Кучинская Е. В. Метавселенная как новая экономика // Гуманитарный научный журнал. 2022. № 2. С. 129–131.

8. Мажорина М. В. О коллизии права и «неправа», реновации lex mercatoria, смарт-контрактах и блокчейн-арбитраже // Lex russica. 2019. № 7. С. 93–107.

9. Метавселенные и право: какие законы будут действовать в цифровом мире // Лига Цифровой Экономики. URL: https://vc.ru/u/606142-liga-cifrovoy-ekonomiki/537179-metavselennye-i-pravo-kakie-zakony-budut-deystvovat-v-cifrovom-mire

10. Овчинников А. И. Метавселенные и право: вызовы новых технологий в условиях дальнейшего развития интернета // Вестник юридического факультета Южного федерального университета. 2023. Т. 10, № 2. С. 27–34.

11. Платунов А. Скайнет в эпоху киберпанка. Теория сверхразума и вызовы перед человечеством в XXI веке. М.: Автор, 2023. С. 96.

12. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7–32.

13. Чечурин А. М. Право компьютерных игр и оборот виртуальных (внутриигровых) объект в призме российского законодательства: монография. М.: Проспект, 2023. С. 104.

14. Чечурин А. М., Сотникова Е. В. Правовая природа «виртуального игрового имущества» и права пользователя на него // Научно-практическая конференция «Ноябрьские студенческие правовые чтения: генезис правовой науки в XXI веке». Научно-практическая конференция «Актуальные вопросы юриспруденции»: сборник докладов. М.: Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2023. С. 227–230.

15. Чечурин А. М. К вопросу об электронных методах осуществления государственной биополитики // Нравственные императивы в праве, образовании, науке и культуре: сборник материалов X Международного молодежного форума, 27 мая 2022 г. / под ред. Е. В. Сафроновой, А. Н. Пасенова. Белгород: ИД «БелГУ» НИУ «БелГУ», 2022. С. 847–851.

16. Чечурин А. М. Теоретико-правовое понимание глобализации // Молодежь и XXI век – 2022: материалы 12-й Международной молодежной научной конференции. В 4-х томах, Курск, 17–18 февраля 2022 г. / отв. ред. М. С. Разумов. Т. 2. Курск: Юго-Западный государственный университет, 2022. С. 211–215.

17. Чечурин А. М., Алонцева Д. В. Права человека в условиях глобализации // Закон и право. 2021. № 12. С. 24–26.

18. Duranske B. T. Virtual Law. Navigating the Legal Landscape of Virtual Worlds // Chicago. 2008. P. 461.

В. А. Шохова,
магистрант,
Новосибирский национальный исследовательский
государственный университет

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЛАТФОРМЕННОЙ ЗАНЯТОСТИ В РОССИИ

Аннотация. Статья посвящена изучению феномена платформенной занятости с правовой точки зрения. Целью исследования выступает комплексный анализ нормативного регулирования платформенной занятости, внедрения цифровых технологий в трудовые отношения. Исследуется проблема отсутствия правового регулирования платформенной занятости в России, а также предлагаются возможные варианты законодательных изменений с целью устранения пробелов и недостатков в регулировании данного вопроса. В статье также исследуется дискуссия о правовой природе платформенной занятости, а также о критериях разграничения трудовых и гражданско-правовых отношений в данной сфере. В выводах содержатся конкретные предложения по внесению изменений в законодательство.

Ключевые слова: право, цифровые технологии, трудовое право, гражданское право, трудовые отношения, цифровизация трудовых отношений, платформенная занятость, проблемы трудового права

LEGAL REGULATION OF PLATFORM EMPLOYMENT IN RUSSIA

Abstract. The article is devoted to the study of the phenomenon of platform employment from a legal point of view. The purpose of the study is a comprehensive analysis of the regulatory regulation of platform employment, the introduction of digital technologies in labor relations. The author explores the problem of the lack of legal regulation of platform employment in Russia, and also suggests possible options for legislative changes in order to eliminate gaps and shortcomings in the regulation of this issue. The article also explores the discussion about the legal nature of platform employment, as well as the criteria for distinguishing labor and civil law relations in this area. The conclusions of the study contain specific proposals for amendments to the legislation.

Keywords: law, digital technologies, labor law, civil law, labor relations, digitalization of labor relations, platform employment, problems of labor law

С развитием цифровых технологий и информатизацией всех сфер современного общества растет популярность использования современных цифровых технологий в сфере труда. Согласно оценкам Института социальной политики, в апреле 2022 г. 14,7 % россиян в возрасте 18–72 лет имели опыт платформенной занятости, причем 1,6 % респондентов указали занятость через онлайн-платформы в качестве основной [4. С. 4]. Число россиян, работающих с помощью цифровых платформ, продолжает расти с каждым днем, при этом законодатель не успевает регулировать эту сферу общественных отношений, что порождает нарушение прав работников, коллизии и пробелы в правовом регулировании платформенной занятости, неопределенности в правовом статусе лица, основной вид деятельности которого осуществляется через онлайн-платформы. В связи с этим необходим анализ правовой природы и сущности отношений, складывающихся между исполнителем (работником), цифровой платформой и потребителем результата выполненной работы, а также внесение законодательных инициатив для совершенствования правового регулирования названного вопроса.

В марте 2023 г. в Государственной Думе Российской Федерации был рассмотрен и принят в первом чтении законопроект № 275599-8, которым планируется внесение изменений в Закон РФ «О занятости населения». В данном законопроекте платформенная занятость определяется как деятельность граждан (платформенных занятых) по личному выполнению работ и (или) оказанию услуг на основе заключаемых договоров, организуемая с использованием информационных систем (цифровых платформ занятости), обеспечивающих взаимодействие платформенных занятых, заказчиков и операторов цифровых платформ занятости посредством информационно-телекоммуникационной сети «Интернет» [3]. Как можно заметить, в данном определении присутствуют «атрибуты» гражданско-правового характера, в частности,

есть указание на то, что субъект выполняет работы или оказывает услуги на основе неких договоров. При этом есть указание на личный характер выполнения работы, что является безусловным признаком трудовых отношений. Данный законопроект также не содержит указаний на то, регулирует ли он трудовые отношения.

Как можно заметить, неслучайно в научной литературе существует дискуссия относительно правовой природы отношений по выполнению работ с помощью цифровых платформ, ведь разграничение в данном случае трудовых и гражданско-правовых отношений носит неоднозначный характер. Один лагерь ученых считает отношения в сфере платформенной занятости сугубо гражданско-правовыми, поскольку исполнитель, устанавливая приложение и принимая все условия его использования, предлагает через цифровую платформу свои услуги, а заказчик, изучив информацию о предлагаемых услугах, заключает через эту же цифровую платформу соответствующий договор с исполнителем (например, исполнитель предлагает оформление презентаций) [2. С. 10]. При этом платформа выступает лишь инструментом для заключения договора, а владелец платформы – посредником в таких отношениях. Другие же считают, что платформенная занятость должна входить в предмет регулирования трудового права, поскольку цифровые платформы (агрегаторы), предлагая определенные услуги потребителям, выступают в качестве работодателей для лиц, которые непосредственно выполняют работу [1. С. 398]. Например, известная платформа для доставки еды ЯндексЕда привлекает курьеров, выдает им фирменную одежду, выплачивает вознаграждение за выполнение работы в интересах владельца данной платформы. При этом чаще всего курьеры осуществляют доставку на собственных транспортных средствах, т. е. такие трудовые отношения все же отличаются от классических трудовых отношений, где работа производится с помощью материальных ресурсов работодателя (выдается оборудование, предоставляется рабочее место и пр.).

Следует сказать, что отношения в сфере платформенной занятости могут быть как гражданско-правовыми, так и трудовыми в зависимости от особенности условий участия и работы гражданина на той или иной платформе. Как известно, трудовые отношения обладают следующими отличительными признаками:

– личный характер выполнения работы, принимаемых прав и обязанностей по трудовому договору (работник трудится самостоятельно);

– отношения субординации, подчинение правилам внутреннего трудового распорядка и иным правилам работодателя;

– выполнение работы в интересах работодателя;

– возмездность отношений;

– выполнение конкретных трудовых функций в соответствии со специальностью, квалификацией и должностью;

– обеспечение работника необходимыми материальными средствами для выполнения трудовой функции.

Если соотносить с данными критериями работу таксиста через онлайн-агрегатор, то можно заметить соответствие личному характеру выполнения работы (путем регистрации водитель подтверждает свою личность и несет ответственность за достоверность представленных данных), возмездности (водитель

получает оплату за каждую поездку), отношениям субординации (водитель принимает правила агрегатора, когда выполняет работу), выполнению работы в интересах работодателя (агрегатор взимает процент в свою пользу с каждой поездки, расширяет сеть такси, когда присоединяются новые водители, получает рекламу, требуя размещения на автомобилях водителей опознавательных знаков агрегатора). При этом водитель выполняет конкретную трудовую функцию, однако владелец платформы в данном случае не предоставляет автомобили для перевозки пассажиров, что является единственным отличием таких отношений от типичных трудовых. Стоит сказать, что агрегаторы пользуются этим, квалифицируют данные отношения как гражданско-правовые, устанавливая в договорах минимальную ответственность для себя.

Совершенно иным образом стоит квалифицировать отношения онлайн-платформы, которая предлагает различные услуги, и исполнителей на таких платформах (например, Profi.ru). Цифровая платформа предлагает разместить объявления о различных услугах, при этом не взимает плату за само размещение объявления (только за дополнительные услуги продвижения), при этом исполнитель (к примеру, репетитор) получает оплату за занятия в полном объеме без удержаний процентов, выполняет работу исключительно в своих интересах, используя собственные средства для ее выполнения. Причем, если в случае с такси или курьерской доставкой исполнители (работники) обычно имеют на себе опознавательные знаки той или иной компании (цифровой платформы), то репетиторы, дизайнеры, писатели не обозначают принадлежность к определенной платформе, так как правила таких платформ того не требуют.

На наш взгляд, для квалификации отношений в сфере платформенной занятости необходимо, прежде всего, определять, кому и какие выгоды приносит выполняемая работа. Если все выгоды (материальные, репутационные и иные) идут в пользу исполнителя, то такие отношения являются гражданско-правовыми и даже могут подпадать под определение предпринимательской деятельности. Если же исполнитель получает только оплату за свой труд, при этом часть оплаты удерживается владельцем цифровой платформы, на исполнителя налагаются дополнительные обязанности носить униформу при выполнении своей трудовой функции, говорить конкретные фразы-приветствия, обладать какими-либо опознавательными знаками той или иной платформы, то значительную часть выгод от такого труда получает владелец цифровой платформы. Следовательно, в данных отношениях их стоит признавать в качестве работодателей и налагать на них обязанности по внесению страховых взносов, уплате налогов, обеспечению работников материальными средствами для выполнения трудовой функции и соблюдению иных трудовых прав в соответствии с ТК РФ.

На данный момент платформенная занятость не урегулирована трудовым законодательством никак, что приводит к нарушению прав граждан в сфере труда. В частности, цифровые платформы выстраивают рейтинговую систему исполнителей заказов, что приводит к автоматическому «отключению» лица, чей рейтинг опустился ниже установленного значения. Такая практика фактически приводит к тому, что гражданин не имеет возможности продолжать трудовую деятельность.

Некоторые ученые предлагают квалифицировать такие действия, как незаконное увольнение, поскольку в основе блокировки аккаунта такого исполнителя лежит не оценка его профессиональных компетенций и их соответствия профессиональным стандартам, а рейтинговый критерий, который вовсе не отражает профессиональных характеристик исполнителя.

Возвращаясь к упомянутому в начале законопроекту, стоит сказать, что он упоминает лишь определение платформенной занятости, но никак не предлагает ее квалифицировать и не устанавливает никаких особенностей ее правового регулирования. В связи с этим принятие такого законопроекта представляется нецелесообразным, поскольку положения о платформенной занятости можно внести в Трудовой кодекс РФ, изложить в нем определение платформенной занятости, признать лиц, трудящихся через цифровые платформы, работниками, предоставив им весь спектр трудовых и вытекающих из них социальных прав.

На данный момент платформенная занятость является неурегулированной сферой общественной жизни в России, несмотря на рост популярности данного вида занятости. Неопределенность правового статуса платформенного работника (исполнителя) порождает повсеместное нарушение прав таких лиц, в том числе ненадлежащие условия труда, отсутствие минимального размера оплаты труда и отсутствие иных гарантий в соответствии с трудовым законодательством. С целью восполнения пробела в правовом регулировании данного вопроса предлагается ввести в Трудовой кодекс РФ главу, посвященную платформенной занятости, которая определяла бы сам термин, отличительные черты платформенной занятости, устанавливала бы особенности данного вида труда с предоставлением работникам всех необходимых гарантий.

Список литературы

1. Акманов Д. Р. Платформенная занятость: проблемы и перспективы законодательного регулирования // Вопросы российской юстиции. 2021. № 14. С. 398. URL: https://cyberleninka.ru/article/n/platformennaya-zanyatos-problemy-i-perspektivy-zakonodatelnogo-regulirovaniya

2. Бобков В. Н., Черных Е. А. Платформенная занятость: масштабы и признаки неустойчивости // Мир новой экономики. 2020. № 2. С. 6–15. URL: https://cyberleninka.ru/article/n/platformennaya-zanyatost-masshtaby-i-priznaki-neustoychivosti

3. Законопроект № 275599-8 «О занятости населения в Российской Федерации» от 11.01.2023. URL: https://sozd.duma.gov.ru/bill/275599-8

4. Платформенная занятость в России: масштабы, мотивы и барьеры участия: аналитический доклад / О. В. Синявская, С. С. Бирюкова, Е. С. Горват, Д. Е. Карева, Д. А. Стужук, К. О. Чертенков; Нац. исслед. ун-т «Высшая школа экономики». М.: НИУ ВШЭ, 2022. С. 4. URL: https://ipquorum.ru/upload/NCMU_Platform_Employment_Report_2022-hp8W7d8o.pdf

СОДЕРЖАНИЕ | CONTENTS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ПРАВОВЫХ ОТНОШЕНИЙ (МОЛОДЕЖНОЕ ПРОСТРАНСТВО НАУКИ) | DIGITAL TECHNOLOGIES IN THE SYSTEM OF LEGAL RELATIONS (YOUTH SPACE OF SCIENCE)

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 3

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

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технический редакторы: *О. А. Аймурзаева, С. Р. Каримова*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0816-1

Подписано в печать 30.11.2023. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 24,18. Уч.-изд. л. 22,88.
Тираж 500 экз. (1-й завод – 50 экз.) Заказ № 98.

Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17